# Ruijie RG-WLAN Series Access Points

# RGOS Command Reference, Release 11.9(0)B1

## 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 11.9(0)B1.

## Audience

This manual is intended for:

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

## Obtaining Technical Assistance

- Ruijie Networks Website: https://www.ruijienetworks.com/
- Technical Support Website: https://ruijienetworks.com/support
- Case Portal: https://caseportal.ruijienetworks.com
- Community: https://community.ruijienetworks.com
- Technical Support Email: service_rj@ruijienetworks.com
- Skype: service_rj@ruijienetworks.com

## Related Documents

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

## Conventions

This manual uses the following conventions:

| Convention | Description |
| --- | --- |
| **boldface** font | Commands, command options, and keywords are in **boldface**. |
| *italic* font | Arguments for which you supply values are in *italics*. |
| [ ] | Elements in square brackets are optional. |

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

### Symbols

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

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

# WLAN Basic Configuration Commands

# 1 WLAN Basic Configuration Commands

## 1.1 ap-mode

Use these commands to switch AP to fit mode or to fat mode.

**ap-mode** { **fit** | **fat** [ **dhcp** ] | **macc** }

**Parameter Description**

| Parameter | Description |
|---|---|
| **fit** | Switches the AP to fit mode. |
| **fat** | Swiches the AP to fat mode. |
| **dhcp** | When this parameter is configured, the AP enables DHCP to obtain IP address by default; Otherwise the AP uses static IP addresses by default. |
| **macc** | Switches the AP to MACC mode. |

**Defaults** N/A

**Command Mode** AP configuration mode

**Usage Guide**

After switching the AP working mode, restart the device to ensure the configuration consistency.
For Ruijie Networks' WALL-AP ,when working as a fat AP, the default IP address of the rear end wired interface (Which is connected to the PoE switching device) is 192.168.110.1/255.255.255.0; the default IP address of the front end wired interface (the Ethernet port on the front panel) is 192.168.111.1/255.255.255.0.\
When the command **ap-mode fat dhcp** is configured, once the AP is switched to fat mode, the fat AP will obtain IP address through DHCP. After AP is restarted without further related configuration, it will still obtain IP address through DHCP.

When the command **ap-mode fat dhcp** is configured on the WALL-AP, DHCP is enabled only on the rear end wired interface by default; that is to say,by default, the front end interface still uses static IP address.

You cannot use commands **ap-mode fat dhcp** and **ap-mode fat** to perform direct switchover in the fat mode. You should switch to fit mode and then perform such switchover.

**Configuration Examples** The following example switches the AP to fit mode:

```
Ruijie(config)# ap-mode fit
```

**Related Commands**

| Command | Description |
|---|---|
| N/A | N/A |

**Platform Description** The command is supported only on APs.

## 1.2 hide-ssid sta-reach-limit

Use this command to hide the SSID when the number of STAs associated with the AP reaches the limit. Use the **no** form of this command to restore the default setting.

**hide-ssid sta-reach-limit**

**no hide-ssid sta-reach-limit** [ **radio** { **2.4g** | **5g** } ]

**Parameter Description**

| Parameter | Description |
|---|---|
| **radio** | Enables this function on the specified radio. If no radio is specified, it is enabled on both radio. |
| **2.4g** | Enables this function on 2.4G radio. |
| **5g** | Enables this function on 5G radio. |

**Defaults** This function is disabled by default.

**Command Mode** Global configuration mode

**Usage Guide** N/A

**Configuration Examples** The following example hides the SSID for 5G radio when the number of STAs associated with the AP reaches the limit.

```
Ruijie(config)# hide-ssid sta-reach-limit radio 5g
```

**Related Commands**

| Command | Description |
|---|---|
| N/A | N/A |

**Platform Description** N/A

## 1.3 show ap-mode

Use this command to display the AP mode.

**show ap-mode**

**Parameter**

| Parameter | Description |
|---|---|

**Description**

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

**Defaults** N/A

**Command Mode** Privileged EXEC mode

**Usage Guide** N/A

**Configuration Examples** The following example displays the AP mode.

```
Ruijie#show ap-mode
current mode: FIT
```

**Related Commands**

| Command | Description |
|---|---|
| N/A | N/A |

**Platform Description**

# 2 WLAN STAMG Commands

## 2.1 ap

Use this command to configure the AP information in the association control zone. Use the **no** form of this command to delete the specified AP from the association control zone.

**ap** *WORD*

**no ap** [ *WORD* ]

**Parameter Description**

| Parameter | Description |
|---|---|
| *WORD* | AP name. The name length range is from 1 to 64. |

**Defaults** No AP information in the association control zone is configured by default.

**Command mode** Association control zone configuration mode

**Usage Guide** Up to five APs can be configured in an association control zone. The system will prompt an error message if the number of the configured APs exceeds five. In addition, when configuring AP information for an association control zone, we do not require that APs are online.

**Configuration Examples** The following example configures a set of AP information with MAC address of 00d0.f800.1001 for an association control zone named “Class (1) Grade 1”.

```
Ruijie(config)#control-zone Class (1) Grade 1
Ruijie(config-cznoe)# ap 00d0.f800.1001
```

**Related Commands**

| Command | Description |
|---|---|
| **show control-zone** | Displays the association control zone. |

**Platform Description** N/A

## 2.2 assoc-control

Use this command to enable the association control function. Use **no** form of this command to restore the default setting.

**assoc-control**

**no assoc-control**

**Parameter**

| Parameter | Description |
|---|---|

**Description**

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

**Defaults** This function is disabled by default.

**Command mode** Global configuration mode

**Usage Guide** When the association control function is disabled, the association control related commands can still be configured with the ineffective association control function.

**Configuration Examples** The following example enables the association control function.

```
Ruijie(config)#assoc-control
```

The following example disables the association control function.

```
Ruijie (config)#no assoc-control
```

**Related Commands**

| Command | Description |
|---|---|
| N/A | N/A |

**Platform Description** N/A

## 2.3 control-zone

Use this command to create an association control zone and enter association control zone configuration mode. Use the **no** form of this command to restore the default setting.

**control-zone** *czone-name*

**no control-zone** *czone-name*

**Parameter Description**

| Parameter | Description |
|---|---|
| *czone-name* | Association control zone name. The name length range is 1 to 64. |

**Defaults** No association control zone is configured by default.

**Command mode** Global configuration mode

**Usage Guide** Only one association control zone is allowed to be configured on a fat AP. The system will prompt an error message if the upper limit is exceeded.

**Configuration Examples** The following example configures an association control zone named “Class (1) Grade 1”.

```
Ruijie(config)#control-zone Class (1) Grade 1
Ruijie(config- czone)#
```

The following example deletes an association control zone named “Class (1) Grade 1”.

```
Ruijie(config)# no control-zone Class (1) Grade 1
The operation will clear the control zone configuration, which may cause
corresponding STAs offline. Continue? [no] y
Ruijie(config)#
```

**Related Commands**

| Command | Description |
|---|---|
| **show control-zone summary** | Displays the summary of association control zones. |

**Platform Description** N/A

## 2.4 inter-radio-balance flow-balance dual-band

Use this command to configure the enabling threshold and balancing threshold for the traffic balancing between the different radios (2.4G and 5.0G) of AP devices or AP groups. Use the **no** form of this command to restore the default settings.

**inter-radio-balance flow-balance dual-band enable-load** *en-num* **threshold** *thrs-num*

**no inter-radio-balance flow-balance dual-band**

**Parameter Description**

| Parameter | Description |
|---|---|
| *en-num* | The enabling threshold value. Load balancing is enabled only when the traffic on the associated radio exceeds the threshold. The unit is 100 Kbps. The range is from 1 to 1000. |
| *thrs-num* | The balancing threshold value. The STA will be disassociated with the radio when the traffic difference between the associated radio and lowest load radio. The unit is 100 Kbps. The range is from 1 to 1000. |

**Defaults** By default, the enabling threshold is 1 Mbps and the balancing threshold is 1 Mbps.

**Command mode** AP /AP group configuration mode

**Usage Guide** When the load balancing between radios is enabled, if the traffic of associated radio exceeds the enabling threshold and the traffic difference between the associated radio and lowest load radio exceeds the balancing threshold, the STA will be disassociated with the radio and the traffic will be balanced to radio of lower load. This configuration takes effect only when the radio of lowest load is on the different radio to be associated. The **inter-radio-balance flow-balance same-band** takes effect If the two radios are on the same radio.

**Configuration Examples** The following example configures the enabling threshold and balancing threshold to 800 Kbps and 800 Kbps respectively for the different radios on AP0001.

```
Ruijie(config)# ap-config AP0001
Ruijie(config-ap)# inter-radio-balance flow-balance same-band enable-load 8
threshold 8
```

The following example restores the default load balancing settings for different radios on AP0001.

```
Ruijie(config)# ap-config AP0001
Ruijie(config-ap)# no inter-radio-balance flow-balance dual-band
```

The following example configures the enabling threshold and balancing threshold to 300 Kbps and 500 Kbps respectively for different radios of AP devices in the AP group.

```
Ruijie(config)# ap-group default
Ruijie(config-group)# inter-radio-balance flow-balance dual-band enable-load 3 threshold 5
```

The following example configures the enabling threshold and balancing threshold to 3 Mbps and 3 Mbps respectively for different radios on all AP devices.

```
Ruijie(config)# ap-config all
Ruijie(config-ap)# inter-radio-balance flow-balance dual-band enable-load 30 threshold 30
```

**Related Commands**

| Command | Description |
|---|---|
| N/A | N/A |

**Platform Description** This command is supported only on ACs.

## 2.5 inter-radio-balance flow-balance enable

Use this command to enable load balancing for traffic between different radios (2.4G and 5.0G) on the AP device or AP group. Use the **no** form of this command to disable load balancing between radios on the AP device or AP group.

**inter-radio-balance flow-balance enable**

**no inter-radio-balance flow-balance enable**

**Parameter Description**

| Parameter | Description |
|---|---|
| N/A | N/A |

**Defaults** By default, load balancing between radios is disabled.

**Command mode** AP /AP group configuration mode

**Usage Guide** After load balancing between radios is enabled on an AP device, the AC device will make the traffic difference between radios on the AP device not exceed the threshold value.

**Configuration Examples** The following example enables load balancing for traffic between radios on AP0001.

```
Ruijie(config)# ap-config AP0001
Ruijie(config-ap)# inter-radio-balance flow-balance enable
```

The following example disables load balancing for traffic between radios on AP0001.

```
Ruijie(config)# ap-config AP0001
Ruijie(config-ap)# no inter-radio-balance flow-balance enable
```

The following example enables load balancing for traffic between radios on the AP devices in the default group.

```
Ruijie(config)# ap-group default
Ruijie(config-group)# inter-radio-balance flow-balance enable
```

The following example enables load balancing for traffic between radios on all AP devices.

```
Ruijie(config)# ap-config all
Ruijie(config-ap)# inter-radio-balance flow-balance enable
```

**Related Commands**

| Command | Description |
|---|---|
| N/A | N/A |

**Platform Description** This command is supported only on ACs.

## 2.6 inter-radio-balance flow-balance same-band

Use this command to configure the enabling threshold and balancing threshold for the traffic balancing between the same radios (both 2.4G or 5.0G) of AP devices or AP groups. Use the **no** form of this command to restore the default settings.

**inter-radio-balance flow-balance same-band enable-load** *en-num* **threshold** *thrs-num*

**no inter-radio-balance flow-balance same-band**

**Parameter Description**

| Parameter | Description |
|---|---|
| *en-num* | The enabling threshold value. Load balancing is enabled only when the traffic on the associated radio exceeds the threshold. The unit is 100 Kbps. The range is from 1 to 1000. |
| *thrs-num* | The balancing threshold value. The STA will be disassociated with the radio when the traffic difference between the associated radio and lowest load radio. The unit is 100 Kbps. The range is from 1o to 1000. |

**Defaults** By default, the enabling threshold is 500 Kbps and the balancing threshold is 500 Kbps.

**Command mode** AP /AP group configuration mode

**Usage Guide** When the load balancing between radios is enabled, if the traffic of associated radio exceeds the enabling threshold and the traffic difference between the associated radio and lowest load radio exceeds the balancing threshold, the STA will be disassociated with the radio and the traffic will be balanced to the radio of lower load. This configuration takes effect only when the radio of lowest load is on the different the radio to be associated. The **inter-radio-balance flow-balance dual-band** takes effect If the two radios are on the different radio.

**Configuration Examples** The following example configures the enabling threshold and balancing threshold to 800 Kbps and 800 Kbps respectively for the same radios on AP0001.

```
Ruijie(config)# ap-config AP0001
Ruijie(config-ap)# inter-radio-balance flow-balance same-band enable-load 8
threshold 8
```

The following example restores the default load balancing settings for the same radios on AP0001.

```
Ruijie(config)# ap-config AP0001
Ruijie(config-ap)# no inter-radio-balance flow-balance same-band
```

The following example configures the enabling threshold and balancing threshold to 300 Kbps and 500 Kbps respectively for the same radios of AP devices in the AP group.

```
Ruijie(config)# ap-group default
Ruijie(config-group)# inter-radio-balance flow-balance same-band enable-load 3 threshold 5
```

The following example configures the enabling threshold and balancing threshold to 3 Mbps and 3 Mbps respectively for the same radios on all AP devices.

```
Ruijie(config)# ap-config all
Ruijie(config-ap)# inter-radio-balance flow-balance same-band enable-load 30 threshold 30
```

**Related Commands**

| Command | Description |
|---|---|
| N/A | N/A |

**Platform Description** This command is supported only on ACs.

## 2.7 inter-radio-balance radio weight

Use this command to configure the weight for load balancing among radio. Use the **no** form of this command to restore the default setting.

**inter-radio-balance radio** *radio-id* **weight** *weight-num*

**no inter-radio-balance radio** *radio-id* **weight**

**Parameter Description**

| Parameter | Description |
|---|---|
| *radio-id* | Specifies a radio. |
| *weight-num* | Configures the weight, in the range from 1 to 100. |

**Defaults** The default weight is 100, that is, radio 1: radio 2=100:100 (1:1).

**Command mode** Global configuration mode

**Usage Guide** If you want to configure radio 1: radio 2= 50:100 (1:2). please set the weight of radio 1 to 50,

**Configuration Examples** The following example sets the weight of radio 1 to 50, that is, radio 1: radio 2=50:100 (1:2).

```
Ruijie(config)# inter-radio-balance radio 1 weight 50
```

**Related**

| Command | Description |
|---|---|

**Commands**

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

**Platform Description** N/A

## 2.8 package

Use this command to create a terminal package and enter terminal package configuration mode. Use the **no** form of this command to restore the default setting.

**package** *pkg-name*

**no package** [ *pkg-name* ]

**Parameter Description**

| Parameter | Description |
|---|---|
| *pkg-name* | Terminal package name. The name length range is from 1 to 32. |

**Defaults** No terminal packets are configured by default.

**Command mode** Global configuration mode

**Usage Guide** Only 50 terminal packages are allowed to be configured on a fat AP. The system will prompt an error message if the upper limit is exceeded.

**Configuration Examples** The following example configures a terminal package named “Cart”1.

```
Ruijie(config)#package Cart 1
Ruijie(config-package)#
```

The following example configures the package named “Cart”1.

```
Ruijie(config)# no package Cart 1
The operation will clear package(s) configuration, which may cause
corresponding STAs offline. Continue? [no] y
Ruijie(config)#
```

**Related Commands**

| Command | Description |
|---|---|
| **show package** | Displays the terminal package configuration. |

**Platform Description** N/A

## 2.9 primary-sta

**Parameter Description**

Use this command to configure a primary STA in a terminal package. Use the **no** form of this command to remove the configuration.

**primary-sta** *mac-address*

**no primary-sta**

| Parameter | Description |
|---|---|
| *mac-address* | The MAC address of the primary STA, in the format of H.H.H. |

**Defaults** N/A

**Command mode** Terminal package configuration mode

**Usage Guide** A terminal package can be configured up to one primary STA. Therefore the newly configured primary STA will cover the one which has been configured in a terminal packet.

**Configuration Examples** The following example configures a primary STA with MAC address of 00d0.f800.0001 for the terminal package “Cart 1”.

```
Ruijie(config)#package Cart 1
Ruijie(config- package)#primary-sta 00d0.f800.0001
```

**Related Commands**

| Command | Description |
|---|---|
| **show package** | Displays the terminal package configuration. |

**Platform Description** N/A

## 2.10 secondary-sta

**Parameter Description**

Use this command to configure secondary STAs in a terminal package. Use the **no** form of this command to remove the configuration**.**

**secondary-sta** *mac-address*

**no secondary-sta** [ *mac-address* ]

| Parameter | Description |
|---|---|
| *mac-address* | The MAC address of the secondary STA, in the format of H.H.H. |

**Defaults** N/A

**Command** Terminal package configuration mode

**mode**

**Usage Guide** Up to 100 secondary STAs can be configured in one terminal package. The system will prompt the error message in the following conditions if you use this command to configure the secondary STA:
The secondary STA configured has existed in the terminal package.
The number of STAs in a terminal package exceeds 100.

**Configuration Examples** The following example configures a secondary STA with MAC address of 00d0.f800.0002 for the package “Cart 1”.

```
Ruijie(config)#package Cart 1
Ruijie(config- package)#secondary-sta 00d0.f800.0002
```

**Related Commands**

| Command | Description |
| --- | --- |
| **show package** | Displays the terminal package configuration. |

**Platform Description** N/A

## 2.11 show assoc-control

Use this command to display the state of the association control.

**show assoc-control**

**Parameter Description**

| Parameter | Description |
| --- | --- |
| N/A | N/A |

**Defaults** N/A

**Command mode** Privileged EXEC mode

**Usage Guide** N/A

**Configuration Examples** The following example displays the state of the association control.

```
Ruijie# show assoc-control
Association control is enabled.
```

The following example displays the state of the association control.

```
Ruijie# show assoc-control
Association control is disabled.
```

**Related Commands**

| Command | Description |
| --- | --- |

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

**Platform Description** N/A

## 2.12 show control-zone

Use this command to display the association control-zone configuration.

**show control-zone** [ **summary** | *czone-name* ]

**Parameter Description**

| Parameter | Description |
|---|---|
| **summary** | Displays summary information. |
| *czone-name* | The name of the association control-zone to be displayed. The name length range is from 1 to 64. |

**Defaults** N/A

**Command mode** Privileged EXEC mode

**Usage Guide** Use the **show control-zone summary** command to display the configured association control zone. Use the **show control-zone** or the **show control-zone czone-name** command to display not only the association control zone information but also the AP information in the control zone.

**Configuration Examples** The following example displays all association control zones.

```
Ruijie# show control-zone summary
control zone num :  4
Class 1 Grade 1
Class 2 Grade 1
Class 3 Grade 1
Class 1 Grade 2
```

The following example displays all association control zones.

```
Ruijie# show control-zone summary
No control zone configuration.
```

The following example displays the detailed configuration information of all the association control zones.

```
Ruijie# show control-zone
control zone num :  3
control-znoe       AP
-------------      ------------------------
Class 1 Grade 1          AP1(1)-1  00d0.f800.889f
                   AP1(1)-2  00d0.f800.7869
Class 2 Grade 2          AP2(2)-1  00d0.f800.889f
Class 3 Grade 3          AP2(3)-1  offline
```

```
Class 3 Grade 2          n/a
```

The following example displays the detailed configuration information of all association control zone.

```
Ruijie# show control-zone
No control zone configuration.
```

The following example displays the detailed configuration information of the association control zone named “Class 1 Grade 1”.

```
Ruijie# show control-zone Class 1 Grade 1
control-zone       AP
-------------      ------------------------
Class 1 Grade 1          AP1(1)-1  00d0.f800.889f
                   AP1(1)-2  00d0.f800.7869
Class 2 Grade 2          AP2(2)-1  00d0.f800.889f
Class 3 Grade 3          AP2(3)-1  offline
Class 3 Grade 2          n/a
```

The following example displays the detailed configuration information of the association control zone named “Class 1 Grade 5”.

```
Ruijie# show control-zone Class 1 Grade 5
No such control zone configuration.
```

**Related Commands**

| Command | Description |
| --- | --- |
| **control-zone** | Configures an association control zone and enter association control zone configuration mode. |
| **ap** | Configures AP information in the association control zone. |

**Platform Description** N/A

## 2.13 show package

Use this command to display the terminal package configuration.

**show package** [ *pkg-name* ]

**Parameter Description**

| Parameter | Description |
| --- | --- |
| *pkg-name* | The name of the terminal package to be displayed. The name length range is from 1 to 32. |

**Defaults** N/A

**Command mode** Privileged EXEC mode

**Usage Guide** N/A

**Configuration Examples** The following example displays the configuration of all terminal packages.

```
Ruijie# show package
total package num :  2
========= package_1 =========
primary STA :  none
secondary STA num :  0
========= package_2 =========
primary STA :  00d0.f809.0092
secondary STA num :  4
00d0.f809.0096
00d0.f809.0097
00d0.f809.0098
00d0.f809.0099
```

The following example displays the configuration of all terminal packages.

```
Ruijie# show package
No package configuration
```

**Related Commands**

| Command | Description |
| --- | --- |
| **package** | Enters terminal package configuration mode |
| **primary-sta** | Configures a primary STA. |
| **secondary-sta** | Configures a secondary STA. |

**Platform Description** N/A

# 3 WBS Commands

## 3.1 show dot11 associations

Use this command to display the session information.

**show dot11 associations** *H.H.H interface-name*

**Parameter Description**

| Parameter | Description |
|---|---|
| *H.H.H* | Specifies the STA MAC address in the format of H.H.H |
| *Interface-name* | Specifies a radio |

**Defaults** N/A

**Command mode** Privileged EXEC mode

**Usage Guide** N/A

**Configuration Examples** The following example displays session information of STA 0025.9c9b.aeb5.

```
Ruijie# show dot11 associations 0025.9c9b.aeb5 1/0
The details of client 0cd6.bd11.7f9d.
   RSSI..................... 38
   SNR...................... -57
   AID...................... 1
   RX Data.................. 357
   RX Management............ 42
   RX Control............... 0
   RX Unicast............... 89
   RX Multicast............. 17
   RX Bytes................. 18681
   TX Data.................. 9
   TX Management............ 4
   TX Unicast............... 9
   TX Multicast............. 0
   TX Bytes................. 990
   TX Probe................. 0
   TX Assoc................. 1
   TX Assoc Fail............ 0
   TX Auth.................. 3
   TX Auth Fail............. 0
   TX Deauth................ 0
```

```
TX Disassoc.............. 0
Packet Load.............. 0
```

**Related Commands**

| Command | Description |
| --- | --- |
| N/A | N/A |

**Platform Description** N/A

## 3.2 show dot11 associations all-client

Use this command to display the information of all wireless clients.

**show dot11 associations all-client**

**Parameter Description**

| Parameter | Description |
| --- | --- |
| N/A | N/A |

**Defaults** N/A

**Command mode** Privileged EXEC mode

**Usage Guide** N/A

**Configuration Examples** The following example displays the information of all wireless clients.

```
Ruijie# show dot11 associations all-client
RADIO-ID WLAN-ID ADDR              AID  CHAN RATE_DOWN RATE_UP RSSI ASSOC_TIME IDLE TXSEQ
RXSEQ  ERP  STATE  CAPS HTCAPS VHT_MU_CAP HECAPS
1        7       00:25:9c:9b:ae:b5 1    1     52.0M      6.0M  39      0:00:18 0    7
544    0x0  0x3    ESs         SU
```

**Related Commands**

| Command | Description |
| --- | --- |
| N/A | N/A |

**Platform Description** N/A

## 3.3 show dot11 channels active

Use this command to display active channels supported by a radio.

**show dot11 channel active** *interface-name*

**Parameter Description**

| Parameter | Description |
| --- | --- |
| *interface-name* | Specifies a radio in the format of radioid/0. |

**Defaults** N/A

**Command mode** Privileged EXEC mode

**Usage Guide** N/A

**Configuration Examples** The following example displays active channels supported by radio1.

```
Ruijie# show dot11 channel active 1/0
Channel   1 : 2412 Mhz 11ng C CU       Channel   8 : 2447 Mhz 11ng C CU CL
Channel   2 : 2417 Mhz 11ng C CU       Channel   9 : 2452 Mhz 11ng C CU CL
Channel   3 : 2422 Mhz 11ng C CU       Channel  10 : 2457 Mhz 11ng C CL
Channel   4 : 2427 Mhz 11ng C CU       Channel  11 : 2462 Mhz 11ng C CL
Channel   5 : 2432 Mhz 11ng C CU CL    Channel  12 : 2467 Mhz 11ng C CL
Channel   6 : 2437 Mhz 11ng C CU CL    Channel  13 : 2472 Mhz 11ng C CL
Channel   7 : 2442 Mhz 11ng C CU CL
```

**Related Commands**

| Command | Description |
| --- | --- |
| N/A | N/A |

**Platform Description** N/A

## 3.4 show dot11 channels all

Use this command to all channels supported by a radio.

**show dot11 channels all** *interface-name*

**Parameter Description**

| Parameter | Description |
| --- | --- |
| *interface-name* | Specifies a radio in the format of radioid/0. |

**Defaults** N/A

**Command mode** Privileged EXEC mode

**Usage Guide** N/A

**Configuration Examples** The following example displays all channels supported by radio1.

```
Ruijie# show dot11 channels all 1/0
The Details of Client 0025.9c9b.aeb5:
Channel   1 : 2412 Mhz 11ng C CU       Channel   8 : 2447 Mhz 11ng C CU CL
Channel   2 : 2417 Mhz 11ng C CU       Channel   9 : 2452 Mhz 11ng C CU CL
Channel   3 : 2422 Mhz 11ng C CU       Channel  10 : 2457 Mhz 11ng C CL
Channel   4 : 2427 Mhz 11ng C CU       Channel  11 : 2462 Mhz 11ng C CL
Channel   5 : 2432 Mhz 11ng C CU CL     Channel  12 : 2467 Mhz 11ng C CL
Channel   6 : 2437 Mhz 11ng C CU CL     Channel  13 : 2472 Mhz 11ng C CL
Channel   7 : 2442 Mhz 11ng C CU CL
```

**Related Commands**

| Command | Description |
|---|---|
| N/A | N/A |

**Platform Description** N/A

## 3.5 show dot11 radio-status

Use this command to display status and capacity of all RF ports.

**show dot11 radio-status**

**Parameter Description**

| Parameter | Description |
|---|---|
| N/A | N/A |

**Defaults** N/A

**Command mode** Privileged EXEC mode

**Usage Guide** N/A

**Configuration Examples** The following example displays status and capacity of all RF ports.

```
Ruijie#show dot11 radio-status
radio status    capability
```

```
----- ---------- ----------
1    online    b/g/n
2    online    a/n/ac/ax
```

**Related Commands**

| Command | Description |
| --- | --- |
| N/A | N/A |

**Platform Description** N/A

## 3.6 show dot11 rate-set

Use this command to display speed set of all RF ports.

**show dot11 rate-set**

**Parameter Description**

| Parameter | Description |
| --- | --- |
| N/A | N/A |

**Defaults** N/A

**Command mode** Privileged EXEC mode

**Usage Guide** N/A

**Configuration Examples** The following example displays speed set of all RF ports.

```
Ruijie# show dot11 rate-set
LLCB(1) RATE SET
Mandatory rate:  11M,
Support   rate:  6M, 9M, 12M, 18M, 24M, 36M, 48M, 54M,
Mandatory 11n MCS index:
Support   11n MCS index: 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15,
LLCB(2) RATE SET
Mandatory rate:  6M, 12M, 24M,
Support   rate:  9M, 18M, 36M, 48M, 54M,
Mandatory 11n MCS index:
Support   11n MCS index: 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15,
```

**Related Commands**

| Command | Description |
| --- | --- |
| N/A | N/A |

**Platform Description** N/A

## 3.7 show dot11 mbssid

Use this command to display the BSS list.

**show dot11 mbssid**

**Parameter Description**

| Parameter | Description |
|---|---|
| N/A | N/A |

**Defaults** N/A

**Command mode** Privileged EXEC mode

**Usage Guide** N/A

**Configuration Examples** The following example displays the BSS list.

```
Ruijie# show dot11 mbssid
   name: Dot11radio 47/0.1
wlan id: 1
   ssid: ssid-wlan-2
  bssid: 0a0c.3067.fbbf
```

**Related Commands**

| Command | Description |
|---|---|
| N/A | N/A |

**Platform Description** N/A

## 3.8 show dot11 wireless

Use this command to display the information and configuration of a radio.

**show dot11 wireless** *interface-num*

**Parameter Description**

| Parameter | Description |
|---|---|
| *interface-num* | Specifies a radio in the format of radioid/0. |

**Defaults** N/A

**Command mode** Privileged EXEC mode

**Usage Guide** N/A

**Configuration Examples** The following example displays the information and configuration of radio1.

```
Ruijie# show dot11 wireless 1/0
Network Name (SSID): NULL
   Interface..................... Dot11radio 1/0
   Vlan (group) id.............. 0
   MAC Address.................. 000c.3067.fbbf
   Beacon Period................ 100
   RTS Threshold................ 2347
   Fragment Threshold........... 2346
   Radio Mode................... 11ng_ht20
   Channel...................... 2412(1)
   Noise Floor.................. -103 dBm
   Channel width................ 20Mhz
   Current Tx Power Level....... 100%
   Current CCA ................. 28
Tx/Rx Chain:
   Antenna Gain................. 3
   Tx Chain Mask................ 0x3
   Num of Antenna Tx............ 2
   Rx Chain Mask................ 0x3
   Num of Antenna Rx............ 2
Power Save:
   DTIM Period.................. 1
   DTIM Count................... 0
   Stations In Power Save....... 0
   Stations Total............... 0
11n Aggregation:
   A-mpdu Status................ Enable
Tx Retries:
   Tx short   retries.......... 7
   Tx long    retries.......... 4
Total Stations:
   Total........................ 0
   Non-ERP...................... 0
   Non-HT....................... 0
   HT20......................... 0
```

**Related**

| Command | Description |
|---|---|

| Commands | | |
|---|---|---|
| | N/A | N/A |

**Platform Description** N/A

## 3.9 show dot11 wlan

Use this command to display WLAN information and configuration.

**show dot11 wlan** *wlan-id*

| Parameter Description | Parameter | Description |
|---|---|---|
| | *wlan-id* | Specifies a WLAN |

**Defaults** N/A

**Command mode** Privileged EXEC mode

**Usage Guide** N/A

**Configuration Examples** The following example displays the information and configuration of WLAN2.

```
Ruijie# show dot11 wlan 2
Network Name (SSID): ssid-wlan-2
   Interface..................... Dot11radio 2/0.2
   Vlan (group) id.............. 0
   MAC Address................... 0e14.5876.675b
   Beacon Period................. 100
   RTS Threshold................. 2347
   Fragment Threshold............ 2346
   Radio Mode.................... 11ac_vht20_5g
   Channel....................... 5825(165)
   Noise Floor................... -107 dBm
   Channel width................. 20Mhz
   Current Tx Power Level....... 100%
   Mcast rate ................... 24
   Current CCA .................. 28
Tx/Rx Chain:
   Antenna Gain.................. 3
   Tx Chain Mask................. 0x3
   Num of Antenna Tx............. 2
   Rx Chain Mask................. 0x3
   Num of Antenna Rx............. 2
```

```
Power Save:
   DTIM Period.................. 1
   DTIM Count................... 0
   Stations In Power Save....... 0
   Stations Total............... 0
11n Aggregation:
   A-mpdu Status................ Enable
Tx Retries:
   Tx short    retries.......... 7
   Tx long     retries.......... 4
Total Stations:
   Total........................ 0
   Non-ERP...................... 0
   Non-HT....................... 0
   HT20......................... 0
```

**Related Commands**

| Command | Description |
| --- | --- |
| N/A | N/A |

**Platform Description** N/A

## 3.10 show ebag

Use this command to display Ebag information and configuration.

**show ebag**

**Parameter Description**

| Parameter | Description |
| --- | --- |
| N/A | N/A |

**Defaults** N/A

**Command mode** Privileged EXEC mode

**Usage Guide** N/A

**Configuration Examples** The following example displays Ebag information and configuration.

```
Ruijie# show ebag
auto ebag status: disable
```

**Related**

| Command | Description |
| --- | --- |

**Commands**

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

**Platform Description** N/A

# 4 DATA-PLANE Commands

## 4.1 data-plane

Use this command to configure the forwarding weights of different packets.
Use the **no** form of this command to restore the default setting.
**data-plane queue-weight** *unicast-packet-weight multicast-packet-weight broadcast-packet-weight unknown-multicast-packet-weight unknown-unicast-packet-weight*
**no data-plane queue-weight**

Use this command to configure the update interval and token rate of token bucket.
Use the no form of this command to restore the default setting.
**data-plane token** *token-interval token-base-rate*
**no data-plane token**

Use this command to enable or disable the wireless broadcast function.
Use the **no** form of this command to restore the default setting.
**data-plane wireless-broadcast** { **enable** | **disable** }
**no data-plane wireless-broadcast**

**Parameter Description**

| Parameter | Description |
|---|---|
| **queue-weight** | Configures the forwarding weights for different packets. |
| **wireless-broadcast** | Configures the wireless broadcast function. |
| *unicast-packet-weight* | Sets the forwarding weight of unicast packets. The range is from 1 to 100. The default value is 16. |
| *multicast-packet-weight* | Sets the forwarding weight of multicast packets. The range is from 1 to 50. The default value is 4. |
| *broadcast-packet-weight* | Sets the forwarding weight of broadcast packets. The range is from 1 to 50. The default value is 2. |
| *unknown-multicast-packet-weight* | Sets the forwarding weight of unknown multicast packets. The range is from 1 to 25. The default value is 1. |
| *unknown-unicast-packet-weight* | Sets the forwarding weight of unknown unicast packets. The range is from 1 to 25. The default value is 1. |
| **token** | Configures the update interval and token rate of token bucket. |
| *token-interval* | Sets the update interval of the token bucket. The default value is 1 in the unit of 10 milliseconds. |
| *token-base-rate* | Sets the token rate of the token bucket. The default value is 64 for AC and 5 for AP. |

**Defaults** The forwarding weight configuration for different types of packets is enabled by default.
The wireless broadcast function is disabled by default.

| | |
|---|---|
| **Command Modes** | Global configuration mode |
| **Usage Guide** | N/A |
| **Configuration Examples** | The following example configures the forwarding weights of different packet types and enables the wireless broadcast function.<br>`Ruijie(config)#data-plane queue-weight 100 50 50 25 25`<br>`Ruijie(config)#data-plane token 10 10`<br>`Ruijie(config)#data-plane wireless-broadcast enable` |
| **Platform Description** | N/A. |

# 5 WLOG Commands

## 5.1 show wlan diag sta

Use the following command to display STA statistics on an AP:

**show wlan diag sta** [ **sta-mac** *STA_MAC* ] [ **number** *NUMBER* ]

**Parameter Description**

| Parameter | Description |
|---|---|
| *STA_MAC* | Specifies the MAC address of an STA. |
| *NUMBER* | Specifies the maximum number of records to be displayed. |

**Defaults** N/A

**Command Mode** Privileged EXEC mode

**Usage Guide** The memory pre-allocation is performed when the WLAN-WLOG function is enabled. If the memory is insufficient, the WLAN-WLOG function cannot be enabled.
Memories of all saved information and pre-allocated memories are set free when the WLOG function is disabled.

**Configuration Examples** This example displays STA statistics on an AP:

```
Ruijie# show wlan diag sta
sta mac: c83a.35c6.0c72
================================================================================
============================================================
2012-05-28 19:31:08
wlan id  state    rssi_rt  rs_rate_mcs tx_frm_cnts rx_frm_cnts tx_frm_flow
rx_frm_flow tx_cnts_error tx_flow_error mgmt_cnts mgmt_flow
-------- -------- -------- ----------- ----------- ----------- -----------
----------- ------------ ------------ --------- ---------
1        3        23       80          18          59          4384        5967
0           0           3        381


tx/rxmcs     mcs0, mcs1   mcs2, mcs3   mcs4, mcs5   mcs6, mcs7   mcs8, mcs9
mcs10, mcs11   mcs12, mcs13 mcs14, mcs15
-------------   -------------   -------------   -------------   -------------
------------ ------------ ------------ -------------
txmcspercent : 0       0       0      0      0     0     0     0
rxmcspercent : 0       0       0      0      0     0     0     0
```

```
tx/rxrate    1, 2    5.5, 11 6, 9    12, 18  24, 36  48, 54   --      --
------------ ------- ------- ------- ------- ------- ------- ------- -------
txratepercent: 16     0       0       7       50      27      0       0
rxratepercent: 57     3       0       5       13      22      0       0
```

| Field | Description |
|---|---|
| sta_record | Specifies STA records. |
| TIME | Specifies the time when STA records are collected. |
| IP Address | Specifies the IP address of an STA whose statistics are collected. |
| Rssi | Specifies signal strength. |
| Link Rate | Specifies a connection rate. |
| AP MAC | Specifies the MAC address of an AP associated with the STA. |
| SSID | Specifies the SSID of the WLAN associated with the STA. |
| RADIO | Specifies the ID of the radio associated with the STA. |
| Action | Specifies the type of STA action records. |
| Result | Specifies the result of STA action records. |
| Reason | Specifies the reason for STA action records. |

**Related Commands**

| Command | Description |
|---|---|
| N/A | N/A |

**Platform Description** N/A

## 5.2 wlan diag enable

Use this command to enable the WLAN log (WLOG) . Use the **no** form of this command to disable WLOG.

**wlan diag enable**

**no wlan diag enable**

**Parameter Description**

| Parameter | Description |
|---|---|
| N/A | N/A |

**Defaults** The WLOG function is disabled on APs by default.

**Command Mode** Global configuration mode

**Usage Guide** The memory pre-allocation is performed when the WLAN-WLOG function is enabled. If the memory is insufficient, the
Memories of all saved information and pre-allocated memories are set free when the WLOG function is disabled.

**Configuration Examples** The following example enables and disables the WLOG function:

```
Ruijie# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Ruijie(config)#wlan diag enable
Ruijie(config)#no wlan diag enable
```

**Related Commands**

| Command | Description |
| --- | --- |
| N/A | N/A |

**Platform Description** N/A

# 1 WLAN RF Commands

## 1.1 schedule session

Use this command to configure a scheduling session for a WLAN. Use the **no** form of this command to remove the configuration.

**schedule session** *sid*

**no schedule session** *sid*

**Parameter Description**

| Parameter | Description |
|---|---|
| *sid* | Specifies the ID of the scheduling session to be created or to be applied to a WLAN. The range is from 1 to 64 for an AC and from 1 to 8 for a fat AP. |

**Defaults**

No scheduling session is configured by default.

No scheduling session is applied to a WLAN or a radio by default.

**Command mode**

Global configuration mode/WLAN configuration mode/Fat AP interface configuration mode

**Usage Guide**

In global configuration mode, you can use this command to create a scheduling session and configure parameters for it. If the scheduling session has been created, the configuration is invalid. On fit AP networking topology, the scheduling session created in WLAN configuration mode will be applied to a WLAN.

If you delete the scheduling session in the global configuration mode, the scheduling session on WLAN or Radio is deleted automatically.

**Configuration Examples**

The following example creates or configures scheduling session 1.

```
Ruijie(config)# schedule session 1
```

The following example applies scheduling session 1 to WLAN 1

```
Ruijie(config)# wlan-config 1
Ruijie(config-wlan)# schedule session 1
```

**Related Commands**

| Command | Description |
|---|---|
| **show schedule session** | Displays configuration about the scheduling session. |
| **show running-config** | Displays current configuration. |

**Platform**

N/A

**Description**

## 1.2 schedule session time-range

Use this command to set scheduling time for a scheduling session. Use the **no** form of this command to delete the configuration.

**schedule session** *sid* **time-range** *n* **period** *day1* [ **to** *day2* ] **time** *hh1:mm1* **to** *hh2:mm2*

**no schedule session** *sid* **time-range** *n*

**Parameter Description**

| Parameter | Description |
|---|---|
| *sid* | Specifies the ID of the scheduling session to be created or to be applied to a WLAN. The range is from 1 to 8 for a fat AP. |
| *n* | Specifies the scheduling session time-range ID, in the range from 1 to 8. |
| *day1* | Specifies the start day of the scheduling session time range. Select a value from { sun \| mon \| tue \| wed \| thu \| fri \| sat }. |
| **to** *day2* | Specifies the end day of the scheduling session time range. The default scheduling session time range is one day. |
| **time** *hh1:mm1* **to** *hh2:mm2* | Specifies the start and end time. hh1:mm1indicate the start hour and minute; hh2:mm2 indicate the end hour and minute. The hour value is in the range from 0 to 23 and the minute value is in the range from 0 to 59. |

**Defaults** No scheduling time is set for a scheduling session by default.

**Command mode** Global configuration mode

**Usage Guide** A scheduling session has only one period of scheduling time. If you run this command for many times, only the configuration at the last time takes effect.

If *hh2:mm2* is not set, the scheduling time lasts to 23:59 by default.

If *hh2:mm2* is earlier than *hh1:mm1*, *hh2:mm2* is the time on the next day.

**Configuration Examples** The following example sets the scheduling time of scheduling session 1 to the range from 2:30 am to 9:30 am.

```
Ruijie(config)#schedule session 1 time 2:30 to 9:30
```

The following example sets the scheduling time of scheduling session 1 to the range from 10:45 pm to 9:00 am on the next day.

```
Ruijie(config)# schedule session 1 time 22:45 to 9:00
```

**Related Commands**

| Command | Description |
|---|---|
| **show schedule session** | Displays configuration about the scheduling |

| | |
|---|---|
| | session. |

**Platform Description** N/A

## 1.3 show schedule session

Use this command to display configuration about scheduling sessions.

**show schedule session** [ *sid* ]

**Parameter Description**

| Parameter | Description |
|---|---|
| *sid* | Specifies a scheduling session ID in the range from 1 to 64. |

**Defaults**

**Command mode** Privileged EXEC mode

**Usage Guide** If no scheduling session ID is specified, configuration about all scheduling sessions will be displayed.

**Configuration Examples** The following example displays configuration about all scheduling sessions.

```
Ruijie(config)#show schedule session
Schedule session [1]:
  Schedule period ............................... Sun, Wed to Fri
  Schedule time ................................. 0:00 to 9:30
Schedule session [3]:
  Schedule period ............................... Mon to Fri
  Schedule time ................................. 2:00 to 9:00
```

**Related Commands**

| Command | Description |
|---|---|
| **schedule session** | Configures a scheduling session. |

**Platform Description** N/A

# 2 Band Select Commands

## 2.1 band-select acceptable-rssi

Use this command to configure an acceptable STA RSSI lower limit. Use the **no** form of this command to restore the default setting.

**band-select acceptable-rssi** *value*

**no band-select acceptable-rssi**

**Parameter Description**

| Parameter | Description |
|---|---|
| *value* | Indicates acceptable STA RSSI lower limits, in the range from -100 to -50 in the unit of dBm. |

**Defaults** The default is -80 dBm.

**Command Mode** Global configuration mode

**Usage Guide** This lower limit value is used to differentiate associable STAs from non-associable STAs. If the RSSI value is greater than this value, such STAs are associable and their information will be paid attention to. If the RSSI value is less than this value, the information of such STAs will be ignored. It is not recommended that users modify the default value.

**Configuration Examples** The following example sets the acceptable STA RSSI low limit to -70 dBm.

```
Ruijie(config)#band-select acceptable-rssi -70
```

**Related Commands**

| Command | Description |
|---|---|
| **show band-select configuration** | Displays the Band Select configuration. |

**Platform Description** N/A

## 2.2 band-select access-denial

Use this command to set the access-denial count. Use the **no** form of this command to restore the default setting.

**band-select access-denial** *value*

**no band-select access-denial**

**Parameter**

| Parameter | Description |
|---|---|

**Description**

| | |
|---|---|
| *value* | Sets the access-denial count, in the range from 0 to 10. |

**Defaults** The default is 2.

**Command Mode** Global configuration mode

**Usage Guide** The value **n** indicates that the AP does not respond until it receives n consecutive link authentication requests from the dual-band STA on 2.4-GHz band.

This parameter can increase the navigation rate for high frequency spectrum, but it may cause difficulty in access to some dual-band STAs.

**Configuration Examples** The following example sets the access-denial count to 4.

```
Ruijie(config)# band-select access-denial 4
```

**Related Commands**

| Command | Description |
|---|---|
| N/A | N/A |

**Platform Description** N/A

## 2.3 band-select age-out

Use this command to configure the aging cycle of STA information. Use the **no** form of this command to restore the default setting.

**band-select age-out** { **dual-band** *value* **| suppression** *value* }

**no band-select age-out** { **dual-band | suppression** }

**Parameter Description**

| Parameter | Description |
|---|---|
| **dual-band** *value* | The aging cycle of dual-band STA information, in the range from 20 to 120 in the unit of seconds. |
| **suppression** *value* | The aging cycle of suppressed STA information, in the range from 10 to 60 in the unit of seconds. |

**Defaults** The default aging cycle of dual-band STA information is 60 seconds.
The default aging cycle of suppressed STA information is 20 seconds.

**Command Mode** Global configuration mode

**Usage Guide** The AP is less sensitive to the STA band switching as the life cycle of the dual-band STA information increases. If the wireless users' network cards often switch between 2.4-GHz and 5-GHz bands, a smaller value can be configured; otherwise, a bigger value can be configured.

It is recommended to configure the aging cycle of dual-band STA information as two or three times as that of the suppressed STAs.

**Configuration Examples** The following example sets the aging cycle of dual-band STA information to 120 seconds.

```
Ruijie(config)#band-select age-out dual-band 120
```

The following example sets the aging cycle of suppressed STA information to 60 seconds.

```
Ruijie(config)# band-select age-out suppression 60
```

**Related Commands**

| Command | Description |
| --- | --- |
| N/A | N/A |

**Platform Description** N/A

## 2.4 band-select enable

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

**band-select enable**

**no band-select enable**

**Parameter Description**

| Parameter | Description |
| --- | --- |
| N/A | N/A |

**Defaults** This function is disabled by default.

**Command Mode** WLAN configuration mode

**Usage Guide** Enabling the spectrum navigation requires that:

1. WLAN is mapped to a dual-band AP.
2. WLAN is mapped to two radios of the dual-band AP.

If the scenario cannot meet the above requirements, it is recommended not to enable the spectrum navigation.

If the WLAN with the spectrum navigation enabled is mapped to a single-band 2.4GHz AP, the dual-band STA within AP signal coverage cannot navigate to the 5GHz band.

**Configuration Examples** The following example enables the spectrum navigation for WLAN1.

```
Ruijie(config)# wlan-config 1
Ruijie(config-wlan)# band-select enable
```

The following example disables the spectrum navigation for WLAN1.

```
Ruijie(config)# wlan-config 1
Ruijie(config-wlan)# no band-select enable
```

**Related Commands**

| Command | Description |
|---|---|
| N/A | N/A |

**Platform Description** N/A

## 2.5 band-select probe-count

Use this command to configure the probe count of the suppressed STAs. Use the **no** form of this command to restore the default setting.

**band-select probe-count** *value*

**no band-select probe-count**

**Parameter Description**

| Parameter | Description |
|---|---|
| *value* | Indicates the probe-count of the suppressed STAs, in the range is from 1 to 10. |

**Defaults** The default is 2.

**Command Mode** Global configuration mode

**Usage Guide** This item indicates the extent of suppression to a suppressed STA: The value **n** indicates that the AP respond once after a STA transmits **n** probe requests.

**Configuration Examples** The following example sets the probe count of the suppressed STAs to 1.

```
Ruijie(config)#band-select probe-count 1
```

**Related Commands**

| Command | Description |
|---|---|
| **show band-select configuration** | Displays the Band Select configuration. |

**Platform Description** N/A

## 2.6 band-select scan-cycle

Use this command to configure the aging scanning cycle of STA information. Use the **no** form of this command to restore the default setting.

**band-select scan-cycle** *period*

**no band-select scan-cycle**

**Parameter Description**

| Parameter | Description |
|---|---|
| *period* | Indicates the aging scanning cycle, in the range from 1 to 1000 in the unit of milliseconds. |

**Defaults** The default is 200 milliseconds.

**Command Mode** Global configuration mode

**Usage Guide** A bigger aging scanning cycle value degrades the Band Select performance, but it can save the system resources.

**Configuration Examples** The following example sets the aging scanning cycle to 1 millisecond.

```
Ruijie(config)#band-select scan-cycle 1
```

**Related Commands**

| Command | Description |
|---|---|
| **show band-select configuration** | Displays the Band Select configuration. |

**Platform Description** N/A

## 2.7 show band-select configuration

Use this command to display the Band Select configuration.

**show band-select configuration**

**Parameter Description**

| Parameter | Description |
|---|---|
| N/A | N/A |

**Defaults** N/A

**Command Mode** Privileged EXEC mode

**Usage Guide** Use this command to show all configurations of the Band Select function.

**Configuration Examples** The following example displays the Band Select configuration.

```
Ruijie# show band-select configuration
Band Select Configuration
  Band Select Enable.............................. Disable
  Probe Cycle Count.................................... 2
  Scan Cycle Period Threshold (milliseconds)............... 200
  Age Out Suppression (seconds)........................... 20
  Age Out Dual Band (seconds)............................. 60
  Acceptable Client RSSI (dBm)........................... -80
```

**Related Commands**

| Command | Description |
| --- | --- |
| **show band-select statistics** | Displays the Band Select statistics. |

**Platform Description** N/A

## 2.8 show band-select statistics

Use this command to display the Band Select statistics.

**show band-select statistics**

**Parameter Description**

| Parameter | Description |
| --- | --- |
| N/A | N/A |

**Defaults** N/A

**Command Mode** Privileged EXEC mode

**Usage Guide** Use this command to display the Band Select statistics.

**Configuration Examples** The following example displays the Band Select statistics.

```
Ruijie# show band-select statistics
Band Select Statistics
  Number of dual band client.............................. 4
  Number of dual band client added........................ 132
  Number of dual band client expired...................... 128
  Number of suppressed client............................. 6
  Number of suppressed client added...................... 234
```

```
Number of suppressed client expired..... 228
```

**Related Commands**

| Command | Description |
| --- | --- |
| **show band-select configuration** | Displays the Band Select configuration. |

**Platform Description** N/A

# WLAN Security Commands

# 1 Wireless Security Commands

## 1.1 authtimeout forbidcount

Use this command to configure the forbidcount after a four-way handshake fails to accomplish key exchange. Use the **no** or **default** form of this command to restore the default setting.

**authtimeout forbidcount** *count*

**no authtimeout forbidcount**

**default authtimeout forbidcount**

**Parameter Description**

| Parameter | Description |
|---|---|
| *count* | Sets the forbidcount after a four-way handshake fails to accomplish key exchange. |

**Defaults** The default is 10.

**Command mode** WLAN security configuration mode

**Usage Guide** N/A

**Configuration Examples** The following example sets the forbidcount to 5 after a four-way handshake fails to accomplish key exchange.

```
Ruijie(config-wlansec)#authtimeout forbidcount 5
```

**Related Commands**

| Command | Description |
|---|---|
| N/A | N/A |

**Platform Description** N/A

## 1.2 authtimeout forbidtime

Use this command to set the forbidtime after a four-way handshake fails to accomplish key exchange. Use the **no** or **default** form of this command to restore the default setting.

**authtimeout forbidtime** *time*

**no authtimeout forbidtime**

**default authtimeout forbidtime**

**Parameter**

| Parameter | Description |
|---|---|

**Description**

| | |
|---|---|
| *time* | Sets the forbidtime after a four-way handshake fails to accomplish key exchange, in the unit of seconds. |

**Defaults** The default is 5.

**Command mode** WLAN security configuration mode

**Usage Guide** N/A

**Configuration Examples** The following example sets the forbidtime to 6 seconds after a four-way handshake fails to accomplish key exchange,

```
Ruijie(config-wlansec)#authtimeout forbidtime 6
```

**Related Commands**

| Command | Description |
|---|---|
| N/A | N/A |

**Platform Description** N/A

## 1.3 authtimeout groupcount

Use this command to set the retransmission count for the multicast key agreement packet. Use the **no** or **default** form of this command to restore the default setting.

**authtimeout groupcount** *count*

**no authtimeout groupcount**

**default authtimeout groupcount**

**Parameter Description**

| Parameter | Description |
|---|---|
| *count* | Sets the retransmission count for the multicast key negotiation packet. |

**Defaults** The default is 7.

**Command mode** WLAN security configuration mode

**Usage Guide** N/A

**Configuration Examples** The following example set the retransmission count for the multicast key negotiation packet to 5.

```
Ruijie(config-wlansec)#authtimeout groupcount 5
```

**Related Commands**

| Command | Description |
| --- | --- |
| N/A | N/A |

**Platform Description** N/A

## 1.4 authtimeout grouptime

Use this command to set the timeout period for the multicast key negotiation packet. Use the **no** or **default** form of this command to restore the default setting.

**authtimeout grouptime** *timeout*

**no authtimeout grouptime**

**default authtimeout grouptime**

**Parameter Description**

| Parameter | Description |
| --- | --- |
| *timeout* | Sets the timeout period for the multicast key negotiation packet, in the unit of milliseconds. |

**Defaults** The default is 1200 milliseconds.

**Command mode** WLAN security configuration mode

**Usage Guide** N/A

**Configuration Examples** The following example sets the timeout period for the multicast key negotiation packet to 100 milliseconds.

```
Ruijie(config-wlansec)#authtimeout grouptime 100
```

**Related Commands**

| Command | Description |
| --- | --- |
| N/A | N/A |

**Platform Description** N/A

## 1.5 authtimeout paircount

Use this command to set the retransmission count for the unicast key negotiation packet. Use the **no** or **default** form of this command to restore the default setting.

**authtimeout paircount** *count*
**no authtimeout paircount**
**default authtimeout paircount**

**Parameter Description**

| Parameter | Description |
| --- | --- |
| *count* | Sets the retransmission count for the unicast key negotiation packet. |

**Defaults** The default is 7.

**Command mode** WLAN security configuration mode

**Usage Guide** N/A

**Configuration Examples** The following example sets the retransmission count for the unicast key negotiation packet to 5.

```
Ruijie(config-wlansec)#authtimeout paircount 5
```

**Related Commands**

| Command | Description |
| --- | --- |
| N/A | N/A |

**Platform Description** N/A

## 1.6 authtimeout pairtime

Use this command to set the timeout period for the unicast key negotiation packet. Use the **no** or **default** form of this command to restore the default setting.
**authtimeout pairtime** *timeout*
**no authtimeout pairtime**
**default authtimeout pairtime**

**Parameter Description**

| Parameter | Description |
| --- | --- |
| *timeout* | Sets the timeout period for the unicast key negotiation packet, in the unit of milliseconds. |

**Defaults** The default is 1200 milliseconds.

**Command mode** WLAN security configuration mode

**Usage Guide** N/A

**Configuration Examples** The following example sets the timeout period for the unicast key negotiation packet to 100 milliseconds.

```
Ruijie(config-wlansec)#authtimeout pairtime 100
```

**Related Commands**

| Command | Description |
| --- | --- |
| N/A | N/A |

**Platform Description** N/A

## 1.7 dot1x-mab

Use this command to configure MAB authentication for the specified WLAN. Use the **no** form of this command to restore the default setting.

**dot1x-mab**

**no dot1x-mab**

**Parameter Description**

| Parameter | Description |
| --- | --- |
| **no** | Clears the MAB authentication configuration. |

**Defaults** MAB authentication is disabled by default.

**Command mode** WLAN security configuration mode

**Usage Guide** This command is used to enable MAB authentication. It can be used in combination with PSK access authentication but not with 802.1X access authentication.

**Configuration Examples** The following example enables MAB authentication for WLAN 1.

```
Ruijie(config)#wlansec 1
Ruijie(config-wlansec)# dot1x-mab
```

The following example disables MAB authentication for WLAN 1.

```
Ruijie(config)#wlansec 1
Ruijie(config-wlansec)# no dot1x-mab
```

**Related Commands**

| Command | Description |
| --- | --- |
| N/A | N/A |

**Platform Description** N/A

## 1.8 security rsn

Use this command to configure RSN authentication for a WLAN.

**security rsn** { **enable** | **disable** }

**Parameter Description**

| Parameter | Description |
|---|---|
| **enable** | Enables the RSN authentication mode. |
| **disable** | Disables the RSN authentication mode. |

**Defaults** This function is disabled by default.

**Command mode** WLAN security configuration mode

**Usage Guide** The command is used to enable the RSN authentication mode. Only after the RSN authentication mode is enabled can encryption and authentication methods be configured in the RSN mode. Otherwise, any configuration is invalid. When you use the RSN authentication, you need to configure an encryption method and an authentication method. If only an encryption or authentication method is configured, or neither is configured, the wireless client cannot be associated with the wireless network. The RSN authentication mode is what is usually called WPA2 authentication mode. If both WPA and RSN authentication modes are configured simultaneously for a WLAN, the encryption and authentication methods in these two authentication modes are identical, and the newly configured encryption and authentication methods will override the previous ones.

**Configuration Examples** The following example sets the authentication mode of WLAN1 to RSN.

```
Ruijie(config)#wlansec 1
Ruijie(wlansec)# security rsn enable
```

**Related Commands**

| Command | Description |
|---|---|
| **security rsn akm** { **psk** | **802.1x** } { **enable** | **disable** } | Configures an authentication method in the RSN authentication mode. |
| **security rsn ciphers** { **aes** | **tkip** } { **enable** | **disable** } | Configures an encryption method in the RSN authentication mode. |
| **security rsn akm psk set-key ascci** | Configures a shared password for RSNs. |

**Platform Description** N/A

## 1.9 security rsn akm

Use this command to configure RSN authentication for a WLAN.

**security rsn akm** { **psk** | **802.1x** } { **enable** | **disable** }

**Parameter Description**

| Parameter | Description |
|---|---|
| **psk** | Configures the authentication method to pre-shared key identity verification. |
| **802.1x** | Configures the authentication method to IEEE802.1x authentication. |
| **enable** | Enables an authentication method in the RSN authentication mode. |
| **disable** | Disables an authentication method in the RSN authentication mode. |

**Defaults** N/A

**Command mode** WLAN security configuration mode

**Usage Guide** The command is used to enable an authentication method in the RSN authentication mode. Only after the RSN authentication mode is enabled can an authentication method be configured. There are two authentication methods: PSK and 802.1x.

**Configuration Examples** The following example configures the authentication method for WLAN1 in the RSN authentication mode to PSK.

```
Ruijie (config)#wlansec 1
Ruijie(wlansec)# security rsn akm psk enable
```

The following example sets the authentication method for WLAN1 in the RSN authentication mode to 802.1x authentication.

```
Ruijie (config)#wlansec 1
Ruijie(wlansec)# security rsn akm 802.1x enable
```

**Related Commands**

| Command | Description |
|---|---|
| **security rsn** { **enable** | **disable** } | Configures the WLAN configuration mode. |
| **security rsn ciphers** { **aes** | **tkip** } { **enable** | **disable** } | Configures an encryption method in the RSN authentication mode. |
| **security rsn akm psk set-key ascci** | Configures a shared password for RSNs. |

**Platform Description** N/A

## 1.10 security rsn akm psk set-key

Use this command to configure a shared password for RSNs in the PSK authentication mode.

**security rsn akm psk set-key** { **ascii** *ascii-key* | **hex** *hex-key* }

**Parameter Description**

| Parameter | Description |
|---|---|
| **ascii** | Specifies the ASCII password. |
| *ascii-key* | The ASCII password, containing 8-63 characters. |
| **hex** | Specifies the hexadecimal password. |
| *hex-key* | The hexadecimal password, containing 64 characters. |

**Defaults** N/A

**Command mode** WLAN security configuration mode

**Usage Guide** This shared password is of use only when the PSK authentication mode is enabled.

**Configuration Examples** The following example sets the shared password for WLAN 1 RSN to 12345678.

```
Ruijie (config)#wlansec 1
Ruijie(wlansec)# security rsn enable
Ruijie(wlansec)# security rsn akm psk enable
Ruijie(wlansec)# security rsn akm psk set-key ascci 12345678
```

**Related Commands**

| Command | Description |
|---|---|
| **security rsn** { **enable** | **disable** } | Configures the RSN authentication mode. |
| **security rsn ciphers** { **aes** | **tkip** } { **enable** | **disable** } | Configures an encryption method in the RSN authentication mode. |
| **security rsn akm** { **psk** | **802.1x** } { **enable** | **disable** } | Configures an authentication method in the RSN authentication mode. |

**Platform Description** N/A

## 1.11 security rsn ciphers

Use this command to configure an encryption method for a WLAN in the RSN authentication mode.

**security rsn ciphers** { **aes** | **tkip** } { e**nable** | **disable** }

**Parameter Description**

| Parameter | Description |
|---|---|

| | |
|---|---|
| **aes** | Configures the encryption method to AES. |
| **tkip** | Configures the encryption method to TKIP. |
| **enable** | Enables an encryption method in the RSN authentication mode. |
| **disable** | Disables an encryption method in the RSN authentication mode. |

**Defaults** N/A

**Command mode** WLAN security configuration mode

**Usage Guide** The command is used to enable an encryption method in the RSN authentication mode. There are two encryption methods: AES and TKIP.

**Configuration Examples** The following example configures the encryption method for WLAN1 in the RSN authentication mode to AES.

```
Ruijie (config)#wlansec 1
Ruijie(wlansec)# security rsn ciphers aes enable
```

The following example disables the AES encryption method for WLAN1 in the RSN authentication mode.

```
Ruijie (config)#wlansec 1
Ruijie(wlansec)# security wpa ciphers aes disable
```

The following example sets the encryption method for WLAN1 in the RSN authentication mode to TKIP.

```
Ruijie (config)#wlansec 1
Ruijie(wlansec)# security rsn ciphers tkip enable
```

The following example disables the TKIP encryption method for WLAN1 in the RSN authentication mode.

```
Ruijie (config)#wlansec 1
Ruijie(wlansec)# security rsn ciphers tkip disable
```

**Related Commands**

| Command | Description |
|---|---|
| **security rsn** { **enable** \| **disable** } | Configures the RSN authentication mode. |
| **security rsn akm** { **psk** \| **802.1x** } { **enable** \| **disable** } | Configures an authentication method in the RSN authentication mode. |
| **security rsn akm psk set-key ascci** | Configures a shared password for RSNs. |

**Platform Description** N/A

## 1.12 security static-wep-key authentication

Use this command to configure an authentication method for a WLAN in the static WEP mode.

**security static-wep-key authentication** { **open** | **share-key** }

**Parameter Description**

| Parameter | Description |
| --- | --- |
| **open** | The open system authentication mode. |
| **share-key** | The shared key authentication mode. |

**Defaults** The default is **open**.

**Command mode** WLAN security configuration mode

**Usage Guide** This command must be used with the **security static-wep-key encryption** command. Usually, the static WEP key must be configured before the shared key authentication method can be configured. In any security mode other than the static WEP security mode, it is of no use to configure the link authentication mode.

**Configuration Examples** The following example sets the authentication mode of WLAN1 to shared key authentication.

```
Ruijie (config)#wlansec 1
Ruijie(wlansec)# security static-wep-key authentication share-key
```

**Related Commands**

| Command | Description |
| --- | --- |
| **security static-wep-key encryption** | Configures the static WEP key, and enables the static WEP security mode. |

**Platform Description** N/A

## 1.13 security static-wep-key encryption

Use this command to configure the static WEP key for a WLAN and configure the security mode of this WLAN to static WEP.

**security static-wep-key encryption** *key-length* { **ascii | hex** } *key-index key*

**Parameter Description**

| Parameter | Description |
| --- | --- |
| *key-length* | The key length is measured by bit, which can be 40, 104, and 128 bits. |
| *key-index* | The parameter indicates a key index number, ranging from 1 to 4. |
| *key* | The parameter indicates key data. In the ascii mode, 5-byte, 13-byte, and 16-byte data can serve as a key depending on the **key-length** parameter. In the hex mode, 10-byte, 26-byte, and 32-byte data can serve as a key depending on the **key-length** parameter. |

| | |
|---|---|
| **ascii** | The parameter indicates that the password takes the form of ASCII code. |
| **hex** | The parameter indicates that the password is hexadecimal. |

**Defaults** The static WEP mode is disabled by default.

**Command mode** WLAN security configuration mode

**Usage Guide** The prerequisite of configuring security mode for a WLAN is that this WLAN has been created. Attention should be paid to the following points:

1. This command can be used repeatedly for configuration, and the last configuration will take effect.
2. This command configures the static WEP key as well as the static-WEP security mode.

**Configuration Examples** The following example sets the static WEP key of WLAN 1 to 12345.

```
Ruijie (config)#wlansec 1
Ruijie(wlansec)# security static-wep-key encryption 40 ascii 1 12345
```

**Related Commands**

| Command | Description |
|---|---|
| **security static-wep-key authentication** { **open** \| **share-key** } | Configures the authentication method in the static WEP security mode to open system authentication or shared key authentication. |

**Platform Description** The client cannot support a 128-bit WEP password if you use the Windows XP operating system in the wireless client management software. If the client software does not support a 128-bit WEP password, as Ruijie devices are configured with 128-bit encryption, the consequence is either the client software cannot be associated with the wireless network or the data channel is unavailable, depending on the authentication mode.

## 1.14 security wpa

Use this command to configure WPA authentication for a WLAN.

**security wpa** { **enable** | **disable** }

**Parameter Description**

| Parameter | Description |
|---|---|
| **enable** | Enables WPA authentication. |
| **disable** | Disables WPA authentication. |

**Defaults** WPA authentication is disabled by default.

**Command** WLAN security configuration mode

**mode**

**Usage Guide** The command is used to enable the WPA authentication mode. Only after the WPA authentication mode is enabled can encryption and authentication methods be configured in the WPA mode. Otherwise, configuration is impossible. When you use the WPA authentication, you need to configure an encryption method and an authentication method. If only an encryption or authentication method is configured, or neither is configured, the wireless client cannot be associated with the wireless network.

**Configuration Examples** The following example sets the authentication mode of WLAN1 to WPA.

```
Ruijie (config)#wlansec 1
Ruijie(wlansec)# security wpa enable
```

**Related Commands**

| Command | Description |
| --- | --- |
| **security wpa akm** { **psk** \| **802.1x** } { **enable** \| **disable** } | Configures an authentication method in the WPA authentication mode. |
| **security wpa ciphers** { **aes** \| **tkip** } { **enable** \| **disable** } | Configures an encryption method in the WPA authentication mode. |
| **security wpa akm psk set-key ascci** | Configures the shared password in the WPA authentication mode. |

**Platform Description** N/A

## 1.15 security wpa akm

Use this command to configure an authentication method for a WLAN in the WPA authentication mode.

**security wpa akm** { **psk** | **802.1x** } { **enable** | **disable** }

**Parameter Description**

| Parameter | Description |
| --- | --- |
| **psk** | Configures the authentication method to pre-shared key identity verification. |
| **802.1x** | Configures the authentication method to IEEE802.1x authentication. |
| **enable** | Enables an authentication method in the WPA authentication mode. |
| **disable** | Disables an authentication method in the WPA authentication mode. |

**Defaults** N/A

**Command mode** WLAN security configuration mode

**Usage Guide** The command is used to enable an authentication method in the WPA authentication mode. Only after the WPA authentication mode is enabled can an authentication method be configured. There are two authentication methods: PSK and 802.1x. When you use the WPA authentication, you need to configure an encryption method and an authentication method. If only an encryption or authentication method is configured, or neither is configured, the wireless client cannot be associated with the wireless network.

**Configuration Examples** The following example sets the authentication method for WLAN1 in the WPA authentication mode to pre-shared key identity authentication.

```
Ruijie (config)#wlansec 1
Ruijie(wlansec)# security wpa akm psk enable
```

The following example sets the authentication method for WLAN1 in the WPA authentication mode to 802.1x authentication.

```
Ruijie (config)#wlansec 1
Ruijie(wlansec)# security wpa akm 802.1x enable
```

**Related Commands**

| Command | Description |
|---|---|
| **security wpa** { **enable** \| **disable** } | Configures the WLAN configuration mode. |
| **security wpa ciphers** { **aes** \| **tkip** } { **enable** \| **disable** } | Configures an encryption method in the WPA authentication mode. |

**Platform Description** N/A

## 1.16 security wpa akm psk set-key ascci

Use this command to configure a WPA shared password for a WLAN.
**security wpa akm psk set-key** { **ascii** *ascii-key* | **hex** *hex-key* }

**Parameter Description**

| Parameter | Description |
|---|---|
| **ascii** | Specifies the ASCII password. |
| *ascii-key* | The ASCII password, containing 8-63 characters. |
| **hex** | Specifies the hexadecimal password. |
| *hex-key* | The hexadecimal password, containing 64 characters. |

**Defaults** N/A

**Command mode** WLAN security configuration mode

**Usage Guide** This shared password is of use only when the PSK authentication mode is enabled.

**Configuration Examples** The following example sets the shared password for WLAN 1 WPA to 12345678.

```
Ruijie (config)#wlansec 1
Ruijie(wlansec)# security wpa enable
Ruijie(wlansec)# security wpa akm psk enable
Ruijie(wlansec)# security wpa akm psk set-key ascci 12345678
```

**Related Commands**

| Command | Description |
|---|---|
| **security wpa** { **enable** \| **disable** } | Configures the WLAN configuration mode. |
| **security wpa ciphers** { **aes** \| **tkip** } { **enable** \| **disable** } | Configures an encryption method in the WPA authentication mode. |
| **security wpa akm** { **psk** \| **802.1x** } { **enable** \| **disable** } | Configures an authentication method in the WPA authentication mode. |

**Platform Description** N/A

## 1.17 security wpa ciphers

Use this command to configure an encryption method for a WLAN in the WPA authentication mode.
**security wpa ciphers** { **aes** | **tkip** } { **enable** | **disable** }

**Parameter Description**

| Parameter | Description |
|---|---|
| **aes** | Configures the encryption method to AES. |
| **tkip** | Configures the encryption method to TKIP. |
| **enable** | Enables an encryption method in the WPA authentication mode. |
| **disable** | Disables an encryption method in the WPA authentication mode. |

**Defaults** N/A

**Command mode** WLAN security configuration mode

**Usage Guide** The command is used to enable an encryption method in the WPA authentication mode. Only after the WPA authentication mode is enabled can an encryption method be configured. There are two encryption methods: AES and TKIP. When you use the WPA authentication, you need to configure an encryption method and an authentication method. If only an encryption or authentication method is configured, or neither is configured, the wireless client cannot be associated with the wireless network.

**Configuration Examples** The following example sets the encryption method for WLAN1 in the WPA authentication mode to AES.

```
Ruijie (config)#wlansec 1
```

```
Ruijie(wlansec)# security wpa ciphers aes enable
```

The following example disables the AES encryption method for WLAN1 in the WPA authentication mode.

```
Ruijie (config)#wlansec 1
Ruijie(wlansec)# security wpa ciphers aes disable
```

The following example sets the encryption method for WLAN1 in the WPA authentication mode to TKIP.

```
Ruijie (config)#wlansec 1
Ruijie(wlansec)# security wpa ciphers tkip enable
```

The following example disables the TKIP encryption method for WLAN1 in the WPA authentication mode.

```
Ruijie (config)#wlansec 1
Ruijie(wlansec)# security wpa ciphers tkip disable
```

**Related Commands**

| Command | Description |
|---|---|
| **security wpa** { **enable** \| **disable** } | Configures the WLAN configuration mode. |
| **security wpa akm** { **psk** \| **802.1x** } { **enable** \| **disable** } | Configures an authentication method in the WPA authentication mode. |
| **security wpa akm psk set-key ascci** | Configures a shared password in the WPA authentication mode. |

**Platform Description** N/A

## 1.18 show wclient security

Use this command to display security configuration of STAs.

**show wclient security** *mac-address*

**Parameter Description**

| Parameter | Description |
|---|---|
| *mac-address* | The MAC address of the STA to be displayed. |

**Defaults** N/A

**Command mode** Privileged EXEC mode/Global configuration mode/WLAN security configuration mode

**Usage Guide** N/A

**Configuration Examples** The following example displays the security configuration of wireless client 1 with a MAC address of 3848.4c48.d953.

```
Ruijie# show wclient security 3848.4c48.d953
```

```
Security policy finished     :TRUE
Security policy type         :PSK
Security WPA version         :WPA2
Security Ucast cipher        :CCMP
Security EAP type           :NONE
```

| Field | Description |
|---|---|
| Security policy finished | Whether the authentication is complete. |
| Security policy type | Security policy type. |
| Security WPA version | WPA version. |
| Security Ucast cipher | Unicast cipher suite |
| Security EAP type | EAP Type |

**Related Commands**

| Command | Description |
|---|---|
| N/A | N/A |

**Platform Description** N/A

## 1.19 show wlan security

Use this command to display security configuration of a WLAN.

**show wlan security** *wlan-id*

**Parameter Description**

| Parameter | Description |
|---|---|
| *wlan-id* | The ID of the WLAN to be checked, in the range from 1 to 512. |

**Defaults** N/A

**Command mode** Privileged EXEC mode/Global configuration mode/WLAN security configuration mode

**Usage Guide** N/A

**Configuration Examples** The following example displays the security configuration of WLAN1.

```
Ruijie#show wlan security 1
WLAN SSID         : ruijie-psk
Security Policy    : PSK
WPA version        : RSN(WPA2)
AKM type          : preshare key
pairwise cipher type: AES
```

```
group cipher type   : AES
wpa_passphrase_len  : 8
wpa_passphrase     : 31 32 33 34 35 36 37 38
group key          : 39 de c7 57 5c 58 9a af 84 84 cf 18 3e ce ff 5c
```

| Field | Description |
|---|---|
| WLAN SSID | WLAN SSID |
| Security Policy | Security Policy. |
| WPA version | WPA version. |
| AKM type | AKM suite, indicating the authentication mode. |
| pairwise cipher type | Unicast cipher suite. |
| group cipher type | Multicast cipher suite. |
| wpa_passphrase_len | Password length. |
| wpa_passphrase | PSK password. |
| group key | Multicast key. |

**Related Commands**

| Command | Description |
|---|---|
| N/A | N/A |

**Platform Description** N/A

## 1.20 webauth prevent-jitter

Use this command to set the timeout for jitter prevention during Web authentication of a particular WLAN. Use the **no** or **default** form of this command to restore the default setting.

**webauth prevent-jitter** *timeout*

**no webauth prevent-jitter**

**default webauth prevent-jitter**

**Parameter Description**

| Parameter | Description |
|---|---|
| *timeout* | Sets the timeout for jitter prevention during Web authentication, in the range from 0 to 86400 in the unit of seconds. |

**Defaults** The default is 300 seconds.

**Command mode** WLAN security configuration mode

**Usage Guide** The jitter prevention time in Web authentication can be configured only after Web authentication is enabled.

**Configuration Examples** The following example sets the timeout for jitter prevention during Web authentication of WLAN 1 to 900 seconds.

```
Ruijie(config)#wlansec 1
Ruijie(config-wlansec)#webauth
Ruijie(config-wlansec)#webauth prevent-jitter 900
```

**Related Commands**

| Command | Description |
| --- | --- |
| N/A | N/A |

**Platform Description** N/A

## 1.21 wlansec

Use this command to configure security configuration mode for the specified WLAN. Use the **no** or **default** form of this command to restore the default setting.

**wlansec** *wlan-id*

**no wlansec** *wlan-id*

**default wlansec** *wlan-id*

**Parameter Description**

| Parameter | Description |
| --- | --- |
| *wlan-id* | Sets WLAN ID. |

**Defaults** No WLAN security configuration mode is configured by default.

**Command mode** Global configuration mode

**Usage Guide** Create a WLAN before entering its security configuration mode. You can use the **no wlansec** *wlan-id* command to clear the WLAN security configuration.

**Configuration Examples** The following example configures security configuration mode for WLAN 1.

```
Ruijie(config)#wlansec 1
```

**Related Commands**

| Command | Description |
| --- | --- |
| N/A | N/A |

**Platform Description** N/A

# 2 CPU Protection Commands

## 2.1 cpu-protect type pps

Use this command to set the bandwidth for receiving packets of a specified type for on the CPU port. Use the **no** form of this command to restore the default setting.

**cpu-protect type** { **arp** | **bpdu** | **capwap-disc** | **d1x** | **dhcp-option82** | **dhcp-relay-client** | **dhcp-relay-server** | **dhcps** | **igmp** | **ipmc** | **ipv6-nans** | **isis** | **lldp | ospf** | **ospfv3** | **pim** | **pppoe** | **rip** | **ripng** | **tcp80 | tcp443** | **vrrp** } **pps** *value*

**no cpu-protect type** { **arp** | **bpdu** | **capwap-disc** | **d1x** | **dhcp-option82** | **dhcp-relay-client** | **dhcp-relay-server** | **dhcps** | **igmp** | **ipmc** | **ipv6-nans** | **isis** | **lldp** | **ospf** | **ospfv3** | **pim** | **pppoe** | **rip** | **ripng** | **tcp80 | tcp443** | **vrrp** } **pps**

**Parameter Description**

| Parameter | Description |
|---|---|
| **arp** | ARP packets. |
| **bpdu** | IEEE BPDU packets. |
| **capwap-disc** | CAPWAP Discover packets. |
| **d1x** | 802.1x EAPOL packets. |
| **dhcp-option82** | DHCP option82 packets. |
| **dhcp-relay-client** | DHCP relay client packets. |
| **dhcp-relay-server** | DHCP relay server packets. |
| **dhcps** | DHCP Snooping packets. |
| **igmp** | IGMP packets. |
| **ipmc** | IPv4 multicast packets. |
| **ipv6-nans** | IPv6 neighbor discovery packets. |
| **isis** | ISIS packets. |
| **lldp** | LLDP packets. |
| **ospf** | OSPF packets. |
| **ospfv3** | OSPF version 3 packets. |
| **pim** | PIM packets. |
| **pppoe** | PPPOE packets. |
| **rip** | IPv4 RIP packets. |
| **ripng** | IPv6 RIP packets. |
| **tcp80** | Web authentication redirection packets. |
| **tcp443** | HTTPS packets. |
| **vrrp** | VRRP packets. |
| *value* | Number of received packets per second, in the range from 0 to 148810 in the unit of pps. |

**Defaults** The default value varies with the product model.

**Command Mode** Global configuration mode

**Usage Guide** N/A

**Configuration Examples** The following example sets the CPU's bandwidth for receiving ARP packets to 200pps.

```
Ruijie(config)# cpu-protect type arp pps 200
```

**Related Commands**

| Command | Description |
| --- | --- |
| **cpu-protect type packet-type pri** *pri_num* | Sets the priority of the packets of a specified type received by the CPU port. |

**Platform Description** N/A

## 2.2 show cpu-protect summary

Use this command to display bandwidth of packets of each type received on the CPU port.
show cpu-protect summary

**Parameter Description**

| Parameter | Description |
| --- | --- |
| N/A | N/A |

**Defaults** N/A

**Command Mode** Privileged EXEC mode

**Usage Guide** N/A

**Configuration Examples** The following example displays bandwidth of packets of each type received on the CPU port.

```
Ruijie# show cpu-protect summary
```

**Related Command**

| Command | Description |
| --- | --- |
| N/A | N/A |

**Platform Description** N/A

## 2.3 show cpu-protect type

Use this command to display statistics about the packets of a specified type.
**show cpu-protect type** { **arp** | **bpdu** | **capwap-disc** | **d1x** | **dhcp-option82** | **dhcp-relay-client** | **dhcp-relay-server** | **dhcps** | **igmp** | **ipmc** | **ipv6-nans** | **isis** | **lldp** | **ospf** | **ospfv3** | **pim** | **pppoe** | **rip** | **ripng** | **tcp80 | tcp443** | **vrrp** }

**Parameter**

| Parameter | Description |
| --- | --- |

**Description**

| | |
|---|---|
| **arp** | ARP packets. |
| **bpdu** | IEEE BPDU packets. |
| **capwap-disc** | CAPWAP Discover packets. |
| **d1x** | 802.1x EAPOL packets. |
| **dhcp-option82** | DHCP Option82 packets. |
| **dhcp-relay-client** | DHCP relay client packets. |
| **dhcp-relay-server** | DHCP relay server packets. |
| **dhcps** | DHCP Snooping packets. |
| **igmp** | IGMP packets. |
| **ipmc** | IPv4 multicast packets. |
| **ipv6-nans** | IPv6 neighbor discovery packets. |
| **isis** | ISIS packets. |
| **lldp** | LLDP packets. |
| **ospf** | OSPF packets. |
| **ospfv3** | OSPF version 3 packets. |
| **pim** | PIM packets. |
| **pppoe** | PPPOE packets. |
| **rip** | IPv4 RIP packets. |
| **ripng** | IPv6 RIP packets. |
| **tcp80** | Web authentication redirection packets. |
| **tcp443** | HTTPS packets. |
| **vrrp** | VRRP packets. |

**Defaults** N/A

**Command Mode** Privileged EXEC mode

**Usage Guide** N/A

**Configuration Examples**

The following example displays statistics about received BPDU packets.

```
Ruijie(config)# show cpu-protect type arp
Slot     Type        Pps      Total     Drop
--------- ------------ --------- --------- ---------
MainBoard bpdu         100        30        0
Slot-2    bpdu         100        30        0
```

**Related Command**

| Command | Description |
|---|---|
| **show cpu-protect type** *packet-type* | Displays statistics of packets of a specified type protected by the CPU. |

**Platform Description** N/A

# 3 NFPP Commands

## 3.1 arp-guard attack-threshold

Use this command to set the global attack threshold. When the packet rate exceeds the attack threshold, the attack occurs. Use the **no** or **default** form of this command to restore the default setting.

**arp-guard attack-threshold** { **per-src-ip** | **per-src-mac** | **per-port** } *pps*

**no arp-guard attack-threshold** { **per-src-ip** | **per-src-mac** | **per-port** }

**default arp-guard attack-threshold** { **per-src-ip** | **per-src-mac** | **per-port** }

**Parameter Description**

| Parameter | Description |
|---|---|
| **per-src-ip** | Sets the attack threshold for each source IP address. |
| **per-src-mac** | Sets the attack threshold for each source MAC address. |
| **per-port** | Sets the attack threshold for each port. |
| *pps* | Sets the attack threshold, in the range from 1 to 9999 in unit of pps. |

**Defaults** By default, the attack threshold for each source IP address and source MAC address is 16pps; and the attack threshold for each port is 200pps.

**Command Mode** NFPP configuration mode

**Usage Guide** The attack threshold shall be equal to or greater than the rate-limit threshold.

**Configuration Examples** The following example sets the global attack threshold.

```
Ruijie(config)# nfpp
Ruijie(config-nfpp)# arp-guard attack-threshold per-src-ip 2
Ruijie(config-nfpp)# arp-guard attack-threshold per-src-mac 3
Ruijie(config-nfpp)# arp-guard attack-threshold per-port 50
```

**Related Commands**

| Command | Description |
|---|---|
| **nfpp arp-guard policy** | Displays the rate-limit threshold and attack threshold. |
| **show nfpp arp-guard summary** | Displays the configuration. |
| **show nfpp arp-guard hosts** | Displays the monitored host. |
| **clear nfpp arp-guard hosts** | Clears the isolate host. |

**Platform Description** N/A

## 3.2 arp-guard enable

Use this command to enable anti-ARP guard function globally. Use the **no** form of this command to disable anti-ARP guard. Use the **default** form of this command to restore the default setting.

**arp-guard enable**

**no arp-guard enable**

**default arp-guard enable**

**Parameter Description**

| Parameter | Description |
|---|---|
| N/A | N/A |

**Defaults** This function is enabled by default.

**Command Mode** NFPP configuration mode

**Usage Guide** N/A

**Configuration Examples** The following example enables anti-ARP guard function globally.

```
Ruijie(config)# nfpp
Ruijie(config-nfpp)# arp-guard enable
```

**Related Commands**

| Command | Description |
|---|---|
| **nfpp arp-guard enable** | Enables ARP anti-attack on the interface. |
| **show nfpp arp-guard summary** | Displays the configuration. |

**Platform Description** N/A

## 3.3 arp-guard isolate-period

Use this command to set the arp-guard isolate time globally. Use the **no** or **default** form of this command to restore the default setting.

**arp-guard isolate-period** { *seconds* | **permanent** }

**no arp-guard isolate-period**

**default arp-guard isolate-period**

**Parameter Description**

| Parameter | Description |
|---|---|
| *seconds* | Sets the isolate time. The value is 0, or in the range from 30 to 86400 in the unit of seconds. |

| | |
|---|---|
| **permanent** | Permanent isolation. |

**Defaults** The default is 0 second, which means no isolation.

**Command Mode** NFPP configuration mode

**Usage Guide** N/A

**Configuration Examples** The following example sets the arp-guard isolate time globally to 180 seconds.

```
Ruijie(config)# nfpp
Ruijie(config-nfpp)# arp-guard isolate-period 180
```

**Related Commands**

| Command | Description |
|---|---|
| **nfpp arp-guard isolate-period** | Sets the isolate time on the interface. |
| **show nfpp arp-guard summary** | Displays the configuration. |

**Platform Description** N/A

## 3.4 arp-guard monitored-host-limit

Use this command to set the maximum number of monitored hosts. Use the **no** or **default** form of this command to restore the default setting.

**arp-guard monitored-host-limit** *number*

**no arp-guard monitored-host-limit**

**default arp-guard monitored-host-limit**

**Parameter Description**

| Parameter | Description |
|---|---|
| *number* | The maximum number of monitored hosts, in the range from 1 to 4294967295. |

**Defaults** The default is 1000.

**Command Mode** NFPP configuration mode

**Usage Guide** 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.

**Configuration Examples** The following example sets the maximum number of monitored hosts to 200.

```
Ruijie(config)# nfpp
Ruijie(config-nfpp)# arp-guard monitored-host-limit 200
```

**Related Commands**

| Command | Description |
| --- | --- |
| **show nfpp arp-guard summary** | Displays the configuration. |

**Platform Description** N/A

## 3.5 arp-guard monitor-period

Use this command to configure the arp guard monitor time. Use the **no** or **default** form of this command to restore the default setting.
**arp guard monitor-period** *seconds*
**no arp-guard monitor-period**
**default arp-guard monitor-period**

**Parameter Description**

| Parameter | Description |
| --- | --- |
| *seconds* | Sets the monitor time, in the range from 180 to 86400 in the unit of seconds. |

**Defaults** The default is 600 seconds.

**Command Mode** NFPP configuration mode

**Usage Guide** When the attacker is detected, if the isolate period is 0, the attacker will be monitored by the software and the timeout time will be the monitor period. During the software monitoring, if the isolate period is not 0, the software-monitored attacker will be auto-isolated by the hardware and the timeout time will be the isolate period. The monitor period is valid with the isolate period 0.
If the isolate period has changed to be 0, the attackers on the interface will be removed rather than being monitored by the software.

**Configuration Examples** The following example sets the arp-guard monitor time to 180 seconds.

```
Ruijie(config)# nfpp
Ruijie(config-nfpp)# arp-guard monitor-period 180
```

**Related**

| Command | Description |
| --- | --- |

**Commands**

| | |
|---|---|
| **show nfpp arp-guard summary** | Displays the configuration. |
| **show nfpp arp-guard hosts** | Displays the monitored host list. |
| **clear nfpp arp-guard hosts** | Clears the isolate host. |

**Platform Description** N/A

## 3.6 arp-guard rate-limit

Use this command to set the arp-guard rate limit. Use the **no** or **default** form of this command to restore the default setting.

**arp-guard rate-limit** { **per-src-ip** | **per-src-mac** | **per-port** } *pps*

**no arp-guard rate-limit** { **per-src-ip | per-src-mac | per-port** }

**default arp-guard rate-limit** { **per-src-ip | per-src-mac | per-port** }

**Parameter Description**

| Parameter | Description |
|---|---|
| **per-src-ip** | Sets the rate limit for each source IP address. |
| **per-src-mac** | Sets the rate limit for each source MAC address. |
| **per-port** | Sets the rate limit for each port. |
| *pps* | Sets the rate limit, in the range of 1 to 9999. |

**Defaults** The default rate limit for each source IP address and MAC address is 8pps; the default rate limit for each port is 100pps.

**Command Mode** NFPP configuration mode

**Usage Guide** N/A

**Configuration Examples** The following example sets the arp guard rate limit.

```
Ruijie(config)# nfpp
Ruijie(config-nfpp)# arp-guard rate-limit per-src-ip 2
Ruijie(config-nfpp)# arp-guard rate-limit per-src-mac 3
Ruijie(config-nfpp)# arp-guard rate-limit per-port 50
```

**Related Commands**

| Command | Description |
|---|---|
| **nfpp arp-guard policy** | Sets the rate limit and the attack threshold. |
| **show nfpp arp-guard summary** | Displays the configuration. |

**Platform** N/A

**Description**

## 3.7 arp-guard scan-threshold

Use this command to set the global scan threshold. Use the **no** or **default** form of this command to restore the default setting.

**arp-guard scan-threshold** *pkt-cnt*

**no arp-guard scan-threshold**

**default arp-guard scan-threshold**

**Parameter Description**

| Parameter | Description |
|---|---|
| *pkt-cnt* | Sets the scan threshold, in the range from 1 to 9999. |

**Defaults** The default scan threshold is 15, in 10 seconds.

**Command Mode** NFPP configuration mode

**Usage Guide** The scanning may occur on the condition that:
more than 15 packets are received within 10 seconds;
the source MAC address for the link layer is constant while the source IP address is uncertain;
The source MAC and IP address for the link layer is constant while the destination IP address is uncertain.

**Configuration Examples** The following example sets the global scan threshold to 20pps.

```
Ruijie(config)# nfpp
Ruijie(config-nfpp)# arp-guard scan-threshold 20
```

**Related Commands**

| Command | Description |
|---|---|
| **nfpp arp-guard scan-threshold** | Sets the scan threshold on the port. |
| **show nfpp arp-guard summary** | Displays the configuration. |
| **show nfpp arp-guard scan** | Displays the ARP guard scan table. |
| **clear nfpp arp-guard scan** | Clears the ARP guard scan table. |

**Platform Description** N/A

## 3.8 arp-guard trusted-host

Use this command to set the trusted host. Use the **no** or **default** form of this command to restore the default setting.

**arp-guard trusted-host** *ip mac*
**no arp-guard trusted-host** { **all** | *ip mac* }
**default arp-guard trusted-host**

**Parameter Description**

| Parameter | Description |
|---|---|
| *ip* | Sets the IP address. |
| *mac* | Sets the MAC address. |
| **all** | Deletes all trusted hosts. |

**Defaults** N/A

**Command Mode** NFPP configuration mode

**Usage Guide** After this function is enabled, the ARP packets are sent from the trusted host to CPU without rate limit or alarm notification.
Up to 500 hosts are supported.

**Configuration Examples** The following example sets the host whose IP address and MAC address are 1.1.1.1 and 0000.0000.1111 respectively as the trusted host.

```
Ruijie(config)# nfpp
Ruijie(config-nfpp)#arp-guard trusted-host 1.1.1.1 0000.0000.1111
```

**Related Commands**

| Command | Description |
|---|---|
| N/A | N/A |

**Platform Description** N/A

## 3.9 clear nfpp arp-guard hosts

Use this command to clear the monitored host isolation.
**clear nfpp arp-guard hosts** [ **vlan** *vid* ] [ **interface** *interface-id* ] [ *ip-address* | *mac-address* ]

**Parameter Description**

| Parameter | Description |
|---|---|
| *vid* | Sets the VLAN ID. |
| *interface-id* | Sets the interface name and number. |
| *ip-address* | Sets the IP address. |
| *mac-address* | Sets the MAC address. |

**Defaults** N/A

**Command Mode** Privileged EXEC mode

**Usage Guide**

**Configuration Examples** The following example clears the monitored host isolation.

```
Ruijie# clear nfpp arp-guard hosts vlan 1 interface g0/1
```

**Related Commands**

| Command | Description |
| --- | --- |
| **arp-guard attack-threshold** | Sets the global attack threshold. |
| **nfpp arp-guard policy** | Sets the limit threshold and attack threshold. |
| **show nfpp arp-guard hosts** | Displays the monitored host. |

**Platform Description** N/A

## 3.10 clear nfpp arp-guard scan

Use this command to clear ARP scanning table.

**clear nfpp arp-guard scan**

**Parameter Description**

| Parameter | Description |
| --- | --- |
| N/A | N/A |

**Defaults** N/A

**Command Mode** Privileged EXEC mode

**Usage Guide** N/A

**Configuration Examples** The following example clears ARP scanning table.

```
Ruijie# clear nfpp arp-guard scan
```

**Related Commands**

| Command | Description |
| --- | --- |
| **arp-guard attack-threshold** | Sets the global attack threshold. |
| **nfpp arp-guard policy** | Sets the attack threshold. |
| **show nfpp arp-guard scan** | Displays the ARP scanning table. |

**Platform Description** N/A

## 3.11 clear nfpp dhcp-guard hosts

Use this command to clear the monitored host isolation.

**clear nfpp dhcp-guard hosts** [ **vlan** *vid* ] [ interface *interface-id* ] [ *mac-address* ]

**Parameter Description**

| Parameter | Description |
|---|---|
| *vid* | Sets the VLAN ID. |
| *interface-id* | Sets the interface name and number. |
| *mac-address* | Sets the MAC address. |

**Defaults** N/A

**Command Mode** Privileged EXEC mode

**Usage Guide** Use this command without the parameter to clear all monitored hosts.

**Configuration Examples** The following example clears the monitored host isolation.

```
Ruijie# clear nfpp dhcp-guard hosts vlan 1 interface g0/1
```

**Related Commands**

| Command | Description |
|---|---|
| **dhcp-guard attack-threshold** | Sets the global attack threshold. |
| **nfpp dhcp-guard policy** | Sets the limit threshold and attack threshold. |
| **show nfpp dhcp-guard hosts** | Displays the monitored host. |

**Platform Description** N/A

## 3.12 clear nfpp dhcpv6-guard hosts

Use this command to clear the monitored host isolation.

**clear nfpp dhcpv6-guard hosts** [ **vlan** *vid* ] [ **interface** *interface-id* ] [ *mac-address* ]

**Parameter Description**

| Parameter | Description |
|---|---|
| *vid* | Sets the VLAN ID. |
| *interface-id* | Sets the interface name and number. |

| | |
|---|---|
| *mac-address* | Sets the MAC address. |

**Defaults** N/A

**Command Mode** Privileged EXEC mode

**Usage Guide** Use this command without the parameter to clear all monitored hosts

**Configuration Examples** The following example clears the monitored host isolation.

```
Ruijie# clear nfpp dhcpv6-guard hosts vlan 1 interface g0/1
```

**Related Commands**

| Command | Description |
|---|---|
| **dhcpv6-guard attack-threshold** | Sets the global attack threshold. |
| **nfpp dhcpv6-guard policy** | Sets the limit threshold and attack threshold. |
| **show nfpp dhcpv6-guard hosts** | Displays the monitored host. |

**Platform Description** N/A

## 3.13 clear nfpp icmp-guard hosts

Use this command to clear the monitored host isolation.

**clear nfpp icmp-guard hosts** [ **vlan** *vid* ] [ **interface** *interface-id* ] [ *ip-address* ]

**Parameter Description**

| Parameter | Description |
|---|---|
| *vid* | Sets the VLAN ID. |
| *interface-id* | Sets the interface name and number. |
| *ip-address* | Sets the IP address. |

**Defaults** N/A

**Command Mode** Privileged EXEC mode

**Usage Guide** Use this command without the parameter to clear all monitored hosts.

**Configuration Examples** The following example clears the monitored host isolation.

```
Ruijie# clear nfpp icmp-guard hosts vlan 1 interface g0/1
```

**Related**

| Command | Description |
|---|---|

**Commands**

| | |
|---|---|
| **icmp-guard attack-threshold** | Sets the global attack threshold. |
| **nfpp icmp-guard policy** | Sets the limit threshold and attack threshold. |
| **show nfpp icmp-guard hosts** | Displays the monitored host. |

**Platform Description** N/A

## 3.14 clear nfpp ip-guard hosts

Use this command to clear the monitored host isolation.

**clear nfpp ip-guard hosts** [ **vlan** *vid* ] [ **interface** *interface-id* ] [ *ip-address* ]

**Parameter Description**

| Parameter | Description |
|---|---|
| *vid* | Sets the VLAN ID. |
| *interface-id* | Sets the interface name and number. |
| *ip-address* | Sets the IP address. |

**Defaults** N/A

**Command Mode** Privileged EXEC mode

**Usage Guide** Use this command without the parameter to clear all monitored hosts.

**Configuration Examples** The following example clears the monitored host isolation.

```
Ruijie# clear nfpp ip-guard hosts vlan 1 interface g0/1
```

**Related Commands**

| Command | Description |
|---|---|
| **ip-guard attack-threshold** | Sets the global attack threshold. |
| **nfpp ip-guard policy** | Sets the limit threshold and attack threshold. |
| **show nfpp ip-guard hosts** | Displays the monitored host. |

**Platform Description** N/A

## 3.15 clear nfpp log

Use this command to clear the NFPP log buffer.

**clear nfpp log**

**Parameter Description**

| Parameter | Description |
| --- | --- |
| N/A | N/A |

**Defaults** N/A

**Command Mode** Privileged EXEC mode

**Usage Guide** N/A

**Configuration Examples** The following example clears the NFPP log buffer.

```
Ruijie# clear nfpp log
32 log-buffer entries were cleared.
```

**Related Commands**

| Command | Description |
| --- | --- |
| **show nfpp log** | Displays the NFPP log configuration or the log buffer. |

**Platform Description** N/A

## 3.16 cpu-protect sub-interface percent

Use this command to configure the percentage of packets of each type in the buffer. Use the **no** or **default** form of this command to restore the default setting.

**cpu-protect sub-interface** { **manage** | **protocol** | **route** } **percent** *percent_vaule*

**no cpu-protect sub-interface** {*manage*|*protocol*|*route*} **percent**

**default cpu-protect sub-interface** {*manage*|*protocol*|*route*} **percent**

**Parameter Description**

| Parameter | Description |
| --- | --- |
| **manage** | Specifies the management packets. |
| **protocol** | Specifies the protocol packets. |
| **route** | Specifies the route packets. |
| *percent_value* | The percent value, in the range from 1 to 100. |

**Defaults** The default percentage of packets of different types in the buffer are:

**manage** packets: 30;

**route** packets: 20;

**protocol** packets: 45.

**Command Mode** Global configuration mode

**Usage Guide** N/A

**Configuration Examples** The following example sets the percentage of management packets in the buffer to 60.

```
Ruijie(config)# cpu-protect sub-interface manage
percent 60
```

**Related Commands**

| Command | Description |
| --- | --- |
| **cpu-protect sub-interface** { **manage** \| **protocol** \| **route** } pps | Configures traffic bandwidth for packets of each type. |

**Platform Description** N/A

## 3.17 cpu-protect sub-interface pps

Use this command to configure traffic bandwidth for packets of each type. Use the **no** or **default** form of this command to restore the default setting.

**cpu-protect sub-interface** { **manage** | **protocol** | route} **pps** *pps_vaule*

**no cpu-protect sub-interface** { *manage* | *protocol* | *route* } **pps**

**default cpu-protect sub-interface** { *manage* | *protocol* | *route* } **pps**

**Parameter Description**

| Parameter | Description |
| --- | --- |
| **manage** | Specifies the management packets. |
| **protocol** | Specifies the protocol packets. |
| **route** | Specifies the route packets. |
| *pps_value* | The rate limit threshold, in the range from 1 to 100000. |

**Defaults** The default traffic bandwidths for packets of different types are:

**manage** packets: 3000pps;

**route** packets: 3000pps;

**protocol** packets: 3000pps.

**Command Mode** Global configuration mode

**Usage Guide** N/A

**Configuration Examples** The following example sets the traffic bandwidth for management packets to 2000 pps.

```
Ruijie(config)# cpu-protect sub-interface manage pps 2000
```

| Related Commands | Command | Description |
|---|---|---|
| | **cpu-protect sub-interface** { **manage** \| **protocol** \| **route** } **percent** | Configures the percent value of each type of packets occupied in the buffer. |

**Platform Description** N/A

## 3.18 dhcp-guard attack-threshold

Use this command to set the global attack threshold. When the packet rate exceeds the attack threshold, the attack occurs. Use the **no** or **default** form of this command to restore the default setting.

**dhcp-guard attack-threshold** { **per-src-mac** | **per-port** } *pps*

**no dhcp-guard attack-threshold** { **per-src-mac** | **per-port** }

**default dhcp-guard attack-threshold** { **per-src-mac** | **per-port** }

**Parameter Description**

| Parameter | Description |
|---|---|
| **per-src-mac** | Sets the attack threshold for each source MAC address. |
| **per-port** | Sets the attack threshold for each port. |
| *pps* | Sets the attack threshold in the range from 1 to 9999 in the unit of pps. |

**Defaults** 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 Guide** N/A

**Configuration Examples** The following example sets the global attack threshold.

```
Ruijie(config)# nfpp
Ruijie(config-nfpp)# dhcp-guard attack-threshold per-src-mac 15
Ruijie(config-nfpp)# dhcp-guard attack-threshold per-port 200
```

| Related Commands | Command | Description |
|---|---|---|
| | **nfpp dhcp-guard policy** | Displays the rate-limit threshold and attack threshold. |
| | **show nfpp dhcp-guard summary** | Displays the configuration. |

| | |
|---|---|
| **show nfpp dhcp-guard hosts** | Displays the monitored host list. |
| **clear nfpp dhcp-guard hosts** | Clears the monitored host. |

**Platform Description** N/A

## 3.19 dhcp-guard enable

Use this command to enable the DHCP anti-attack function. Use the **no** or **default** form of this command to restore the default setting.

**dhcp-guard enable**

**no dhcp-guard enable**

**default dhcp-guard enable**

**Parameter Description**

| Parameter | Description |
|---|---|
| N/A | N/A |

**Defaults** This function is disabled by default.

**Command Mode** NFPP configuration mode

**Usage Guide** N/A

**Configuration Examples** The following example enables the DHCP anti-attack function.

```
Ruijie(config)# nfpp
Ruijie(config-nfpp)# dhcp-guard enable
```

**Related Commands**

| Command | Description |
|---|---|
| N/A | N/A |

**Platform Description** N/A

## 3.20 dhcp-guard isolate-period

Use this command to set the isolate time globally. Use the **no** or **default** form of this command to restore the default setting.

**dhcp-guard isolate-period** { *seconds* | **permanent** }

**no dhcp-guard isolate-period**

**default dhcp-guard isolate-period**

**Parameter Description**

| Parameter | Description |
| --- | --- |
| *seconds* | Sets the isolate time. The value is 0 or in the range from 30 to 86400 in the unit of seconds. |
| **permanent** | Permanent isolation. |

**Defaults** The default is 0 second, which means no isolation.

**Command Mode** NFPP configuration mode

**Usage Guide** The isolate period can be configured globally or based on the interface. For one interface, if the isolate period is not set based on the interface, the global value shall be adopted; or the interface-based isolate period shall be adopted.

**Configuration Examples** The following example sets the isolate time globally to 180 seconds.

```
Ruijie(config)# nfpp
Ruijie(config-nfpp)# dhcp-guard isolate-period 180
```

**Related Commands**

| Command | Description |
| --- | --- |
| **nfpp dhcp-guard isolate-period** | Sets the isolate time on the interface. |
| **show nfpp dhcp-guard summary** | Displays the configuration. |

**Platform Description** N/A

## 3.21 dhcp-guard monitored-host-limit

Use this command to set the maximum number of monitored hosts. Use the **no** or **default** form of this command to restore the default setting.

**dhcp-guard monitored-host-limit** *number*

**no dhcp-guard monitored-host-limit**

**default dhcp-guard monitored-host-limit**

**Parameter Description**

| Parameter | Description |
| --- | --- |
| *number* | The maximum number of monitored hosts, in the range from 1 to 4294967295. |

**Defaults** The default is 1000.

**Command** NFPP configuration mode

**Mode**

**Usage Guide** If the number of monitored hosts 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 number of monitored hosts 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.

**Configuration Examples** The following example sets the maximum number of monitored hosts to 200.

```
Ruijie(config)# nfpp
Ruijie(config-nfpp)# dhcp-guard monitored-host-limit 200
```

**Related Commands**

| Command | Description |
| --- | --- |
| **show nfpp dhcp-guard summary** | Displays the configuration. |

**Platform Description** N/A

## 3.22 dhcp-guard monitor-period

Use this command to configure the monitor time. Use the **no** or **default** form of this command to restore the default setting.
**dhcp-guard monitor-period** *seconds*
**no dhcp-guard monitor-period**
**default dhcp-guard monitor-period**

**Parameter Description**

| Parameter | Description |
| --- | --- |
| *seconds* | Sets the monitor time, in the range from 180 to 86400 in the unit of seconds. |

**Defaults** The default is 600 seconds.

**Command Mode** NFPP configuration mode

**Usage Guide** When the attacker is detected, if the isolate period is 0, the attacker will be monitored by the software and the timeout time will be the monitor period. During the software monitoring, if the isolate period is not 0, the software-monitored attacker will be auto-isolated by the hardware and the timeout time will be the isolate period. The monitor period is valid with the isolate period 0.
If the isolate period has changed to be 0, the attackers on the interface will be removed rather than

being monitored by the software.

**Configuration Examples** The following example sets the monitor time to 180 seconds.

```
Ruijie(config)# nfpp
Ruijie(config-nfpp)# dhcp-guard monitor-period 180
```

**Related Commands**

| Command | Description |
|---|---|
| **show nfpp dhcp-guard summary** | Displays the configuration. |
| **show nfpp dhcp-guard hosts** | Displays the monitored host list. |
| **clear nfpp dhcp-guard hosts** | Clears the isolate host. |

**Platform Description** N/A

## 3.23 dhcp-guard rate-limit

Use this command to set the rate-limit threshold globally. Use the **no** or **default** form of this command to restore the default setting.

**dhcp-guard rate-limit** { **per-src-mac | per-port** } *pps*

**no dhcp-guard rate-limit** { **per-src-mac | per-port** }

**default dhcp-guard rate-limit** { **per-src-mac | per-port** }

**Parameter Description**

| Parameter | Description |
|---|---|
| **per-src-mac** | Sets the rate limit for each source MAC address. |
| **per-port** | Sets the rate limit for each port. |
| *pps* | Sets the rate limit, in the range of 1 to 9999. |

**Defaults** 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 Guide** N/A

**Configuration Examples** The following example sets the rate-limit threshold globally.

```
Ruijie(config)# nfpp
Ruijie(config-nfpp)# dhcp-guard rate-limit per-src-mac 8
Ruijie(config-nfpp)# dhcp-guard rate-limit per-port 100
```

**Related**

| Command | Description |
|---|---|

**Commands**

| | |
|---|---|
| **nfpp dhcp-guard policy** | Sets the rate limit and the attack threshold. |
| **show nfpp dhcp-guard summary** | Displays the configuration. |

**Platform Description** N/A

## 3.24 dhcp-guard trusted-host

Use this command to set the trusted host. Use the **no** or **default** form of this command to restore the default setting.

**dhcp-guard trusted-host** *mac*

**no dhcp-guard trusted-host** { **all** | *mac* }

**default dhcp-guard trusted-host**

**Parameter Description**

| Parameter | Description |
|---|---|
| *mac* | Sets the MAC address. |
| **all** | Deletes all trusted hosts. |

**Defaults** N/A

**Command Mode** NFPP configuration mode

**Usage Guide** After this function is enabled, the DHCP packets are sent from the trusted host to CPU without rate limit or alarm notification.

Up to 500 trusted hosts are supported.

**Configuration Examples** The following example sets the host whose MAC address is 0000.0000.1111 as the trusted host.

```
Ruijie(config)# nfpp
Ruijie(config-nfpp)#dhcp-guard trusted-host 0000.0000.1111
```

**Related Commands**

| Command | Description |
|---|---|
| N/A | N/A |

**Platform Description** N/A

## 3.25 dhcpv6-guard attack-threshold

Use this command to set the global attack threshold. When the packet rate exceeds the attack

threshold, the attack occurs. Use the **no** or **default** form of this command to restore the default setting.

**dhcpv6-guard attack-threshold** { **per-src-mac** | **per-port** } *pps*

**no dhcpv6-guard attack-threshold** {**per-src-mac** | **per-port**}

**default dhcpv6-guard attack-threshold** { **per-src-mac** | **per-port**}

**Parameter Description**

| Parameter | Description |
|---|---|
| **per-src-mac** | Sets the attack threshold for each source MAC address. |
| **per-port** | Sets the attack threshold for each port. |
| *pps* | Sets the attack threshold, in the range is from 1 to 9999 pps. |

**Defaults** 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 Guide** N/A

**Configuration Examples** The following example sets the global attack threshold.

```
Ruijie(config)# nfpp
Ruijie(config-nfpp)# dhcpv6-guard attack-threshold per-src-mac 15
Ruijie(config-nfpp)# dhcpv6-guard attack-threshold per-port 200
```

**Related Commands**

| Command | Description |
|---|---|
| **nfpp dhcpv6-guard policy** | Displays the rate-limit threshold and attack threshold. |
| **show nfpp dhcpv6-guard summary** | Displays the configuration. |
| **show nfpp dhcpv6-guard hosts** | Displays the monitored host list. |
| **clear nfpp dhcpv6-guard hosts** | Clears the monitored host. |

**Platform Description** N/A

## 3.26 dhcpv6-guard enable

Use this command to enable the DHCPv6 anti-attack function. Use the **no** or **default** form of this command to restore the default setting.

**dhcpv6-guard enable**

**no dhcpv6-guard enable**

**default dhcpv6-guard enable**

**Parameter Description**

| Parameter | Description |
| --- | --- |
| N/A | N/A |

**Defaults** This function is disabled by default.

**Command Mode** NFPP configuration mode

**Usage Guide** N/A

**Configuration Examples** The following example enables the DHCPv6 anti-attack function globally.

```
Ruijie(config)# nfpp
Ruijie(config-nfpp)# dhcpv6-guard enable
```

**Related Commands**

| Command | Description |
| --- | --- |
| N/A | N/A |

**Platform Description** N/A

## 3.27 dhcpv6-guard isolate-period

Use this command to set the isolate time globally. Use the **no** or **default** form of this command to restore the default setting.

**dhcpv6-guard isolate-period** { *seconds* | **permanent** }

**no dhcpv6-guard isolate-period**

**default dhcpv6-guard isolate-period**

**Parameter Description**

| Parameter | Description |
| --- | --- |
| *seconds* | Sets the isolate time. The value is 0 or in the range is from 30 to 86400 in the unit of seconds. |
| **permanent** | Permanent isolation. |

**Defaults** The default is 0 second, which means no isolation.

**Command Mode** NFPP configuration mode

**Usage Guide** The isolate period can be configured globally or based on the interface. For one interface, if the isolate period is not set based on the interface, the global value shall be adopted; or the

interface-based isolate period shall be adopted.

**Configuration Examples** The following example sets the isolate time globally to 180 seconds.

```
Ruijie(config)# nfpp
Ruijie(config-nfpp)# dhcpv6-guard isolate-period 180
```

**Related Commands**

| Command | Description |
|---|---|
| **nfpp dhcpv6-guard isolate-period** | Sets the isolate time on the interface. |
| **show nfpp dhcpv6-guard summary** | Displays the configuration. |

**Platform Description** N/A

## 3.28 dhcpv6-guard monitored-host-limit

Use this command to set the maximum monitored host number. Use the **no** or **default** form of this command to restore the default setting.
**dhcpv6-guard monitored-host-limit** *number*
**no dhcpv6-guard monitored-host-limit**
**default dhcpv6-guard monitored-host-limit**

**Parameter Description**

| Parameter | Description |
|---|---|
| *number* | The maximum monitored host number, in the range from 1 to 4294967295. |

**Defaults** The default is1000.

**Command Mode** NFPP configuration mode

**Usage Guide** 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.

**Configuration Examples** The following example sets the maximum monitored host number to200.

```
Ruijie(config)# nfpp
Ruijie(config-nfpp)# dhcpv6-guard monitored-host-limit 200
```

**Related Commands**

| Command | Description |
| --- | --- |
| **show nfpp dhcpv6-guard summary** | Displays the configuration. |

**Platform Description** N/A

## 3.29 dhcpv6-guard monitor-period

Use this command to configure the monitor time. Use the **no** or **default** form of this command to restore the default setting.

**dhcpv6-guard monitor-period** *seconds*

**no dhcpv6-guard monitor-period**

**default dhcpv6-guard monitor-period**

**Parameter Description**

| Parameter | Description |
| --- | --- |
| *seconds* | Sets the monitor time, in the range from 180 to 86400 in the unit of seconds. |

**Defaults** The default is 600 seconds.

**Command Mode** NFPP configuration mode

**Usage Guide** When the attacker is detected, if the isolate period is 0, the attacker will be monitored by the software and the timeout time will be the monitor period. During the software monitoring, if the isolate period is not 0, the software-monitored attacker will be auto-isolated by the hardware and the timeout time will be the isolate period. The monitor period is valid with the isolate period 0.

If the isolate period has changed to be 0, the attackers on the interface will be removed rather than being monitored by the software.

**Configuration Examples** The following example sets the monitor time to 180 seconds.

```
Ruijie(config)# nfpp
Ruijie(config-nfpp)# dhcpv6-guard monitor-period 180
```

**Related Commands**

| Command | Description |
| --- | --- |
| **show nfpp dhcpv6-guard summary** | Displays the configuration. |
| **show nfpp dhcpv6-guard hosts** | Displays the monitored host list. |
| **clear nfpp dhcpv6-guard hosts** | Clears the isolate host. |

**Platform Description** N/A

## 3.30 dhcpv6-guard rate-limit

Use this command to set the rate-limit threshold globally. Use the **no** or **default** form of this command to restore the default setting.

**dhcpv6-guard rate-limit** { **per-src-mac** | **per-port** } *pps*

**no dhcpv6-guard rate-limit** { **per-src-mac** | **per-port** }

**default dhcpv6-guard rate-limit** { **per-src-mac** | **per-port** }

**Parameter Description**

| Parameter | Description |
|---|---|
| **per-src-mac** | Sets the rate limit for each source MAC address. |
| **per-port** | Sets the rate limit for each port. |
| *pps* | Sets the rate limit, in the range from 1 to 9999. |

**Defaults** 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 Guide** N/A

**Configuration Examples** The following example sets the rate-limit threshold globally.

```
Ruijie(config)# nfpp
Ruijie(config-nfpp)# dhcpv6-guard rate-limit per-src-mac 8
Ruijie(config-nfpp)# dhcpv6-guard rate-limit per-port 100
```

**Related Commands**

| Command | Description |
|---|---|
| **nfpp dhcpv6-guard policy** | Sets the rate limit and the attack threshold. |
| **show nfpp dhcpv6-guard summary** | Displays the configuration. |

**Platform Description** N/A

## 3.31 dhcpv6-guard trusted-host

Use this command to set the trusted host. Use the **no** or **default** form of this command to restore the default setting.

**dhcpv6-guard trusted-host** *mac*

**no dhcpv6-guard trusted-host** { **all** | *mac* }

**default dhcpv6-guard trusted-host**

**Parameter Description**

| Parameter | Description |
| --- | --- |
| *mac* | Sets the MAC address. |
| **all** | Deletes all trusted hosts. |

**Defaults** N/A

**Command Mode** NFPP configuration mode

**Usage Guide** After this function is enabled, the DHCPv6 packets are sent from the trusted host to CPU without rate limit or alarm notification.
Up to 500 trusted hosts are supported.

**Configuration Examples** The following example sets the host whose MAC address is 0000.0000.1111 as the trusted host.

```
Ruijie(config)# nfpp
Ruijie(config-nfpp)#dhcpv6-guard trusted-host 0000.0000.1111
```

**Related Commands**

| Command | Description |
| --- | --- |
| N/A | N/A |

**Platform Description** N/A

## 3.32 icmp-guard attack-threshold

Use this command to set the global attack threshold. When the packet rate exceeds the attack threshold, the attack occurs. Use the **no** or **default** form of this command to restore the default setting.
**icmp-guard attack-threshold** { **per-src-ip** | **per-port** } *pps*
**no icmp-guard attack-threshold** { **per-src-ip** | **per-port** }
**default icmp-guard attack-threshold** { **per-src-ip** | **per-port** }

**Parameter Description**

| Parameter | Description |
| --- | --- |
| **per-src-ip** | Sets the attack threshold for each source IP address. |
| **per-port** | Sets the attack threshold for each port. |
| *pps* | Sets the attack threshold, in the range from 1 to 9999 in the unit of pps. |

**Defaults** 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 Guide** N/A

**Configuration Examples** The following example sets the global attack threshold.

```
Ruijie(config)# nfpp
Ruijie(config-nfpp)# icmp-guard attack-threshold per-src-ip 600
Ruijie(config-nfpp)# icmp-guard attack-threshold per-port 1200
```

**Related Commands**

| Command | Description |
| --- | --- |
| **nfpp icmp-guard policy** | Displays the rate-limit threshold and attack threshold. |
| **show nfpp icmp-guard summary** | Displays the configuration. |
| **show nfpp icmp-guard hosts** | Displays the monitored host list. |
| **clear nfpp icmp-guard hosts** | Clears the monitored host. |

**Platform Description** N/A

## 3.33 icmp-guard enable

Use this command to enable the ICMP anti-attack function. Use the **no** or **default** form of this command to restore the default setting.

**icmp-guard enable**

**no icmp-guard enable**

**default icmp-guard enable**

**Parameter Description**

| Parameter | Description |
| --- | --- |
| N/A | N/A |

**Defaults** This function is enabled by default.

**Command Mode** NFPP configuration mode

**Usage Guide** N/A

**Configuration Examples** The following example enables the ICMP anti-attack function globally.

```
Ruijie(config)# nfpp
Ruijie(config-nfpp)# icmp-guard enable
```

**Related Commands**

| Command | Description |
| --- | --- |
| **nffp icmp-guard enable** | Enables the ICMP anti-attack function on the interface. |
| **show nfpp icmp-guard summary** | Displays the configuration. |

**Platform Description** N/A

## 3.34 icmp-guard isolate-period

Use this command to set the isolate time globally. Use the **no** or **default** form of this command to restore the default setting.

**icmp-guard isolate-period** { *seconds* | **permanent** }

**no icmp-guard isolate-period**

**default icmp-guard isolate-period**

**Parameter Description**

| Parameter | Description |
| --- | --- |
| *seconds* | Sets the isolate time. The value is in the range is 0 or from 30 to 86400 in the unit of seconds. |
| **permanent** | Permanent isolation. |

**Defaults** The default is 0 second, which means no isolation.

**Command Mode** NFPP configuration mode

**Usage Guide** The isolate period can be configured globally or based on the interface. For one interface, if the isolate period is not set based on the interface, the global value shall be adopted; or the interface-based isolate period shall be adopted.

**Configuration Examples** The following example sets the isolate time globally to 180 seconds.

```
Ruijie(config)# nfpp
Ruijie(config-nfpp)# icmp-guard isolate-period 180
```

**Related Commands**

| Command | Description |
| --- | --- |
| **nfpp icmp-guard isolate-period** | Sets the isolate time on the interface. |
| **show nfpp icmp-guard summary** | Displays the configuration. |

**Platform** N/A

**Description**

## 3.35 icmp-guard monitored-host-limit

Use this command to set the maximum monitored host number. Use the **no** or **default** form of this command to restore the default setting.
**icmp-guard monitored-host-limit** *number*
**no icmp-guard monitored-host-limit**
**default icmp-guard monitored-host-limit**

**Parameter Description**

| Parameter | Description |
|---|---|
| *number* | The maximum monitored host number, in the range from 1 to 4294967295. |

**Defaults** The default is 1000.

**Command Mode** NFPP configuration mode

**Usage Guide** 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.

**Configuration Examples** The following example sets the maximum monitored host number to 200.

```
Ruijie(config)# nfpp
Ruijie(config-nfpp)# icmp-guard monitored-host-limit 200
```

**Related Commands**

| Command | Description |
|---|---|
| **show nfpp icmp-guard summary** | Displays the configuration. |

**Platform Description** N/A

## 3.36 icmp-guard monitor-period

Use this command to configure the monitor time. Use the **no** or **default** form of this command to restore the default setting.

**icmp-guard monitor-period** *seconds*
**no icmp-guard monitor-period**
**default icmp-guard monitor-period**

**Parameter Description**

| Parameter | Description |
|---|---|
| *seconds* | Sets the monitor time, in the range from180 to 86400 seconds. |

**Defaults** The default is 600 seconds.

**Command Mode** NFPP configuration mode

**Usage Guide** When the attacker is detected, if the isolate period is 0, the attacker will be monitored by the software and the timeout time will be the monitor period. During the software monitoring, if the isolate period is not 0, the software-monitored attacker will be auto-isolated by the hardware and the timeout time will be the isolate period. The monitor period is valid with the isolate period 0.
If the isolate period has changed to be 0, the attackers on the interface will be removed rather than being monitored by the software.

**Configuration Examples** The following example sets the monitor time to 180 seconds.

```
Ruijie(config)# nfpp
Ruijie(config-nfpp)# icmp-guard monitor-period 180
```

**Related Commands**

| Command | Description |
|---|---|
| **show nfpp icmp-guard summary** | Displays the configuration. |
| **show nfpp icmp-guard hosts** | Displays the monitored host list. |
| **clear nfpp icmp-guard hosts** | Clears the isolate host. |

**Platform Description** N/A

## 3.37 icmp-guard rate-limit

Use this command to set the rate-limit threshold globally. Use the **no** or **default** form of this command to restore the default setting.
**icmp-guard rate-limit** { **per-src-ip** | **per-port** } *pps*
**no icmp-guard rate-limit** { **per-src-ip | per-port** }
**default icmp-guard rate-limit** { **per-src-ip | per-port** }

**Parameter Description**

| Parameter | Description |
|---|---|
| **per-src-ip** | Sets the rate limit for each source IP address. |

| | |
|---|---|
| **per-port** | Sets the rate limit for each port. |
| *pps* | Sets the rate limit, in the range from1 to9999. |

**Defaults** N/A

**Command Mode** NFPP configuration mode

**Usage Guide** N/A

**Configuration Examples** The following example sets the rate-limit threshold globally.

```
Ruijie(config)# nfpp
Ruijie(config-nfpp)# icmp-guard rate-limit per-src-ip 500
Ruijie(config-nfpp)# icmp-guard rate-limit per-port 800
```

**Related Commands**

| Command | Description |
|---|---|
| **nfpp icmp-guard policy** | Sets the rate limit and the attack threshold. |
| **show nfpp icmp-guard summary** | Displays the configuration. |

**Platform Description** N/A

## 3.38 icmp-guard trusted-host

Use this command to set the trusted hosts free form monitoring. Use the **no** or **default** form of this command to restore the default setting.

**icmp-guard trusted-host** *ip mask*

**no icmp-guard trusted-host** { **all** | *ip mask* }

**default icmp-guard trusted-host**

**Parameter Description**

| Parameter | Description |
|---|---|
| *ip* | Sets the IP address. |
| *mask* | Sets the IP mask. |
| **all** | Deletes the configuration of all trusted hosts. |

**Defaults** No trusted host is configured by default.

**Command Mode** NFPP configuration mode

**Usage Guide** The administrator can use this command to set the trusted host free from monitoring. The ICMP

packets are allowed to send to the trusted host CPU without any rate-limit and warning configuration.
Configure the mask to set all hosts in one network segment free from monitoring.
UP to 500 trusted hosts are supported.

**Configuration Examples** The following example sets the trusted hosts free form monitoring.

```
Ruijie(config)# nfpp
Ruijie(config-nfpp)# icmp-guard trusted-host 1.1.1.0 255.255.255.0
```

**Related Commands**

| Command | Description |
| --- | --- |
| **show nfpp icmp-guard trusted-host** | Displays the configuration. |

**Platform Description** N/A

## 3.39 ip-guard attack-threshold

Use this command to set the global attack threshold. When the packet rate exceeds the attack threshold, the attack occurs. Use the **no** or **default** form of this command to restore the default setting.
**ip-guard attack-threshold** { **per-src-ip** | **per-port** } *pps*
**no ip-guard attack-threshold** { **per-src-ip** | **per-port** }
**default ip-guard attack-threshold** { **per-src-ip** | **per-port** }

**Parameter Description**

| Parameter | Description |
| --- | --- |
| **per-src-ip** | Sets the attack threshold for each source IP address. |
| **per-port** | Sets the attack threshold for each port. |
| *pps* | Sets the attack threshold, in pps. The valid range is 1 to 9999. |

**Defaults** By default, the attack threshold for each source IP address and each port are 20pps and 2000pps respectively.

**Command Mode** NFPP configuration mode

**Usage Guide** The attack threshold shall be equal to or larger than the rate-limit threshold.

**Configuration Examples** The following example sets the global attack threshold.

```
Ruijie(config)# nfpp
Ruijie(config-nfpp)# ip-guard attack-threshold per-src-ip 2
Ruijie(config-nfpp)# ip-guard attack-threshold per-port 50
```

**Related**

| Command | Description |
| --- | --- |

**Commands**

| | |
|---|---|
| **nfpp ip-guard policy** | Displays the rate-limit threshold and attack threshold. |
| **show nfpp ip-guard summary** | Displays the configuration. |
| **show nfpp ip-guard hosts** | Displays the monitored host list. |
| **clear nfpp ip-guard hosts** | Clears the monitored host. |

**Platform Description** N/A

## 3.40 ip-guard enable

Use this command to enable the IP anti-scan function. Use the **no** or **default** form of this command to restore the default setting.

**ip-guard enable**

**no ip-guard enable**

**default ip-guard enable**

**Parameter Description**

| Parameter | Description |
|---|---|
| N/A | N/A |

**Defaults** This function is enabled by default.

**Command Mode** NFPP configuration mode

**Usage Guide** N/A

**Configuration Examples** The following example enables the IP anti-scan function globally.

```
Ruijie(config)# nfpp
Ruijie(config-nfpp)# ip-guard enable
```

**Related Commands**

| Command | Description |
|---|---|
| **nffp ip-guard enable** | Enables the IP anti-scan function on the interface. |

**Platform Description** N/A

## 3.41 ip-guard isolate-period

Use this command to set the isolate time globally. Use the **no** or **default** form of this command to restore the default setting.

**ip-guard isolate-period** { *seconds* | **permanent** }

**no ip-guard isolate-period**

**default ip-guard isolate-period**

**Parameter Description**

| Parameter | Description |
|---|---|
| *seconds* | Sets the isolate time. The value is 0 or in the range from 30 to 86400 in the unit of seconds. |
| **permanent** | Permanent isolation. |

**Defaults** The default is 0 second, which means no isolation.

**Command Mode** NFPP configuration mode

**Usage Guide** N/A

**Configuration Examples** The following example sets the isolate time globally to 180 seconds.

```
Ruijie(config)# nfpp
Ruijie(config-nfpp)# ip-guard isolate-period 180
```

**Related Commands**

| Command | Description |
|---|---|
| **nfpp ip-guard isolate-period** | Sets the isolate time on the interface. |
| **show nfpp ip-guard summary** | Displays the configuration. |

**Platform Description** N/A

## 3.42 ip-guard monitored-host-limit

Use this command to set the maximum number of monitored hosts. Use the **no** or **default** form of this command to restore the default setting.

**ip-guard monitored-host-limit** *number*

**no ip-guard monitored-host-limit**

**default ip-guard monitored-host-limit**

**Parameter Description**

| Parameter | Description |
|---|---|

| | |
|---|---|
| *number* | The maximum monitored host number, in the range from 1 to 4294967295. |

**Defaults** The default is 1000.

**Command Mode** NFPP configuration mode

**Usage Guide** If the number of monitored hosts 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 number of monitored hosts 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.

**Configuration Examples** The following example sets the maximum number of monitored hosts to 200.

```
Ruijie(config)# nfpp
Ruijie(config-nfpp)# ip-guard monitored-host-limit 200
```

**Related Commands**

| Command | Description |
|---|---|
| **show nfpp ip-guard summary** | Displays the configuration. |

**Platform Description** N/A

## 3.43 ip-guard monitor-period

Use this command to configure the monitor time. Use the **no** or **default** form of this command to restore the default setting.
**ip-guard monitor-period** *seconds*
**no ip-guard monitor-period**
**default ip-guard monitor-period**

**Parameter Description**

| Parameter | Description |
|---|---|
| *seconds* | Sets the monitor time, in the range from 180 to 86400 in the unit of seconds. |

**Defaults** The default is 600 seconds.

**Command Mode** NFPP configuration mode

**Usage Guide** When the attacker is detected, if the isolate period is 0, the attacker will be monitored by the software and the timeout time will be the monitor period. During the software monitoring, if the isolate period is not 0, the software-monitored attacker will be auto-isolated by the hardware and the timeout time will be the isolate period. The monitor period is valid with the isolate period 0.
If the isolate period has changed to be 0, the attackers on the interface will be removed rather than being monitored by the software

**Configuration Examples** The following example sets the monitor time to 180 seconds.

```
Ruijie(config)# nfpp
Ruijie(config-nfpp)# ip-guard monitor-period 180
```

**Related Commands**

| Command | Description |
|---|---|
| **show nfpp ip-guard summary** | Displays the configuration. |
| **show nfpp ip-guard hosts** | Displays the monitored host list. |
| **clear nfpp ip-guard hosts** | Clears the isolate host. |

**Platform Description** N/A

## 3.44 ip-guard rate-limit

Use this command to set the rate-limit threshold globally. Use the **no** or **default** form of this command to restore the default setting.
**ip-guard rate-limit** { **per-src-ip** | **per-port** } *pps*
**no ip-guard rate-limit** { **per-src-ip** | **per-port** }
**default ip-guard rate-limit** {**per-src-ip** | **per-port** }

**Parameter Description**

| Parameter | Description |
|---|---|
| **per-src-ip** | Sets the rate limit for each source IP address. |
| **per-port** | Sets the rate limit for each port. |
| *pps* | Sets the rate limit, in the range of 1 to 9999. |

**Defaults** By default, the rate-limit threshold for each source IP address and each port is 20pps and 100pps respectively.

**Command Mode** NFPP configuration mode

**Usage Guide** N/A

**Configuration** The following example sets the rate-limit threshold globally.

**Examples**

```
Ruijie(config)# nfpp
Ruijie(config-nfpp)# ip-guard rate-limit per-src-ip 2
Ruijie(config-nfpp)# ip-guard rate-limit per-port 50
```

**Related Commands**

| Command | Description |
| --- | --- |
| **nfpp ip-guard policy** | Sets the rate limit and the attack threshold. |
| **show nfpp ip-guard summary** | Displays the configuration. |

**Platform Description** N/A

## 3.45 ip-guard scan-threshold

Use this command to set the global scan threshold. Use the **no** or **default** form of this command to restore the default setting.

**ip-guard scan-threshold** *pkt-cnt*

**no ip-guard scan-threshold**

**default ip-guard scan-threshold**

**Parameter Description**

| Parameter | Description |
| --- | --- |
| *pkt-cnt* | Sets the scan threshold, in the range from 1 to 9999. |

**Defaults** The default is 100, in 10 seconds.

**Command Mode** NFPP configuration mode

**Usage Guide** N/A

**Configuration Examples** The following example sets the global scan threshold to 20pps.

```
Ruijie(config)# nfpp
Ruijie(config-nfpp)# ip-guard scan-threshold 20
```

**Related Commands**

| Command | Description |
| --- | --- |
| **nfpp ip-guard scan-threshold** | Sets the scan threshold on the port. |
| **show nfpp ip-guard summary** | Displays the configuration. |

**Platform Description** N/A

## 3.46 ip-guard trusted-host

Use this command to set the trusted host free form monitoring. Use the **no** or **default** form of this command to restore the default setting.

**ip-guard trusted-host** *ip mask*

**no ip-guard trusted-host** { **all** | *ip mask* }

**default ip-guard trusted-host**

**Parameter Description**

| Parameter | Description |
|---|---|
| *ip* | Sets the IP address. |
| *mask* | Sets the IP mask. |
| **all** | Deletes the configuration of all trusted hosts. |

**Defaults** N/A

**Command Mode** NFPP configuration mode

**Usage Guide** The administrator can use this command to set the trusted host free from monitoring. The ICMP packets are allowed to sent to the trusted host CPU without any rate-limit and warning. Configure the mask to set all hosts in one network segment free from monitoring.

Up to 500 trusted hosts are supported.

**Configuration Examples** The following example sets the trusted host free form monitoring.

```
Ruijie(config)# nfpp
Ruijie(config-nfpp)# ip-guard trusted-host 1.1.1.0 255.255.255.0
```

**Related Commands**

| Command | Description |
|---|---|
| **show nfpp ip-guard trusted-host** | Displays the configuration. |

**Platform Description** N/A

## 3.47 log-buffer entries

Use this command to set the size of the NFPP log buffer. Use the **no** or **default** form of this command to restore the default setting.

**log-buffer entries** *number*

**no log-buffer entries**

**default log-buffer entries**

**Parameter Description**

| Parameter | Description |
| --- | --- |
| *number* | The buffer size, in the range from 0 to 1024. |

**Defaults** The default is 256.

**Command Mode** NFPP configuration mode

**Usage Guide** N/A

**Configuration Examples** The following example sets the size of the NFPP log buffer.

```
Ruijie(config)# nfpp
Ruijie(config-nfpp)# log-buffer entries 50
```

**Related Commands**

| Command | Description |
| --- | --- |
| **log-buffer logs** *number_of_message* **interval** *length_in_seconds* | Displays the rate of the syslog generated from the NFPP buffer. |
| **show nfpp log** | Displays the NFPP log configuration or the log buffer. |

**Platform Description** N/A

## 3.48 log-buffer logs

Use this command to set the rate of syslog generation from the NFPP log buffer. Use the **no** or **default** form of this command to restore the default setting.

**log-buffer logs** *number_of_message* **interval** *length_in_seconds*

**no log-buffer logs**

**default log-buffer logs**

**Parameter Description**

| Parameter | Description |
| --- | --- |
| *number_of_message* | The valid range is from 0 to1024.<br>0 indicates that all logs are recorded in the specific buffer and no syslogs are generated. |
| *length_in_seconds* | The valid range is from 0 to 86400(one day).<br>0 indicates not to write the log to the buffer but generate the syslog immediately.<br>With both the *number_of_message* and *length_in_seconds* values are 0, it indicates not to write the log to the buffer but generate the syslog immediately. |

| | |
|---|---|
| | The parameter *number_of_message /length_in_second* indicates the rate of syslog generated from the NFPP log buffer. |

**Defaults** By default, *number_of_message* is 1 and *length_in_seconds* is 30 seconds.

**Command Mode** NFPP configuration mode

**Usage Guide** N/A

**Configuration Examples** The following example sets the rate of syslog generation from the NFPP log buffer.

```
Ruijie(config)# nfpp
Ruijie(config-nfpp)# log-buffer logs 2 interval 12
```

**Related Commands**

| Command | Description |
|---|---|
| **log-buffer entries** *number* | Sets the NFPP log buffer size. |
| **show nfpp log summary** | Displays the NFPP log configuration or the log buffer. |

**Platform Description** N/A

## 3.49 logging

Use this command to set the VLAN or the interface log for NFPP. Use the **no** or **default** form of this command to restore the default setting.

**logging vlan** *vlan-range*

**logging interface** *interface-id*

**no logging vlan** *vlan-range*

**no logging interface** *interface-id*

**default logging**

**Parameter Description**

| Parameter | Description |
|---|---|
| *vlan-range* | Sets the specified VLAN range, in the format such as “1-3, 5”. |
| *interface-id* | Sets the interface ID. |

**Defaults** All logs are recorded by default.

**Command Mode** NFPP configuration mode

**Usage Guide** Use this command to filter the logs and records the logs within the specified VLAN range or the

specified port

**Configuration Examples** The following example records the logs in VLAN 1,VLAN 2,VLAN 3 and VLAN 5 only.

```
Ruijie(config)# nfpp
Ruijie(config-nfpp)# logging vlan 1-3,5
```

The following example records the logs on the interface GigabitEthernet 0/1 only.

```
Ruijie(config)# nfpp
Ruijie(config-nfpp)# logging interface G 0/1
```

**Related Commands**

| Command | Description |
| --- | --- |
| **show nfpp log summary** | Displays the NFPP log configuration or the log buffer. |

**Platform Description** N/A

## 3.50 nd-guard attack-threshold

Use this command to set the global attack threshold. When the packet rate exceeds the attack threshold, the attack occurs. Use the **no** or **default** form of this command to restore the default setting.

**nd-guard attack-threshold per-port** { **ns-na** | **rs** | **ra-redirect** } *pps*

**no nd-guard attack-threshold per-port** { **ns-na** | **rs** | **ra-redirect** }

**default nd-guard attack-threshold per-port** { **ns-na** | **rs** | **ra-redirect** }

**Parameter Description**

| Parameter | Description |
| --- | --- |
| **ns-na** | Sets the neighbor request and neighbor advertisement. |
| **rs** | Sets the router request. |
| **ra-redirect** | Sets the router advertisement and the redirect packets. |
| *pps* | Sets the attack threshold, in the range from1 to 9999 in the unit of seconds. |

**Defaults** By default, the default attack threshold for the **ns-na**, **rs** and **ra-redirect** on each port is 30 seconds.

**Command Mode** NFPP configuration mode

**Usage Guide** The attack threshold shall be equal to or larger than the rate-limit threshold.

**Configuration Examples** The following example sets the global attack threshold.

```
Ruijie(config)# nfpp
```

```
Ruijie(config-nfpp)# nd-guard attack-threshold per-port ns-na 20
Ruijie(config-nfpp)# nd-guard attack-threshold per-port rs 10
Ruijie(config-nfpp)# nd-guard attack-threshold per-port ra-redirect 10
```

**Related Commands**

| Command | Description |
| --- | --- |
| **nfpp ip-guard policy** | Displays the rate-limit threshold and attack threshold. |
| **show nfpp ip-guard summary** | Displays the configuration. |

**Platform Description** N/A

## 3.51 nd-guard enable

Use this command to enable ND anti-attack function. Use the **no** form of this command to disable ND anti-attack function. Use the **default** form of this command to restore the default setting.

**nd-guard enable**

**no nd-guard enable**

**default nd-guard enable**

**Parameter Description**

| Parameter | Description |
| --- | --- |
| N/A | N/A |

**Defaults** This function is enabled by default.

**Command Mode** NFPP configuration mode

**Usage Guide** N/A

**Configuration Examples** The following example enables ND anti-attack function.

```
Ruijie(config)# nfpp
Ruijie(config-nfpp)# nd-guard enable
```

**Related Commands**

| Command | Description |
| --- | --- |
| **nffp nd-guard enable** | Enables ND anti-attack function on the interface. |
| **show nfpp nd-guard summary** | Displays the configuration. |

**Platform Description** N/A

## 3.52 nd-guard rate-limit

Use this command to set the rate-limit threshold globally. Use the **no** or **default** form of this command to restore the default setting.

**nd-guard rate-limit per-port** { **ns-na** | **rs** | **ra-redirect** } *pps*

**no nd-guard rate-limit per-port** { **ns-na** | **rs** | **ra-redirect** }

**default nd-guard rate-limit per-port** { **ns-na** | **rs** | **ra-redirect** }

**Parameter Description**

| Parameter | Description |
|---|---|
| **ns-na** | Sets the neighbor request and neighbor advertisement. |
| **rs** | Sets the router request. |
| **ra-redirect** | Sets the router advertisement and the redirect packets. |
| *pps* | Sets the attack threshold, in the range is from 1 to 9999 in the unit of pps. |

**Defaults** By default, the default rate-limit threshold for the **ns-na**, **rs** and **ra-redirect** on each port is 15 pps.

**Command Mode** NFPP configuration mode

**Usage Guide** N/A

**Configuration Examples** The following example sets the rate-limit threshold globally.

```
Ruijie(config)# nfpp
Ruijie(config-nfpp)# nd-guard rate-limit per-port ns-na 10
Ruijie(config-nfpp)# nd-guard rate-limit per-port rs 5
Ruijie(config-nfpp)# nd-guard rate-limit per-port ra-redirect 5
```

**Related Commands**

| Command | Description |
|---|---|
| **nfpp nd-guard policy** | Sets the rate limit and the attack threshold. |
| **show nfpp nd-guard summary** | Displays the configuration. |

**Platform Description** N/A

## 3.53 nd-guard trusted-host

Use this command to set the trusted host. Use the **no** or **default** form of this command to restore the default setting.

**nd-guard trusted-host** *mac*

**no nd-guard trusted-host** { **all** | *mac* }

**default nd-guard trusted-host**

**Parameter Description**

| Parameter | Description |
|---|---|
| *mac* | Sets the MAC address. |
| **all** | Deletes all trusted hosts. |

**Defaults** N/A

**Command Mode** NFPP configuration mode

**Usage Guide** After this function is enabled, the ND packets are sent from the trusted host to CPU without rate limit or alarm notification.
Up to 500 trusted hosts are supported.

**Configuration Examples** The following example sets the host whose MAC address is 0000.0000.1111 as the trusted host.

```
Ruijie(config)# nfpp
Ruijie(config-nfpp)#nd-guard trusted-host 0000.0000.1111
```

**Related Commands**

| Command | Description |
|---|---|
| N/A | N/A |

**Platform Description** N/A

## 3.54 nfpp arp-guard enable

Use this command to enable ARP anti-attack function on the interface. Use the **no** or **default** form of this command to restore the default setting.
**nfpp arp-guard enable**
**no nfpp arp-guard enable**
**default nfpp arp-guard enable**

**Parameter Description**

| Parameter | Description |
|---|---|
| N/A | N/A |

**Defaults** The ARP anti-attack function is not enabled on the interface.

**Command Mode** Interface configuration mode

**Usage Guide** The interface ARP anti-attack configuration is prior to the global configuration.

**Configuration Examples** The following example enables ARP anti-attack function on the interface.

```
Ruijie(config)# interface G0/1
Ruijie(config-if)# nfpp arp-guard enable
```

**Related Commands**

| Command | Description |
|---|---|
| **arp-guard enable** | Enables ARP anti-attack function. |
| **show nfpp arp-guard summary** | Displays the configuration. |

**Platform Description** N/A

## 3.55 nfpp arp-guard isolate-period

Use this command to set the isolate period in the interface configuration mode. Use the **no** or **default** form of this command to restore the default setting.

**nfpp arp-guard isolate-period** { *seconds* | **permanent** }

**no nfpp arp-guard isolate-period**

**default nfpp arp-guard isolate-period**

**Parameter Description**

| Parameter | Description |
|---|---|
| *seconds* | Sets the isolate period. The value is 0, or in the range from 30 to 86400 in the unit of seconds. |
| **permanent** | Permanent isolation. |

**Defaults** By default, the isolate period is not configured.

**Command Mode** Interface configuration mode

**Usage Guide** N/A

**Configuration Examples** The following example sets the isolate period in the Interface configuration mode

```
Ruijie(config)# interface G0/1
Ruijie(config-if)# nfpp arp-guard isolate-period 180
```

**Related Commands**

| Command | Description |
|---|---|
| **arp-guard isolate-period** | Sets the global isolate period. |
| **show nfpp arp-guard summary** | Displays the configuration. |

**Platform Description** N/A

## 3.56 nfpp arp-guard policy

Use this command to set the rate-limit threshold and the attack threshold. Use the **no** or **default** form of this command to restore the default setting.

**nfpp arp-guard policy** { **per-src-ip** | **per-src-mac** | **per-port** } *rate-limit-pps attack-threshold-pps*

**no nfpp arp-guard policy** { **per-src-ip** | **per-src-mac** | **per-port** }

**default nfpp arp-guard policy** { **per-src-ip** | **per-src-mac** | **per-port** }

**Parameter Description**

| Parameter | Description |
|---|---|
| **per-src-ip** | Sets the rate-limit threshold and the attack threshold for each source IP address. |
| **per-src-mac** | Sets the rate-limit threshold and the attack threshold for each source MAC address. |
| **per-port** | Sets the rate-limit threshold and the attack threshold for each port. |
| *rate-limit-pps* | Sets the rate-limit threshold , in the range from 1 to 9999. |
| *attack-threshold-pps* | Sets the attack threshold, in the range from1 to 9999. |

**Defaults** By default, the rate-limit threshold and the attack threshold are not configured.

**Command Mode** Interface configuration mode

**Usage Guide** The attack threshold value shall be equal to or greater than the rate-limit threshold.

**Configuration Examples** The following example sets the rate-limit threshold and the attack threshold.

```
Ruijie(config)# interface G 0/1
Ruijie(config-if)# nfpp arp-guard policy per-src-ip 2 10
Ruijie(config-if)# nfpp arp-guard policy per-src-mac 3 10
Ruijie(config-if)# nfpp arp-guard policy per-port 50 100
```

**Related Commands**

| Command | Description |
|---|---|
| **arp-guard attack-threshold** | Sets the global attack threshold. |
| **arp-guard rate-limit** | Sets the global rate-limit threshold. |
| **show nfpp arp-guard summary** | Displays the configuration. |
| **show nfpp arp-guard hosts** | Displays the monitored host. |
| **clear nfpp arp-guard hosts** | Clears the isolate host. |

**Platform Description** N/A

## 3.57 nfpp arp-guard scan-threshold

Use this command to set the scan threshold. Use the **no** or **default** form of this command to restore the default setting.

**nfpp arp-guard scan-threshold** *pkt-cnt*

**no nfpp arp-guard scan-threshold**

**default nfpp arp-guard scan-threshold**

**Parameter Description**

| Parameter | Description |
|---|---|
| *pkt-cnt* | Sets the scan threshold, in the range from1 to 9999. |

**Defaults** By default, the sport-based scan threshold is not configured.

**Command Mode** Interface configuration mode

**Usage Guide** N/A

**Configuration Examples** The following example sets the scan threshold to 20pps.

```
Ruijie(config)# interface G 0/1
Ruijie(config-if)# nfpp arp-guard scan-threshold 20
```

**Related Commands**

| Command | Description |
|---|---|
| **arp-guard attack-threshold** | Sets the global attack threshold. |
| **show nfpp arp-guard summary** | Displays the configuration. |
| **show nfpp arp-guard scan** | Displays the ARP scan table. |
| **clear nfpp arp-guard scan** | Clears the ARP scan table. |

**Platform Description** N/A

## 3.58 nfpp dhcp-guard enable

Use this command to enable DHCP anti-attack function on the interface. Use the **no** or **default** form of this command to restore the default setting.

**nfpp dhcp-guard enable**

**no nfpp dhcp-guard enable**

**default nfpp dhcp-guard enable**

**Parameter Description**

| Parameter | Description |
| --- | --- |
| N/A | N/A |

**Defaults** The DHCP anti-attack function is not enabled on the interface.

**Command Mode** Interface configuration mode

**Usage Guide** The interface DHCP anti- attack configuration is prior to the global configuration.

**Configuration Examples** The following example enables DHCP anti-attack function on the interface.

```
Ruijie(config)# interface G0/1
Ruijie(config-if)# nfpp dhcp-guard enable
```

**Related Commands**

| Command | Description |
| --- | --- |
| **dhcp-guard enable** | Enables DHCP anti-attack function. |
| **show nfpp dhcp-guard summary** | Displays the configuration. |

**Platform Description** N/A

## 3.59 nfpp dhcp-guard isolate-period

Use this command to set the isolate period in the interface configuration mode. Use the **no** or **default** form of this command to restore the default setting.

**nfpp dhcp-guard isolate-period** { *seconds* | **permanent** }

**no nfpp dhcp-guard isolate-period**

**default nfpp dhcp-guard isolate-period**

**Parameter Description**

| Parameter | Description |
| --- | --- |
| *seconds* | Sets the isolate period. The value is 0 or in the range from 30 to 86400 in the unit of seconds. |
| **permanent** | Permanent isolation. |

**Defaults** By default, the isolate period is not configured

**Command Mode** Interface configuration mode

**Usage Guide** N/A

**Configuration Examples** The following example sets the isolate period to 180 seconds.

```
Ruijie(config)# interface G0/1
Ruijie(config-if)# nfpp dhcp-guard isolate-period 180
```

**Related Commands**

| Command | Description |
| --- | --- |
| **dhcp-guard isolate-period** | Sets the global isolate period. |
| **show nfpp dhcp-guard summary** | Displays the configuration. |

**Platform Description** N/A

## 3.60 nfpp dhcp-guard policy

Use this command to set the rate-limit threshold and the attack threshold. Use the **no** or **default** form of this command to restore the default setting.

**nfpp dhcp-guard policy** { **per-src-mac** | **per-port** } *rate-limit-pps attack-threshold-pps*

**no nfpp dhcp-guard policy** { **per-src-mac** | **per-port** }

**default nfpp dhcp-guard policy** { **per-src-mac** | **per-port** }

**Parameter Description**

| Parameter | Description |
| --- | --- |
| **per-src-mac** | Sets the rate-limit threshold and the attack threshold for each source MAC address. |
| **per-port** | Sets the rate-limit threshold and the attack threshold for each port. |
| *rate-limit-pps* | Sets the rate-limit threshold, in the range from1 to 9999. |
| *attack-threshold-pps* | Sets the attack threshold, in the range from1 to9999. |

**Defaults** By default, the rate-limit threshold and the attack threshold are not configured.

**Command Mode** Interface configuration mode

**Usage Guide** The attack threshold value should be no smaller than the rate-limit threshold.

**Configuration Examples** The following example sets the rate-limit threshold and the attack threshold.

```
Ruijie(config)# interface G 0/1
Ruijie(config-if)# nfpp dhcp-guard policy per-src-mac 3 10
Ruijie(config-if)# nfpp dhcp-guard policy per-port 50 100
```

**Related Commands**

| Command | Description |
| --- | --- |

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

**Platform Description** N/A

## 3.61 nfpp dhcpv6-guard enable

Use this command to enable the DHCPv6 anti-attack function on the interface. Use the **no** or **default** form of this command to restore the default setting.

**nfpp dhcpv6-guard enable**

**no nfpp dhcpv6-guard enable**

**default nfpp dhcpv6-guard enable**

**Parameter Description**

| Parameter | Description |
|---|---|
| N/A | N/A |

**Defaults** The DHCPv6 anti-attack function is not enabled on the interface.

**Command Mode** Interface configuration mode

**Usage Guide** The interface DHCPv6 anti- attack configuration is prior to the global configuration.

**Configuration Examples** The following example enables the DHCPv6 anti-attack function on interface G0/1.

```
Ruijie(config)# interface G0/1
Ruijie(config-if)# nfpp dhcpv6-guard enable
```

**Related Commands**

| Command | Description |
|---|---|
| **dhcpv6-guard enable** | Enables the ARP anti-attack function. |
| **show nfpp dhcpv6-guard summary** | Displays the configuration. |

**Platform Description** N/A

## 3.62 nfpp dhcpv6-guard isolate-period

Use this command to set the isolate period in the interface configuration mode. Use the **no** or **default** form of this command to restore the default setting.

**nfpp dhcpv6-guard isolate-period** { *seconds* | **permanent** }

**no nfpp dhcpv6-guard isolate-period**

**default nfpp dhcpv6-guard isolate-period**

**Parameter Description**

| Parameter | Description |
| --- | --- |
| *seconds* | Sets the isolate period. The value is 0 or in the range from 30 to 86400 in the unit of seconds. |
| **permanent** | Permanent isolation. |

**Defaults** By default, the isolate period is not configured.

**Command Mode** Interface configuration mode

**Usage Guide** N/A

**Configuration Examples** The following example sets the isolate period in the interface configuration mode to 180 seconds.

```
Ruijie(config)# interface G0/1
Ruijie(config-if)# nfpp dhcpv6-guard isolate-period 180
```

**Related Commands**

| Command | Description |
| --- | --- |
| **dhcpv6-guard isolate-period** | Sets the global isolate period. |
| **show nfpp dhcpv6-guard summary** | Displays the configuration. |

**Platform Description** N/A

## 3.63 nfpp dhcpv6-guard policy

Use this command to set the rate-limit threshold and the attack threshold. Use the **no** or **default** form of this command to restore the default setting.

**nfpp dhcpv6-guard policy** { **per-src-mac** | **per-port** } *rate-limit-pps attack-threshold-pps*

**no nfpp dhcpv6-guard policy** { **per-src-mac** | **per-port**}

**default nfpp dhcpv6-guard policy** { **per-src-mac** | **per-port**}

**Parameter Description**

| Parameter | Description |
| --- | --- |
| **per-src-mac** | Sets the rate-limit threshold and the attack threshold for each source MAC address. |
| **per-port** | Sets the rate-limit threshold and the attack threshold for each port. |
| *rate-limit-pps* | Sets the rate-limit threshold, in the range from1 to 9999. |
| *attack-threshold-pps* | Sets the attack threshold, in the range from1 to9999. |

**Defaults** By default, the rate-limit threshold and the attack threshold are not configured.

**Command Mode** Interface configuration mode

**Usage Guide** The attack threshold value should be no smaller than the rate-limit threshold.

**Configuration Examples** The following example sets the rate-limit threshold and the attack threshold.

```
Ruijie(config)# interface G 0/1
Ruijie(config-if)# nfpp dhcpv6-guard policy per-src-mac 3 10
Ruijie(config-if)# nfpp dhcpv6-guard policy per-port 50 100
```

**Related Commands**

| Command | Description |
| --- | --- |
| **dhcpv6-guard attack-threshold** | Sets the global attack threshold. |
| **dhcpv6-guard rate-limit** | Sets the global rate-limit threshold. |
| **show nfpp dhcpv6-guard summary** | Displays the configuration. |
| **show nfpp dhcpv6-guard hosts** | Displays the monitored host. |
| **clear nfpp dhcpv6-guard hosts** | Clears the isolate host. |

**Platform Description** N/A

## 3.64 nfpp icmp-guard enable

Use this command to enable the ICMP anti-attack function on the interface. Use the **no** or **default** form of this command to restore the default setting.

**nfpp icmp-guard enable**

**no nfpp icmp-guard enable**

**default nfpp icmp-guard enable**

**Parameter Description**

| Parameter | Description |
| --- | --- |
| N/A | N/A |

**Defaults** The ICMP anti-attack function is not enabled on the interface.

**Command Mode** Interface configuration mode

**Usage Guide** The interface ICMP anti- attack configuration is prior to the global configuration.

**Configuration Examples** The following example enables the ICMP anti-attack function on the interface.

```
Ruijie(config)# interface G0/1
Ruijie(config-if)# nfpp icmp-guard enable
```

**Related Commands**

| Command | Description |
| --- | --- |
| **icmp-guard enable** | Enables the ARP anti-attack function. |
| **show nfpp icmp-guard summary** | Displays the configuration. |

**Platform Description** N/A

## 3.65 nfpp icmp-guard isolate-period

Use this command to set the isolate period in the interface configuration mode. Use the **no** or **default** form of this command to restore the default setting.

**nfpp icmp-guard isolate-period** { *seconds* | **permanent** }

**no nfpp icmp-guard isolate-period**

**default nfpp icmp-guard isolate-period**

**Parameter Description**

| Parameter | Description |
| --- | --- |
| *seconds* | Sets the isolate period. The value is 0 or in the range from 30 to 86400 in the unit of seconds. |
| **permanent** | Permanent isolation. |

**Defaults** By default, the isolate period is not configured.

**Command Mode** Interface configuration mode

**Usage Guide** N/A

**Configuration Examples** The following example sets the isolate period in the interface configuration mode.

```
Ruijie(config)# interface G0/1
Ruijie(config-if)# nfpp icmp-guard isolate-period 180
```

**Related Commands**

| Command | Description |
| --- | --- |
| **icmp-guard isolate-period** | Sets the global isolate period. |
| **show nfpp icmp-guard summary** | Displays the configuration. |

**Platform Description** N/A

## 3.66 nfpp icmp-guard policy

Use this command to set the rate-limit threshold and the attack threshold. Use the **no** or **default** form of this command to restore the default setting.

**nfpp icmp-guard policy** { p**er-src-ip** | **per-port** } *rate-limit-pps attack-threshold-pps*

**no nfpp icmp-guard policy** { **per-src-ip** | **per-port** }

**default nfpp icmp-guard policy** { **per-src-ip** | **per-port** }

**Parameter Description**

| Parameter | Description |
|---|---|
| **per-src-ip** | Sets the rate-limit threshold and the attack threshold for each source IP address. |
| **per-port** | Sets the rate-limit threshold and the attack threshold for each port. |
| *rate-limit-pps* | Sets the rate-limit threshold, in the range from1 to 9999. |
| *attack-threshold-pps* | Sets the attack threshold, in range from1 to 9999. |

**Defaults** By default, the rate-limit threshold and the attack threshold are not configured.

**Command Mode** Interface configuration mode

**Usage Guide** The attack threshold value shall be equal to or greater than the rate-limit threshold.

**Configuration Examples** The following example sets the rate-limit threshold and the attack threshold.

```
Ruijie(config)# interface G 0/1
Ruijie(config-if)# nfpp icmp-guard policy per-src-ip 5 10
Ruijie(config-if)# nfpp icmp-guard policy per-port 100 200
```

**Related Commands**

| Command | Description |
|---|---|
| **icmp-guard attack-threshold** | Sets the global attack threshold. |
| **icmp-guard rate-limit** | Sets the global rate-limit threshold. |
| **show nfpp icmp-guard summary** | Displays the configuration. |
| **show nfpp icmp-guard hosts** | Displays the monitored host. |
| **clear nfpp icmp-guard hosts** | Clears the isolate host. |

**Platform Description** N/A

## 3.67 nfpp ip-guard enable

Use this command to enable the ICMP anti-attack function on the interface. Use the **no** or **default** form of this command to restore the default setting.

**nfpp ip-guard enable**
**no nfpp ip-guard enable**
**default nfpp ip-guard enable**

**Parameter Description**

| Parameter | Description |
|---|---|
| N/A | N/A |

**Defaults** The IP anti-scan function is not enabled on the interface.

**Command Mode** Interface configuration mode

**Usage Guide** The interface IP anti-scan configuration is prior to the global configuration.

**Configuration Examples** The following example enables the ICMP anti-attack function on the interface.

```
Ruijie(config)# interface G0/1
Ruijie(config-if)# nfpp ip-guard enable
```

**Related Commands**

| Command | Description |
|---|---|
| **ip-guard enable** | Enables the ARP anti-attack function. |
| **show nfpp ip-guard summary** | Displays the configuration. |

**Platform Description** N/A

## 3.68 nfpp ip-guard isolate-period

Use this command to set the isolate period in the interface configuration mode. Use the **no** or **default** form of this command to restore the default setting.
**nfpp ip-guard isolate-period** { *seconds* | **permanent** }
**no nfpp ip-guard isolate-period**
**default nfpp ip-guard isolate-period**

**Parameter Description**

| Parameter | Description |
|---|---|
| *seconds* | Sets the isolate period, in the range from 30 to 86400 in the unit of seconds. |
| **permanent** | Permanent isolation. |

**Defaults** By default, the isolate period is not configured.

**Command** Interface configuration mode

**Mode**

**Usage Guide** N/A

**Configuration Examples** The following example sets the isolate period in the interface configuration mode.

```
Ruijie(config)# interface G0/1
Ruijie(config-if)# nfpp ip-guard isolate-period 180
```

**Related Commands**

| Command | Description |
|---|---|
| **ip-guard isolate-period** | Sets the global isolate period. |
| **show nfpp ip-guard summary** | Displays the configuration. |

**Platform Description** N/A

## 3.69 nfpp ip-guard policy

Use this command to set the rate-limit threshold and the attack threshold. Use the **no** or **default** form of this command to restore the default setting.

**nfpp ip-guard policy** { **per-src-ip** | **per-port** } *rate-limit-pps attack-threshold-pps*

**no nfpp ip-guard policy** { **per-src-ip** | **per-port** }

**default nfpp ip-guard policy** { **per-src-ip** | **per-port** }

**Parameter Description**

| Parameter | Description |
|---|---|
| **per-src-ip** | Sets the rate-limit threshold and the attack threshold for each source IP address. |
| **per-port** | Sets the rate-limit threshold and the attack threshold for each port. |
| *rate-limit-pps* | Sets the rate-limit threshold, in the range from 1 to 9999. |
| *attack-threshold-pps* | Sets the attack threshold, in the range from 1 to 9999. |

**Defaults** By default, the rate-limit threshold and the attack threshold are not configured.

**Command Mode** Interface configuration mode

**Usage Guide** The attack threshold value shall be equal to or greater than the rate-limit threshold.

**Configuration Examples** The following example sets the rate-limit threshold and the attack threshold.

```
Ruijie(config)# interface G 0/1
Ruijie(config-if)# nfpp ip-guard policy per-src-ip 2 10
Ruijie(config-if)# nfpp ip-guard policy per-port 50 100
```

**Related Commands**

| Command | Description |
| --- | --- |
| **ip-guard attack-threshold** | Sets the global attack threshold. |
| **ip-guard rate-limit** | Sets the global rate-limit threshold. |
| **show nfpp ip-guard summary** | Displays the configuration. |
| **show nfpp ip-guard hosts** | Displays the monitored host. |
| **clear nfpp ip-guard hosts** | Clears the isolate host. |

**Platform Description** N/A

## 3.70 nfpp ip-guard scan-threshold

Use this command to set the scan threshold. Use the **no** or **default** form of this command to restore the default setting.

**nfpp ip-guard scan-threshold** *pkt-cnt*

**no nfpp ip-guard scan-threshold**

**default nfpp ip-guard scan-threshold**

**Parameter Description**

| Parameter | Description |
| --- | --- |
| *pkt-cnt* | Sets the scan threshold, in the range from 1 to 9999. |

**Defaults** By default, the sport-based scan threshold is not configured.

**Command Mode** Interface configuration mode

**Usage Guide** N/A

**Configuration Examples** The following example sets the scan threshold to 20pps.

```
Ruijie(config)# interface G 0/1
Ruijie(config-if)# nfpp ip-guard scan-threshold 20
```

**Related Commands**

| Command | Description |
| --- | --- |
| **ip-guard attack-threshold** | Sets the global attack threshold. |
| **show nfpp ip-guard summary** | Displays the configuration. |

**Platform Description** N/A

## 3.71 nfpp nd-guard enable

Use this command to enable the ND anti-attack function on the interface. Use the **no** or **default** form of this command to restore the default setting.

**nfpp nd-guard enable**

**no nfpp nd-guard enable**

**default nfpp nd-guard enable**

**Parameter Description**

| Parameter | Description |
|---|---|
| N/A | N/A |

**Defaults** The ND anti-attack function is not enabled on the interface.

**Command Mode** Interface configuration mode

**Usage Guide** The interface ND anti-attack configuration is prior to the global configuration.

**Configuration Examples** The following example enables the ND anti-attack function on the interface.

```
Ruijie(config)# interface G0/1
Ruijie(config-if)# nfpp nd-guard enable
```

**Related Commands**

| Command | Description |
|---|---|
| **nd-guard enable** | Enables the ND anti-attack function. |
| **show nfpp nd-guard summary** | Displays the configuration. |

**Platform Description** N/A

## 3.72 nfpp nd-guard policy

Use this command to set the rate-limit threshold and the attack threshold. Use the **no** or **default** form of this command to restore the default setting.

**nfpp nd-guard policy per-port** { **ns-na** | **rs** | **ra-redirect** } *rate-limit-pps attack-threshold-pps*

**no nfpp nd-guard policy per-port** { **ns-na** | **rs** | **ra-redirect** }

**default nfpp nd-guard policy per-port** { **ns-na** | **rs** | **ra-redirect** }

**Parameter Description**

| Parameter | Description |
|---|---|
| **ns-na** | Sets the neighbor request and neighbor advertisement. |
| **rs** | Sets the router request. |

| | |
|---|---|
| **ra-redirect** | Sets the router advertisement and the redirect packets. |
| *rate-limit-pps* | Sets the rate-limit threshold, in the range from 1 to 9999. |
| *attack-threshold-pps* | Sets the attack threshold, in the range from 1 to 9999. |

**Defaults** By default, the rate-limit threshold and the attack threshold are not configured.

**Command Mode** Interface configuration mode

**Usage Guide** The attack threshold value shall be equal to or greater than the rate-limit threshold.
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-limit 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.

**Configuration Examples** The following example sets the rate-limit threshold and the attack threshold.

```
Ruijie(config)# interface G 0/1
Ruijie(config-if)# nfpp nd-guard policy per-port ns-na 50 100
Ruijie(config-if)# nfpp nd-guard policy per-port rs 10 20
Ruijie(config-if)# nfpp nd-guard policy per-port ra-redirect 10 20
```

**Related Commands**

| Command | Description |
|---|---|
| **nd-guard attack-threshold** | Sets the global attack threshold. |
| **nd-guard rate-limit** | Sets the global rate-limit threshold. |
| **show nfpp nd-guard summary** | Displays the configuration. |

**Platform Description** N/A

## 3.73 show nfpp arp-guard hosts

Use this command to display the monitored host.
**show nfpp arp-guard hosts** [ **statistics** | [ [ **vlan** *vid* ] [ **interface** *interface-id* ] [ *ip-address* | *mac-address* ] ] ]

**Parameter Description**

| Parameter | Description |
|---|---|
| statistics | Displays the statistical information of the monitored host. |
| *vid* | The VLAN ID. |
| *interface-id* | The interface name. |

| | |
|---|---|
| *ip-address* | The IP address. |
| *mac-address* | The MAC address. |

**Defaults** N/A

**Command Mode** Privileged EXEC mode

**Usage Guide** N/A

**Configuration Examples** The following example displays the statistical information of the monitored host.

```
Ruijie# show nfpp arp-guard hosts statistics
success    fail    total
-------    ----    -----
100        20       120
```

The following example shows the monitored host:

```
Ruijie# show nfpp arp-guard hosts
If column 1 shows '*', it means "hardware do not isolate user" .
VLAN  interface IP address   MAC address   remain-time(s)
----  --------   ---------   -----------   -------------
1     Gi0/1      1.1.1.1     -               110
2     Gi0/2      1.1.2.1     -               61
*3    Gi0/3      -           0000.0000.1111  110
4     Gi0/4      -           0000.0000.2222   61
Total:4 hosts
```

**Related Commands**

| Command | Description |
|---|---|
| **clear nfpp arp-guard hosts** | Clears the monitored host. |

**Platform Description** N/A

## 3.74 show nfpp arp-guard scan

Use this command to display the ARP scan list.

**show nfpp arp-guard scan** [ **statistics** | [ [ **vlan** *vid* ] [ **interface** *interface-id* ] [ *mac-address* ] ] ]

**Parameter Description**

| Parameter | Description |
|---|---|
| **statistics** | Displays the statistical information of the ARP scan list. |
| *vid* | The VLAN ID. |
| *interface-id* | The interface name. |

| | |
|---|---|
| *mac-address* | The MAC address. |

**Defaults** N/A

**Command Mode** Privileged EXEC mode

**Usage Guide** N/A

**Configuration Examples** The following example displays the ARP scan statistics.

```
Ruijie# show nfpp arp-guard scan statistics
ARP scan table has 4 record(s).
```

The following example displays the ARP scan list.

```
Ruijie# show nfpp arp-guard scan
VLAN    interface   IP address   MAC address    timestamp
----    --------   ----------  -----------    ---------
1       Gi0/1      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)
```

The following example displays the ARP scan for VLAN 1.

```
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** | Sets the global scan threshold. |
| **nfpp arp-guard scan-threshold** | Sets the scan threshold. |
| **clear nfpp arp-guard scan** | Clears the ARP scan list. |

**Platform Description** N/A

## 3.75 show nfpp arp-guard summary

Use this command to display the configuration.

**show nfpp arp-guard summary**

**Parameter Description**

| Parameter | Description |
| --- | --- |
| N/A | N/A |

**Defaults** N/A

**Command Mode** Privileged EXEC mode

**Usage Guide** N/A

**Configuration Examples** The following example displays the configuration.

```
Ruijie# show nfpp arp-guard summary
(Format of column Rate-limit and  Attack-threshold is
per-src-ip/per-src-mac/per-port.)
Interface  Status  Isolate-period Rate-limit Attack-threshold Scan-threshold
Global     Enable  300            4/5/60    8/10/100         15
Gi 0/1      Enable  180            5/-/-      8/-/-             -
Gi 0/2      Disable 200            4/5/60    8/10/100         20

Maximum count of monitored hosts: 1000
Monitor period:300s
```

| Field | Description |
| --- | --- |
| Interface(Global) | Global configuration mode. |
| Status | Enables/Disables the anti-attack function. |
| Rate-limit | In the format of the rate-limit threshold for the source IP address/ the rate-limit threshold for the source MAC address/ the rate-limit threshold for the port |
| Attack-threshold | In the same format as the rate-limit. |
| - | No configuration. |

**Related Commands**

| Command | Description |
| --- | --- |
| **arp-guard attack-threshold** | Sets the global attack threshold. |
| **arp-guard enable** | Enables the ARP anti-attack function. |
| **arp-guard isolate-period** | Sets the global isolate time. |
| **arp-guard monitor-period** | Sets the monitor period. |
| **arp-guard monitored-host-limit** | Sets the maximum number of the monitored hosts. |
| **arp-guard rate-limit** | Sets the global rate-limit threshold. |
| **arp-guard scan-threshold** | Sets the global scan threshold. |
| **nfpp arp-guard enable** | Enables the ARP anti-attack function on the interface. |

| | |
|---|---|
| **nfpp arp-guard isolate-period** | Sets the isolate time. |
| **nfpp arp-guard policy** | Sets the rate-limit threshold and attack threshold. |
| **nfpp arp-guard scan-threshold** | Sets the scan threshold. |

**Platform Description** N/A

## 3.76 show nfpp arp-guard trusted-host

Use this command to display the trusted host.

**show nfpp arp-guard trusted-host**

**Parameter Description**

| Parameter | Description |
|---|---|
| N/A | N/A |

**Defaults** N/A

**Command Mode** Privileged EXEC mode

**Usage Guide** N/A

**Configuration Examples** The following example displays the trusted host.

```
Ruijie# show nfpp arp-guard trusted-host
IP address     mac
---------      ------
1.1.1.1        0000.0000.1111
1.1.2.1        0000.0000.2222
Total: 2 record(s)
```

**Related Commands**

| Command | Description |
|---|---|
| N/A | N/A |

**Platform Description** N/A

## 3.77 show nfpp dhcp-guard hosts

Use this command to display the monitored host.

**show nfpp dhcp-guard hosts** [ **statistics** | [ [ **vlan** *vid* ] [ **interface** *interface-id* ] [ *mac-address* ] ] ]

**Parameter Description**

| Parameter | Description |
| --- | --- |
| **statistics** | Displays the statistical information of the monitored host. |
| *vid* | The VLAN ID. |
| *interface-id* | The interface name. |
| *mac-address* | The MAC address. |

**Defaults** N/A

**Command Mode** Privileged EXEC mode

**Usage Guide** N/A

**Configuration Examples** The following example displays the statistical information of the monitored host.

```
Ruijie# show nfpp dhcp-guard hosts statistics
success    fail    total
-------    ----    -----
100        20       120
```

The following example shows the monitored host:

```
Ruijie# show nfpp dhcp-guard hosts
If column 1 shows '*', it means "hardware failed to isolate host".
VLAN  interface   MAC address    remain-time(seconds)
----    ---------   -----------        -------------------
 1    gi0/2     0000.0000.0001   10
 *2   gi0/1     0000.0000.0002   20
Total:2 host(s)
```

**Related Commands**

| Command | Description |
| --- | --- |
| **clear nfpp dhcp-guard hosts** | Clears the monitored host. |

**Platform Description** N/A

## 3.78 show nfpp dhcp-guard summary

Use this command to display the configuration.

**show nfpp dhcp-guard summary**

**Parameter Description**

| Parameter | Description |
| --- | --- |

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

**Defaults** N/A

**Command Mode** Privileged EXEC mode

**Usage Guide** N/A

**Configuration Examples** The following example displays the configuration.

```
Ruijie# show nfpp dhcp-guard summary
(Format of column Rate-limit and  Attack-threshold is
per-src-ip/per-src-mac/per-port.)
Interface  Status  Isolate-period Rate-limit Attack-threshold
Global     Enable  300            -/5/150    -/10/300
Gi 0/1      Enable  180            -/6/-      -/8/-
Gi 0/2      Disable 200            -/5/30     -/10/50

Maximum count of monitored hosts: 1000
Monitor period:300s
```

| Field | Description |
|---|---|
| Interface(Global) | Global configuration mode. |
| Status | Enables/Disables the anti-attack function. |
| Rate-limit | In the format of the rate-limit threshold for the source IP address/ the rate-limit threshold for the source MAC address/ the rate-limit threshold for the port |
| Attack-threshold | In the same format as the rate-limit. |
| - | No configuration. |

**Related Commands**

| Command | Description |
|---|---|
| **dhcp-guard attack-threshold** | Sets the global attack threshold. |
| **dhcp-guard enable** | Enables the DHCP anti-attack function. |
| **dhcp-guard isolate-period** | Sets the global isolate time. |
| **dhcp-guard monitor-period** | Sets the monitor period. |
| **dhcp-guard monitored-host-limit** | Sets the maximum number of the monitored hosts. |
| **dhcp-guard rate-limit** | Sets the global rate-limit threshold. |
| **nfpp dhcp-guard enable** | Enables the DHCP anti-attack function on the interface. |
| **nfpp dhcp-guard isolate-period** | Sets the isolate time. |
| **nfpp dhcp-guard policy** | Sets the rate-limit threshold and attack threshold. |

**Platform Description** N/A

## 3.79 show nfpp dhcp-guard trusted-host

Use this command to display the trusted host.

**show nfpp dhcp-guard trusted-host**

**Parameter Description**

| Parameter | Description |
|---|---|
| N/A | N/A |

**Defaults** N/A

**Command Mode** Privileged EXEC mode

**Usage Guide** N/A

**Configuration Examples** The following example displays the trusted host.

```
Ruijie# show nfpp dhcp-guard trusted-host
mac
------
0000.0000.1111
0000.0000.2222
Total: 2 record(s)
```

**Related Commands**

| Command | Description |
|---|---|
| N/A | N/A |

**Platform Description** N/A

## 3.80 show nfpp dhcpv6-guard hosts

Use this command to display the monitored host.

**show nfpp dhcpv6-guard hosts** [ **statistics** | [ [ *vlan vid* ] [ **interface** *interface-id* ] [ *mac-address* ] ] ]

**Parameter Description**

| Parameter | Description |
|---|---|
| **statistics** | Displays the statistical information of the monitored host. |

| | |
|---|---|
| *vid* | The VLAN ID. |
| *interface-id* | The interface name. |
| *mac-address* | The MAC address. |

**Defaults** N/A

**Command Mode** Privileged EXEC mode

**Usage Guide** N/A

**Configuration Examples** The following example displays the statistical information of the monitored host.

```
Ruijie# show nfpp 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** | Clears the monitored host. |

**Platform Description** N/A

## 3.81 show nfpp dhcpv6-guard summary

Use this command to display the configuration.

**show nfpp dhcpv6-guard summary**

**Parameter Description**

| Parameter | Description |
|---|---|
| N/A | N/A |

**Defaults** N/A

**Command Mode** Privileged EXEC mode

**Usage Guide** N/A

**Configuration Examples** The following example displays the configuration.

```
Ruijie# show nfpp dhcpv6-guard summary
(Format of column Rate-limit and  Attack-threshold is
per-src-ip/per-src-mac/per-port.)
Interface  Status  Isolate-period Rate-limit Attack-threshold
Global     Enable  300            -/5/150    -/10/300
Gi 0/1      Enable  180            -/6/-      -/8/-
Gi 0/2      Disable 200            -/5/30     -/10/50

Maximum count of monitored hosts: 1000
Monitor period:300s
```

| Field | Description |
|---|---|
| Interface(Global) | Global configuration |
| Status | Enables/Disables the anti-attack function. |
| Rate-limit | In the format of the rate-limit threshold for the source IP address/ the rate-limit threshold for the source MAC address/ the rate-limit threshold for the port |
| Attack-threshold | In the same format as the rate-limit. |
| - | No configuration. |

**Related Commands**

| Command | Description |
|---|---|
| **dhcpv6-guard attack-threshold** | Sets the global attack threshold. |
| **dhcpv6-guard enable** | Enables the DHCPv6 anti-attack function. |
| **dhcpv6-guard isolate-period** | Sets the global isolate time. |
| **dhcpv6-guard monitor-period** | Sets the monitor period. |
| **dhcpv6-guard monitored-host-limit** | Sets the maximum number of the monitored hosts. |
| **dhcpv6-guard rate-limit** | Sets the global rate-limit threshold. |
| **nfpp dhcpv6-guard enable** | Enables the DHCPv6 anti-attack function on the interface. |
| **nfpp dhcpv6-guard isolate-period** | Sets the isolate time. |
| **nfpp dhcpv6-guard policy** | Sets the rate-limit threshold and attack threshold. |

**Platform Description** N/A

## 3.82 show nfpp dhcpv6-guard trusted-host

Use this command to display the trusted host.

**show nfpp dhcpv6-guard trusted-host**

**Parameter Description**

| Parameter | Description |
|---|---|
| N/A | N/A |

**Defaults** N/A

**Command Mode** Privileged EXEC mode

**Usage Guide** N/A

**Configuration Examples** The following example displays the trusted host.

```
Ruijie# show nfpp dhcpv6-guard trusted-host
mac
------
0000.0000.1111
0000.0000.2222
Total: 2 record(s)
```

**Related Commands**

| Command | Description |
|---|---|
| N/A | N/A |

**Platform Description** N/A

## 3.83 show nfpp icmp-guard hosts

Use this command to display the monitored host.

**show nfpp icmp-guard hosts** [ **statistics** | [ [ *vlan vid* ] [ **interfac**e *interface-Id* ] [ *ip-address* ] ] ]

**Parameter Description**

| Parameter | Description |
|---|---|
| **statistics** | Displays the statistical information of the monitored host. |
| *vid* | The VLAN ID. |
| *interface-id* | The interface name. |
| *ip-address* | The IP address. |

**Defaults** N/A

**Command Mode** Privileged EXEC mode

**Usage Guide** N/A

**Configuration Examples** The following example displays the statistical information of the monitored host.

```
Ruijie# show nfpp icmp-guard hosts statistics
success    fail    total
-------    ----    -----
100        20       120
```

The following example displays the monitored host.

```
Ruijie# show nfpp icmp-guard hosts
If column 1 shows '*', it means "hardware failed to isolate host".
VLAN  interface IP address     remain-time(s)
----    --------   ---------         -------------
1     Gi0/1      1.1.1.1     110
2     Gi0/2      1.1.2.1     61
Total:2 host(s)
```

**Related Commands**

| Command | Description |
| --- | --- |
| **clear nfpp icmp-guard hosts** | Clears the monitored host. |

**Platform Description** N/A

## 3.84 show nfpp icmp-guard summary

Use this command to display the configuration.

**show nfpp icmp-guard summary**

**Parameter Description**

| Parameter | Description |
| --- | --- |
| N/A | N/A |

**Defaults** N/A

**Command Mode** Privileged EXEC mode

**Usage Guide** N/A

**Configuration Examples** The following example displays the configuration.

```
Ruijie# show nfpp icmp-guard summary
(Format of column Rate-limit and  Attack-threshold is
per-src-ip/per-src-mac/per-port.)
Interface  Status  Isolate-period Rate-limit Attack-threshold
Global     Enable  300            4/-/60    8/-/100
Gi 0/1      Enable  180            5/-/-      8/-/-
Gi 0/2      Disable 200            4/-/60    8/-/100

Maximum count of monitored hosts: 1000
Monitor period:300s
```

| Field | Description |
|---|---|
| Interface(Global) | Global configuration mode. |
| Status | Enables/Disables the anti-attack function. |
| Rate-limit | In the format of the rate-limit threshold for the source IP address/ the rate-limit threshold for the source MAC address/ the rate-limit threshold for the port |
| Attack-threshold | In the same format as the rate-limit. |
| - | No configuration. |

**Related Commands**

| Command | Description |
|---|---|
| **icmp-guard attack-threshold** | Sets the global attack threshold. |
| **icmp-guard enable** | Enables the ICMP anti-attack function. |
| **icmp-guard isolate-period** | Sets the global isolate time. |
| **icmp-guard monitor-period** | Sets the monitor period. |
| **icmp-guard monitored-host-limit** | Sets the maximum number of the monitored hosts. |
| **icmp-guard rate-limit** | Sets the global rate-limit threshold. |
| **nfpp icmp-guard enable** | Enables the ICMP anti-attack function on the interface. |
| **nfpp icmp-guard isolate-period** | Sets the isolate time. |
| **nfpp icmp-guard policy** | Sets the rate-limit threshold and attack threshold. |

**Platform Description** N/A

## 3.85 show nfpp icmp-guard trusted-host

Use this command to display the trusted host free from being monitored.

**show nfpp icmp-guard summary**

**Parameter Description**

| Parameter | Description |
|---|---|
| N/A | N/A |

**Defaults** N/A

**Command Mode** Privileged EXEC mode

**Usage Guide** N/A

**Configuration Examples** The following example displays the trusted host free from being monitored.

```
Ruijie# show nfpp icmp-guard trusted-host
IP address     mask
---------      ------
1.1.1.0        255.255.255.0
1.1.2.0        255.255.255.0
Total:2 record(s)
```

**Related Commands**

| Command | Description |
|---|---|
| **icmp-guard trusted-host** | Sets the trusted host. |

**Platform Description** N/A

## 3.86 show nfpp ip-guard hosts

Use this command to display the monitored host.

**show nfpp ip-guard hosts** [ **statistics** | [ [ **vlan** *vid* ] [ **Interface** *interface-id* ] [ *ip-address* ] ] ]

**Parameter Description**

| Parameter | Description |
|---|---|
| **statistics** | Displays the statistical information of the monitored host. |
| *vid* | The VLAN ID. |
| *interface-id* | The interface name. |
| *ip-address* | The IP address. |

**Defaults** N/A

**Command** Privileged EXEC mode

**Mode**

**Usage Guide** N/A

**Configuration Examples** The following example displays the statistical information of the monitored host.

```
Ruijie# show nfpp ip-guard hosts statistics
success    fail    total
-------    ----    -----
100        20       120
```

The following example displays the monitored host for the IP anti-attack.

```
Ruijie#show nfpp ip-guard hosts
If column 1 shows '*', it means "hardware do not isolate host" .
VLAN  interface IP address   Reason     remain-time(s)
----  --------  ---------    -------     -------------
1     Gi0/1     1.1.1.1     ATTACK     110
2     Gi0/2     1.1.2.1     SCAN        61
Total:2 host(s)
```

**Related Commands**

| Command | Description |
| --- | --- |
| **clear nfpp ip-guard hosts** | Clears the monitored host. |

**Platform Description** N/A

## 3.87 show nfpp ip-guard summary

Use this command to display the configuration.

**show nfpp ip-guard summary**

**Parameter Description**

| Parameter | Description |
| --- | --- |
| N/A | N/A |

**Defaults** N/A

**Command Mode** Privileged EXEC mode

**Usage Guide** N/A

**Configuration Examples** The following example displays the configuration.

```
Ruijie# show nfpp ip-guard summary
```

```
(Format of column Rate-limit and  Attack-threshold is
per-src-ip/per-src-mac/per-port.)
Interface Status Isolate-period Rate-limit Attack-threshold Scan-threshold
Global     Enable  300            4/-/60    8/-/100         15
Gi 0/1      Enable  180            5/-/-      8/-/-           -
Gi 0/2      Disable 200            4/-/60    8/-/100         20

Maximum count of monitored hosts: 1000
Monitor period..300s
```

| Field | Description |
| --- | --- |
| Interface(Global) | Global configuration |
| Status | Enables/Disables the anti-attack function. |
| Rate-limit | In the format of the rate-limit threshold for the source IP address/ the rate-limit threshold for the source MAC address/ the rate-limit threshold for the port |
| Attack-threshold | In the same format as the rate-limit. |
| - | No configuration. |

**Related Commands**

| Command | Description |
| --- | --- |
| **ip-guard attack-threshold** | Sets the global attack threshold. |
| **ip-guard enable** | Enables the IP anti-scan function. |
| **ip-guard isolate-period** | Sets the global isolate time. |
| **ip-guard monitor-period** | Sets the monitor period. |
| **ip-guard monitored-host-limit** | Sets the maximum number of the monitored hosts. |
| **ip-guard rate-limit** | Sets the global rate-limit threshold. |
| **nfpp ip-guard enable** | Enables the IP anti-scan function on the interface. |
| **nfpp ip-guard isolate-period** | Sets the isolate time. |
| **nfpp ip-guard policy** | Sets the rate-limit threshold and attack threshold. |

**Platform Description** N/A

## 3.88 show nfpp ip-guard trusted-host

Use this command to display the trusted host free from being monitored.

**show nfpp ip-guard summary**

**Parameter**

| Parameter | Description |
| --- | --- |

**Description**

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

**Defaults** N/A

**Command Mode** Privileged EXEC mode

**Usage Guide** N/A

**Configuration Examples** The following example displays the trusted host free from being monitored.

```
Ruijie# show nfpp ip-guard trusted-host
IP address     mask
---------      ------
1.1.1.0        255.255.255.0
1.1.2.0        255.255.255.0
Total.2 record(s)
```

**Related Commands**

| Command | Description |
|---|---|
| **ip-guard trusted-host** | Sets the trusted host. |

**Platform Description** N/A

## 3.89 show nfpp log

Use this command to display the NFPP log configuration.

**show nfpp log summary**

Use this command to display the NFPP log buffer content.

**show nfpp log buffer** [ **statistics** ]

**Parameter Description**

| Parameter | Description |
|---|---|
| **statistics** | Displays the statistical information of the NFPP log buffer. |

**Defaults** N/A

**Command Mode** Privileged EXEC mode

**Usage Guide** When the log buffer is full, the subsequent logs are to be dropped, and an entry with all attributes ”-” is displayed in the log buffer. The administrator shall increase the capacity of the log buffer or improve the rate of generating the syslog.

The generated syslog in the log buffer carries with the timestamp, for example:
%NFPP_ARP_GUARD-4-DOS_DETECTED:
Host<IP=N/A,MAC=0000.0000.0004,port=Gi4/1,VLAN=1> was detected.(2009-07-01 13:00:00)

**Configuration Examples**

The following example displays the NFPP log configuration.

```
Ruijie#show nfpp log summary
Total log buffer size : 10
Syslog rate : 1 entry per 2 seconds
Logging:
VLAN 1-3, 5
interface Gi 0/1
interface Gi 0/2
```

The following example displays the log number in the buffer.

```
Ruijie#show nfpp log buffer statistics
There are 6 logs in buffer.
```

The following example displays the NFPP log buffer:

```
Ruijie#show nfpp log buffer
Protocol VLAN  Interface IP address MAC address    Reason         Timestamp
------- ----  --------   ---------  -----------    ------         ---------
ARP    1     Gi0/1      1.1.1.1     -      DoS            2009-05-30
16:23:10
ARP    1     Gi0/1      1.1.1.1     -      ISOLATED       2009-05-30
16:23:10
ARP    1     Gi0/1      1.1.1.2     -       DoS            2009-05-30
16:23:15
ARP    1     Gi0/1      1.1.1.2     -       ISOLATE_FAILED 2009-05-30
16:23:15
ARP    1     Gi0/1      -         0000.0000.0001  SCAN           2009-05-30
16:30:10
ARP    -     Gi0/2      -         -         PORT_ATTACKED   2009-05-30
16:30:10
```

| Field | Description |
|---|---|
| Protocol | ARP, IP, ICMP, DHCP,DHCPv6, NS-NA, RS, RA-REDIRECT |
| Reason | 1. DoS<br>2. ISOLATED<br>3. ISOLATE_FAILE<br>4. SCAN<br>5. PORT_ATTACKED |

**Related**

| Command | Description |
|---|---|

| Commands | | |
|---|---|---|
| | **clear nfpp log** | Clears the NFPP log buffer. |

**Platform Description** N/A

## 3.90 show nfpp nd-guard summary

Use this command to display the configuration.

**show nfpp nd-guard summary**

| Parameter Description | Parameter | Description |
|---|---|---|
| | N/A | N/A |

**Defaults** N/A

**Command Mode** Privileged EXEC mode

**Usage Guide** N/A

**Configuration Examples** The following example displays the configuration.

```
Ruijie# show nfpp nd-guard summary
(Format of column Rate-limit and  Attack-threshold is NS-NA/RS/RA-REDIRECT.)
Interface Status Rate-limit Attack-threshold
Global     Enable  20/5/10    40/10/20
Gi 0/1      Enable  15/15/15   30/30/30
Gi 0/2      Disable -/5/30      -/10/50
```

| Field | Description |
|---|---|
| Interface(Global) | Global configuration mode. |
| Status | Enables/Disables the anti-attack function. |
| Rate-limit | In the format of the rate-limit threshold for the NS-NA/RS/RA-REDIRECT. |
| Attack-threshold | In the same format as the rate-limit. |
| - | No configuration. |

| Related Commands | Command | Description |
|---|---|---|
| | **nd-guard attack-threshold** | Sets the global attack threshold. |
| | **nd-guard enable** | Enables the ND anti-attack function. |
| | **nd-guard rate-limit** | Sets the global rate-limit threshold. |

| | |
|---|---|
| **nfpp nd-guard enable** | Enables the ND anti-attack function on the interface. |
| **nfpp nd-guard policy** | Sets the rate-limit threshold and attack threshold. |

**Platform Description** N/A

## 3.91 show nfpp nd-guard trusted-host

Use this command to display the trusted host.

**show nfpp nd-guard trusted-host**

**Parameter Description**

| Parameter | Description |
|---|---|
| N/A | N/A |

**Defaults** N/A

**Command Mode** Privileged EXEC mode

**Usage Guide** N/A

**Configuration Examples** The following example displays the trusted host.

```
Ruijie# show nfpp nd-guard trusted-host
mac
------
0000.0000.1111
0000.0000.2222
Total: 2 record(s)
```

**Related Commands**

| Command | Description |
|---|---|
| N/A | N/A |

**Platform Description** N/A

1. WLAN QoS Commands

# 1 WLAN QoS Commands

## 1.1 fair-schedule

Use this command to enable fair scheduling on the wireless AP.

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

**fair-schedule**

**no fair-schedule**

**Parameter Description**

| Parameter | Description |
|---|---|
| N/A | N/A |

**Defaults** This function is enabled by default.

**Command mode** AC: AP configuration mode

Fat AP: AP configuration mode

**Usage Guide**

**Configuration Examples**

**Related Commands**

| Command | Description |
|---|---|
| N/A | N/A |

**Platform Description**

## 1.2 sta-fair

Use this command to specify the fair scheduling priority for a specified user.

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

**sta-fair** *mac-address* **priority** *priority*

**no sta-fair** *mac-address*

**Parameter Description**

| Parameter | Description |
|---|---|
| *mac-address* | Specifies the user's MAC address. |

| | |
|---|---|
| *priority* | Sets the fair scheduling priority, in the range from 1 to 6. |

**Defaults** The default is 1 for all STAs by default.

**Command Mode** Global configuration mode

**Usage Guide** N/A

**Configuration Example**

**Platform Description**

## 1.3 wlan-qos ap-based

Use this command to configure the upstream and downstream traffic limit of the current AP.
Use the **no** form of this command to restore the default setting.
**wlan-qos ap-based** { **per-user-limit** | **total-user-limit** } { **down-streams** | **up-streams** } **average-data-rate** *average-data-rate* **burst-data-rate** *burst-data-rate*
**no wlan-qos ap-based** { **per-user-limit** | **total-user-limit** } { **down-streams** | **up-streams** }

Use this command to configure the intelligent total-user-limit for of the current AP.
Use the **no** form of this command to restore the default setting.
**wlan-qos ap-based total-user-limit** { **down-streams** | **up-streams** } **intelligent**
**no wlan-qos ap-based total-user-limit** { **down-streams** | **up-streams** } **intelligent**

**Parameter Description**

| Parameter | Description |
|---|---|
| **per-user-limit** | Limit for each user on the AP. |
| **total-user-limit** | Limit for the entire AP. |
| **down-streams** | Total downstream traffic limit of the AP. |
| **up-streams** | Total upstream traffic limit of the AP. |
| **intelligent** | Whether to enable intelligent total-user-limit. |
| *average-data-rate* | Average rate limit, ranging from 8 to 261,120 in the unit of 8 Kbps. |
| *burst-data-rate* | Burst rate limit, ranging from 8 to 261,120 in the unit of 8 Kbps. |

**Defaults** These functions are disabled by default.

**Command mode** Global configuration mode.

**Usage Guide** N/A

**Configuration Examples**

**Related Commands**

| Command | Description |
| --- | --- |
| **wlan-qos netuser** *mac-address* { **inbound** \| **outbound** } **average-data-rate** *average-data-rate* **burst-data-rate** *burst-data-rate* | Configures the Client-based in-band and out-of-band traffic rate limits. |
| **wlan-qos wlan-based** { *wlan-id* \| *ssid* } { **per-user-limit** \| **total-user-limit** } { **down-streams** \| **up-streams** } **average-data-rate** *average-data-rate* **burst-data-rate** *burst-data-rate* | Configures the WLAN-based in-band and out-of-band traffic rate limits. |

**Platform Description**

## 1.4 wlan-qos netuser

Use this command to configure the in-band and out-of-band traffic limits for a specified user in the current WLAN.

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

**wlan-qos netuser** *mac-address* { **inbound** | **outbound** } **average-data-rate** *average-data-rate* **burst-data-rate** *burst-data-rate*

**no wlan-qos netuser** *mac-address* { **inbound** | **outbound** }

**Parameter Description**

| Parameter | Description |
| --- | --- |
| *mac-address* | User's MAC address to be set. |
| **inbound** | User’s in-band traffic limit. |
| **outbound** | User’s out-of-band traffic limit. |
| *average-data-rate* | Average rate limit, ranging from 8 to 261120 in the unit of 8Kbps. |
| *burst-data-rate* | Burst rate limit, ranging from 8 to 261120 in the unit of 8Kbps. |

**Defaults** No traffic limit is set by default.

**Command mode** Global configuration mode

**Usage Guide** N/A

**Configuration Examples**

**Related Commands**

| Command | Description |
| --- | --- |
| **wlan-qos wlan-based** { *wlan-id* \| *ssid* } { **per-user-limit** \| **total-user-limit}** { **down-streams** \| **up-streams** } **average-data-rate** *average-data-rate* **burst-data-rate** *burst-data-rate* | Configures the WLAN-based in-band and out-of-band traffic rate limits. |
| **wlan-qos ap-based** { **per-user-limit** \| **total-user-limit** } { **down-streams** \| **up-streams** } **average-data-rate** *average-data-rate* **burst-data-rate** *burst-data-rate* | Configures the AP-based in-band and out-of-band traffic rate limits. |

**Platform Description**

## 1.5 wlan-qos wlan-based

Use this command to configure the upstream and downstream traffic limit of the current WLAN. Use the **no** form of this command to restore the default setting.
**wlan-qos wlan-based** { *wlan-id* | *ssid* } { **per-user-limit** | **total-user-limit** } { **down-streams** | **up-streams** } **average-data-rate** *average-data-rate* **burst-data-rate** *burst-data-rate*
**no wlan-qos wlan-based** { *wlan-id* | *ssid* } { **per-user-limit** | **total-user-limit** } { **down-streams** | **up-streams** }

Use this command to configure the intelligent total-user-limit of the current WLAN. Use the **no** form of this command to restore the default setting.
**wlan-qos wlan-based** { *wlan-id* | *ssid* } **total-user-limit** { **down-streams** | **up-streams** } **intelligent**
**no wlan-qos wlan-based** { *wlan-id* | *ssid* } **total-user-limit** { **down-streams** | **up-streams } intelligent**

**Parameter Description**

| Parameter | Description |
| --- | --- |
| *wlan-id* | WLAN ID. |
| *ssid* | SSID configured by the WLAN. |
| **per-user-limit** | Limit for each user on the WLAN. |
| **total-user-limit** | Limit for the entire WLAN. |
| **down-streams** | Total downstream traffic limit of the WLAN. |
| **up-streams** | Total upstream traffic limit of the WLAN. |
| **intelligent** | Whether to enable intelligent total-user-limit. |
| *average-data-rate* | Average rate limit, ranging from |

| | |
|---|---|
| *burst-data-rate* | Burst rate limit, ranging from 8 to 261120 in the unit of 8Kbps. |

**Defaults** The traffic limit and intelligent total-user-limit are disabled by default.

**Command mode** Global configuration mode

**Usage Guide** N/A

**Configuration Examples**

**Related Commands**

| Command | Description |
|---|---|
| **wlan-qos ap-based** { **per-user-limit** \| **total-user-limit** } { **down-streams** \| **up-streams** } **average-data-rate** *average-data-rate* **burst-data-rate** *burst-data-rate* | Configures the AP-based in-band and out-of-band traffic rate limits. |
| **netuser** *mac-address* { **inbound** \| **outbound** } **average-data-rate** *average-data-rate* **burst-data-rate** *burst-data-rate* | Configures the Client-based in-band and out-of-band traffic rate limits. |

**Platform Description**

## 1.6 wqos fs enable

Use this command to enable WQoS traffic statistics.
Use the **no** form of this command to restore the default setting.

**wqos fs enable**

**no wqos fs enable**

**Parameter Description**

| Parameter | Description |
|---|---|
| N/A | N/A |

**Defaults** This function is disabled by default.

**Command Mode** Global configuration mode

**Usage Guide** When dot1x authentication and Web authentication are disabled, use this command to enable WQoS traffic statistics. Otherwise, WQoS traffic statistics is enabled by default and this command becomes

invalid.

**Configuration**

**Example**

**Platform**

**Description**

# Access Service Commands

# 1 Interface Commands

## 1.1 bandwidth

Use this command to set the bandwidth on the interface. Use the **no** form of this command to restore the default setting.

**bandwidth** *kilobits*

**no bandwidth**

**Parameter Description**

| Parameter | Description |
|---|---|
| *kilobits* | Bandwidth per second, in the unit of Kbps. |

**Defaults** If this command is not configured on the interface, use the show interface command to display the default setting in privileged EXEC mode.

**Command Mode** Interface configuration mode

**Usage Guide** This command does not affect the actual bandwidth on the interface. Instead, it is used to display the system the bandwidth specification. By default, the bandwidth is determined by the actual link rate on the interface. It can be set by the user as well.

**Configuration Examples** The following example sets the bandwidth on the interface to 64 Kbps.

```
Ruijie(config)#interface gigabitEthernet 0/1
Ruijie(config-if-GigabitEthernet 0/1)# bandwidth 64
```

**Related Commands**

| Command | Description |
|---|---|
| N/A | N/A |

**Platform Description** N/A

## 1.2 carrier-delay

Use this command to set the carrier delay on the interface. Use the no form of this command to restore the default value.

**carrier-delay** { *seconds* }

no carrier-delay

**Parameter Description**

| Parameter | Description |
| --- | --- |
| *seconds* | (Optional) in the range from 0 to 60 in the unit of seconds. |

**Defaults** The default is 2 seconds.

**Command Mode** Interface configuration mode

**Usage Guide** This parameter refers to the delay after which the carrier detection signal DCD of the interface link changes from the Down status to the Up status or vice versa. If the DCD changes within the delay, the system will ignore such changes without disconnecting the upper data link layer for renegotiation. If the DCD carrier is disconnected for a long time, the parameter should be set longer to accelerate route aggregation so that the routing table can be converged more quickly. On the contrary, if the DCD carrier interruption period is shorter than the time used for route aggregation, you should set the parameter to a higher value to avoid unnecessary route vibration.

**Configuration Examples** The following example sets the carrier delay of serial interface to 5 seconds.

```
Ruijie(config)# interface gigabitethernet 1/1
Ruijie(config)# carrier-delay 5
```

**Related Commands**

| Command | Description |
| --- | --- |
| N/A | N/A |

**Platform Description** N/A

## 1.3 clear counters

Use this command to clear the counters on the specified interface.

**clear counters** [ *interface-type interface-numbe*r ]

**Parameter Description**

| Parameter | Description |
| --- | --- |
| *interface-number* | Interface ID |
| *interface-type* | Interface type |

**Defaults** N/A

**Command Mode** Privileged EXEC mode.

**Usage Guide** In the privileged EXEC mode, use the **show interfaces** command to display the counters or the **clear counters** command to clear the counters. If the interface is not specified, the counters on all interfaces will be cleared.

**Configuration Examples** The following example clears the counters on interface gigabitethernet 1/1.

```
Ruijie# clear counters gigabitethernet 1/1
```

**Related Commands**

| Command | Description |
| --- | --- |
| **show interfaces** | Displays the interface information. |

**Platform Description** N/A

## 1.4 clear interface

Use this command to reset the interface.

**clear interface** *interface-type interface-number*

**Parameter Description**

| Parameter | Description |
| --- | --- |
| *interface-type* | Interface type and interface ID |
| *interface-number* | |

**Defaults** N/A

**Command Mode** Privileged EXEC mode.

**Usage Guide** This command is only used on the switch port, member port of the L2 Aggregate port, routing port, and member port of the L3 aggregate port. This command is equal to the **shutdown** and **no shutdown** commands.

**Configuration Examples** The following example resets the interface gigabitethernet 1/1.

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

**Related Commands**

| Command | Description |
| --- | --- |
| **shutdown** | Disables the interface. |

**Platform Description** N/A

## 1.5 description

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

**description** *string*

**no description**

**Parameter Description**

| Parameter | Description |
|---|---|
| *string* | Interface alias |

**Defaults** No alias is configured by default.

**Command Mode** Interface configuration mode.

**Usage Guide** Use **show interfaces** to display the interface information, including the alias.

**Configuration Examples** The following example configures the alias of interface.

```
Ruijie(config)# interface serial gigabitEthernet 0/1/0
Ruijie(config-if)# description ShanDong-Bandwidth2M
```

**Related Commands**

| Command | Description |
|---|---|
| **show interfaces** | Displays the interface information. |

**Platform Description** N/A

## 1.6 duplex

Use this command to specify the duplex mode for the interface. Use the **no** form of this command to restore the default setting.

**duplex** { **auto** | **full** | **half** }

**no duplex**

**Parameter Description**

| Parameter | Description |
|---|---|
| **auto** | Self-adaptive full duplex and half duplex |
| **full** | Full duplex |
| **half** | Half duplex |

**Defaults** The default is **auto**,

**Command Mode** Interface configuration mode.

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

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

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

**Related Commands**

| Command | Description |
| --- | --- |
| **show interfaces** | Displays the interface information. |

**Platform Description** N/A

## 1.7 encapsluation dot1q

Use this command to encapsulate IEEE 802.1Q in interface mode. Use the **no** form of this command to restore the default setting.

**encapsulation dot1Q** *VLANID*

**no encapsulation**

**Parameter Description**

| Parameter | Description |
| --- | --- |
| *VLANID* | Indicates the VLAN ID. The value range is from **1** to **4094**. |

**Defaults** By default, the VLAN encapsulation protocol is disabled for interfaces.

**Command Mode** Interface configuration mode.

**Usage Guide** N/A

**Configuration Examples** The following example encapsulates IEEE 802.1Q for interface 20.

```
Ruijie(config)# interface fastEthernet 0/0.20
Ruijie(config-subif)# encapsulation dot1Q 20
```

**Related Commands**

| Command | Description |
| --- | --- |
| **N/A** | N/A. |

**Platform Description** N/A.

## 1.8 interface

Use this command to enter the interface configuration mode.

**interface** *interface-type slot-number/interface-number* [ *sub-interface-number* ]

**Parameter Description**

| Parameter | Description |
|---|---|
| *interface-type* | The interface type. |

**Defaults** N/A

**Command Mode** Global configuration mode

**Usage Guide** For virtual interface, when input an interface number, just input the virtual number directly, for example, interface looback 0.

**Configuration Examples** The following example enters configuration mode on Aggregateport 1.

```
Ruijie(config)# interface serial Gi1/1/0.123
```

**Related Commands**

| Command | Description |
|---|---|
| N/A | N/A |

**Platform Description** N/A

## 1.9 interface range

Use this command to enter interface configuration mode on multiple interfaces.

**interface range** { *port-range* | **macro** *macro_name* }

Use this command to define the macro name of the **interface range** command.

**define interface-range** *macro_name*

**Parameter Description**

| Parameter | Description |
|---|---|
| *port-range* | The interface type and ID range, entered in the form of *interface-type slot-number/interface-number*. The interface can be either an Ethernet physical interface or a loopback interface. |

| | |
|---|---|
| **macro** *macro_name* | The macro name which represents the interface range. |

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

**Command Mode** Global configuration mode

**Usage Guide** Use the define interface-range command to define a range of interfaces as the macro name and then use the **interface** range macro macro_name command to enter interface configuration mode on multiple interfaces.

**Configuration Examples** The following example enters interface configuration mode on multiple interfaces by setting the interface range.

```
Ruijie(config)# interface range gigabitEthernet 0/0, 0/2
```

The following example enters interface configuration mode on multiple interfaces by defining the macro name.

```
Ruijie(config)# define interface-range route1 gigabitEthernet 0/0-2
Ruijie(config)# interface range macro route1
Ruijie(config-if-range)# bandwidth 100
```

**Related Commands**

| Command | Description |
|---|---|
| N/A | N/A |

**Platform Description** N/A

## 1.10 load-interval

Use this command to set the interval for calculating load on the interface. Use the **no** form of this command to restore the default setting.

**load-interval** *seconds*

**no load-interval**

**Parameter Description**

| Parameter | Description |
|---|---|
| *seconds* | In the range from 5 to 600 in the unit of seconds. |

**Defaults** The default is 10.

**Command Mode** Interface configuration mode

**Usage Guide** This command is used to set the interval for calculating load on the interface. In general, the numbers

of incoming and outgoing packets and bytes are calculated every 10 seconds. For example, if the parameter is set to 180 seconds, the following outcome is displayed when the **show interface gigabitEthernet 0/1** command is run.

```
3 minutes input rate 15 bits/sec, 0 packets/sec
3 minutes output rate 14 bits/sec, 0 packets/sec
```

**Configuration Examples** The following example sets the interval for calculating load on interface GigabitEthernet 0/1 to 180 seconds.

```
Ruijie(config)# interface gigabitEthernet 0/1
Ruijie(config-if-GigabitEthernet 0/1)# load-interval 180
```

**Related Commands**

| Command | Description |
| --- | --- |
| N/A | N/A |

**Platform Description** N/A

## 1.11 mtu

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

**mtu** *num*

**Parameter Description**

| Parameter | Description |
| --- | --- |
| *num* | 64 to 9216 (or 65536, which varies by products) |

**Defaults** The default is 1500.

**Command Mode** Interface configuration mode.

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

**Configuration Examples** The following example sets the MTU supported on interface to 576.

```
Ruijie(config)# interface serial 1/gigabitEthernet 0/1
Ruijie(config-if)# mtu 576
```

**Related Commands**

| Command | Description |
| --- | --- |
| show interfaces | Displays the interface information. |

**Platform** N/A

**Description**

## 1.12 show interfaces

Use this command to display the interface information and optical module information.

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

**Parameter Description**

| Parameter | Description |
|---|---|
| *interface-type interface-number* | Interface (including Ethernet interface, aggregate port, SVI or loopback interface). |
| **description** | The description of the interface, including the link status. |

**Defaults**

**Command Mode** All CLI user modes.

**Usage Guide** This command is used to show all basic information if no parameter is specified.

**Configuration Examples** The following example displays the information of Ethenet interface FastEtheret 0/0.

```
Ruijie# show interface fastEthernet 0/0
Index(dec):1 (hex):1
FastEthernet 0/0 is UP  , line protocol is UP
Hardware is Nat-Semi DP83815DVNG FastEthernet, address is 0a0b.0c0d.0e0f (bia
0a0b.0c0d.0e0f)
Interface address is: 1.1.1.1/24
ARP type: ARPA,ARP Timeout: 3600 seconds
Interface IPv6 address is:
No IPv6 address
MTU 1500 bytes, BW 100000 Kbit
Encapsulation protocol is Ethernet-II, loopback not set
Keepalive interval is 10 sec , set
Carrier delay is 2 sec
Ethernet attributes:
   Medium-type is Copper
   Last link state change time: 2012-12-22 14:00:48
   Time duration since last link state change: 3 days, 2 hours, 50 minutes, 50
seconds
   Priority is 0
   Admin duplex mode is AUTO, oper duplex is Unknown
   Admin speed is AUTO, oper speed is Unknown
   Flow control admin status is OFF,flow control oper status is OFF
```

```
  Queueing strategy: FIFO
Output queue 0/40, 0 drops;
Input queue 0/75, 0 drops
Rxload is 1/255 ,Txload is 1/255
5 minutes input rate 0 bits/sec, 0 packets/sec
5 minutes output rate 0 bits/sec, 0 packets/sec
782 packets input, 88920 bytes, 0 no buffer
Received 782 broadcasts, 0 runts, 0 giants
0 input errors, 0 CRC, 0 frame, 0 overrun, 0 abort
0 packets output, 0 bytes, 0 underruns
0 output errors, 0 collisions, 1 interface resets

Ruijie#
Ruijie#show interfaces gigabitEthernet 0/0 description
Interface                      Status   Administrative Description
------------------------------- -------- -------------- -----------
GigabitEthernet 0/0             up      up           connet_to_g0/1
```

**Related Commands**

| Command | Description |
|---|---|
| **duplex** | Duplex |
| **flowcontrol** | Flow control status. |
| **interface gigabitEthernet** | Selects the interface and enter the interface configuration mode. |
| **interface aggregateport** | Creates or accesses the aggregate port, and enters the interface configuration mode. |
| **interface vlan** | Creates or accesses the switch virtual interface (SVI), and enters the interface configuration mode. |
| **shutdown** | Disables the interface. |
| **speed** | Configures the speed on the port. |
| **switchport priority** | Configures the default 802.1q interface priority. |
| **switchport protected** | Configures the interface as a protected port. |

**Platform Description** N/A

## 1.13 show interfaces link-state-change statistics

Use this command to display the link state change statistics, including the time and count.

**show interfaces** [ *interface-type interface-number* ] **link-state-change statistics**

**Parameter Description**

| Parameter | Description |
|---|---|

| | |
|---|---|
| *interface-type* *interface-number* | The interface type and ID. |

**Defaults** N/A

**Command Mode** All CLI user modes

**Usage Guide** If you do not specify an interface, the link state statistics of all interfaces are displayed.

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

```
Ruijie# show interfaces GigabitEthernet 0/1 link-state-change statistics
Interface    Link state    Link state change times     Last change time
-----------  ---------     -----------------------
-------------------
Gi 0/1       down          100                         2012-12-24
15:00:00
```

| Interface | Description |
|---|---|
| Link state | Current link state. |
| Link state change times | The count of link state change. |
| Last change time | The time when the last link state change occurs. |

**Related Commands**

| Command | Description |
|---|---|
| N/A | N/A |

**Platform Description** N/A

## 1.14 show vlans

Use this command to display the sub interface information of VLAN in privileged EXEC mode.

**show vlans** [ *VLANID* ]

**Parameter Description**

| Parameter | Description |
|---|---|
| *VLANID* | Indicates ID of a VLAN. |

**Defaults**

**Command** Any CLI mode

**Mode**

**Usage Guide** The IP MTU automatically changes to the value of the link MTU of an interface when the globally set link MTU changes.

**Configuration Examples**

```
Ruijie# show vlans
Virtual LAN ID:  3 (IEEE 802.1Q Encapsulation)
VLAN Interface FastEthernet 0/0.1
IP address: 1.1.1.1
Received:30 packets,
Transmitted: 30 packets
Virtual LAN ID:  4 (IEEE 802.1Q Encapsulation)
VLAN Interface FastEthernet 0/0.2
IP address: 1.1.2.1
Received:0 packets,
Transmitted: 0 packets
```

**Related Commands**

| Command | Description |
| --- | --- |
| N/A | N/A |

**Platform Description** N/A

## 1.15 show interfaces usage

Use this command to display bandwidth usage of the interface.
**show interfaces** [ *interface-type interface-number* ] **usage**

**Parameter Description**

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

**Defaults** N/A

**Command Mode** Any CLI mode

**Usage Guide** If you do not specify an interface, the bandwidth usage of all interfaces is displayed. Bandwidth refers to the actual link bandwidth rather than the *bandwidth* parameter configured on the interface.

**Configuration Examples** The following example displays bandwidth usage of interface GigabitEthernet 0/1.

```
Interface                    Bandwidth    Bandwidth Usage
```

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

Bandwidth refers to the interface link bandwidth, the maximum speed of link. Average Usage refers to the current usage.

**Related Commands**

| Command | Description |
| --- | --- |
| N/A | N/A |

**Platform Description** N/A

## 1.16 show interfaces counters

Use this command to display the received and transmitted packet statistics.

**show interfaces** [ *interface-type interface-number* ] **counters** [ **increment** | **error** | **rate** | **summary** ]

**Parameter Description**

| Parameter | Description |
| --- | --- |
| *interface-type interface-number* | (Optional) The interface type and ID. |
| **increment** | Displays the packet statistics increased during the last sample interval. |
| **error** | Displays error packet statistics. |
| **rate** | Displays packet receiving and transmitting rate. |
| **summary** | Displays packet statistics summary. |

**Defaults** N/A

**Command Mode** Any CLI mode

**Usage Guide** If you do not specify an interface, the packet statistics on all interfaces are displayed.

**Configuration Examples** The following example displays packet statistics on interface GigabitEthernet 0/1.

```
Ruijie#show interfaces GigabitEthernet 0/1 counters
Interface : GigabitEthernet 0/1
5 minute input rate  : 9144 bits/sec, 9 packets/sec
5 minute output rate : 1280 bits/sec, 1 packets/sec
Rxload             : 1%
InOctets           : 17310045
InPkts             : 1000(Unicast: 10%, Multicast: 10%, Broadcast: 80%)
```

```
InUcastPkts         : 100
InMulticastPkts     : 100
InBroadcastPkts     : 800
Txload             : 1%
OutOctets          : 1282535
OutPkts            : 1000(Unicast: 10%, Multicast: 10%, Broadcast: 80%)
OutUcastPkts        : 100
OutMulticastPkts    : 100
OutBroadcastPkts    : 800
Undersize packets   : 0
Oversize packets    : 0
collisions          : 0
Fragments           : 0
Jabbers            : 0
CRC alignment errors : 0
AlignmentErrors     : 0
FCSErrors           : 0
dropped packet events (due to lack of resources): 0
packets received of length (in octets):
  64:46264
  65-127: 47427
  128-255: 3478
  256-511: 658
  512-1023: 18016
  1024-1518: 125
Packet increment in last sampling interval(5 seconds):
  InOctets           : 10000
  InPkts             : 1000(Unicast: 10%, Multicast: 10%, Broadcast: 80%)
  InUcastPkts         : 100
  InMulticastPkts     : 100
  InBroadcastPkts     : 800
  OutOctets          : 10000
  OutPkts            : 1000(Unicast: 10%, Multicast: 10%, Broadcast: 80%)
  OutUcastPkts        : 100
  OutMulticastPkts    : 100
```

Rxload refers to the receive bandwidth usage and Txload refers to the Tx bandwidth usage. InPkts is the total number of receive unicast, multicast and broadcast packets. OutPkts is the total number of transmit unicast, multicast and broadcast packets.

Packet increment in last sampling interval (5 seconds) represents the packet statistics increased during the last sample interval (5 seconds).

The following example displays the packet statistics on interface GigabitEthernet 0/1 increased during the last sample interval.

```
Ruijie#show interfaces GigabitEthernet 0/1 counters increment
```

```
Interface : GigabitEthernet 0/1
Packet increment in last sampling interval(5 seconds):
  InOctets           : 10000
  InPkts             : 1000(Unicast: 10%, Multicast: 10%, Broadcast: 80%)
  InUcastPkts         : 100
  InMulticastPkts     : 100
  InBroadcastPkts     : 800
  OutOctets          : 10000
  OutPkts            : 1000(Unicast: 10%, Multicast: 10%, Broadcast: 80%)
  OutUcastPkts        : 100
  OutMulticastPkts    : 100
```

The following example displays error packet statistics on interface GigabitEthernet 0/1.

```
Ruijie#show interfaces GigabitEthernet 0/1 counters increment
Interface    UnderSize          OverSize           Collisions
Fragments
------------ -------------------- ------------------- --------------------
--------------------
Gi0/1       0                 0                 0                 0
Interface    Jabbers            CRC-Align-Err       Align-Err
FCS-Err
------------ -------------------- ------------------- --------------------
--------------------
Gi0/1       0                 0                 0                 0
```

UnderSize is the number of valid packets smaller than 64 bytes.
OverSize is the number of valid packets smaller than 1518 bytes.
Collisions is the number of colliding transmit packets.
Fragments is the number of packets with CRC error or frame alignment error which are smaller than 64 bytes.
Jabbers is the number of packets with CRC error or frame alignment error which are smaller than 1518 bytes.
CRC-Align-Err is the number of receive packets with CRC error.
Align_Err is the number of receive packets with frame alignment error.
FCS-Err is the number of receive packets with FCS error.

The following example displays packet receiving and transmitting rate on interface GigabitEthernet 0/1.

```
Ruijie#show interface gigabitEthernet 0/1 counters rate
Interface    Sampling Time        Input Rate          Input Rate
Output Rate         Output Rate
                                 (bits/sec)          (packets/sec)
(bits/sec)          (packets/sec)
------------ -------------------- ------------------- --------------------
------------------- --------------------
Gi0/1        5 seconds            23391               23
```

```
124                 0
```

Sampling Time is the time when packets are sampled. Input rate is packet receiving rate and Output rate is packet transmitting rate.

The following example displays packet statistics summary on interface GigabitEthernet 0/1.

```
Ruijie#show interface gigabitEthernet 0/1 counters summary
Interface    InOctets           InUcastPkts        InMulticastPkts
InBroadcastPkts
------------ ------------------- ------------------- --------------------
--------------------
Gi0/1        1475788005         1389               45880503
11886621
Interface    OutOctets          OutUcastPkts       OutMulticastPkts
OutBroadcastPkts
------------ ------------------- ------------------- --------------------
--------------------
Gi0/1         6667915             6382               31629
13410
```

InOctets is the total number of packets received on the interface. InUcastPkts is the number of unicast packets received on the interface. InMulticastPkts is the number of multicast packets received on the interface. InBroadcastPkts is the number of broadcast packets received on the interface.

OutOctets is the total number of packets transmitted on the interface. OutUcastPkts is the number of unicast packets transmitted on the interface. OutMulticastPkts is the number of multicast packets transmitted on the interface. OutBroadcastPkts is the number of broadcast packets transmitted on the interface.

**Related Commands**

| Command | Description |
| --- | --- |
| N/A | N/A |

**Platform Description** N/A

## 1.17 shutdown

Use this command to disable an interface. Use the **no** form of this command to enable a disabled port.

**shutdown**

**no shutdown**

**Parameter Description**

| Parameter | Description |
| --- | --- |

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

**Defaults** By default, the administrative status of an interface is Up.

**Command Mode** Interface configuration mode

**Usage Guide** Use this command to stop the forwarding on the interface (Gigabit Ethernet interface, Aggregate port or SVI). You can enable the port with the **no shutdown** command. If you shut down the interface, the configuration of the interface exists, but does not take effect. You can view the interface status by using the **show interfaces** command.

If you use the script to run no shutdown frequently and rapidly, the system may prompt the interface status reversal.

**Configuration Examples** The following example disables an interface.

```
Ruijie(config)# interface serial 1gigabitEthernet 0/1
Ruijie(config-if)# shutdown
%LINK CHANGED: Interface serial 1gigabitEthernet 0/1, changed state to
administratively down
Ruijie(config-if)# no shutdown
```

**Related Commands**

| Command | Description |
|---|---|
| **clear interface** | Resets the hardware. |
| **show interfaces** | Displays the interface information. |

**Platform Description** N/A

## 1.18 speed

Use this command to configure the speed on the port. Use the **no** form of this command to restore the default setting.

**speed** [ **10 | 100 | 1000 | auto** ]

**no speed**

**Parameter Description**

| Parameter | Description |
|---|---|
| **10** | The transmission rate of the interface is 10Mbps. |
| **100** | The transmission rate of the interface is 100Mbps. |
| **1000** | The transmission rate of the interface is 1000Mbps. |
| **auto** | Self-adaptive |

**Defaults** The default is **auto**.

**Command Mode** Interface configuration mode.

**Usage Guide** If an interface is the member of an aggregate port, the rate of the interface depends on the rate of the aggregate port. You can set the rate of the interface, but it does not take effect until the interface exits the aggregate port. Use **show interfaces** to display configuration. The rate varies by interface types. For example, you cannot set the rate of a SFP interface to 10M or 100M.

**Configuration Examples** The following example sets the speed on interface gigabitethernet 1/1 to 100Mbps.

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

**Related Commands**

| Command | Description |
| --- | --- |
| **show interfaces** | Displays the interface information. |

**Platform Description** N/A

## 1.19 snmp trap link-status

Use this command to send LinkTrap on a port. Use the **no** form of this command to disable this function.

**snmp trap link-status**

**no snmp trap link-status**

**Parameter Description**

| Parameter | Description |
| --- | --- |
| N/A | N/A |

**Defaults** This function is enabled by default

**Command Mode** Interface configuration mode.

**Usage Guide** For an interface (for instance, Ethernet interface, AP interface, and SVI interface), this command sets whether to send LinkTrap on the interface. If the function is enabled, the SNMP sends the LinkTrap when the link status of the interface changes.

**Configuration Examples** The following example disables the interface from sending LinkTrap on the interface.

```
Ruijie(config)# interface gigabitEthernet 1/1
Ruijie(config-if)# no snmp trap link-status
```

The following example enables the interface to forward Link trap.

```
Ruijie(config)# interface gigabitEthernet 1/1
Ruijie(config-if)# snmp trap link-status
```

**Related Commands**

| Command | Description |
| --- | --- |
| **snmp trap link-status** | Enables the interface to send LinkTrap on the interface. |
| **no snmp trap link-status** | Disables the interface from sending LinkTrap on the interface. |

**Platform Description** N/A

## 1.20 snmp-server if-index persist

Use this command to set the interface index persistence. The interface index remains the same after the device is restarted.

**snmp-server if-index persist**

**Parameter Description**

| Parameter | Description |
| --- | --- |
| N/A | N/A |

**Defaults** This function is disabled by default.

**Command Mode** Global configuration mode

**Usage Guide** After this command is configured, all interface indexes are saved in the configuration file. After the device is restarted, interface indexes remain the same as before.

**Configuration Examples** The following example enables the interface index persistence.

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

**Related Commands**

| Command | Description |
| --- | --- |
| N/A | N/A |

**Platform Description** N/A

# 2 MAC Address Commands

## 2.1 clear mac-address-table dynamic

Use this command to clear the dynamic MAC address.

**clear mac-address-table dynamic** [ **address** *mac-addr* [ **interface** *interface-id* ] [ **vlan** *vlan-id* ] | { [ **interface** *interface-id* ] [ **vlan** *vlan-id* ] } ]

**Parameter Description**

| Parameter | Description |
|---|---|
| **dynamic** | Clears all the dynamic MAC addresses. |
| **address** *mac-addr* | Clears the specified dynamic MAC address. |
| **interface** *interface-id* | Clears all the dynamic MAC addresses of the specified interface. |
| **vlan** *vlan-id* | Clears all the dynamic MAC addresses of the specified VLAN, in the range from 1 to 4094. |

**Defaults** N/A

**Command Mode** Privileged EXEC mode.

**Usage Guide** Use the **show mac-address-table dynamic** command to display all the dynamic MAC addresses.

**Configuration Examples** The following command clears all the dynamic MAC addresses.

```
Ruijie# clear mac-address-table dynamic
```

**Related Commands**

| Command | Description |
|---|---|
| **show mac-address-table dynamic** | Displays dynamic MAC address. |

**Platform Description** N/A

## 2.2 mac-address-table aging-time

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

**mac-address-table aging-time** *seconds*

**no mac-address-table aging-time**

**default mac-address-table aging-time**

**Parameter**

| Parameter | Description |
|---|---|

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

**Defaults** The default is 300.

**Command Mode** Global configuration mode.

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

**Configuration Examples** The following example sets the aging time of the dynamic MAC address to 500 seconds.

```
Ruijie(config)# mac-address-table aging-time 500
```

| Related Commands | Command | Description |
|---|---|---|
| | **show mac-address-table aging-time** | Displays the aging time of the dynamic MAC address. |
| | **show mac-address-table dynamic** | Displays dynamic MAC address. |

**Platform Description** N/A

## 2.3 mac-address-table filtering

Use this command to configure the filtering MAC address. Use the **no** or **default** form of the command to restore the default setting.

**mac-address-table filtering** *mac-address* **vlan** *vlan-id*

**no mac-address-table filtering** *mac-address* **vlan** *vlan-id*

**default mac-address-table filtering** *mac-address* **vlan** *vlan-id*

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

**Defaults** No filtering address is configured by default.

**Command Mode** Global configuration mode.

**Usage Guide** The filtering MAC address shall not be a multicast address.

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

```
Ruijie(config)#mac-address-table filtering 0000.0202.0303  vlan 3
```

| Related Commands | Command | Description |
|---|---|---|
| | **clear mac-address-table filtering** | Clears the filtering MAC address. |

**Platform Description** N/A

## 2.4 mac-address-table notification

Use this command to enable the MAC address notification function. Use The **no** or **default** form of the command to restore the default setting.

**mac-address-table notification** [ **interval** *value* | **history-size** *value* ]

**no mac-address-table notification** [**interval** | **history-size** ]

**default mac-address-table notification [ interval | history-size ]**

| Parameter Description | Parameter | Description |
|---|---|---|
| | **interval** *value* | Sets the interval of sending the MAC address trap message, 1 second by default. |
| | **history-size** *value* | Sets the maximum number of the entries in the MAC address notification table, 50 entries by default. |

**Defaults** By default, the interval is 1 and the maximum number of the entries in the MAC address notification table is 50.

**Command Mode** Global configuration mode.

**Usage Guide** The MAC address notification function is specific for only dynamic MAC address and secure MAC address. No MAC address trap message is generated for static MAC addresses. In the global configuration mode, you can use the **snmp-server enable traps mac-notification** command to enable or disable the switch to send the MAC address trap message.

**Configuration Examples** The following example enables the MAC address notification function.

```
Ruijie(config)# mac-address-table notification
Ruijie(config)# mac-address-table notification interval 40
Ruijie(config)# mac-address-table notification history-size 100
```

| Related Commands | Command | Description |
|---|---|---|
| | **snmp-server enable traps** | Sets the method of handling the MAC address trap message.. |
| | **show mac-address-table notification** | Displays the MAC address notification configuration and the MAC address trap notification table. |
| | **snmp trap mac-notification** | Enables the MAC address trap notification function on the specified interface. |

**Platform Description** N/A

## 2.5 mac-address-table static

Use this command to configure a static MAC address. Use the **no** or **default** form of the command to restore the default setting.

**mac-address-table static** *mac-addr* **vlan** *vlan-id* **interface** *interface-id*

**no mac-address-table static** *mac-addr* **vlan** *vlan-id* **interface** *interface-id*

**default mac-address-table static** *mac-addr* **vlan** *vlan-id* **interface** *interface-id*

**Parameter Description**

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

**Defaults** No static MAC address is configured by default.

**Command Mode** Global configuration mode.

**Usage Guide** A static MAC address has the same function as the dynamic MAC address that the switch learns. Compared with the dynamic MAC address, the static MAC address will not be aged out. It can only be configured and removed by manual. Even if the switch is reset, the static MAC address will not be lost. A static MAC address shall not be configured as a multicast address. Use **show mac-address-table static** to display the static MAC address.

**Configuration Examples** N/A

**Related Commands**

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

**Platform Description** N/A

## 2.6 show mac-address-learning

Use this command to display the MAC address learning.

**show mac-address-learning**

**Parameter Description**

| Parameter | Description |
|---|---|
| N/A | N/A |

**Defaults** N/A

**Command Mode** All modes.

**Usage Guide** N/A

**Configuration Examples** The following example displays the MAC address learning.

```
Ruijie# show mac-address-learning
GigabitEthernet 0/0     learning ability: disable
GigabitEthernet 0/1     learning ability: enable
GigabitEthernet 0/2     learning ability: enable
GigabitEthernet 0/3     learning ability: enable
```

**Related Commands**

| Command | Description |
|---|---|
| N/A | N/A |

**Platform Description** N/A

## 2.7 show mac-address-table

Use this command to display all types of MAC addresses (including dynamic address, static address and filter address).

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

**Parameter Description**

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

**Defaults** N/A

**Command Mode** All modes

**Usage Guide** N/A

**Configuration Examples** The following example displays the MAC address.

```
Ruijie# show mac-address-table address 00d0.f800.1001
Vlan       MAC Address         Type     Interface
-------    ------------      --------   --------
```

```
1          00d0.f800.1001      STATIC  GigabitEthernet 1/1
```

| Field | Description |
|---|---|
| Vlan | The interface address. |
| MAC Address | The MAC address. |
| Type | The MAC address type. |
| Interface | The interface corresponding to the MAC address. |

| Related Commands | Command | Description |
|---|---|---|
| | N/A | N/A |

**Platform Description** N/A

## 2.8 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** All modes.

**Usage Guide** N/A

**Configuration Examples** The following example displays the aging time of the dynamic MAC address.

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

| Related Commands | Command | Description |
|---|---|---|
| | **mac-address-table aging-time** | Sets the aging time of the dynamic MAC address. |

**Platform Description** N/A

## 2.9 show mac-address-table count

Use this command to display the number of address entries in the address table.

**show mac-address-table count** [ **interface** *interface-id* **| vlan** *vlan-id* ]

**Parameter Description**

| Parameter | Description |
|---|---|
| **interface** *interface-id* | Interface ID |
| **vlan** *vlan-id* | VLAN ID, in the range from 1 to 4094. |

**Defaults** N/A

**Command Mode** Privileged EXEC mode.

**Usage Guide** The **show mac-address-table count** command is used to display the number of entries based on the type of MAC address entry.
The **show mac-address-table count interface** command is used to display the number of entries based on the interface associated with the MAC address entry.
The **show mac-address-table count vlan** command is used to display the number of entries based on the VLAN of MAC address entries.

**Configuration Examples** The following example displays the number of MAC address entries.

```
Ruijie# show mac-address-table count
Dynamic Address Count : 51
Static Address Count : 0
Filter Address Count : 0
Total Mac Addresses  : 51
Total Mac Address Space Available: 8139
```

The following example displays the number of MAC address in VLAN 1.

```
Ruijie# show mac-address-table count vlan 1
Dynamic Address Count : 7
Static Address Count : 0
Filter Address Count : 0
Total Mac Addresses   : 7
```

The following example displays the number of MAC addresses on interface g0/1.

```
Ruijie# show mac-address-table interface g0/1
Dynamic Address Count : 10
Static Address Count : 0
Filter Address Count : 0
Total Mac Addresses   : 10
```

**Related Commands**

| Command | Description |
|---|---|
| **show mac-address-table static** | Displays the static address. |
| **show mac-address-table filtering** | Displays the filtering address. |
| **show mac-address-table dynamic** | Displays the dynamic address. |
| **show mac-address-table address** | Displays all the address information of the specified address. |

| | |
|---|---|
| **show mac-address-table interface** | Displays all the address information of the specified interface. |
| **show mac-address-table vlan** | Displays all the address information of the specified vlan. |

**Platform Description** N/A

## 2.10 show mac-address-table dynamic

Use this command to display the dynamic MAC address.

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

**Parameter Description**

| Parameter | Description |
|---|---|
| *mac-addr* | Destination MAC address of the entry |
| *vlan-id* | VLAN of the entry, in the range from 1 to 4094. |
| *interface-id* | Interface that the packet is forwarded to.<br>It may be a physical port or an aggregate port |

**Defaults**

**Command Mode** All modes.

**Usage Guide** N/A

**Configuration Examples** The following example displays the dynamic MAC address.

```
Ruijie# show mac-address-table dynamic
Vlan   MAC Address     Type   Interface
------------------------- -------- --------------------
1   0000.0000.0001    DYNAMIC gigabitethernet 1/1
1   0001.960c.a740    DYNAMIC gigabitethernet 1/1
1   0007.95c7.dff9    DYNAMIC gigabitethernet 1/1
1   0007.95cf.eee0    DYNAMIC gigabitethernet 1/1
1   0007.95cf.f41f    DYNAMIC gigabitethernet 1/1
1   0009.b715.d400    DYNAMIC gigabitethernet 1/1
1   0050.bade.63c4    DYNAMIC gigabitethernet 1/1
```

**Related Commands**

| Command | Description |
|---|---|
| **clear mac-address-table dynamic** | Clears the dynamic MAC address. |

**Platform Description** N/A

## 2.11 show mac-address-table filtering

Use this command to display the filtering MAC address.

**show mac-address-table filtering** [ **ddr** *mac-addr* ] [ **vlan** *vlan-Id* ]

**Parameter Description**

| Parameter | Description |
|---|---|
| *mac-addr* | Destination MAC address of the entry |
| *vlan-id* | VLAN ID of the entry, in the range from 1 to 4094. |

**Defaults** N/A

**Command Mode** Privileged EXEC mode.

**Usage Guide** N/A

**Configuration Examples** The following example displays the filtering MAC address.

```
Ruijie# show mac-address-table filtering
Vlan    MAC Address    Type   Interface
------- ----------------- ------- -----------
 1    0000.2222.2222   FILTER Not available
```

**Related Commands**

| Command | Description |
|---|---|
| **mac-address-table filtering** | Configures the filtering MAC address. |

**Platform Description** N/A

## 2.12 show mac-address-table interface

Use this command to display all the MAC addresses on the specified interface including static and dynamic MAC address

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

**Parameter Description**

| Parameter | Description |
|---|---|
| *interface-id* | Displays the MAC address information of the specified Interface (physical interface or aggregate port). |
| *vlan-id* | VLAN ID of the entry, in the range from 1 to 4094.. |

**Defaults** N/A

**Command Mode** Privileged EXEC mode.

**Usage Guide** N/A

**Configuration Examples** The following example displays all the MAC addresses on interface gigabitethernet 1/1.

```
Ruijie# show mac-address-table interface
gigabitethernet 1/1
Vlan  MAC Address  Type   Interface
----- ------------- -------- ----------------
1   00d0.f800.1001 STATIC  gigabitethernet 1/1
1   00d0.f800.1002 STATIC  gigabitethernet 1/1
1   00d0.f800.1003 STATIC  gigabitethernet 1/1
1   00d0.f800.1004 STATIC  gigabitethernet 1/1
```

**Related Commands**

| Command | Description |
|---|---|
| **show mac-address-table static** | Displays the static MAC address. |
| **show mac-address-table filtering** | Displays the filtering MAC address. |
| **show mac-address-table dynamic** | Displays the dynamic MAC address. |
| **show mac-address-table address** | Displays all types of MAC addresses. |
| **show mac-address-table vlan** | Displays all types of MAC addresses of the specified VLAN. |
| **show mac-address-table count** | Displays the address counts in the MAC address table. |

**Platform Description** N/A

## 2.13 show mac-address-table notification

Use this command to display the MAC address notification configuration and the MAC address notification table.

**show mac-address-table notification** [ **interface** [ *interface-id* ] | **history** ]

**Parameter Description**

| Parameter | Description |
|---|---|
| **interface** | Displays the MAC address notification configuration on all interfaces. |
| **interface** *interface-id* | Displays the MAC address notification configuration on a specific interface. |
| **history** | Displays the MAC address notification history. |

**Defaults**

**Command Mode** Privileged EXEC mode.

**Usage Guide** N/A

**Configuration Examples** The following example displays the MAC address notification configuration globally.

```
Ruijie#show mac-address-table notification
MAC Notification Feature : Enabled
Interval(Sec): 300
Maximum History Size : 50
Current History Size : 0
```

**Related Commands**

| Command | Description |
|---|---|
| **mac-address-table notification** | Enables MAC address notification. |
| **snmp trap mac-notification** | Enables the MAC address trap notification function on the specified interface. |

**Platform Description** N/A

## 2.14 show mac-address-table static

Use this command to display the static MAC address.

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

**Parameter Description**

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

**Defaults** N/A

**Command Mode** Privileged EXEC mode.

**Usage Guide** N/A

**Configuration Examples** The following example displays the static MAC addresses

```
Ruijie# show mac-address-table static
Vlan    MAC Address     Type   Interface
---------- -------------------- -------- ---------
1  00d0.f800.1001  STATIC  gigabitethernet 1/1
1  00d0.f800.1002  STATIC  gigabitethernet 1/1
1  00d0.f800.1003  STATIC  gigabitethernet 1/1
```

**Related Commands**

| Command | Description |
|---|---|
| **mac-address-table static** | Configures the static MAC address. |

**Platform Description** N/A

## 2.15 show mac-address-table vlan

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

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

| **Parameter Description** | **Parameter** | **Description** |
|---|---|---|
| | *vlan-id* | VLAN ID of the entry, within the range from 1 to 4094. |

**Defaults** N/A

**Command Mode** Privileged EXEC mode

**Usage Guide** N/A

**Configuration Examples** The following example displays all addresses of the specified VLAN.

```
Ruijie# show mac-address-table vlan 1
Vlan  MAC Address    Type    Interface
----- -------------  ------- ------------------
1   00d0.f800.1001  STATIC  gigabitethernet 1/1
1   00d0.f800.1002  STATIC  gigabitethernet 1/1
1   00d0.f800.1003  STATIC  gigabitethernet 1/1
```

| **Related Commands** | **Command** | **Description** |
|---|---|---|
| | **show mac-address-table static** | Displays static addresses. |
| | **show mac-address-table filtering** | Displays filtered addresses. |
| | **show mac-address-table dynamic** | Displays dynamic addresses. |
| | **show mac-address-table address** | Displays all address information about the specified address. |
| | **show mac-address-table interface** | Displays all address information about the specified interface. |
| | **show mac-address-table count** | Displays the number of addresses in the address table. |

**Platform Description** N/A

## 2.16 snmp trap mac-notification

Use this command to enable the MAC address trap notification on the specified interface. Use The **no**

or **default** form of the command to restore the default setting.

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

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

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

**Parameter Description**

| Parameter | Description |
|---|---|
| *added* | Notifies when a MAC address is added. |
| *removed* | Notifies when a MAC address is removed |

**Defaults**

**Command Mode** Interface configuration mode.

**Usage Guide** Use **show mac-address-table notification interface** to display configuration.

**Configuration Examples** The following example enables the MAC address trap notification on interface gigabitethernet 1/1.

```
Ruijie(config)# interface gigabitethernet 1/1
Ruijie(config-if)# snmp trap mac-notification added
```

**Related Commands**

| Command | Description |
|---|---|
| **mac-address-table notification** | Enables MAC address notification. |
| **show mac-address-table notification** | Displays the MAC address notification configuration and the MAC address notification table. |

**Platform Description** N/A

# 3 VLAN Commands

## 3.1 name

Use this command to specify the name of a VLAN. Use the **no** or **default** form of this command to restore the default setting.

**name** *vlan-name*

**no name**

**default name**

**Parameter Description**

| Parameter | Description |
|---|---|
| *vlan-name* | VLAN name |

**Defaults** The default name of a VLAN is the combination of “VLAN” and VLAN ID, for example, the default name of the VLAN 2 is “VLAN0002”.

**Command mode** VLAN configuration Mode.

**Usage Guide** N/A

**Configuration Examples** The following example sets the name of VLAN to 10.

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

**Related Commands**

| Command | Description |
|---|---|
| **show vlan** | Displays member ports of the VLAN. |

**Platform Description** N/A

## 3.2 show vlan

Use this command to display member ports of the VLAN.

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

**Parameter**

| Parameter | Description |
|---|---|

**Description**

| | |
|---|---|
| *vlan-id* | VLAN ID |

**Defaults** N/A

**Command mode** All modes

**Usage Guide** N/A

**Configuration Examples** The following command displays the status of VLAN 1.

```
Ruijie(config-vlan)#show vlan id 20
VLAN Name                            Status    Ports
---- -------------------------------- ---------
-----------------------------------
  20 VLAN0020                         STATIC    Gi0/1
```

The following command displays the status of all VLANs.

```
Ruijie(config-vlan)#show vlan
VLAN Name                            Status    Ports
---- -------------------------------- --------- -----------------------------------
   1 VLAN0001                         STATIC    Gi0/1, Gi0/2, Gi0/4, Gi0/5
                                                Gi0/6, Gi0/7, Gi0/8, Gi0/9
                                                Gi0/10, 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
   2 VLAN0002                         STATIC    Gi0/1
  20 VLAN0020                         STATIC    Gi0/1
```

**Related Commands**

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

**Platform Description** N/A

## 3.3 vlan

Use this command to enter the VLAN configuration mode. Use the **no** or **default** form of this command to restore the default setting.

**vlan** { *vlan-id* | **range** *vlan-range* }

**no vlan** { *vlan-id* | **range** *vlan-range* }

**default vlan** { *vlan-id* | **range** *vlan-range* }

**Parameter Description**

| Parameter | Description |
| --- | --- |
| *vlan-id* | VLAN ID<br>Default VLAN (VLAN 1) cannot be removed. |
| *vlan-range* | VLAN ID range. |

**Defaults** The default is static VLAN.

**Command mode** Global configuration mode.

**Usage Guide** N/A

**Configuration Examples** The following example creates VLAN 10.

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

**Related Commands**

| Command | Description |
| --- | --- |
| **show vlan** | Displays member ports of the VLAN. |

**Platform Description** N/A

# 4 MAC VLAN Commands

## 4.1 show mac-vlan

Use this command to display the MAC VLAN entries.

**show mac-vlan** { **all** | **vlan** *vlan-id* | **mac-address** *mac-address* }

**Parameter Description**

| Parameter | Description |
|---|---|
| **all** | Displays all MAC VLAN entries. |
| **mac-address mac-address** | Displays the MAC VLAN entry of the specified MAC address. |
| **vlan** vlan-id | Displays the MAC VLAN entries of the specified VLAN. |

**Defaults** N/A

**Command mode** All configuration modes

**Usage Guide** N/A

**Configuration Examples** The following example displays all MAC VLAN entries.

```
Ruijie# show mac-vlan all
The following MAC VLAN addresses exist:

MAC ADDR          VLAN ID
-------------------------------------------------------
0011.1100.0000     100
0022.2222.0000     200
0000.0000.0003     300
0000.0000.0004     400
0000.0000.0005     500
0000.0000.0006     600
0000.0000.0007     700
Total MAC VLAN address count: 7
```

**Related Commands**

| Command | Description |
|---|---|
| N/A | N/A |

**Platform Description** N/A

# 5 VLAN Group Commands

## 5.1 vlan-assign-mode

Use this command to set the VLAN assignment mode.

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

**vlan-assign-mode** *dot1x*

**no vlan-assign-mode**

**Parameter Description**

| Parameter | Description |
|---|---|
| **dot1x** | Indicates that the authentication server assigns VLANs to users that pass the 802.1x authentication. |

**Defaults**

No VLAN assignment mode is specified by default.

**Configuration Mode**

VLAN group configuration mode/Global configuration mode

**Usage Guide**

The VLAN assignment mode configured in global configuration mode takes effect on all VLAN groups.

The VLAN assignment mode configured in VLAN group configuration mode takes effect only on the specified VLAN group.

The configuration of VLAN assignment mode in VLAN group configuration mode has higher priority than that configured in global configuration mode.

**Configuration Examples**

The following example configures the dot1x-based VLAN assignment mode for VLAN group 10.

```
Ruijie(config)# vlan-group 10
Ruijie(config-vlan-group)# vlan-assign-mode dot1x
```

**Related Commands**

| Command | Description |
|---|---|
| **show vlan-group** [*group-id*] | Displays the VLAN group configuration. |

**Platform Description**

N/A

## 5.2 vlan-group

Use this command to create a VLAN group on an AP or AC device.

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

**vlan-group** *group-id*

**no vlan-group** *group-id*

**Parameter Description**

| Parameter | Description |
| --- | --- |
| *group-id* | VLAN group ID. The range is from 1 to 128. |

**Defaults** N/A

**Configuration Mode** Global configuration mode

**Usage Guide** N/A

**Configuration Examples** The following example creates VLAN group 100 on a device.

```
Ruijie# configure terminal
Ruijie(config)# vlan-group 100
Ruijie(config-vlan-group)#
```

**Related Commands**

| Command | Description |
| --- | --- |
| **show vlan-group** [*group-id*] | Displays the VLAN group configuration. |

**Platform Description** N/A

## 5.3 default-vlan

Use this command to configure a default VLAN.

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

**default-vlan** *vlan-id*

**no default-vlan** *vlan-id*

**Parameter Description**

| Parameter | Description |
| --- | --- |
| *vlan-id* | Specifies a VLAN ID, which should be in the VLAN group list. |

**Defaults** The default VLAN is not configured by default.

**Configuration Mode** VLAN group configuration mode

**Usage Guide** The default VLAN must be in the VLAN group list.

The default VLAN takes effect only in the 802.1x authentication server VLAN assignment

mode.

**Configuration Examples**

The following example sets VLAN 10 to the default VLAN of VLAN group 100.

```
Ruijie# configure terminal
Ruijie(config)# vlan-group 100
Ruijie(config-vlan-group)# default-vlan 10
```

**Related Commands**

| Command | Description |
|---|---|
| **show vlan-group** [*group-id*] | Displays the VLAN group configuration. |

**Platform Description**

N/A

## 5.4 vlan-list

Use this command to configure the VLAN list for a VLAN group on an AP .

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

**vlan-list** *vlan-list*

**no vlan-list**

**Parameter Description**

| Parameter | Description |
|---|---|
| *vlan-list* | Specifies a VLAN list for a VLAN group. A VLAN group includes up to 128 VLANs. |

**Defaults**

No VLAN list is configured by default.

**Configuration Mode**

VLAN group configuration mode

**Usage Guide**

If a WLAN needs to associate multiple VLANs, you can use this command to configure these VLANs to a VLAN group, and then associate the VLAN group with the WLAN.

**Configuration Examples**

The following example adds VLANs 100-105 to VLAN group 100.

```
Ruijie# configure terminal
Ruijie(config)# vlan-group 100
Ruijie(config-vlan-group)# vlan-list 100-105
```

**Related Commands**

| Command | Description |
|---|---|
| **show vlan-group** [*group-id*] | Displays the VLAN group configuration. |

**Platform Description** N/A

## 5.5 vlan-group

Use this command to create a VLAN group in WLAN configuration mode on an AP device.
**vlan-group** *group-id*

**Parameter Description**

| Parameter | Description |
|---|---|
| *group-id* | VLAN group ID. The range is from 1 to 128. |

**Defaults** The WLAN is not associated with any VLAN group by default.

**Configuration Mode** WLAN configuration mode

**Usage Guide** N/A

**Configuration Examples** The following example associates WLAN 1 with VLAN group 100.

```
Ruijie# configure terminal
Ruijie(config)# dot11 wlan 1
Ruijie(dot11-wlan-config)# vlan-group 100
```

**Related Commands**

| Command | Description |
|---|---|
| N/A | N/A |

**Platform Description** N/A

## 5.6 encapsulation dot1Q

Use this command to configure encapsulation for a VLAN or VLAN group on the dot11 radio sub-interface of an AP.
Use the **no** form of this command to remove the configuration.
**encapsulation dot1Q** [**group**] {*vlan-id* | *vlan-group-id*}
**no encapsulation dot1Q** [**group**] {*vlan-id* | *vlan-group-id*}

**Parameter Description**

| Parameter | Description |
|---|---|
| *vlan -id* | Specifies a VLAN ID. |
| *vlan-group-id* | VLAN group ID. The range is from 1 to 128. |

**Defaults** Packets of a VLAN or VLAN group are not encapsulated.

**Configuration Mode** Interface configuration mode

**Usage Guide** Use the **encapsulation dot1Q** *vlan-id* command to configure VLAN encapsulation on a dot1q sub-interface..
Use the **encapsulation dot1Q group** *vlan-group-id* command to configure VLAN group encapsulation on a dot1q sub-interface..

**Configuration Examples** The following example configures encapsulation for VLAN group 100 on the sub-interface **Dot11radio 1/0.1** on an AP:

```
Ruijie# configure terminal
Ruijie(config)# interface dot11radio 1/0.1
Ruijie(config-subif)# encapsulation dot1Q group 100
```

**Related Commands**

| Command | Description |
|---|---|
| N/A | N/A |

**Platform Description** N/A

## 5.7 show vlan-group

Use this command to display the VLAN group configuration on an AP.
**show vlan-group** [*group-id*]

**Parameter Description**

| Parameter | Description |
|---|---|
| *group-id* | Specifies the ID of a VLAN group. |

**Defaults** N/A

**Configuration Mode** Privileged EXEC mode

**Usage Guide** N/A

**Configuration Examples** The following example displays information about VLANs in the VLAN group on an AP:

```
Ruijie# show vlan-group
VLAN-Group ID   Default VLAN  Assign-Mode       VLAN-List
--------- ----------- ----------------  ----------------------------
128           NA          dot1x              110-130, 141-150
```

**Related Commands**

| Command | Description |
| --- | --- |
| N/A | N/A |

**Platform Description**

N/A

# 6 LLDP Commands

## 6.1 civic-location

Use this command to configure a common LLDP address. Use the **no** form of this command to delete the address.

**civic-location** { **country | state | county | city | division | neighborhood | street-group | leading-street-dir | trailing-street-suffix | street-suffix | number | street-number-suffix | landmark | additional-location-information | name | postal-code | building | unit | floor | room | type-of-place | postal-community-name | post-office-box | additional-code** } *ca-word*

**no civic-location** { **country | state | county | city | division | neighborhood | street-group | leading-street-dir | trailing-street-suffix | street-suffix | number | street-number-suffix | landmark | additional-location-information | name | postal-code | building | unit | floor | room | type-of-place | postal-community-name | post-office-box | additional-code** } *ca-word*

**Parameter Description**

| Parameter | Description |
|---|---|
| **country** | Country code, two bytes. For example, the country code of China is CH. |
| **state** | Address information, CA type 1 |
| **county** | CA type 2 |
| **city** | CA type 3 |
| **division** | CA type 4 |
| **neighborhood** | CA type 5 |
| **street-group** | CA type 6 |
| **leading-street-dir** | CA type 16 |
| **trailing-street-suffix** | CA type 17 |
| **street-suffix** | CA type 18 |
| **number** | CA type 19 |
| **street-number-suffix** | CA type 20 |
| **landmark** | CA type 21 |
| **additional-location-information** | CA type 22 |
| **name** | CA type 23 |
| **postal-code** | CA type 24 |
| **building** | CA type 25 |
| **unit** | CA type 26 |
| **floor** | CA type 27 |
| **room** | CA type 28 |
| **type-of-place** | CA type 29 |
| **postal-community-name** | CA type 30 |

| | |
|---|---|
| **post-office-box** | CA type 31 |
| **additional-code** | CA type 32 |
| *ca-word* | Address information |

**Defaults** N/A

**Command Mode** LLDP Civic address configuration mode

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

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

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

**Related Commands**

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

**Platform Description** N/A

## 6.2 clear lldp statistics

Use this command to clear LLDP statistics.

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

**Parameter Description**

| Parameter | Description |
|---|---|
| *interface-name* | Interface name |

**Defaults** N/A

**Command Mode** Privileged EXEC mode

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

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

```
Ruijie# clear lldp statistics interface GigabitEthernet 0/1
Ruijie# show lldp statistics interface GigabitEthernet 0/1
Lldp statistics information of port [GigabitEthernet 0/1]
```

```
-------------------------------------------------------------
The number of lldp frames transmitted  : 0
The number of frames discarded    : 0
The number of error frames     : 0
The number of lldp frames received   : 0
The number of TLVs discarded    : 0
The number of TLVs unrecognized    : 0
The number of neighbor information aged out : 0
```

| Related Commands | Command | Description |
|---|---|---|
| | N/A | N/A |

**Platform Description** N/A

## 6.3 clear lldp table

Use this command to clear LLDP neighbor information.

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

| Parameter Description | Parameter | Description |
|---|---|---|
| | *interface-name* | Interface name |

**Defaults** N/A

**Command Mode** Privileged EXEC mode

**Usage Guide** If the **interface** parameter is specified, the LLDP neighbor information on the specified interface is cleared.

If the **interface** parameter is not specified, the LLDP neighbor information on all interfaces is cleared.

**Configuration Examples** The following example clears the LLDP neighbor information on interface 1.

```
Ruijie# show lldp neighbors interface GigabitEthernet 0/1
Capability codes:
    (R) Router, (B) Bridge, (T) Telephone, (C) DOCSIS Cable Device
    (W) WLAN Access Point, (P) Repeater, (S) Station, (O) Other
System Name                Local Intf          Port ID                Capability
Aging-time

Total entries displayed: 0
Ruijie# clear lldp table interface GigabitEthernet 0/1
Ruijie# show lldp neighbors interface GigabitEthernet 0/1
```

| Related Commands | Command | Description |
|---|---|---|
| | N/A | N/A |

**Platform Description** N/A

## 6.4 device-type

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

**device-type** *device-type*

**no device-type**

| Parameter Description | Parameter | Description |
|---|---|---|
| | *device-type* | Device type. The value ranges from 0 to 2.<br>0: The device type is DHCP Server.<br>1: The device type is switch.<br>2: The device type is LLDP MED terminal. |

**Defaults**

**Command Mode** LLDP Civic address configuration mode

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

**Configuration Examples** The following example sets the device type to switch.

```
Ruijie#config
Ruijie(config)# lldp location civic-location identifier 1
Ruijie(config-lldp-civic)# device-type 1
```

| Related Commands | Command | Description |
|---|---|---|
| | **show lldp location civic-location** { **identifier** *id* **\| interface** *interface-name* **\| static** } | Displays LLDP Civic Address information. |

**Platform Description** N/A

## 6.5 lldp enable

Use this command to enable the LLDP globally or on the interface. Use **no** form of this command to disable this function.

**lldp enable**

**no lldp enable**

| Parameter Description | Parameter | Description |
|---|---|---|
| | N/A | N/A |

**Defaults** This function is enabled by default.

**Command Mode** Global (or interface) configuration mode

**Usage Guide** LLDP takes effect on an interface only when LLDP is enabled globally.

**Configuration Examples** The following example disables LLDP globally and on the interface.

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

| Related Commands | Command | Description |
|---|---|---|
| | **show lldp status** | Displays LLDP status information. |

**Platform Description** N/A

## 6.6 lldp encapsulation snap

Use this command to configure the encapsulation format of LLDP packets. Use the **no** form of this command to restore the default setting.

**lldp encapsulation snap**

**no lldp encapsulation snap**

| Parameter Description | Parameter | Description |
|---|---|---|
| | N/A | N/A |

**Defaults** By default, Ethernet II encapsulation format is used.

**Command Mode** Interface configuration mode.

**Usage Guide**

To guarantee the normal communication between local device and neighbor device, the same LLDP packet encapsulation format must be used.

**Configuration Examples** The following example sets LLDP packet encapsulation format to SNAP.

```
Ruijie#config
Ruijie(config)#interface gigabitethernet 0/1
Ruijie(config-if)#lldp encapsulation snap
```

**Related Commands**

| Command | Description |
| --- | --- |
| **show lldp status** | Displays LLDP status information. |

**Platform Description** N/A

## 6.7 lldp error-detect

Use this command to configure the LLDP error detection, including the detection of VLAN configurations on both sides of the link, port state detection, port aggregation configuration detection, MTU configuration detection and loop detection. If any error is detected by LLDP, warning message will be printed to notify the administrator. Use the **no** form of this command to disable this function.

**lldp error-detect**

**no lldp error-detect**

**Parameter Description**

| Parameter | Description |
| --- | --- |
| N/A | N/A |

**Defaults** This function is enabled by default.

**Command Mode** Interface configuration mode.

**Usage Guide** LLDP error detection relies on the specific TLV in the LLDP packets exchanged between devices on both sides of the link. To ensure normal functioning of the detection feature, correct TLVs must be advertised.

**Configuration Examples** The following example configures LLDP error detection.

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

**Related Commands**

| Command | Description |
| --- | --- |
| **show interface status** | Displays LLDP status information. |

**Platform Description** N/A

## 6.8 lldp fast-count

When a new neighbor is detected or when LLDP operating mode changes from shutdown or Rx to TxRx or Tx, to allow the neighbor device to quickly study the information about this device, the fast sending mechanism will be initiated. The fast sending mechanism shortens the LLDPDU sending interval to 1 second and continuously transmits a certain number of LLDPDUs before restoring to the normal transmit interval. Use the **no** form of this command to restore the default setting.

**lldp fast-count** *value*

**no lldp fast-count**

**Parameter Description**

| Parameter | Description |
|---|---|
| *value* | The number of fast sent LLDP packets, in the range from 1 to 10. |

**Defaults** The default is 3.

**Command Mode** Global configuration mode.

**Usage Guide** N/A

**Configuration Examples** The following example sets the number of fast sent LLDP packets to 5.

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

**Related Commands**

| Command | Description |
|---|---|
| **show interface status** | Displays LLDP status information. |

**Platform Description** N/A

## 6.9 lldp hold-multiplier

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

**lldp hold-multiplier** *value*

**no lldp hold-multiplier**

**Parameter Description**

| Parameter | Description |
|---|---|
| *value* | TTL multiplier, in the range from 2 to 10. |

**Defaults** The default is 4.

**Command** Global configuration mode.

**Mode**

**Usage Guide** The value of Time To Live (TLV) in LLDP packet = TTL multiplier × LLDP packet transmit interval + 1. Therefore, the TTL of local device information on the neighbor device can be controlled by adjusting TTL multiplier.

**Configuration Examples** The following example sets TTL multiplier to 5.

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

**Related Commands**

| Command | Description |
|---|---|
| **show lldp status** | Displays LLDP status information. |

**Platform Description** N/A

## 6.10 lldp location civic-location identifier

Use this command to create a common address of a device connected to the network in LLDP Civic Address configuration mode. Use the **no** form of this command to delete the address.

**lldp location civic-location identifier** *id*

**no lldp location civic-location identifier** *id*

**Parameter Description**

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

**Defaults** N/A

**Command Mode** Global configuration mode

**Usage Guide** This command can be used to enter the LLDP Civic Address configuration mode.

**Configuration Examples** The following example creates the Civic Address information in LLDP MED-TLV as follows: set *id* to **1**.

```
Ruijie#config
Ruijie(config)#lldp location civic-location identifier 1
Ruijie(config-lldp-civic)#
```

**Related Commands**

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

**Platform** N/A

**Description**

## 6.11 lldp location elin identifier

Use this command to set an emergency number encapsulated in a Location Identification TLV. Use the **no** form of this command to delete the number.

**lldp location elin identifier** *id* **elin-location** *tel-number*

**no lldp location elin identifier** *id*

**Parameter Description**

| Parameter | Description |
|---|---|
| *id* | ID of an emergency number, in the range from 1 to 1024. |
| *tel-number* | Emergency number, in the range from 10 to 25 bytes. |

**Defaults** N/A

**Command Mode** Global configuration mode

**Usage Guide** This command is used to configure an emergency number.

**Configuration Examples** The following example sets an emergency number.

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

**Related Commands**

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

**Platform Description** N/A

## 6.12 lldp management-address-tlv

Use this command to configure the management address advertised in LLDP packets. Use the **no** form of this command to disable the advertisement of management address.

**lldp management-address-tlv** [ *ip-address* ]

**no lldp management-address-tlv**

**Parameter Description**

| Parameter | Description |
|---|---|
| *ip-address* | The management address advertised in LLDP packets. |

**Defaults** N/A

**Command Mode** Interface configuration mode.

**Usage Guide** By default, the management address is advertised in LLDP packets, and is the IPv4 address of the lowest-ID VLAN carried on the port. If IPv4 address is not configured for this VLAN, the next lowest-ID VLAN carried on the port will be tried until the IPv4 address is obtained.
If the IPv4 address is still not found, the IPv6 address of the lowest-ID VLAN carried on the port will be tried.
If the IPv6 address is still not found, the MAC address of the device will be advertised as the management address.

**Configuration Examples** The following example configures the management address advertised in LLDP packets to 192.168.1.1.

```
Ruijie#config
Ruijie(config)#interface gigabitethernet 0/1
Ruijie(config-if)#lldp management-address-tlv 192.168.1.1
```

**Related Commands**

| Command | Description |
|---|---|
| **show lldp local-information** | Displays LLDP local information |

**Platform Description** N/A

## 6.13 lldp mode

Use this command to configure the LLDP operating mode. Use **no** form of this command to restore the default setting.
**lldp mode** { **rx** | **tx** | **txrx** }
**no lldp mode**

**Parameter Description**

| Parameter | Description |
|---|---|
| **rx** | Only sends LLDPDUs. |
| **tx** | Only receives LLDPDUs. |
| **txrx** | Sends and receives LLDPDUs. |

**Defaults** The default is **txrx**.

**Command Mode** Interface configuration mode

**Usage Guide** Disable LLDP operating mode on the interface. The interface won't send and receive LLDP packets. The precondition for enabling LLDP on the interface is that LLDP has been enabled globally and LLDP operates in tx, rx or txrx mode.

**Configuration Examples** The following example sets LLDP operating mode to tx on the interface.

```
Ruijie#config
Ruijie(config)#interface gigabitethernet 0/1
Ruijie(config-if)#lldp mode tx
```

**Related Commands**

| Command | Description |
|---|---|
| **show lldp status** | Displays LLDP status information |

**Platform Description** N/A

## 6.14 lldp network-policy profile

Use this command to create an LLDP network policy and enter the LLDP network policy configuration mode. Use the no form of this command to delete the policy.

**lldp network-policy profile** *profile-num*

**no lldp network-policy profile** *profile-num*

**Parameter Description**

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

**Defaults** N/A

**Command Mode** Global configuration mode

**Usage Guide** This command is used to enter the LLDP network policy configuration mode. When this command is run, the policy ID must be specified.

In LLDP network-policy mode, the { **voice** | **voice-signaling** } **vlan** command can be used to configure the specific network policy.

**Configuration Examples** The following example creates an LLDP network policy whose ID is 1.

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

**Related Commands**

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

**Platform Description** N/A

## 6.15 lldp notification remote-change enable

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

**lldp notification remote-change enable**

**no lldp notification remote-change enable**

**Parameter Description**

| Parameter | Description |
|---|---|
| N/A | N/A |

**Defaults** This function is disabled by default.

**Command Mode** Interface configuration mode.

**Usage Guide** By configuring LLDP Trap, the LLDP information of local device (such as information about the detection of new neighbor or the fault on the communication link) can be sent to the network management server. The administrator can monitor the network operation status according to such information.

**Configuration Examples** The following example configures LLDP Trap.

```
Ruijie#config
Ruijie(config)#interface gigabitethernet 0/1
Ruijie(config-if)#lldp notification remote-change enable
```

**Related Commands**

| Command | Description |
|---|---|
| **show lldp status** | Displays LLDP status information. |

**Platform Description** N/A

## 6.16 lldp timer notification-interval

Use this command to set an interval of sending LLDP Traps. Use the **no** form of this command to restore the default setting.

**lldp timer notification-interval** *seconds*

**no lldp timer notification-interval**

**Parameter Description**

| Parameter | Description |
|---|---|
| *seconds* | Interval of sending LLDP Traps, in the range from 5 to 3600 in the unit of seconds. |

**Defaults** The default is 5.

**Command Mode** Global configuration mode.

**Usage Guide** To prevent excessive LLDP traps from being sent, you can set an interval of sending LLDP Traps. If LLDP information change is detected during this interval, traps will be sent to the network management server.

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

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

**Related Commands**

| Command | Description |
| --- | --- |
| **show lldp status** | Displays LLDP status information. |

**Platform Description** N/A

## 6.17 lldp timer reinit-delay

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

**lldp timer reinit-delay** *seconds*

**no lldp timer reinit-delay**

**Parameter Description**

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

**Defaults** The default is 2.

**Command Mode** Global configuration mode.

**Usage Guide** To prevent LLDP from being initialized too frequently due to the frequent operating mode change, you can configure port initialization delay.

**Configuration Examples** The following example sets LLDP port initialization delay to 3 seconds.

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

| Related Commands | Command | Description |
|---|---|---|
| | **show lldp status** | Displays LLDP status information. |

**Platform Description** N/A

## 6.18 lldp timer tx-delay

Use this command to set LLDP packet transmission delay. Use the **no** form of this command to restore the default setting.

**lldp timer tx-delay** *seconds*

**no lldp timer tx-delay**

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

**Defaults** The default is 2.

**Command Mode** Global configuration mode.

**Usage Guide** An LLDP-enabled port will send LLDP packets when the local device information changes. To avoid frequently sending LLDP packets due to the frequent local device information change, configure the LLDP packet transmission delay to control the frequent transmission of LLDP packets.

**Configuration Examples** The following example sets LLDPDU transmission delay to 3 seconds.

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

| Related Commands | Command | Description |
|---|---|---|
| | **show lldp status** | Displays LLDP status information. |

**Platform Description** N/A

## 6.19 lldp timer tx-interval

Use this command to set the interval of sending the LLDP packets. Use **no** form of this command to restore the default setting.

**lldp timer tx-interval** *seconds*

**no lldp timer tx-interval**

**Parameter Description**

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

**Defaults** The default is 30.

**Command Mode** Global configuration mode.

**Usage Guide** N/A

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

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

**Related Commands**

| Command | Description |
| --- | --- |
| **show lldp status** | Displays LLDP status information. |

**Platform Description** N/A

## 6.20 lldp tlv-enable

Use this command to configure the types of advertisable TLVs. Use the **no** form of this command to restore the default setting.

**lldp tlv-enable** { **basic-tlv** { **all | port-description | system-capability | system-description | system-name** } **| dot1-tlv** { **all | port-vlan-id | protocol-vlan-id** [ *vlan-id* ] **| vlan-name** [ *vlan-id* ] } **| dot3-tlv** { **all | link-aggregation | mac-physic | max-frame-size | power** } **| med-tlv** { **all | capability | inventory | location** { **civic-location | elin** } **identifier** *id* **| network-policy profile** [ *profile-num* ] **| power-over-ethernet** } }

**no lldp tlv-enable** { **basic-tlv** { **all | port-description | system-capability | system-description | system-name** } **| dot1-tlv** { **all | port-vlan-id | protocol-vlan-id | vlan-name** } **| dot3-tlv** { **all | link-aggregation | mac-physic | max-frame-size | power** } **| med-tlv** { **all | capability | inventory | location** { **civic-location | elin** } **identifier** *id* **| network-policy profile** [ *profile-num* ] **| power-over-ethernet** } }

**Parameter Description**

| Parameter | Description |
| --- | --- |
| **basic-tlv** | Basic management TLV |
| **port-description** | Port Description TLV |
| **system-capability** | System Capabilities TLV |

| | |
|---|---|
| **system-description** | System Description TLV |
| **system-name** | System Name TLV |
| **dot1-tlv** | 802.1 organizationally specific TLV |
| **port-vlan-id** | Port VLAN ID TLV |
| **protocol-vlan-id** | Port And Protocol VLAN ID TLV |
| *vlan-id* | VLAN ID |
| vlan-name | VLAN Name TLV |
| *vlan-id* | VLAN ID corresponding to the specified VLAN name |
| **dot3-tlv** | 802.3 organizationally specific TLV |
| **link-aggregation** | Link Aggregation TLV |
| **mac-physic** | MAC/PHY Configuration/Status TLV |
| **max-frame-size** | Maximum Frame Size TLV |
| **power** | Power Via MDI TLV |
| **med-tlv** | LLDP MED TLV |
| **capability** | LLDP-MED Capabilities TLV |
| **inventory** | Inventory management TLVs, including hardware revision TLVs, firmware revision TLVs, software revision TLVs, serial number TLVs, manufacturer name TLVs, model name TLVs, and asset ID TLVs. |
| **location** | Location Identification TLV |
| **civic-location** | Common address information about the network device in location identification TLVs. |
| **elin** | Encapsulated emergency number |
| *id* | Policy ID. Range: 1-1024. |
| **network-policy** | Network Policy TLV |
| *profile-num* | ID of network policy. Range: 1-1024. |
| **power-over-ethernet** | Extended Power-via-MDI TLV |

**Defaults**

If a device supports DCBX by default, all types of TLVs excluding 802.3 TLVs and LLDP-MED TLVs can be advertised on an interface. If the device does not support DCBX, all types of TLVs excluding Location Identification TLVs can be advertised on an interface. The default advertisement policy is none for the network policy in MED.

**Command Mode** Interface configuration mode

**Usage Guide** During configuration of basic management TLVs, IEEE 802.1 TLVs, and IEEE 802.3 TLVs, if the **all** parameter is specified, all optional TLVs of the types are advertised.

During configuration of LLDP-MED TLVs, if the **all** parameter is specified, all LLDP-MED TLVs except Location Identification TLVs are advertised.

When configuring LLDP-MED Capability TLVs, configure LLDP 802.3 MAC/PHY TLVs first. When canceling LLDP 802.3 MAC/PHY TLVs, cancel LLDP-MED Capability TLVs first.

When configuring LLDP-MED TLVs, configure LLDP-MED Capability TLVs first so that LLDP-MED TLVs of other types can be configured.

To cancel LLDP-MED TLVs, cancel LLDP-MED TLVs of other types first so that LLDP-MED

Capability TLVs can be canceled.
If a device connects to an IP phone and the IP phone supports LLDP-MED, the network policy TLV can be configured to deliver policies to the IP phone.
If the device supports DCBX by default, IEEE 802.3 TLVs and LLDP-MED TLVs cannot be advertised on an interface by default.

**Configuration Examples**

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

```
Ruijie# configure terminal
Ruijie(config)#interface gigabitethernet 0/1
Ruijie(config-if-GigabitEthernet 0/1)#lldp tlv-enable dot1-tlv all
```

The following example applies LLDP network policy 1 on the 0/1 interface.

```
Ruijie#config
Ruijie(config)#interface gigabitethernet 0/1
Ruijie(config-if-GigabitEthernet 0/1)#lldp tlv-enable med-tlv network-policy
   profile 1
```

The following example applies the LLDP Civic Address (ID: 1) configuration on the 0/1 interface.

```
Ruijie#config
Ruijie(config)#interface gigabitethernet 0/1
Ruijie(config-if-GigabitEthernet 0/1)#lldp tlv-enable med-tlv location
   civic-location identifier 1
```

The following example applies the emergency number (ID: 1) on the 0/1 interface.

```
Ruijie#config
Ruijie(config)#interface gigabitethernet 0/1
Ruijie(config-if-GigabitEthernet 0/1)#lldp location elin identifier 1
```

**Related Commands**

| Command | Description |
|---|---|
| **show lldp tlv-config interface** | Displays the attributes of advertisable TLVs |

**Platform Description** N/A

## 6.21 show lldp local-information

Use this command to display the LLDP information of local device. The information will be encapsulated in the TLVs and sent to the neighbor device.
**show lldp local-information** [ **global** | **interface** *interface-name* ]

**Parameter Description**

| Parameter | Description |
|---|---|
| *interface-name* | Interface name |

**Defaults** N/A

**Command Mode** Privileged EXEC mode

**Usage Guide**

- **global** parameter: display the global LLDP information to be sent.
- **Interface** parameter: displays the LLDP information to be sent out the interface specified.
- No parameter: display all LLDP information, including global and interface-based LLDP information.

**Configuration Examples** The following example displays the device information to be sent to neighbor device.

```
Ruijie# show lldp local-information
Global LLDP local-information:
 Chassis ID type    : MAC address
 Chassis id     : 00d0.f822.33aa
 System name      : System name
 System description   : System description
 System capabilities supported  : Repeater, Bridge, Router
 System capabilities enabled  : Repeater, Bridge, Router

 LLDP-MED capabilities    : LLDP-MED Capabilities, Network Policy, Location
   Identification, Extended Power via MDI-PD, Inventory
 Device class     : Network Connectivity
 HardwareRev     : 1.0
 FirmwareRev     :
 SoftwareRev     : RGOS 10.4(3) Release(94786)
 SerialNum      : 1234942570001
 Manufacturer name    : Manufacturer name
 Asset tracking identifier   :
----------------------------------------------------------
Lldp local-information of port [GigabitEthernet 0/1]
----------------------------------------------------------
 Port ID type     : Interface name
 Port id      : GigabitEthernet 0/1
 Port description    :

 Management address subtype  : 802 mac address
 Management address    : 00d0.f822.33aa
 Interface numbering subtype  :
 Interface number    : 0
 Object identifier    :



 802.1 organizationally information
 Port VLAN ID     : 1
```

```
Port and protocol VLAN ID(PPVID) : 1
 PPVID Supported    : YES
 PPVID Enabled     : NO
VLAN name of VLAN 1    : VLAN0001
Protocol Identity     :


802.3 organizationally information
Auto-negotiation supported  : YES
Auto-negotiation enabled   : YES
PMD auto-negotiation advertised : 100BASE-TX full duplex mode, 100BASE-TX half
   duplex mode
Operational MAU type    :
PoE support      : NO
Link aggregation supported  : YES
Link aggregation enabled   : NO
Aggregation port ID    : 0
Maximum frame Size    : 1500

LLDP-MED organizationally information
Power-via-MDI device type   : PD
Power-via-MDI power source  : Local
Power-via-MDI power priority  :
Power-via-MDI power value   :
Model name      : Model name
```

**show lldp local-information** command output description:

| Field | Description |
|---|---|
| Chassis ID type | Chassis ID type for identifying the Chassis ID field |
| Chassis ID | Used to identify the device, and is generally represented with MAC address |
| System name | Name of the sending device |
| System description | Description of the sending device, including hardware/software version, operating system and etc. |
| System capabilities supported | Capabilities supported by the system |
| System capabilities enabled | Capabilities currently enabled by the system |
| LLDP-MED capabilities | LLDP-MED capabilities supported by the system |

| | |
|---|---|
| Device class | MED device class, which is divided into 2 categories: network connectivity device and terminal device.<br>Network connectivity device<br>Class I: normal terminal device<br>Class II: media terminal device; besides Class I capabilities, it also supports media streams.<br>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:<br>PSE (power sourcing equipment)<br>PD (powered device) |
| Power-via-MDI power source | Power source type |
| Power-via-MDI power priority | Power supply priority |

| | |
|---|---|
| Power-via-MDI power value | Available power on port |
| Model name | Name of model |

**Related Commands**

| Command | Description |
|---|---|
| N/A | N/A |

**Platform Description** N/A

## 6.22 show lldp location

Use this command to display the common LLDP address or emergency number of the local device.

**show lldp location** { **civic-location | elin** } { **identifier** *id* **| interface** *interface-name* **| static** }

**Parameter Description**

| Parameter | Description |
|---|---|
| **civic-location** | Encapsulates a common address of a network device. |
| **elin** | Encapsulates an emergency number. |
| **identifier** | Displays one address or emergency number configured. |
| *id* | Policy ID of configured information |
| **interface** | Displays the address or emergency number on an interface. |
| *interface-name* | Interface name |
| **static** | Displays all addresses or emergency numbers configured. |

**Defaults** N/A

**Command Mode** Privileged EXEC mode

**Usage Guide** If the policy ID is specified, the specified address or emergency number is displayed.
If the interface name is specified, the address or emergency number configured on the interface is displayed.
If no parameter is specified, all addresses or emergency numbers are displayed.

**Configuration Examples** The following example displays all addresses.

```
Ruijie# show lldp location civic-location static
LLDP Civic location information
--------------------------
Identifier    : testt
County     : china
City Division    : 22
Leading street direction : 44
Street number    : 68
Landmark    : 233
```

```
Name     : liuy
Building    : 19bui
Floor     : 1
Room     : 33
City     : fuzhou
Country    : 86
Additional location  : aaa
Ports     : Gi0/1
--------------------------
Identifier    : tee
--------------------------
```

The following example displays all emergency numbers.

```
Ruijie# show lldp location elin static
Elin location information
--------------------------
Identifier : t
Elin  : iiiiiiiiii
Ports     : Gi1/0/3
--------------------------
```

| Related Commands | Command | Description |
|---|---|---|
| | N/A | N/A |

**Platform Description** N/A

## 6.23 show lldp neighbors

Use this command to display the LLDP information about a neighboring device.

**show lldp neighbors** [ **interface** *interface-name* ] [ **detail** ]

| Parameter Description | Parameter | Description |
|---|---|---|
| | *interface-name* | Interface name |
| | **detail** | All information about a neighboring device |

**Defaults** N/A

**Command Mode** Privileged EXEC mode

**Usage Guide** If the **detail** parameter is not specified, the brief information about a neighboring device is displayed.
If the **detail** parameter is specified, the detailed information about a neighboring device is displayed.

If the **interface** parameter is specified, the neighboring device information received on the specified interface is displayed.

**Configuration Examples** The following example displays the neighboring device information received on all ports.

```
Ruijie# show lldp neighbors detail
Lldp neighbor-information of port [GigabitEthernet 0/1]
 Neighbor index    : 1
 Device type     : LLDP Device
 Update time     : 1hour 53minutes 30seconds
Aging time      : 5seconds

 Chassis ID type    : MAC address
 Chassis id     : 00d0.f822.33cd
 System name     : System name
 System description    : System description
 System capabilities supported  : Repeater, Bridge, Router
 System capabilities enabled  : Repeater, Bridge, Router

 Management address subtype  : 802 mac address
 Management address    : 00d0.f822.33cd
 Interface numbering subtype  :
 Interface number    : 0
 Object identifier    :


 LLDP-MED capabilities    :
 Device class     :
 HardwareRev     :
 FirmwareRev     :
 SoftwareRev     :
 SerialNum      :
 Manufacturer name    :
 Asset tracking identifier   :

 Port ID type     : Interface name
 Port id      : GigabitEthernet 0/1
 Port description    :

 802.1 organizationally information
 Port VLAN ID     : 1
 Port and protocol VLAN ID(PPVID) : 1
  PPVID Supported    : YES
  PPVID Enabled    : NO
 VLAN name of VLAN 1    : VLAN0001
```

```
 Protocol Identity    :
 802.3 organizationally information
 Auto-negotiation supported  : YES
 Auto-negotiation enabled   : YES
 PMD auto-negotiation advertised : 1000BASE-T full duplex mode, 100BASE-TX full
    duplex mode, 100BASE-TX half duplex mode, 10BASE-T full duplex mode,
    10BASE-T half duplex mode
 Operational MAU type    : speed(1000)/duplex(Full)
 PoE support     : NO
 Link aggregation supported  : YES
 Link aggregation enabled   : NO
 Aggregation port ID    : 0
 Maximum frame Size    : 1500
 LLDP-MED organizationally information
 Power-via-MDI device type   :
 Power-via-MDI power source  :
 Power-via-MDI power priority  :
Power-via-MDI power value   :
```

Description of fields:

| Field | Description |
|---|---|
| Neighbor index | Neighbor index |
| Device type | Type of neighboring device |
| Update time | Latest update time of neighbor information |
| Aging time | Aging time of a neighbor, namely the time after which a neighbor is aged and deleted |
| Chassis ID type | Chassis ID type |
| Chassis ID | Used to identify a device. Usually, a MAC address is used. |
| System name | Device name |
| System description | Device description, including hardware/software version and operating system |
| System capabilities supported | Functions supported by the system |
| System capabilities enabled | Functions enabled by the system |
| Management address subtype | Type of management address |
| Management address | Management address |
| Interface numbering subtype | Interface type of management address |
| Interface number | Interface ID of management address |
| Object identifier | Object ID of management address |

| | |
|---|---|
| Device class | MED device type: network connectivity device and terminal device<br>Network connectivity device:<br>Class I: general terminal device<br>Class II: media terminal device, including capabilities of Class I and supporting media stream<br>Class III: communication terminal device, including capabilities of Class I and Class II and supporting IP communication |
| HardwareRev | Hardware version |
| FirmwareRev | Firmware version |
| SoftwareRev | Software version |
| SerialNum | Serial number |
| Manufacturer name | Manufacturer name |
| Asset tracking identifier | Asset ID |
| Port ID type | Port ID type |
| Port ID | Port ID |
| Port description | Port description |
| Port VLAN ID | VLAN ID of a port |
| Port and protocol VLAN ID | Port and protocol VLAN ID |
| PPVID Supported | Whether port and protocol VLAN is supported |
| PPVID Enabled | Whether port and protocol VLAN is enabled |
| VLAN name of VLAN 1 | VLAN 1 name |
| Protocol Identity | Protocol ID |
| Auto-negotiation supported | Whether auto-negotiation is supported |
| Auto-negotiation enabled | Whether auto-negotiation is enabled |
| PMD auto-negotiation advertised | Port auto-negotiation advertisement capability |
| Operational MAU type | Rate and duplex status of port auto-negotiation |
| PoE support | Whether POE is supported |
| Link aggregation supported | Whether link aggregation is supported |
| Link aggregation enabled | Whether link aggregation is enabled |
| Aggregation port ID | ID of link aggregation port |
| Maximum frame Size | Maximum frame length supported by a port |
| Power-via-MDI device type | Device type, including:<br>● PSE<br>● PD |
| Power-via-MDI power source | Power type |
| Power-via-MDI power priority | Power supply priority |
| Power-via-MDI power value | Power value of a port where power is supplied |

**Related Commands**

| Command | Description |
|---|---|
| N/A | N/A |

**Platform Description** N/A

## 6.24 show lldp network-policy profile

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

**show lldp network-policy profile** [ *profile-num* ] | **interface** *interface-name* }

**Parameter Description**

| Parameter | Description |
|---|---|
| *profile-num* | ID of a network policy, in the range from 1 to 1024. |
| *interface-name* | Name of interface. |

**Defaults** N/A

**Command Mode** Privileged EXEC mode

**Usage Guide** If *profile-num* is specified, the information about the specified network policy is displayed.
If no parameter is specified, the information about all network policies is displayed.

**Configuration Examples** The following example displays the information about a network policy.

```
Ruijie# show lldp network-policy profile
Network Policy Profile 1
 voice vlan 2 cos 4 dscp 6
 voice-signaling vlan 2000 cos 4 dscp 6
```

**Related Commands**

| Command | Description |
|---|---|
| N/A | N/A |

**Platform Description** N/A

## 6.25 show lldp statistics

The following example displays LLDP statistics.

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

**Parameter Description**

| Parameter | Description |
|---|---|
| *interface-name* | Interface name |

**Defaults** N/A

**Command Mode** Privileged EXEC mode

**Usage Guide**

- **global** parameter: display the global LLDP statistics.
- **Interface** parameter: display the LLDP statistics of the specified interface.

**Configuration Examples** The following example displays all LLDP statistics.

```
Ruijie# show lldp statistics
lldp statistics global Information:
Neighbor information last changed time  : 1hour 52minute 22second
The number of neighbor information inserted : 2
The number of neighbor information deleted : 0
The number of neighbor information dropped : 0
The number of neighbor information age out : 1

------------------------------------------------------------
Lldp statistics information of port [GigabitEthernet 0/1]
------------------------------------------------------------
The number of lldp frames transmitted  : 26
The number of frames discarded    : 0
The number of error frames     : 0
The number of lldp frames received   : 12
The number of TLVs discarded    : 0
The number of TLVs unrecognized    : 0
The number of neighbor information aged out : 0
```

**show lldp statistics** command output description:

| Field | Description |
|---|---|
| Neighbor information last change time | Time the neighbor information is latest updated |
| The number of neighbor information inserted | Number of times of adding neighbor information |
| The number of neighbor information deleted | Number of times of removing neighbor information |
| The number of neighbor information dropped | Number of times of dropping neighbor information |
| The number of neighbor information aged out | Number of the neighbor information entries that have aged out |
| The number of lldp frames transmitted | Total number of the LLDPDUs transmitted |
| The number of frames discarded | Total number of the LLDPDUs discarded |
| The number of error frames | Total number of the LLDP error frames received |
| The number of lldp frames received | Total number of the LLDPDUs received |

| | |
|---|---|
| The number of TLVs discarded | Total number of the LLDP TLVs dropped |
| The number of TLVs unrecognized | Total number of the LLDP TLVs that cannot be recognized |
| The number of neighbor information aged out | Number of the neighbor information entries that have aged out |

**Related Commands**

| Command | Description |
|---|---|
| N/A | N/A |

**Platform Description** N/A

## 6.26 show lldp status

Use this command to display LLDP status information.

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

**Parameter Description**

| Parameter | Description |
|---|---|
| *interface-name* | Interface name |

**Defaults** N/A

**Command Mode** Privileged EXEC mode

**Usage Guide** **interface** parameter: display the LLDP status information of the specified interface.

**Configuration Examples** The following example displays LLDP status information of all ports.

```
Ruijie# show lldp status
Global status of LLDP    : Enable
Neighbor information last changed time : 1hour 52minute 22second
Transmit interval     : 30s
Hold multiplier     : 4
Reinit delay      : 2s
Transmit delay      : 2s
Notification interval    : 5s
Fast start counts     : 3
------------------------------------------------------------
Port [GigabitEthernet 0/1]
------------------------------------------------------------
Port status of LLDP    : Enable
Port state     : UP
Port encapsulation    : Ethernet II
```

```
Operational mode    : RxAndTx
Notification enable    : NO
Error detect enable    : YES
Number of neighbors    : 1
Number of MED neighbors   : 0
```

**show lldp status** command output description:

| Field | Description |
|---|---|
| Global status of LLDP | Whether LLDP is globally enabled |
| Neighbor information last changed time | Time the neighbor information is latest updated |
| Transmit interval | LLDPDU transmit interval |
| Hold multiplier | TTL multiplier |
| Reinit delay | Port re-initialization delay |
| Transmit delay | LLDPDU transmit delay |
| Notification interval | Interval for sending LLDP Traps |
| Fast start counts | The number of fast sent LLDPDUs |
| Port status of LLDP | Whether LLDP is enabled on the port |
| Port state | Link status of port: UP or DOWN |
| Port encapsulation | LLDPDU encapsulation format |
| Operational mode | Operating mode of LLDP |
| Notification enable | Whether LLDP Trap is enabled on the port |
| Error detect enable | Whether error detection is enabled on the port |
| Number of neighbors | Number of neighbors |
| Number of MED neighbors | Number of MED neighbors |

**Related Commands**

| Command | Description |
|---|---|
| N/A | N/A |

**Platform Description** N/A

## 6.27 show lldp tlv-config

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

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

**Parameter Description**

| Parameter | Description |
|---|---|
| *interface-name* | Interface name |

**Defaults** N/A

**Command** Privileged EXEC mode

**Mode**

**Usage Guide** **Interface** parameter: display the LLDP TLV configuration of the specified interface.

**Configuration Examples** The following example displays TLV information of port 1.

```
Ruijie# show lldp tlv-config interface GigabitEthernet 0/1
LLDP tlv-config of port [GigabitEthernet 0/1]
-----------------------------------------------------
   NAME    STATUS DEFAULT
---------------------------------- ------ -----------
Basic optional TLV:
Port Description TLV   YES YES
System Name TLV    YES YES
System Description TLV   YES YES
System Capabilities TLV   YES YES
Management Address TLV   YES YES

IEEE 802.1 extend TLV:
Port VLAN ID TLV    YES YES
Port And Protocol VLAN ID TLV  YES YES
VLAN Name TLV     YES YES

IEEE 802.3 extend TLV:
MAC-Physic TLV    YES YES
Power via MDI TLV    YES YES
Link Aggregation TLV   YES YES
Maximum Frame Size TLV   YES YES

LLDP-MED extend TLV:
Capabilities TLV    YES YES
Network Policy TLV   YES YES
Location Identification TLV  NO  NO
Extended Power via MDI TLV  YES YES
Inventory TLV     YES YES
```

**Related Commands**

| Command | Description |
| --- | --- |
| N/A | N/A |

**Platform Description** N/A

# 6.28 { voice | voice-signaling } vlan

Use this command to configure the LLDP network policy. Use the **no** form of this command to delete the policy.

{ **voice | voice-signaling** } **vlan** { { *vlan-id* [ **cos** *cvalue* **| dscp** *dvalue* ] } | { **dot1p** [ **cos** *cvalue* **| dscp** *dvalue* ] } **| none | untagged** }

**no** { **voice | voice-signaling** } **vlan**

**Parameter Description**

| Parameter | Description |
|---|---|
| **voice** | Voice application |
| **voice-signaling** | Voice-signaling application |
| *vlan-id* | (Optional) VLAN ID of voice flow. The value ranges from 1 to 4094. |
| **cos** | (Optional) Class of service |
| *cvalue* | (Optional) CoS of the configured voice flow. The value ranges from 0 to 7, and the default value is **5**. |
| **dscp** | (Optional) Differentiated services code point |
| *dvalue* | (Optional) DSCP value of the configured voice flow. The value ranges from 0 to 63. The default value is 46. |
| **dot1p** | (Optional) 802.1p priority tagging. The tag frame includes user_priority and vlan id is 0. |
| **none** | (Optional) The network policy is not advertised. VoIP determines the network policy based on its configuration. |
| **untagged** | (Optional) The untag frame is sent in the voice vlan in VoIP. In this case, the value of vlan id and cos are ignored. |

**Defaults** N/A

**Command Mode** LLDP network policy configuration mode

**Usage Guide** In the LLDP network policy configuration mode, configure the LLDP network policy.

voice indicates the voice data type, and voice-signaling indicates the voice signal type.

If a device connects to an IP phone and the IP phone supports LLDP-MED, the network policy TLV can be configured to deliver policies to the IP phone, so that the IP phone changes the voice stream tag and QoS.Excluding the preceding policy, the following operations need to be performed on the device:

1. Enable the voice VLAN function and add the port connected to the IP phone to the voice VLAN in static mode.
2. Configure the port connected to the IP phone to a QoS trusted port. (It is recommended to use the trusted DSCP mode.)
3. If 802.1X authentication is enabled on the port at the same time, a security channel needs to be configured to transmit packets from the voice VLAN.

If the IP phone does not support LLDP-MED, the voice VLAN function must be enabled. In addition,

the MAC address of the IP phone needs to be added to the voice VLAN OUI list manually.
For details about how to configure the QoS trusted mode, see chapter "IP QoS." For details about how to configure the voice VLAN, see chapter "Voice VLAN." For details about how to configure the security channel, see chapter "ACL."

**Configuration Examples** The following example configures the LLDP network policy (profile-num is 1).

```
Ruijie#config
Ruijie(config)#lldp network-policy profile 1
Ruijie(config-lldp-network-policy)# voice vlan untagged
Ruijie(config-lldp-network-policy)# voice-signaling vlan 3 cos 4
Ruijie(config-lldp-network-policy)# voice-signaling vlan 3 dscp 6
```

**Related Commands**

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

**Platform Description** N/A

# 7 PPP Commands

## 7.1 ppp accm

Use this command to configure the Asynchronous Control Character Map (ACCM) option for PPP negotiation.
**ppp accm** *value*

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

Parameter Description

| Parameter | Description |
|---|---|
| *value* | Value of the ACCM option, in the range from 0 to 0xffffffff. |

Command Mode: Interface configuration mode

Defaults: The default is 0x000A0000.

Default Level: 14

Usage Guide: This command is used to configure the ACCM option involved in the PPP negotiation phase, in the range from 0 to 0xffffffff. The default is 0x000A0000.

Configuration Examples: The following example configures the ACCM option for PPP negotiation.

```
Ruijie(config-if-Virtual-ppp 1)#ppp accm 0x0000000f
Ruijie(config-if-Virtual-ppp 1)#
```

Verification: Run the **show running-config** command to display the value of the ACCM option configured on the current interface for PPP negotiation.

Note: N/A

Platform: N/A

## 7.2 ppp accounting

Use this command to configure the accounting mode of PPP.
**ppp accounting { default |** *list_name* **}**

Use the **no** form of this command to delete the accounting list of PPP.
**no ppp accounting**

Parameter Description

| Parameter | Description |
|---|---|
| **default** | Default accounting list |
| *list_name* | Name of the AAA accounting list |

Command Mode: Interface configuration mode

Default Level: 14

Usage Guide: This command is used to configure the accounting mode of PPP. You can set the accounting mode to the default list or to the name of a specified accounting list. Before configuring this command, you need to enable the AAA module; otherwise, this command is invisible.

Configuration Examples: The following example configures the accounting mode of PPP.

```
Ruijie(config-if-Virtual-ppp 1)#ppp accounting default
Ruijie(config-if-Virtual-ppp 1)#ppp accounting acc_list
Ruijie(config-if-Virtual-ppp 1)#
```

Verification: Run the **show running-config** command to display the name of the PPP accounting list configured on the current interface.

Note: N/A

Platform: N/A

## 7.3 ppp authentication

Use this command to configure the authentication mode of PPP.

**ppp authentication** { { **pap | chap** } [ **callin** | { **chap | pap** } | **default** | *list_name* ] }

Use the **no** form of this command to delete the authentication mode of PPP.

**no ppp authentication** { { **pap | chap** } [ **callin** | { **chap** | **pap** } | **default** | *list_name* ] }

Parameter Description

| Parameter | Description |
|---|---|
| **pap** | Sets the authentication mode to PAP. |
| **callin** | Authenticates incoming request packets only. |
| **chap** | Sets the authentication mode to CHAP. |
| **default** | Uses the default authentication list, no matter whether PAP or CHAP authentication applies. |
| *list_name* | Configures the name of the authentication list. |

Command Mode: Interface configuration mode

Default Level: 14

Usage Guide: This command is used to configure the authentication mode of PPP, which may be PAP or CHAP authentication.

Configuration Examples: The following example configures the authentication mode of PPP.

```
Ruijie(config-if-Virtual-ppp 1)#ppp authentication pap
Ruijie(config-if-Virtual-ppp 1)#ppp authentication chap
Ruijie(config-if-Virtual-ppp 1)#ppp authentication pap chap callin default
Ruijie(config-if-Virtual-ppp 1)#ppp authentication pap chap test_list
Ruijie(config-if-Virtual-ppp 1)#
```

Verification: Run the **show running-config** command to display whether the authentication mode of PPP has been configured on the current interface.

Note: N/A

Common Error: N/A

Platform: N/A

## 7.4 ppp authorization

Use this command to configure the authorization list of AAA authentication of PPP.
**ppp authorization** { **default** | *list_name* }

Use this command to delete the authorization list of AAA authentication of PPP
**no ppp authorization**

Parameter Description

| Parameter | Description |
|---|---|
| **default** | Default authorization list of AAA authentication of PPP |
| *list_name* | Name of the specified authorization list of AAA authentication of PPP |

Command Mode: Interface configuration mode

Default Level: 14

Usage Guide: This command is used to configure the authorization list of AAA authentication of PPP. The authorization list of AAA authentication is used in the PPP authentication phase to perform AAA authentication. This command is visible only after the AAA module is enabled.

Configuration Examples: The following example sets the authorization list of PPP authentication on interface Virtual-PPP 1 to auth_list.

```
Ruijie(config-if-Virtual-ppp 1)#ppp authorization default
Ruijie(config-if-Virtual-ppp 1)#ppp authorization auth_list
Ruijie(config-if-Virtual-ppp 1)#
```

Verification: Run the **show running-config** command to display the authorization list of AAA authentication of PPP configured on the current interface.

Note: N/A

Common Error: N/A

Platform: N/A

## 7.5 ppp chap

The following example configures the user name and password for CHAP authentication of PPP.

**ppp chap hostname** *name*

**ppp chap password** *password*

Use the **no** form of this command to delete the configured user name and password for CHAP authentication of PPP.

**no ppp chap hostname**

Parameter Description

| Parameter | Description |
|---|---|
| *name* | User name for CHAP authentication |
| *password* | Password for CHAP authentication |

Command Mode: Interface configuration mode

Default Level: 14

Usage Guide: PPP negotiation is required for both VPDN and PPPOE dialing. The second phase of PPP negotiation is about user name and password authentication. This command is used to configure the user name and password for CHAP authentication.

Configuration Examples: The following example configures the user name and password for CHAP authentication on interface Virtual-PPP 1.

```
Ruijie(config-if-Virtual-ppp 1)#ppp chap hostname 111
Ruijie(config-if-Virtual-ppp 1)#ppp chap password 111
Ruijie(config-if-Virtual-ppp 1)#no ppp chap hostname
Ruijie(config-if-Virtual-ppp 1)#
```

Verification: Run the **show running-config** command to display the user name and password configured on the current interface for CHAP authentication.

Note: N/A

Common Error: N/A

Platform: N/A

## 7.6 ppp pap sent-username *username* password *password*

Use this command to configure the user name and password for PAP authentication of PPP.
**ppp pap sent-username** *username* **password** *password*

Use the **no** form of this command to delete the configured user name and password for PAP authentication of PPP.
**no ppp pap sent-username**

Parameter Description

| Parameter | Description |
|---|---|
| *username* | User name for PAP authentication |
| *password* | Password for PAP authentication |

Command Mode: Interface configuration mode

Default Level: 14

Usage Guide: PPP negotiation is required for both VPDN and PPPOE dialing. The second phase of PPP negotiation is about user name and password authentication. This command is used to configure the user name and password for PAP authentication.

Configuration Examples: The following example configures the user name and password for PAP authentication on interface Virtual-PPP 1.

```
Ruijie(config-if-Virtual-ppp 1)#ppp pap sent-username 111 password 111
Ruijie(config-if-Virtual-ppp 1)#no ppp pap sent-username
Ruijie(config-if-Virtual-ppp 1)#
```

Verification: Run the **show running-config** command to display the user name and password configured on the current interface for PAP authentication.

Note: N/A

Common Error: N/A

Platform: N/A

## 7.7 ppp ipcp dns

Use this command to configure the DNS option involved in the IPCP phase of PPP negotiation.
**ppp ipcp dns** { *A.B.C.D* [ *A.B.C.D* ] [ **accept** ] **| accept** | **request** | **reject** }

Use this command to delete the configured DNS option.
**no ppp ipcp dns** { *A.B.C.D* [ *A.B.C.D* ] [ **accept** ] | **accept** | **request** | **reject** }

Parameter Description

| Parameter | Description |
|---|---|
| **accept** | Receives all non-0 DNS addresses. |
| **request** | Requests the DNS address from the peer server. |
| **reject** | Refuses to negotiate the DNS option with the peer end. |
| *A.B.C.D* | DNS address |

Defaults: The DNS option is not configured by default.

Command Mode: Interface configuration mode

Default Level: 14

Usage Guide: This command is used to configure the DNS option involved in the IPCP negotiation phase.

Configuration Examples: The following example configures the DNS option involved in the IPCP negotiation phase.

```
Ruijie(config-if-Virtual-ppp 1)#ppp ipcp dns accept
Ruijie(config-if-Virtual-ppp 1)#ppp ipcp dns reject
Ruijie(config-if-Virtual-ppp 1)#ppp ipcp dns request
Ruijie(config-if-Virtual-ppp 1)#ppp ipcp dns 1.1.1.1 2.2.2.2
Ruijie(config-if-Virtual-ppp 1)#no ppp ipcp dns
Ruijie(config-if-Virtual-ppp 1)#
```

Verification: Run the **show running-config** command to display whether the DNS option has been configured on the current interface.

Note: N/A

Common Error: N/A

Platform: N/A

## 7.8 ppp lcp mru negotiate

Use this command to configure the Maximum Receive Unit (MRU) option for PPP auto-negotiation.
**ppp lcp mru negotiate**

Use the no form of this command to remove the MRU configuration.
**no ppp lcp mru**

**Parameter Description**

| Parameter | Description |
|---|---|
| N/A | N/A |

**Command Mode** Interface configuration mode

**Default Level** 14

**Usage Guide** The MRU option, as a common option involved in the PPP negotiation process, will be carried in packets from both ends during negotiation so as to determine the maximum size of packets to be transmitted on the entire link.

**Configuration Examples** The following example configures the MRU option for auto-negotiation on interface Virtual-ppp 1.

```
Ruijie(config-if-Virtual-ppp 1)#ppp lcp mru negotiate
Ruijie(config-if-Virtual-ppp 1)#
```

**Verification** 1. Run the **show running-config** command to display whether the MRU option has been configured on the current interface.

**Note** N/A

**Common Error** N/A

**Platform** N/A

## 7.9 ppp max-bad-auth

Use this command to specify the number of PPP authentication retries.
**ppp max-bad-auth** *number*

Use the **no** form of this command to restore the default setting.
**no ppp max-bad-auth**

Parameter Description

| Parameter | Description |
|---|---|
| *number* | Number of PPP authentication retries, in the range from 1 to 255 |

Defaults: The default is 1.

Command Mode: Interface configuration mode

Default Level: 14

Usage Guide: The number of PPP authentication retries includes the first authentication; that is, if the number of PPP authentication retries is set to 3, twice authentication is still allowed following the failure of the first authentication. When the last authentication fails, the line is interrupted (or reset).

Configuration Examples: The following example sets the number of PPP authentication retries on interface virtual-ppp1 to 3:

```
Ruijie(config-if-Virtual-ppp 1)# ppp max-bad-auth 3
```

2The following example restores the number of PPP authentication retries to the default setting.

```
Ruijie(config-if-Virtual-ppp 1)# no ppp max-bad-auth
```

Verification: Run the **show running-config interface virtual-ppp** *1* command to display the configuration on the current interface.

Note: N/A

Common Error: N/A

Platform: N/A

# 7.10 ppp negotiation-timeout

Use this command to specify the maximum PPP negotiation timeout period.
**ppp negotiation-timeout** *seconds*

Use the **no** form of this command to restore the default setting.
**no ppp negotiation-timeout**

**Parameter Description**

| Parameter | Description |
|---|---|
| *seconds* | Maximum PPP negotiation timeout period, in the range from 10 to 65535 in the unit of seconds |

**Defaults** The default is 20 seconds.

**Command Mode** Interface configuration mode

**Default Level** 14

**Usage Guide** If the maximum negotiation timeout period expires but PPP negotiation is not finished, the PPP negotiation is considered as having failed. The maximum PPP negotiation timeout period is 20s by default.

**Configuration Examples** The following example sets the maximum PPP negotiation timeout period on interface virtual-ppp1 to 200 seconds.

```
Ruijie (config)# interface virtual-ppp 1
Ruijie(config-if-Virtual-ppp 1)# ppp negotiation-timeout 200
```

The following example restores the maximum PPP negotiation timeout period to the default settings.

```
Ruijie(config-if-Virtual-ppp 1)# no ppp negotiation-timeout
```

**Verification** Run the **show running-config interface virtual-ppp** *1* command to check the configuration on the current interface.

**Note** N/A

**Common Error** N/A

**Platform** N/A

# 8 PPPoE-client Commands

## 8.1 clear dialer

Use this command to clear statistics about the DDR dialer interface.

**clear dialer**

**Parameter Description**

| Parameter | Description |
| --- | --- |
| N/A | N/A |

**Command Modes** Global configuration mode

**Usage Guide** N/A

**Configuration Examples** The following example clears statistics about the DDR dialer interface.

```
R1# clear dialer
```

**Platform Description** N/A

## 8.2 clear pppoe tunnel

Use this command to clear all PPPoE tunnels.

**clear pppoe tunnel**

**Parameter Description**

| Parameter | Description |
| --- | --- |
| *N/A* | N/A |

**Command Modes** Global configuration mode

**Usage Guide** N/A

**Configuration Examples** The following example clears all PPPoE tunnels.

```
R1# clear pppoe tunnel
```

**Platform Description** N/A

## 8.3 dialer enable-timeout

Use this command to configure the timeout period for the ASDL line.
**dialer enable-timeout** *seconds*

Use the **no** form of this command to restore the default setting.
**no dialer enable-timeout**

**Parameter Description**

| Parameter | Description |
|---|---|
| *seconds* | Configures the timeout period for the ASDL line in the unit of seconds. |

**Defaults** The default is 15 seconds.

**Command Modes** Interface configuration mode

**Usage Guide** The timeout period for the ASDL line is the period from line disconnection or dial failure to the next dial.

**Configuration Examples** The following example configures the timeout period for the ASDL line to 20 seconds.

```
R1(config)# interface dialer 1
R1(config-if-dialer 1)# dialer enable-timeout 20
```

The following example restores the timeout period for the ASDL line to the default setting.

```
R1(config)# interface dialer 1
R1(config-if-dialer 1)# no dialer enable-timeout
```

**Platform Description** N/A

## 8.4 dialer-group

Use this command to associate a dialer triggering rule with a DDR dialer interface.
**dialer-group** *group-number*

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

**Parameter Description**

| Parameter | Description |
| --- | --- |
| *group-number* | The ID of a dialer triggering rule. |

**Defaults** This function is disabled by default.

**Command Modes** Interface configuration mode

**Usage Guide** The dialer triggering rule is configured by the **dialer-list** command. You should identify what packets can trigger dial before the association.

**Configuration Examples** The following example associates a dialer triggering rule with DDR dialer interface 1.

```
R1(config)# interface dialer 1
R1(config-if-dialer 1)# dialer-group 1
```

The following example restores the default setting.

```
R1(config)# interface dialer 1
R1(config-if-dialer 1)# no dialer-group
```

**Platform Description** N/A

## 8.5 dialer hold-queue

Use this command to configure a hold queue on a DDR dialer interface.
**dialer hold-queue** *packets* [ **timeout** *seconds* ]

Use the **no** form of this command to restore the default setting.
**no dialer hold-queue** [ *packets* [ **timeout** *seconds* ] ]

**Parameter Description**

| Parameter | Description |
| --- | --- |
| *packets* | Sets the number of packets the queue can hold, in the range from 0 to 100. |
| **timeout** *seconds* | Sets the timeout period of the hold queue, in the unit of seconds. The default is 45 seconds. |

**Defaults** This function is disabled by default.

**Command** Interface configuration mode

**Modes**

**Usage Guide** The device discards packets during negotiation after modem dialing. If this command is configured, packets in the hold queue will be saved on the device and sent once connection is created.

**Configuration Examples** The following example sets the hold queue *packets* to 50.

```
R1(config)# interface dialer 1
R1(config-if-dialer 1)# dialer hold-queue 50
```

The following example restores the default setting.

```
R1(config)# interface dialer 1
R1(config-if-dialer 1)# no dialer hold-queue
```

**Platform Description** N/A

## 8.6 dialer idle-timeout

Use this command to specify the idle period for an ADSL line.
**dialer idle-timeout** *seconds*

Use the **no** form of this command to restore the default setting.
**no dialer idle-timeout**

**Parameter Description**

| Parameter | Description |
|---|---|
| *seconds* | Sets the idle period for an ADSL line, in the unit of seconds. |

**Defaults** The default is 120 seconds.

**Command Modes** Interface configuration mode

**Usage Guide** This idle period refers to the period when no data traffic is transmitted in the ASDL line. The timer is reset when any message is received.

**Configuration Examples** The following example sets the idle period to 60 seconds.

```
R1(config)# interface dialer 1
R1(config-if-dialer 1)# dialer idle-timeout 60
```

The following example restores the default setting.

```
R1(config)# interface dialer 1
R1(config-if-dialer 1)# no dialer idle-timeout
```

**Platform Description** This command is supported only on EG/NBR/NPE products.

## 8.7 dialer-list

Use this command to define a dialer triggering rule.

**dialer-list** *dialer-group* **protocol** *protocol-name* **ip** { **permit** | **deny** | **list** *access-list-number* }

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

**no dialer-list** *dialer-group* [ **protocol** *protocol-name* **ip** { **permit** | **deny** | **list** *access-list-number* } ]

**Parameter Description**

| Parameter | Description |
|---|---|
| *dialer-group* | Sets the ID of a dialer triggering rule. |
| **protocol** *protocol-name* | Protocol name. |
| **ip** | Specifies the IP protocol to be used for defining a dialer triggering rule. |
| **permit** | Permits IP packets. |
| **deny** | Denies IP packets. |
| **list** | Specifies an access list to be used for defining a dialer triggering rule. |
| *access-list-number* | Sets the ID of an ACL list. |

**Defaults** This function is disabled by default.

**Command Modes** Global configuration mode

**Usage Guide** This configuration is mandatory to define one or more dialer triggering rules. Use the **dialer-group** command to apply these rules to specific dialer interfaces.

**Configuration Examples** The following example sets dialer triggering rule 1 to **ip**.

```
R1(config)# dialer-list 1 protocol ip permit
```

The following example restores the default setting.

```
R1(config)# no dialer-list 1
```

**Platform Description** N/A

## 8.8 dialer pool

Use this command to associate a dialer pool with a logical interface.
**dialer pool** *number*

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

**Parameter Description**

| Parameter | Description |
|---|---|
| *number* | Sets the ID of a dialer pool, in the range from 1 to 255. |

**Defaults** This function is disabled by default.

**Command Modes** Interface configuration mode

**Usage Guide** Advanced dialup requires association between a physical interface and a dialer interface through a dialer pool. First, add a physical interface to several dialer pools. Second, associate the logical interface with only one of the dialer pools. One physical interface may belong to multiple dialer pools but one logical interface is allowed to associate with one single dialer pool. The dialer interface selects an idle physical interface from the dialer pool randomly.

**Configuration Examples** The following example associates dialer pool 1 with dialer interface1.

```
R1(config)# interface dialer 1
R1(config-if-dialer 1)# dialer pool 1
```

The following example restores the default setting.

```
R1(config)# interface dialer 1
R1(config-if-dialer 1)# no dialer pool
```

**Platform Description** N/A

## 8.9 ip address

Use this command to enable the IP policy on an interface.
**ip address** { **negotiate |** *ip-addr subnet-mask* }

Use this command to disable the IP address acquisition mode.
**no ip address**

**Parameter Description**

| Parameter | Description |
|---|---|
| **negotiate** | Enables an interface to acquire IP address through PPP negotiation. |
| *ip-addr* | The IP address of a specified interface. |
| *subnet-mask* | The mask of a specified interface. |

**Defaults** N/A

**Command Modes** Interface configuration mode

**Usage Guide** Use this command to configure the IP policy on a specified dialer interface. If PPP negotiation is enabled, the IP address is distributed by the server. If the IP address is specified manually, it takes effect only after negotiation with the server succeeds.

**Configuration Examples** The following example sets the IP policy to PPP negotiation.

```
R1(config)# interface dialer 1
R1(config-if-dialer 1)# ip address negotiate
```

The following example removes the IP policy configuration.

```
R1(config)# interface dialer 1
R1(config-if-dialer 1)# no ip address
```

**Platform Description** N/A

## 8.10 ppp max-bad-auth

Use this command to setPPP authentication retry count.
**ppp max-bad-auth** *number*

Use the **no** form of this command to restore the default setting.
**no ppp max-bad-auth**

**Parameter Description**

| Parameter | Description |
|---|---|
| *number* | Sets PPP authentication retry count, in the range from 1 to 255. |

**Defaults** This function is disabled by default.

**Command** Interface configuration mode

**Modes**

**Usage Guide** If *number* is set to 3, you can try twice after one failure t. If the last retry fails, The line will be reset.

**Configuration Examples** The following example Sets PPP authentication retry count to 3.

```
R1(config)# interface dialer 1
R1(config-if-dialer 1)# ppp max-bad-auth 3
```

The following example restores the default setting.

```
R1(config)# interface dialer 1
R1(config-if-dialer 1)# no ppp max-bad-auth
```

**Platform Description** N/A

## 8.11 pppoe enable

Use this command to enable the PPPoE client function on the interface.
**pppoe enable**

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

**Parameter Description**

| Parameter | Description |
|---|---|
| N/A | N/A |

**Defaults** This function is disabled by default.

**Command Modes** Interface configuration mode

**Usage Guide** Use this command on physical WAN interfaces.

**Configuration Examples** The following example enables the PPPoE client function on GigabitEthernet 0/5.

```
R1(config)# interface GigabitEthernet 0/5
R1(config-if- GigabitEthernet 0/5)# pppoe enable
```

The following example restores the default setting.

```
R1(config)# interface GigabitEthernet 0/5
R1(config-if- GigabitEthernet 0/5)# no pppoe enable
```

**Platform** N/A

**Description**

## 8.12 pppoe-client dial-pool-number

Use this command to add an Ethernet interface to a dialer pool and specifies the dial mode.
**pppoe-client dial-pool-number** *number* **no-ddr**

Use the **no** form of this command to restore the default setting.
**no pppoe-client dial-pool-number** *number*

**Parameter Description**

| Parameter | Description |
|---|---|
| *number* | Sets the ID of a dialer pool. |
| **no-ddr** | Applies auto dial. |

**Defaults** This function is disabled by default.

**Command Modes** Interface configuration mode

**Usage Guide** Use this command to add an Ethernet interface to a dialer pool, which is associated with the logical interface, In this way, the Ethernet interface and the logical interface are connected to perform dialing.

**Configuration Examples** The following example adds GigabitEthernet 0/5 to dialer pool 1.

```
R1(config)# interface GigabitEthernet 0/5
R1(config-if- GigabitEthernet 0/5)# pppoe-client dial-pool-number 1 no-ddr
```

The following example restores the default setting.

```
R1(config)# interface GigabitEthernet 0/5
R1(config-if- GigabitEthernet 0/5)# no pppoe-client dial-pool-number 1
```

**Platform Description** N/A

## 8.13 pppoe session mac-address

Use this command to configure the MAC address of a PPPoE session.
**pppoe session mac-address** *H.H.H*

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

**no pppoe session mac-address**

**Parameter Description**

| Parameter | Description |
|---|---|
| *H.H.H* | Configures the MAC address of a PPPoE session. |

**Defaults** This function is disabled by default.

**Command Modes** Interface configuration mode

**Usage Guide** This configuration takes effect only on sub interfaces after the **pppoe enable** command is executed.

**Configuration Examples** The following example configures the MAC address of a PPPoE session on GigabitEthernet 0/5.1.

```
Ruijie (config)# interface GigabitEthernet 0/5.1
Ruijie(config-subif-GigabitEthernet 0/5.1)#pppoe enable
Ruijie(config-subif-GigabitEthernet 0/5.1)#encapsulation dot1Q 1
Ruijie(config-subif-GigabitEthernet 0/5.1)#pppoe sessiom mac-address
00d0.f822.33f3
```

The following example restores the default setting.

```
Ruijie (config)# interface GigabitEthernet 0/5.1
Ruijie(config-subif-GigabitEthernet 0/5.1)#no pppoe sessiom mac-address
```

**Platform Description** N/A

## 8.14 show pppoe

Use this command to display PPPoE information.

**show pppoe** { **ref** | **session** | **tunnel** }

**Parameter Description**

| Parameter | Description |
|---|---|
| **ref** | Displays fast forwarding information about all PPPoE sessions. |
| **session** | Displays all PPPoE session information. |
| **tunnel** | Displays all PPPoE tunnel information. |

**Command Modes** Privileged EXEC mode/Global configuration mode/Interface configuration mode

**Usage Guide** N/A

**Configuration Examples**

The following example displays fast forwarding information about all PPPoE sessions.

```
R1# show pppoe ref

 GigabitEthernet 0/6 Virtual-pppoe 2 dialer 1
  Protocol UP dialer-group 1 last_time 164235070 ms
  Ether Header: 00 60 4F 67 02 50 00 D0 F8 22 33 43 88 64
  PPPoE Header: 11 00 00 7F 00 50
  PPP Header  : 00 21
  DstMac 0060.4f67.0250, SrcMAC 00d0.f822.3343, SessionID 127
  Input Err : 0 MAC, 0 PPPoE Header
  Input Info: 0 Normal, 0 Drop, 345 Reserve, 0 Lost
  Output Err : 0 SessionState, 0 no ref, 0 length
  Output Info: 0 Normal, 0 Drop, 0 Reserve, 0 Lost

 There is 1 pppoe session in System
```

The following example displays all PPPoE session information.

```
R1# show pppoe session
state is SESSION ,my mac is 00.D0.F8.22.33.43 , peer mac is 00.60.4F.67.02.50
   Timer is running: 59750
```

The following example displays all PPPoE tunnel information.

```
R1# show pppoe tunnel
state is SESSION ,my mac is 00.D0.F8.22.33.43 , peer mac is 00.60.4F.67.02.50
   Timer is running: 59003
```

**Platform Description**

N/A

# IP Address & Application Commands

# 1 IP Address/Service Commands

## 1.1 ip-address

Use this command to configure the IP address of an interface. Use the **no** form of this command to restore the default setting.

**ip address** *ip-address network-mask* [ **secondary** ]

**no ip address** [ *ip-address network-mask* [ **secondary** ] ]

**Parameter Description**

| Parameter | Description |
|---|---|
| *ip-address* | 32-bit IP address, with 8 bits in one group in decimal format. Groups are separated by dots. |
| *network-mask* | 32-bit network mask. 1 stands for the mask bit, 0 stands for the host bit, with 8 bits in one group in decimal format. Groups are separated by dots. |

**Defaults** No IP address is configured for the interface by default.

**Command Mode** Interface configuration mode.

**Usage Guide** The equipment cannot receive and send IP packets before it is configured with an IP address. After an IP address is configured for the interface, the interface is allowed to run the Internet Protocol (IP).

The network mask is also a 32-bit value that identifies which bits among the IP address is the network portion. Among the network mask, the IP address bits that correspond to value “1” are the network address. The IP address bits that correspond to value “0” are the host address. For example, the network mask of Class A IP address is “255.0.0.0”. You can divide a network into different subnets using the network mask. Subnet division means to use the bits in the host address part as the network address part, so as to reduce the capacity of a host and increase the number of networks. In this case, the network mask is called subnet mask.

The RGOS software supports multiple IP address for an interface, in which one is the primary IP address and others are the secondary 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.

**Configuration Examples** The following example configures the primary IP address and the network mask as 10.10.10.1 and 255.255.255.0 respectively .

```
Ruijie(config)# interface gigabitEthernet 0/1
Ruijie(config-if-GigabitEthernet 0/1)# ip address 10.10.10.1 255.255.255.0
```

**Related Commands**

| Command | Description |
|---|---|
| **show interface** | Displays detailed information of the interface. |

**Platform Description** N/A

## 1.2 ip address negotiate

Use this command to configure an IP address for the interface through PPP negotiation. Use the **no** form of this command to restore the setting.
**ip address negotiate**
**no ip address negotiate**

**Parameter Description**

| Parameter | Description |
|---|---|
| N/A | N/A |

**Defaults** This function is disabled by default.

**Command Mode** Interface configuration mode

**Usage Guide** Only the PPP interface of the router supports IP address configuration through PPP negotiation. After the interface is configured with the **ip address negotiate** command, the peer end should be configured with the **peer default ip address** command.

**Configuration Examples** The following example obtains an IP address for the interface through PPP negotiation.

```
Ruijie(config)# interface dialer 1
Ruijie(onfig-if-dialer 1)# ip address negotiate
```

**Related Commands**

| Command | Description |
|---|---|
| N/A | N/A |

**Platform Description** N/A

## 1.3 ip address-pool local

Use this command to enable the IP address pool function. Use the **no** form of this command to disable this function.

**ip address-pool local**

**no ip address-pool local**

**Parameter Description**

| Parameter | Description |
|---|---|
| N/A | N/A |

**Defaults** This function is enabled by default.

**Command Mode** Global configuration mode

**Usage Guide** This function is enabled by default. PPP users can allocate an IP address to the peer end from the IP address pool configured. If you can use the **no ip address-pool local** command to disable this function and clear all configured IP address pools.

**Configuration Examples** The following example enables the IP address pool function.

```
Ruijie(config)# ip address-pool local
```

**Related Commands**

| Command | Description |
|---|---|
| N/A | N/A |

**Platform Description** N/A

## 1.4 ip broadcast-addresss

Use this command to define a broadcast address for an interface in the interface configuration mode. Use the **no** form of this command to restore the default setting.

**ip broadcast-addresss** *ip-address*

**no ip broadcast-addresss**

**Parameter Description**

| Parameter | Description |
|---|---|
| *ip-address* | Broadcast address of IP network |

**Defaults** The default IP broadcast address is 255.255.255.255.

**Command Mode** Interface configuration mode.

**Usage Guide** At present, the destination address of IP broadcast packet is all “1”, represented as 255.255.255.255. The RGOS software can generate broadcast packets with other IP addresses through definition, and can receive both all “1” and the broadcast packets defined by itself.

**Configuration Examples** The following example sets he destination address of IP broadcast packets generated by this interface to 0.0.0.0.

```
Ruijie(config-if)# ip broadcast-address 0.0.0.0
```

**Related Commands**

| Command | Description |
|---|---|
| N/A | N/A |

**Platform Description** N/A

## 1.5 ip icmp error-interval

Use this command to set the rate to send the ICMP destination unreachable packets triggered by DF in the IP header. Use the **no** form of this command to restore the default setting.

ip icmp error-interval DF milliseconds [ *bucket-size* ]

**no ip icmp error-interval DF** *milliseconds* [ *bucket-size* ]

Use this command to set the rate to send other ICMP error packets. Use the **no** form of this command to restore the default setting.

ip icmp error-interval milliseconds [bucket-size]

**no ip icmp error-interval** *milliseconds* [ *bucket-siz* ]

**Parameter Description**

| Parameter | Description |
|---|---|
| *milliseconds* | The refresh period of the token bucket, in the range from 0 to 2147483647 in the unit of milliseconds. 0 indicates no limit on the rate to send ICMP error packets.<br>The default is 100. |
| *bucket-size* | The number of tokens in the bucket, in the range is from 1 to 200. The default is 10. |

**Defaults** The default rate is 10 packets per 100 millisecond.

**Command Mode** Global configuration mode.

**Usage Guide** To prevent DoS attack, the token bucket algorithm is adopted to limit the rate to send ICMP error packets.

If IP packets need to be fragmented while the DF is set to 1, the device sends ICMP destination

unreachable packets numbered 4 to the source IP address for path MTU discovery. Rate limits on ICMP destination unreachable packets and other error packets are needed to prevent path MTU discovery failure.
It is recommended to set the refresh period to an integral multiple of 10 milliseconds. If the refresh period is not an integral multiple of 10 milliseconds, it is adjusted automatically. For example, 1 per 5 milliseconds is adjusted to 2 per 10 milliseconds; 3 per 15 milliseconds is adjusted to 2 per 10 milliseconds.

**Configuration Examples**

The following example sets the rate to send the ICMP destination unreachable packets triggered by DF in the IP header to 100 per second.

```
Ruijie(config)# ip icmp error-interval DF 1000 100
```

The following example sets the rate to send other ICMP error packets to 10 per second.

```
Ruijie(config)# ip icmp error-interval 1000 10
```

**Related Commands**

| Command | Description |
|---|---|
| N/A | N/A |

**Platform Description**

N/A

## 1.6 ip icmp timestamp

Use this command to enbale the device to return a Timestamp Reply. Use the **no** form of this command to disable returning of Timestamp Reply.
**ip icmp timestamp**
**no ip icmp timestamp**

**Parameter Description**

| Parameter | Description |
|---|---|
| N/A | N/A |

**Defaults**

This function is enabled by default.

**Command Mode**

Global configuration mode.

**Usage Guide**

N/A

**Configuration Examples**

The following example disables the device to return a Timestamp Reply.

```
Ruijie(config)# no ip icmp timestamp
```

**Related Commands**

| Command | Description |
|---|---|
| N/A | N/A |

**Platform Description** N/A

## 1.7 ip directed-broadcast

Use this command to enable the conversion from IP directed broadcast to physical broadcast in the interface configuration mode. Use the **no** form of this command to restore the default setting.

**ip directed-broadcast** [ *access-list-number* ]

**no ip directed-broadcast**

**Parameter Description**

| Parameter | Description |
|---|---|
| *access-list-number* | (Optional) Access list number, in the range from 1 to 199 and from 1300 to 2699. After an access list number has been defined, only the IP directed broadcast packets that match this access list are converted. |

**Defaults** This function is disabled by default.

**Command Mode** Interface configuration mode.

**Usage Guide** IP directed broadcast packet is an IP packet whose destination address is an IP subnet broadcast address. For example, the packet with the destination address 172.16.16.255 is called a directed broadcast packet. However, the node that generates this packet is not a member of the destination subnet.

The device that is not directly connected to the destination subnet receives an IP directed broadcast packet and handles this packet in the same way as forwarding a unicast packet. After the directed broadcast packet reaches a device that is directly connected to this subnet, the device converts the directed broadcast packet into a flooding broadcast packet (typically the broadcast packet whose destination IP address is all “1”), and then sends the packet to all the hosts in the destination subnet in the manner of link layer broadcast.

You can enable conversion from directed broadcast into physical broadcast on a specified interface, so that this interface can forward a direct broadcast packet to a directly connected network. This command affects only the final transmission of directed broadcast packets that have reached the destination subnet instead of normal forwarding of other directed broadcast packets.

You can also define an access list on an interface to control which directed broadcast packets to forward. After an access list is defined, only the packets that conform to the conditions defined in the access list undergo conversion from directed broadcast into physical broadcast.

If the **no ip directed-broadcast** command is configured on an interface, RGOS will discard the directed broadcast packets received from the directly connected network.

**Configuration Examples** The following example enables forwarding of directed broadcast packet on the fastEthernet 0/1 port of a device.

```
Ruijie(config)# interface fastEthernet 0/1
Ruijie(config-if)# ip directed-broadcast
```

**Related Commands**

| Command | Description |
|---|---|
| N/A | N/A |

**Platform Description** N/A

## 1.8 ip local pool

Use this command to create an IP address pool. Use the **no** form of this command to remove the setting.

**ip local pool** *pool-name low-ip-address* [ *high-ip-address* ]

**no ip local pool** *pool-name* [ *low-ip-address* [ *high-ip-address* ] ]

**Parameter Description**

| Parameter | Description |
|---|---|
| *pool-name* | Specifies the address pool name. The default name is **default**. |
| *low-ip-address* | The start IP address in the address pool. |
| *high-ip-address* | (Optional) The end IP address in the address pool. |

**Defaults** No IP address pool is configured by default.

**Command Mode** Global configuration mode

**Usage Guide** This command is used to create one or multiple IP address pools for PPP to allocate addresses to users.

**Configuration Examples** The following example creates an IP address pool named quark ranging from 172.16.23.0 to 172.16.23.255.

```
Ruijie(config)#ip local pool quark 172.16.23.0 172.16.23.255
```

**Related Commands**

| Command | Description |
|---|---|
| N/A | N/A |

**Platform Description** N/A

## 1.9 ip mask-reply

Use this command to configure the RGOS software to respond the ICMP mask request and send an ICMP response message in the interface configuration mode. Use the **no** form of this

command to restore the default setting.

**ip mask-reply**

**no ip mask-reply**

**Parameter Description**

| Parameter | Description |
|---|---|
| N/A | N/A |

**Defaults** This function is disabled by default.

**Command mode** Interface configuration mode.

**Usage Guide** Sometimes, a network device needs the subnet mask of a subnet on the Internet. To obtain such information, the network device can send an ICMP mask request message, and the network device that receives this message will send a mask response message.

**Configuration Examples** The following example sets the FastEthernet 0/1 interface of a device to respond the ICMP mask request message.

```
Ruijie(config)# interface fastEthernet 0/1
Ruijie(config-if)# ip mask-reply
```

**Related Commands**

| Command | Description |
|---|---|
| N/A | N/A |

**Platform Description** N/A

## 1.10 ip mtu

Use this command to set the Maximum Transmission Unit (MTU) for an IP packet in the interface configuration mode. Use the **no** form of this command is restore the default setting.

**ip mtu** *bytes*

**no ip mtu**

**Parameter Description**

| Parameter | Description |
|---|---|
| *bytes* | Maximum transmission unit of IP packet , in the range from 68 to 1500 bytes |

**Defaults** It is the same as the value configured in the interface command **mtu** by default.

**Command Mode** Interface configuration mode.

**Usage Guide** If an IP packet is larger than the IP MTU, the RGOS software will split this packet. All the devices in the same physical network segment must have the same IP MTU for the

interconnected interface.
If the interface configuration command **mtu** is used to set the maximum transmission unit value of the interface, IP MTU will automatically match with the MTU value of the interface. However, if the IP MTU value is changed, the MTU value of the interface will remain unchanged.

**Configuration Examples** The following iexample sets the IP MTU value of the fastEthernet 0/1 interface to 512 bytes.

```
Ruijie(config)# interface fastEthernet 0/1
Ruijie(config-if)# ip mtu 512
```

**Related Commands**

| Command | Description |
|---|---|
| **mtu** | Sets the MTU value of an interface. |

**Platform Description** N/A

## 1.11 ip redirects

Use this command to allow the RGOS software to send an ICMP redirection message in the interface configuration mode. Use the **no** form of this command to disable this function.
**ip redirects**
**no ip redirects**

**Parameter Description**

| Parameter | Description |
|---|---|
| N/A | N/A |

**Defaults** This function is enabled by default.

**Command Mode** Interface configuration mode.

**Usage Guide** When the route is not optimum, it may make the device to receive packets through one interface and send it though the same interface. If the device sends the packet through the interface through which this packet is received, the device will send an ICMP redirection message to the data source, telling the data source that the gateway for the destination address is another device in the subnet. In this way the data source will send subsequent packets along the optimum path.

**Configuration Examples** The following example disables ICMP redirection for the fastEthernet 0/1 interface.

```
Ruijie(config)# interface fastEthernet 0/1
Ruijie(config-if)# no ip redirects
```

**Related Commands**

| Command | Description |
|---|---|
| N/A | N/A |

**Platform Description** N/A

## 1.12 ip source-route

Use this command to allow the RGOS software to process an IP packet with source route information in global configuration mode. Use the **no** form of this command to disable this function.

**ip source-route**

**no ip source-route**

**Parameter Description**

| Parameter | Description |
|---|---|
| N/A | N/A |

**Defaults** This function is enabled by default.

**Command Mode** Global configuration mode.

**Usage Guide** RGOS supports IP source route. When the device receives an IP packet, it will check the options of the IP packet, such as strict source route, loose source route and record route. Details about these options can be found in RFC 791. If an option is found to be enabled in this packet, a response will be made. If an invalid option is detected, an ICMP parameter problem message will be sent to the data source, and then this packet is discarded.

**Configuration Examples** The following example disables the IP source route.

```
Ruijie(config)# no ip source-route
```

**Related Commands**

| Command | Description |
|---|---|
| N/A | N/A |

**Platform Description** N/A

## 1.13 ip ttl

Use this command to set the TTL value of the unicast packet. Use the **no** form of this command to restore the default setting.

**ip ttl** *value*

**no ip ttl**

**Parameter Description**

| Parameter | Description |
|---|---|
| *value* | Sets the TTL value of the unicast packet, in the range from 0 to 255. |

**Defaults** The default is 64.

**Command Mode** Global configuration mode

**Usage Guide** N/A

**Configuration Examples** The following example sets the TTL value of the unicast packet to 100.

```
Ruijie(config)# ip ttl 100
```

**Related Commands**

| Command | Description |
| --- | --- |
| N/A | N/A |

**Platform Description** N/A

## 1.14 ip ttl-expires enable

This command is used to enable notifications of expired TTL. Use the **no** form of this command to disable this function.

**ip ttl-expires enable**

**no ttl-expires enable**

**Parameter Description**

| Parameter | Description |
| --- | --- |
| N/A | N/A |

**Defaults** By default, notifications are enabled to indicate expired TTL.

**Command mode** Global configuration mode

**Usage Guide** N/A

**Configuration Examples** The following example disables notifications indicating expired TTL.

```
Ruijie(config)# no ttl-expires enable
```

**Related Commands**

| Command | Description |
| --- | --- |
| N/A | N/A |

**Platform Description** N/A

## 1.15 ip unnumbered

This command is used to configure unnumbered interfaces. After an interface is set to an unnumbered interface, IP can be run on the interface and packets can be sent or received on the interface. Use the **no** form of this command to restore the default setting.

**ip unnumbered** *interface-type interface-number*

**no ip unnumbered**

**Parameter Description**

| Parameter | Description |
| --- | --- |
| *interface-type* | Type of the associated interface |
| *interface-number* | No. of the associated interface |

**Defaults** No unnumbered interface is configured by default.

**Command mode** Interface configuration mode

**Usage Guide** An unnumbered interface indicates that IP is enabled on the interface but no IP address is allocated for the interface. An unnumbered interface must associate with an interface with an IP address. The source IP address of the IP packets generated on an unnumbered interface is the IP address of the associated interface. In addition, the routing protocol process determines whether to send route update packets to the unnumbered interface according to the IP address of the associated interface. Pay attention to the following when using an unnumbered interface:

An Ethernet interface cannot be set to an unnumbered interface.

When SLIP, HDLC, PPP, LAPB, and Frame-relay are encapsulated on a serial port, the port can be set to an unnumbered interface. When a frame relay is encapsulated, only a point-to-point subinterface can be set to an unnumbered interface. In the case of X.25 encapsulation, unnumbered interface is not allowed.

The **ping** command cannot be used to check whether an unnumbered interface is working properly because the interface does not have an IP address. The status of an unnumbered interface can be remotely monitored over SNMP.

The network cannot be enabled using an unnumbered interface.

**Configuration Examples** to the following example configures the local interface as an unnumbered interface and sets the associated interfacet to FastEthernet 0/1 (an IP address is configured for the interface).

```
Ruijie(config-if)# ip unnumbered fastEthernet 0/1
```

| Related Commands | Command | Description |
|---|---|---|
| | **show interface** | Displays the detailed information about the interface. |

**Platform Description** N/A

## 1.16 ip unreachables

Use this command to allow the RGOS software to generate ICMP destination unreachable messages. Use the **no** form of this command to disable this function.

**ip unreachables**

**no ip unreachables**

| Parameter Description | Parameter | Description |
|---|---|---|
| | N/A | N/A |

**Defaults** This function is enabled by default.

**Command Mode** Interface configuration mode.

**Usage Guide** RGOS software will send a ICMP destination unreachable message if it receives unicast message with self-destination-address and can not process the upper protocol of this message.
RGOS software will send ICMP host unreachable message to source data if it can not forward a message due to no routing.
This command influences all ICMP destination unreachable messages.

**Configuration Examples** The following example disables sending ICMP destination unreachable message on FastEthernet 0/1.

```
Ruijie(config)# interface fastEthernet 0/1
Ruijie(config-if)# no ip unreachables
```

| Related Commands | Command | Description |
|---|---|---|
| | N/A | N/A |

**Platform Description** N/A

## 1.17 peer default ip address

Use this command to allocate an IP address to the peer end through PPP negotiation. Use the **no** form of this command to restore the default setting.

**peer default ip address** { *ip-address* | **pool** [*pool-name*] }

**no peer default ip address**

**Parameter Description**

| Parameter | Description |
|---|---|
| *ip-address* | Allocates an IP address to the peer end. |
| *pool-name* | (Optional) Specifies the address pool name. If not specified, the default address pool is used. |

**Defaults** No IP address is allocated to the peer end through PPP negotiaon by default.

**Command Mode** Interface configuration mode.

**Usage Guide** If the local end is configured with an IP address while the peer end not, you can enable the local end to allocate an IP address to the peer end by configuring the **ip address negotiate** command on the peer end and the **peer default ip address** on the local end.
This command is configured on PPP interface supporting encapsulation PPP or SLIP.
The **peer default ip address pool** command is used to allocate an IP address to the peer end from the address pool, configured by using the **ip local poo**l command.
The **peer default ip address** *ip-address* command is used to specify an IP address for the peer end. This command cannot be configured on virtual template interfaces and asyn interfaces.

**Configuration Examples** The following example enables interface dialer 1 to allocate IP address 10.0.0.1 to the peer end.

```
Ruijie(config)# interface dialer 1
Ruijie(config-if-dialer 1)# peer default ip address 10.0.0.1
```

**Related Commands**

| Command | Description |
|---|---|
| N/A | N/A |

**Platform Description** N/A

## 1.18 show ip interface

Use this command to display the IP status information of an interface.
**show ip interface** [ *interface-type interface-number* | **brief** ]

**Parameter Description**

| Parameter | Description |
|---|---|
| *interface-type* | Specifies interface type. |
| *interface-number* | Specifies interface number. |
| *brief* | Displays the brief configurations about the IP of the layer-3 interface (including the interface primary ip, secondary ip and interface status) |

**Defaults** N/A.

**Command Mode** Privileged EXEC mode.

**Usage Guide** When an interface is available, RGOS will create a direct route in the routing table. The interface is available in that the RGOS software can receive and send packets through this interface. If the interface changes from available status to unavailable status, the RGOS software removes the appropriate direct route from the routing table.
If the interface is unavailable, for example, two-way communication is allowed, the line protocol status will be shown as “UP”. If only the physical line is available, the interface status will be shown as “UP”.
The results shown may vary with the interface type, because some contents are the interface-specific options

**Configuration Examples** The following exmaple displays the output of the **show ip interface brirf command**.

```
Ruijie#show ip interface brief
Interface IP-Address(Pri) IP-Address(Sec) Status Protocol
GigabitEthernet 0/10 2.2.2.2/24 3.3.3.3/24 down down
GigabitEthernet 0/11 no address no address down down
VLAN 1 1.1.1.1/24 no address down down
```

Description of fields:

| Field | Description |
|---|---|
| Status | Link status of an interface. The value can be **up**, **down**, or **administratively down**. |
| Protocol | IPv4 protocol status of an interface. |

The following example displays the output of the **show ip interface vlan** command.

```
SwitchA#show ip interface vlan 1
VLAN 1
 IP interface state is: DOWN
 IP interface type is: BROADCAST
 IP interface MTU is: 1500
 IP address is:
 1.1.1.1/24 (primary)
 IP address negotiate is: OFF
 Forward direct-broadcast is: OFF
 ICMP mask reply is: ON
 Send ICMP redirect is: ON
 Send ICMP unreachabled is: ON
 DHCP relay is: OFF
 Fast switch is: ON
 Help address is:
 Proxy ARP is: OFF
ARP packet input number: 0
 Request packet:  0
```

```
 Reply packet:  0
 Unknown packet: 0
TTL invalid packet number: 0
ICMP packet input number: 0
 Echo request:  0
Echo reply:  0
 Unreachable:  0
 Source quench:  0
 Routing redirect:  0
```

Description of fields in the results:

| Field | Description |
|---|---|
| IP interface state is: | The network interface is available, and both its interface hardware status and line protocol status are “UP”. |
| IP interface type is: | Show the interface type, such as broadcast, point-to-point, etc. |
| IP interface MTU is: | Show the MTU value of the interface. |
| IP address is: | Show the IP address and mask of the interface. |
| IP address negotiate is: | Show whether the IP address is obtained through negotiation. |
| Forward direct-broadcast is: | Show whether the directed broadcast is forwarded. |
| ICMP mask reply is: | Show whether an ICMP mask response message is sent. |
| Send ICMP redirect is: | Show whether an ICMP redirection message is sent. |
| Send ICMP unreachabled is: | Show whether an ICMP unreachable message is sent. |
| DHCP relay is: | Show whether the DHCP relay is enabled. |
| Fast switch is: | Show whether the IP fash switching function is enabled. |
| Route horizontal-split is: | Show whether horizontal split is enabled, which will affect the route update behavior of the distance vector protocol. |
| Help address is: | Show the helper IP address. |
| Proxy ARP is: | Show whether the agent ARP is enabled. |
| ARP packet input number:<br>Request packet:<br>Reply packet:<br>Unknown packet: | Show the total number of ARP packets received on the interface, including:<br>ARP request packet<br>ARP reply packet<br>Unknown packet |
| TTL invalid packet number: | Show the TTL invalid packet number |
| ICMP packet input number:<br>Echo request:<br>Echo reply:<br>Unreachable: | Show the total number of ICMP packets received on the interface, including:<br>Echo request packet<br>Echo reply packet |

| | |
|---|---|
| Source quench:<br>Routing redirect: | Unreachable packet<br>Source quench packet<br>Routing redirection packet |
| Outgoing access list is | Show whether an outgoing access list has been configured for an interface. |
| Inbound access list is | Show whether an incoming access list has been configured for an interface. |

**Related Commands**

| Command | Description |
|---|---|
| N/A. | N/A. |

**Platform Description** N/A.

## 1.19 show ip packet statistics

Use this command to display the statistics of IP packets.

**show ip packet statistics** [ **total** | *interface-name* ]

**Parameter Description**

| Parameter | Description |
|---|---|
| *interface-name* | Interface name |
| *total* | Displays the total statistics of all interfaces. |

**Defaults** N/A.

**Command Mode** Privileged EXEC mode.

**Usage Guide** N/A.

**Configuration Examples** The following example displays the output of this command.

```
Ruijie# show ip packet statistics
Total
 Received 1000 packets, 1000000 bytes
 Unicast:1000,Multicast:0,Broadcast:0
 Discards:0
 HdrErrors:0(BadChecksum:0,TTLExceeded:0,Others:0)
 NoRoutes:0
 Others:0
 Sent 100 packets, 6000 bytes
 Unicast:50,Multicast:50,Broadcast:0

VLAN 1
 Received 1000 packets, 1000000 bytes
```

```
Unicast:1000,Multicast:0,Broadcast:0
Discards:0
HdrErrors:0(BadChecksum:0,TTLExceeded:0,Others:0)
NoRoutes:0
Others:0
Sent 100 packets, 6000 bytes
Unicast:50,Multicast:50,Broadcast:0
```

**Related Commands**

| Command | Description |
|---|---|
| **ip default-gateway** | Configures the default gateway, which is only supported on the Layer 2 switch. |

**Platform Description** N/A

## 1.20 show ip pool

Use this command to display the IP address pool.

**show ip pool** [ *pool-name* ]

**Parameter Description**

| Parameter | Description |
|---|---|
| *pool-name* | Specifies the IP address pool. |

**Defaults** N/A

**Command Mode** Privileged EXEC mode

**Usage Guide** N/A

**Configuration Examples** The following example displays all IP address ranges.

```
Ruijie# show ip pool
Ruijie(config)#show ip pool
Pool              Begin          End               Free   In use
default           1.1.1.1        1.1.1.1              1       0
pool1             2.2.2.2        2.2.2.254          253       0
pool2             3.1.1.1        3.2.1.1          65537       0
pool3             192.168.1.1    192.168.1.254
```

| Field | Description |
|---|---|
| Pool | Address pool name |
| Begin | The start IP address of the address pool |
| Free | The number of free IP addresses in the address pool |

| | |
|---|---|
| In use | The number of IP addresses in use in the address pool |

| Related Commands | Command | Description |
|---|---|---|
| | N/A | N/A |

**Platform Description** N/A

## 1.21 show ip raw-socket

Use this command to display IPv4 raw sockets.

**show ip raw-socket [** *num* ]

| Parameter Description | Parameter | Description |
|---|---|---|
| | *num* | Protocol. |

**Defaults** N/A.

**Command Mode** Priviledged EXEC mode.

**Usage Guide** N/A.

**Configuration Examples** The following example displays all IPv4 raw sockets.

```
Ruijie# show ip raw-socket
Number Protocol Process name
1      ICMP     dhcp.elf
2      ICMP     vrrp.elf
3      IGMP     igmp.elf
4      VRRP     vrrp.elf
Total: 4
```

Field Description

| Field | Description |
|---|---|
| Number | Number |
| Protocol | Protocol |
| Process name | Process name |
| Total | Total number |

| Related Commands | Command | Description |
|---|---|---|
| | N/A | N/A |

**Platform** N/A

**Description**

## 1.22 show ip sockets

Use this command to display all IPv4 sockets.

**show ip sockets**

| **Parameter Description** | **Parameter** | **Description** |
|---|---|---|
| | N/A. | N/A. |

**Defaults** N/A.

**Command Mode** Privileged EXEC mode.

**Usage Guide** N/A.

**Configuration Examples** The following displays all IPv4 sockets.

```
Ruijie# show ip sockets
Number Process name    Type    Protocol LocalIP:Port  ForeignIP:Port
State
1     dhcp.elf        RAW     ICMP    0.0.0.0:1    0.0.0.0:0
*
2     vrrp.elf        RAW     ICMP    0.0.0.0:1    0.0.0.0:0
*
3     igmp.elf        RAW     IGMP    0.0.0.0:2    0.0.0.0:0
*
4     vrrp.elf        RAW     VRRP    0.0.0.0:112   0.0.0.0:0
*
5     dhcpc.elf       DGRAM   UDP     0.0.0.0:68    0.0.0.0:0
*
6     rg-snmpd        DGRAM   UDP     0.0.0.0:161   0.0.0.0:0
*
7     wbav2           DGRAM   UDP     0.0.0.0:2000  0.0.0.0:0
*
8     vrrp_plus.elf   DGRAM   UDP     0.0.0.0:3333  0.0.0.0:0
*
9     mpls.elf        DGRAM   UDP     0.0.0.0:3503  0.0.0.0:0
*
10    rds_other_th    DGRAM   UDP     0.0.0.0:3799  0.0.0.0:0
*
11    rg-snmpd        DGRAM   UDP     0.0.0.0:14800 0.0.0.0:0
*
12    rg-sshd         STREAM  TCP     0.0.0.0:22    0.0.0.0:0
LISTEN
```

```
13    rg-telnetd      STREAM   TCP     0.0.0.0:23    0.0.0.0:0
LISTEN
14    wbard           STREAM   TCP     0.0.0.0:4389  0.0.0.0:0
LISTEN
15    wbard           STREAM   TCP     0.0.0.0:7165  0.0.0.0:0
LISTEN
Total: 15
```

Field Description

| Field | Description |
|---|---|
| Number | Serial number. |
| Process name | Process name. |
| Type | Socket type, including the following types:<br>RAW: raw sockets<br>DGRAM: datagram type<br>STREAM: stream type. |
| Protocol | Protocol. |
| LocalIP:Port | Local IP address and port. |
| ForeignIP:Port | Peer IP address and port. |
| State | State. This field is for only TCP sockets. |
| Total | The total number of sockets. |

**Related Commands**

| Command | Description |
|---|---|
| N/A | N/A |

**Platform Description** N/A

## 1.23 show ip udp

Use this command to display IPv4 UDP sockets.

**show ip udp** [ **local-port** *num* ]

Use this command to display IPv4 UDP socket statistics.

**show ip udp statistics**

**Parameter Description**

| Parameter | Description |
|---|---|
| **local-port** *num* | Local port number |

**Defaults** N/A.

**Command Mode** Privileged EXEC mode.

**Usage Guide** N/A.

**Configuration Examples** The following example displays all IPv4 UDP sockets.

```
Ruijie# show ip udp
Number Local Address        Peer Address         Process name
1      0.0.0.0:68           0.0.0.0:0           dhcpc.elf
2      0.0.0.0:161          0.0.0.0:0           rg-snmpd
3      0.0.0.0:2000         0.0.0.0:0           wbav2
4      0.0.0.0:3333         0.0.0.0:0           vrrp_plus.elf
5      0.0.0.0:3503         0.0.0.0:0           mpls.elf
6      0.0.0.0:3799         0.0.0.0:0           rds_other_th
7      0.0.0.0:14800        0.0.0.0:0           rg-snmpd
```

Field Description

| Field | Description |
|---|---|
| Number | Number. |
| Local Address | Local IP address and port. |
| Peer Address | Peer IP address and port. |
| Process name | Process name. |

**Related Commands**

| Command | Description |
|---|---|
| N/A | N/A |

**Platform Description** N/A

# 2 ARP Commands

## 2.1 arp

Use this command to add a permanent IP address and MAC address mapping to the ARP cache table. Use the **no** form of this command to restore the default setting.

**arp** *ip-address MAC-address type*

**no arp** *ip-address*

**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 by default.

**Command Mode** Global configuration mode.

**Usage Guide** RGOS finds the 48-bit MAC address according to the 32-bit IP address using the ARP cache table. Since most hosts support dynamic ARP resolution, usually static ARP mapping is not necessary. The **clear arp-cache** command can be used to delete the ARP mapping that is learned dynamically.

**Configuration Examples** The following example sets an ARP static mapping record for a host in the Ethernet.

```
Ruijie(config)# arp 1.1.1.1 4e54.3800.0002 arpa
```

**Related Commands**

| Command | Description |
|---|---|
| clear arp-cache | Clears the ARP cache table |

**Platform Description** N/A

## 2.2 arp-learning

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

**arp-learning enable**

**no arp-learning enable**

**Parameter Description**

| Parameter | Description |
| --- | --- |
| N/A | N/A |

**Defaults** This function is enabled by default

**Command Mode** Interface configuration mode

**Usage Guide** After the device learns the dynamic ARP and turns it to the static ARP through Web, it is recommended to enable ARP learning. Otherwise, it is not recommended to enable this function. If this function is disabled with dynamic ARP existing, you can turn dynamic ARP to static ARP through Web. You can also clear the dynamic ARP using the clear arp command to deny the specified user's access to Internet. Otherwise, the dynamic ARP will be aged and then cleared. After this function is disabled, the AnyIP function and trust ARP detection are disabled.

**Configuration Examples** The following example enables ARP learning.

```
Ruijie(config)# interface gi 0/0
Ruijie(config-if-GigabitEthernet 0/0)# arp-learning enable
```

The following example disbales ARP learning.

```
Ruijie(config)# interface gi 0/0
Ruijie(config-if-GigabitEthernet 0/0)# no arp-learning enable
```

**Related Commands**

| Command | Description |
| --- | --- |
| N/A | N/A |

**Platform Description** N/A

## 2.3 arp cache interface-limit

Use this command to set the maximum number of ARP learned on the interface.
Use the **no** form of this command to restore the default setting.
**arp cache interface-limit** *limit*
**no arp cache interface-limit**

**Parameter Description**

| Parameter | Description |
| --- | --- |
| *limit* | Sets the maximum number of ARP learned on the interface, including static and dynamic ARPs, in the range from 0 to the number supported on the interface. 0 indicates that the number is not limited. |

**Defaults** The default is 0.

**Command Mode** Interface configuration mode

**Usage Guide** This function can prevent ARP attacks from generating ARP entries to consume memory. *limit* must be no smaller than the number of ARPs learned on the interface. Otherwise, the configuration does not take effect.

**Configuration Examples** The following example sets the maximum number of ARP learned on the interface to 300.

```
Ruijie(config)# interface gi 0/0
Ruijie(config-if-GigabitEthernet 0/0)# arp cache interface-limit 300
```

The following example restores the default setting.

```
Ruijie(config)# interface gi 0/0
Ruijie(config-if-GigabitEthernet 0/0)# no arp any-ip
```

**Related Commands**

| Command | Description |
|---|---|
| N/A | N/A |

**Platform Description** N/A

## 2.4 arp gratuitous-send interval

Use this command to set the interval of sending the free ARP request message on the interface. Use the**no** form of this command to restore the default setting.

**arp gratuitous-send interval** *seconds* [ *number* ]

**no arp gratuitous-send**

**Parameter Description**

| Parameter | Description |
|---|---|
| *seconds* | The time interval to send the free ARP request message in the range from 1 to 3600 in the unit of seconds. |
| *number* | The number of free ARP request messages to be sent in the range from 1 to 100 in the unit of seconds. The default value is 1. |

**Defaults** This function is disabled by default.

**Command Mode** Interface configuration mode.

**Usage Guide** If an interface of the switch is used as the gateway of its downlink devices and counterfeit gateway behavior occurs in the downlink devices, you can configure to send the free ARP request message regularly on this interface to notify that the switch is the real gateway.

**Configuration** The following example sets to send one free ARP request to SVI 1 per second.

**Examples**

```
Ruijie(config)# interface vlan 1
Ruijie(config-if)# arp gratuitous-send interval 1
```

The following example stops sending the free ARP request to SVI 1.

```
Ruijie(config)# interface vlan 1
Ruijie(config-if)# no arp gratuitous-send
```

**Related Commands**

| Command | Description |
|---|---|
| N/A | N/A |

**Platform Description** N/A

## 2.5 arp retry interval

Use this command to set the frequency for sending the arp request message locally, namely, the time interval between two continuous ARP requests sent for resolving one IP address. Use the **no** form of this command to restore the default setting.

**arp retry interval** *seconds*

**no arp retry interval**

**Parameter Description**

| Parameter | Description |
|---|---|
| *seconds* | Time for retransmitting the ARP request message in the range from 1 to 3600 in the unit of seconds. |

**Defaults** The default is 1.

**Command Mode** Global configuration mode.

**Usage Guide** The switch sends the ARP request message frequently, and thus causing problems like network busy. In this case, you can set the retry interval of the ARP request message longer. In general, it should not exceed the aging time of the dynamic ARP entry.

**Configuration Examples** The following example sets the retry interval of the ARP request as 30 seconds.

```
Ruijie(config)# arp retry interval 30
```

**Related Commands**

| Command | Description |
|---|---|
| **arp retry times** | Number of times for retransmitting an ARP request message. |

**Platform Description** N/A

## 2.6 arp retry times

Use this command to set the local retry times of the ARP request message, namely, the times of sending the ARP request message to resolve one IP address. Use the **no** form of this command to restore the default setting.

**arp retry times** *number*

**no arp retry times**

**Parameter Description**

| Parameter | Description |
|---|---|
| *number* | The times of sending the same ARP request in the range from 1 to100.When it is set as 1, it indicates that the ARP request is not retransmitted, only 1 ARP request message is sent. |

**Defaults** The default is 5.

**Command Mode** Global configuration mode.

**Usage Guide** The switch sends the ARP request message frequently, and thus causing problems like network busy. In this case, you can set the retry times of the ARP request smaller. In general, the retry times should not be set too large.

**Configuration Examples** The following example sets the local ARP request not to be retried.

```
Ruijie(config)# arp retry times 1
```

The following example sets the local ARP request to be retried for one time.

```
Ruijie(config)# arp retry times 2
```

**Related Commands**

| Command | Description |
|---|---|
| **arp retry interval** | Interval for retransmitting an ARP request message |

**Platform Description** N/A

## 2.7 arp timeout

Use this command to configure the timeout for the ARP static mapping record in the ARP cache. Use the **no** form of this command to restore the default setting.

**arp timeout** *seconds*

**no arp timeout**

**Parameter Description**

| Parameter | Description |
|---|---|
| *secondsv* | The timeout is in the range from 0 to 2147483 in the unit of seconds. |

**Defaults** The default is 3600.

**Command Mode** Interface configuration mode

**Usage Guide** The ARP timeout setting is only applicable to the IP address and the MAC address mapping that are learned dynamically. The shorter the timeout, the truer the mapping table saved in the ARP cache, but the more network bandwidth occupied by the ARP. Hence the advantages and disadvantages should be weighted. Generally it is not necessary to configure the ARP timeout unless there is a special requirement.

**Configuration Examples** The following example sets the timeout for the dynamic ARP mapping record that is learned dynamically from FastEthernet port 0/1 to 120 seconds.

```
Ruijie(config)# interface fastEthernet 0/1
Ruijie(config-if)# arp timeout 120
```

**Related Commands**

| Command | Description |
|---|---|
| **clear arp-cache** | Clears the ARP cache list. |
| **show interface** | Displays the interface information. |

**Platform Description** N/A

## 2.8 arp trust-monitor enable

Use this command to enable egress gateway trusted ARP. Use the **no** form of this command to restore the default setting.

**arp trust-monitor enable**

**no arp trust-monitor enable**

**Parameter Description**

| Parameter | Description |
|---|---|
| N/A | N/A |

**Defaults** This function is disabled by default.

**Command Mode** Interface configuration mode

**Usage Guide** The egress gateway trusted ARP is different from GSN trusted ARP. With this function enabled, the device sends a unicast request for confirmation when learning an ARP table entry. The device learns the ARP table entry after receiving the response. When the device receives the ARP packet, only if the ARP table entry is aged or incomplete and the ARP packet is a response packet will the packet

be handled. After egress gateway trusted ARP is enabled, the aging time of the ARP table entry turns to 60 seconds. After this function is disabled, the aging time restores to 3600 seconds.

**Configuration Examples** The following example enables egress gateway trusted ARP.

```
Ruijie(config)# interface gi 0/0
Ruijie(config-if-GigabitEthernet 0/0)# arp trust-monitor enable
```

The following example disables engress gateway trusted ARP.

```
Ruijie(config)# interface gi 0/0
Ruijie(config-if-GigabitEthernet 0/0)# no arp trust-monitor enable
```

**Related Commands**

| Command | Description |
|---|---|
| N/A | N/A |

**Platform Description** N/A

## 2.9 arp unresolve

Use this command to set the maximum number of the unresolved ARP entries. Use **no** form of this command to restore the default setting.

**arp unresolve** *number*

**no arp unresolve**

**Parameter Description**

| Parameter | Description |
|---|---|
| *number* | The maximum number of the unresolved ARP entries in the range from 1 to the ARP table size supported by the device. |

**Defaults** The default is the ARP table size supported by the device.

**Command Mode** Global configuration mode.

**Usage Guide** If there are a large number of unresolved entries in the ARP cache table and they do not disappear after a period of time, this command can be used to limit the quantity of the unresolved entries.

**Configuration Examples** The following example sets the maximum number of the unresolved items to 500.

```
Ruijie(config)# arp unresolve 500
```

**Related Commands**

| Command | Description |
|---|---|
| N/A | N/A |

**Platform** N/A

**Description**

## 2.10 clear arp-cache

Use this command to remove a dynamic ARP mapping record from the ARP cache table and clear an IP route cache table.

**clear arp-cache** [ *ip* [*mask* ] ] | **interface** *interface-name* ]

**Parameter Description**

| Parameter | Description |
|---|---|
| *ip* | Deletes ARP entries of the specified IP address. by default, all dynamic ARP entries are deleted. |
| *mask* | Deletes ARP entries in a subnet mask. The dynamic ARP entry specified by the IP address is deleted by default. |
| ***interface*** *interface-name* | Deletes dynamic ARP entries on the specified interface. Dynamic ARP entries are deleted on all interfaces by default. |

**Defaults** N/A

**Command Mode** Privileged EXEC mode

**Usage Guide** N/A

**Configuration Examples** The following example deletes all dynamic ARP mapping records.

```
Ruijie# clear arp-cache
```

The following deletes the dynamic ARP entry 1.1.1.1.

```
Ruijie# clear arp-cache 1.1.1.1
```

The following example deletes the dynamic ARP entry on interface SVI1.

```
Ruijie# clear arp-cache interface Vlan 1
```

**Related Commands**

| Command | Description |
|---|---|
| **arp** | Adds a static mapping record to the ARP cache table. |

**Platform Description** N/A

## 2.11 ip proxy-arp

Use this command to enable ARP proxy function on the interface. Use the **no** form of this command to restore the default setting.

**ip proxy-arp**

**no ip proxy-arp**

**Parameter Description**

| Parameter | Description |
| --- | --- |
| N/A | N/A |

**Defaults** N/A

**Command Mode** Interface configuration mode.

**Usage Guide** Proxy ARP helps those hosts without routing message obtain MAC address of other networks or subnet IP address. For example, a device receives an ARP request. The IP addresses of request sender and receiver are in different networks. However, the device that knows the routing of IP address of request receiver sends ARP response, which is Ethernet MAC address of the device itself.

**Configuration Examples** The following example enables ARP on FastEthernet port 0/1.

```
Ruijie(config)# interface fastEthernet 0/1
Ruijie(config-if)# ip proxy-arp
```

**Related Commands**

| Command | Description |
| --- | --- |
| N/A | N/A |

**Platform Description** N/A

## 2.12 show arp

Use this command to display the Address Resolution Protocol (ARP) cache table

**show arp** [ *interface-type interface-number*] | [*ip* [*mask*] | *mac-address* | **static** | **complete** | **incomplete** ] ]

**Parameter Description**

| Parameter | Description |
| --- | --- |
| *interface-type interface-number* | Displays the ARP entry of a specified Layer-2 or Layer-3 port. |
| *ip* | Displays the ARP entry of the specified IP address. |
| *mask* | Displays the ARP entries of the network segment included within the mask. |
| **static** | Displays all the static ARP entries. |
| **complete** | Displays all the resolved dynamic ARP entries. |
| **incomplete** | Displays all the unresolved dynamic ARP entries. |
| *mac-address* | Displays the ARP entry with the specified mac address. |

**Defaults** N/A

**Command Mode** Privileged EXEC mode

**Usage Guide** N/A

**Configuration Examples** The following example displays the output result of the **show arp** command:

```
Ruijie# show arp
Total Numbers of Arp: 7
Protocol Address Age(min) Hardware Type Interface
Internet 192.168.195.68 0 0013.20a5.7a5f arpa VLAN 1
Internet 192.168.195.67 0 001a.a0b5.378d arpa VLAN 1
Internet 192.168.195.65 0 0018.8b7b.713e arpa VLAN 1
Internet 192.168.195.64 0 0018.8b7b.9106 arpa VLAN 1
Internet 192.168.195.63 0 001a.a0b5.3990 arpa VLAN 1
Internet 192.168.195.62 0 001a.a0b5.0b25 arpa VLAN 1
Internet 192.168.195.5 -- 00d0.f822.33b1 arpa VLAN 1
```

The following example displays the output result of show arp 192.168.195.68

```
Ruijie# show arp 192.168.195.68
Protocol Address Age(min) Hardware Type Interface
Internet 192.168.195.68 1 0013.20a5.7a5f arpa VLAN 1
```

The following example displays the output result of **show arp** 192.168.195.0 255.255.255.0

```
Ruijie# show arp 192.168.195.0 255.255.255.0
Protocol Address Age(min) Hardware Type Interface
Internet 192.168.195.64 0 0018.8b7b.9106 arpa VLAN 1
Internet 192.168.195.2 1 00d0.f8ff.f00e arpa VLAN 1
Internet 192.168.195.5 -- 00d0.f822.33b1 arpa VLAN 1
Internet 192.168.195.1 0 00d0.f8a6.5af7 arpa VLAN 1
Internet 192.168.195.51 1 0018.8b82.8691 arpa VLAN 1
```

The following example displays the output result of **show arp** 001a.a0b5.378d

```
Ruijie# show arp 001a.a0b5.378d
Protocol Address Age(min) Hardware Type Interface
Internet 192.168.195.67 4 001a.a0b5.378d arpa VLAN 1
```

The following example displyas the output result of **show arp static**

```
Ruijie# show arp static
Protocol  Address  Age(min)  Hardware  Type   Interface        Origin
Internet  192.168.23.55   <static>  0000.0000.0010  arpa   VLAN 100
Configure
Internet  192.168.23.56   <static>  0000.0000.0020  arpa   VLAN 100
Authentication
2  static arp entries exist.
```

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 |
| Origin | Origin of ARP entries. |

**Related Commands**

| Command | Description |
|---|---|
| N/A | N/A |

**Platform Description** N/A

## 2.13 show arp counter

Use this command to display the number of ARP entries in the ARP cache table.

**show arp counter**

**Parameter Description**

| Parameter | Description |
|---|---|
| N/A | N/A |

**Defaults** N/A

**Command Mode** Privileged EXEC mode

**Usage Guide** N/A

**Configuration Examples** The following example displays the output result of the **show arp counter** command:

```
Ruijie# show arp counter
The Arp Entry counter:0
The Unresolve Arp Entry:0
```

The meaning of each field in the ARP cache table is described in the following Table.

| Parameter | Description |
| --- | --- |
| overlay | Indicates the number of VxLAN-related ARP entries. |
| underlayer | Indicates the number of VxLAN-irrelated ARP entries. |

**Related Commands**

| Command | Description |
| --- | --- |
| N/A | N/A |

**Platform Description** N/A

## 2.14 show arp packet statistics

Use this command to display the statistics of ARP packets.

**show arp packet statistics** [ *interface-name* ]

**Parameter Description**

| Parameter | Description |
| --- | --- |
| *interface-name* | Displays the statistics of ARP packets on the specified interface. |

**Defaults** N/A.

**Command Mode** Privileged EXEC mode.

**Usage Guide** N/A.

**Configuration Examples** The following example displays the output information of the command.

```
Ruijie# show arp packet statistics
Interface Received Received Received Sent Sent
Name Requests Replies Others Requests Replies
--------- -------- -------- -------- -------- -------
VLAN 1 10 20 1 50 10
VLAN 2 5 8 0 10 10
VLAN 3 20 5 0 15 12
VLAN 4 5 8 0 10 10
VLAN 5 20 5 0 15 12
VLAN 6 20 5 0 15 12
VLAN 7 20 5 0 15 12
VLAN 8 5 8 0 10 10
VLAN 9 20 5 0 15 12
VLAN 10 20 5 0 15 12
VLAN 11 20 5 0 15 12
```

```
VLAN 12 20 5 0 15 12
```

Description of fields:

| Field | description |
|---|---|
| Received Requests | Number of received ARP requests |
| Received Replies | Number of received ARP response messages |
| Received Others | Number of other received ARP packets |
| Sent Requests | Number of sent ARP requests |
| Sent Replies | Number of sent ARP requests |

**Related Commands**

| Command | Description |
|---|---|
| N/A. | N/A. |

**Platform Description** N/A

## 2.15 show arp timeout

Use this command to display the aging time of a dynamic ARP entry on the interface.

**show arp timeout**

**Parameter Description**

| Parameter | Description |
|---|---|
| N/A. | N/A. |

**Defaults** N/A.

**Command Mode** Privileged EXEC mode

**Usage Guide** N/A.

**Configuration Examples** The following example displays the output of the **show arp timeout** command:

```
Ruijie# show arp timeout
Interface arp timeout(sec)
---------------------- ----------------
VLAN 1  3600
```

The meaning of each field in the ARP cache table is described in Table 1.

**Related Commands**

| Command | Description |
|---|---|
| N/A. | N/A. |

**Platform Description** N/A

## 2.16 show ip arp

Use this command to display the Address Resolution Protocol (ARP) cache table.

**show ip arp**

| **Parameter Description** | **Parameter** | **Description** |
|---|---|---|
| | N/A | N/A |

**Defaults** N/A.

**Command Mode** Privileged EXEC mode.

**Usage Guide** N/A.

**Configuration Examples** The following example displays the output of **show ip arp**:

```
Ruijie# show ip arp
Protocol Address Age(min)Hardware Type Interface
Internet 192.168.7.233 23 0007.e9d9.0488 ARPA FastEthernet 0/0
Internet 192.168.7.112 10 0050.eb08.6617 ARPA FastEthernet 0/0
Internet 192.168.7.79 12 00d0.f808.3d5c ARPA FastEthernet 0/0
Internet 192.168.7.1 50 00d0.f84e.1c7f ARPA FastEthernet 0/0
Internet 192.168.7.215 36 00d0.f80d.1090 ARPA FastEthernet 0/0
Internet 192.168.7.127 0 0060.97bd.ebee ARPA FastEthernet 0/0
Internet 192.168.7.195 57 0060.97bd.ef2d ARPA FastEthernet 0/0
Internet 192.168.7.183 -- 00d0.f8fb.108b ARPA FastEthernet 0/0
```

Each field in the ARP cache table has the following meanings:

| Field | Description |
|---|---|
| Protocol | Network address protocol, always Internet. |
| Address | The IP address corresponding to the hardware address. |
| Age (min) | Age of the ARP cache record, in minutes; If it is not locally or statically configured, the value of the field is represented with “-”. |
| Hardware | Hardware address corresponding to the IP address |
| Type | The type of hardware address. The value is ARPA for all Ethernet addresses. |
| Interface | Interface associated with the IP address. |

| **Related Commands** | **Command** | **Description** |
|---|---|---|
| | N/A. | N/A. |

**Platform** N/A

**Description**

# 3 IPv6 Commands

## 3.1 clear ipv6 neighbors

Use this command to clear the dynamic IPv6 neighbors.

**clear ipv6 neighbors** [ **oob** ] [*interface-id*]

**Parameter Description**

| Parameter | Description |
|---|---|
| **oob** | Clears the dynamic IPv6 neighbors discovered by neighbors on MGMT interface. |
| *interface-id* | Interface name. Clear the dynamically learned IPv6 neighbors on the specified interface. |

**Defaults** N/A

**Command Mode** Privileged EXEC mode.

**Usage Guide** This command does not clear all the dynamic neighbors on authentication VLAN.
Note that the static neighbors will not be cleared.

**Configuration Examples** The following example clears all the dynamic IPv6 neighbors.

```
Ruijie# clear ipv6 neighbors
```

The following example clears all dynamic IPv6 neighbors learned on the MGMT interface.

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

The following example clears all dynamic IPv6 neighbors learned on the interface, gigabitEthernet 0/1.

```
Ruijie# clear ipv6 neighbors gigabitEthernet 0/1
```

Related Commands

| Command | Description |
|---|---|
| ipv6 neighbor | Configures the neighbor. |
| show ipv6 neighbors | Displays the neighbor information. |

**Platform Description** N/A

## 3.2 ipv6 address

Use this command to configure an IPv6 address for a network interface. Use the **no** form of this command to restore the default setting.

**ipv6 address ipv6-address/prefix-length**

**ipv6 address** *ipv6-prefix/prefix-length* **eui-64**

**ipv6 address** *prefix-name sub-bits/prefix-length* [ **eui-64** ]

**no ipv6 address**

**no ipv6 address** *ipv6-address/prefix-length*

**no ipv6 address** *ipv6-prefix/prefix-length* **eui-64**

**no ipv6 address** *prefix-name sub-bits/prefix-length* [ **eui-64** ]

**Parameter Description**

| Parameter | Description |
|---|---|
| *iipv6-prefix* | IPv6 address prefix in the format defined in RFC4291. The address shall be in hex; the fields in the address shall be separated by comma, and each field shall contain 16 bits. |
| *ipv6-address* | IPv6 address in the format defined in RFC4291. The address shall be in hex; the fields in the address shall be separated by comma, and each field shall contain 16 bits. |
| *prefix-length* | Length of the IPv6 prefix, the network address of the IPv6 address. Note: The prefix length range of the IPv6 address of the interface of S86 is 0 to 64 or 128 to 128. |
| *prefix-name* | The general prefix name. Use the specified general prefix to generate the interface address. |
| *sub-bits* | The value of the sub-prefix bit and the host bit generates the interface address combining with the general prefix. The value shall be in the format defined in the RFC4291. |
| eui-64 | The generated IPV6 address consists of the address prefix and the 64 bit interface ID |

**Defaults** N/A

**Command Mode** Interface configuration mode

**Usage Guide** When an IPv6 interface is created and the link status is UP, the system will automatically generate a local IP address for the interface.

The IPv6 address could also be generated using the general prefix. That is, the IPv6 address consists of the general prefix and the sub-prefix and the host bit. The general prefix could be configured using the **ipv6 general-prefix** command or may be learned through the DHCPv6 agent PD (Prefix Discovery) function (please refer to the *DHCPv6 Configuration*). Use the *sub-bits/prefix-length* parameter of this command to configure the sub-prefix and the host bit.

If no deleted address is specified when using **no ipv6 address**, all the manually configured

addresses will be deleted.

**no ipv6 address** *ipv6-prefix*/*prefix-length* **eui-64** can be used to delete the addresses configured with **ipv6 address** *ipv6-prefix*/*prefix-length* **eui-64**.

**Configuration Examples**

The following example configures an IPv6 address for the interface, GigabitEthernet 0/1.

```
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
```

The following example configures an IPv6 address for the interface, GigabitEthernet 0/1, by using the general prefix.

```
Ruijie(config-if-GigabitEthernet 0/1)# ipv6 address my-prefix
0:0:0:7272::72/64
```

If *my-prefix* is set as 2001:1111:2222::/48, then the IPv6 address generated for an interface is 2001:1111:2222:7272::72/64.

**Related Commands**

| Command | Description |
|---|---|
| N/A | N/A |

**Platform Description** N/A

## 3.3 ipv6 address autoconfig

Use this command to automatically configure an IPv6 stateless address for a network interface. Use the **no** form of this command to restore the default setting.

**ipv6 address autoconfig** [ **default** ]

**no ipv6 address autoconfig**

**Parameter Description**

| Parameter | Description |
|---|---|
| **default** | (Optional) If this keyword is configured, a default routing is generated. Note that only one layer3 interface on the entire device is allowed to use the **default** keyword |

**Defaults** N/A

**Command Mode** Interface configuration mode

**Usage Guide** The stateless automatic address configuration is that when receiving the RA (Route Advertisement) message, the device could use the prefix information of the RA message to automatically generate the EUI-64 interface address.

If the RA message contains the flag of the “other configurations”, the interface will obtain these “other

configurations" through the DHCPv6. The "other configurations" usually means the IPv6 address of the DNS server, the IPv6 address of the NTP server, etc.

**Configuration Examples** The following example automatically configures an IPv6 stateless address for a network interface.

```
Ruijie(config-if)# ipv6 address autoconfig default
```

The following example restores the default setting.

```
Ruijie(config-if)# no ipv6 address autoconfig
```

**Related Commands**

| Command | Description |
| --- | --- |
| **ipv6 address ipv6-***prefix/prefix-length* [ **eui-64** ] | Configures the IPv6 address for the interface manually. |

**Platform Description** N/A

## 3.4 ipv6 icmp error-interval

Use this command to set the frequency with which ICMPv6-oversize error packets are sent. Use the **no** form of this command to restore the default setting.

**ipv6 icmp error-interval too-big** *milliseconds* [ *bucket-size* ]

**no ipv6 icmp error-interval too-big** *milliseconds* [ *bucket-size* ]

Use this command to set the frequency with which other ICMPv6 error packets are sent. Use the **no** form of this command to restore the default setting.

**ipv6 icmp error-interval** *milliseconds* [ *bucket-size* ]

**no ipv6 icmp error-interval** *milliseconds* [ *bucket-size* ]

**Parameter Description**

| Parameter | Description |
| --- | --- |
| *milliseconds* | Sets the refresh interval of the token bucket, in the range from 0 to 2147483647 in the unit of seconds. Setting the value to 0 indicates that the frequency with which ICMPv6 error packets are sent is not fixed. |
| *bucket-size* | Sets the number of tokens in the token bucket, in the range from 1 to 200. |

**Defaults** The default *milliseconds* is 100 and *bucket-size* is 10.

**Command Mode** Global configuration mode

**Usage Guide** The token bucket algorithm is adopted to set the frequency with which ICMPv6 error packets are sent so as to prevent Denial of Service (DoS) attack,

If the forwarded IPv6 packet is greater than the egress IPv6 MTU in size, the router discards the IPv6 packet and sends the ICMPv6-oversize error packet to the source IPv6 address. This kind of ICMPv6

error packet is used for IPv6 path MTU discovery. If there are too many ICMPv6 error packets, the ICMPv6-oversize error packet may not be sent, causing IPv6 path MTU discovery failure. Therefore, it is recommended to set the frequency of ICMPv6-oversize error packet and other ICMPv6 error packet respectively. Note that ICMPv6 redirect packet is not an ICMPv6 error packet and Ruijie sets the frequency of the ICMPv6 redirect packet the same as that of other ICMPv6 error packet.
For the timer is accurate to 10 milliseconds, it is recommended to set the refresh interval of the token bucket to an integer multiple of 10 milliseconds. If the refresh interval is not an integer multiple of 10 milliseconds, it is converted automatically. For example, the frequency of 1 per five milliseconds turns out to be 2 per 10 milliseconds; the frequency of 3 per 15 milliseconds is converted to 2 per 10 milliseconds.

**Configuration Examples** The following example sets the frequency with which ICMPv6-oversize error packets are sent to 100 per second.

```
Ruijie(config)# ipv6 icmp error-interval too-big 1000 100
```

The following example sets the frequency with which other ICMPv6 error packets are sent to 10 per second.

```
Ruijie(config)# ipv6 icmp error-interval 1000 10
```

**Related Commands**

| Command | Description |
|---|---|
| N/A | N/A |

**Platform Description** N/A

## 3.5 ipv6 enable

Use this command to enable the IPv6 function on an interface. Use the **no** form of this command to restore the default setting.
**ipv6 enable**
**no ipv6 enable**

**Parameter Description**

| Parameter | Description |
|---|---|
| N/A | N/A |

**Defaults** This function is disabled by default.

**Command Mode** Interface configuration mode

**Usage Guide** The IPv6 function of an interface can be enabled by configuring **ipv6 enable** or by configuring IPv6 address for the interface.
If an IPv6 address is configured for the interface, the IPv6 function will be enabled automatically on the interface and cannot be disabled with **no ipv6 enable**.

**Configuration Examples** The following example enables IPv6 function on the interface, GigabitEthernet 0/1.

```
Ruijie(config-if)# ipv6 enable
```

**Related Commands**

| Command | Description |
|---|---|
| **show ipv6 interface** | Displays the related information of an interface. |

**Platform Description** N/A

## 3.6 ipv6 general-prefix

Use this command to configure the IPv6 general prefix in the global configuration mode.

**ipv6 general-prefix** *prefix-name ipv6-prefix/prefix-length*

**no ipv6 general-prefix** *prefix-name ipv6-prefix/prefix-length*

**Parameter Description**

| Parameter | Description |
|---|---|
| *prefix-name* | The general prefix name. |
| *pv6-prefix* | The network prefix value of the general-prefix following the format defined in RFC4291. |
| *prefix-length* | The length of the general prefix. |

**Defaults** N/A

**Command Mode** Global configuration mode.

**Usage Guide** It is convenient to number the network by using the general prefix, which defines a prefix so that many longer specified prefixes could refer to it. These specified prefixes are updated whenever the general prefix changes. If the network number changes, just modify the general prefix.

A general prefix could contain multiple prefixes.

These longer specified prefixes are usually used for the Ipv6 address configuration on the interface.

**Configuration Examples** The following example configures manually a general prefix as my-prefix.

```
Ruijie(config)# ipv6 general-prefix my-prefix 2001:1111:2222::/48
```

**Related Commands**

| Command | Description |
|---|---|
| **ipv6 address prefix-name sub-bits/prefix-length** | Configures the interface address using the general prefix. |
| **show ipv6 general-prefix** | Displays the general prefix. |

**Platform Description** N/A

## 3.7 ipv6 hop-limit

Use this command to configure the default hopcount to send unicast messages in the global configuration mode.

**ipv6 hop-limit** *value*

**no ipv6 hop-limit**

**Parameter Description**

| Parameter | Description |
|---|---|
| *vlaue* | Hopcount ranging from 1 to 255. |

**Defaults** The default is 64.

**Command Mode** Global configuration mode.

**Usage Guide** This command takes effect for the unicast messages only, not for multicast messages.

**Configuration Examples** The following example sets the hopcount to 100.

```
Ruijie(config)# ipv6 hop-limit 100
```

**Related Commands**

| Command | Description |
|---|---|
| N/A | N/A |

**Platform Description** N/A

## 3.8 ipv6 mtu

Use this command to configure the MTU of IPv6 packets. Use the **no** form of this command to restore the default setting.

**ipv6 mtu** *bytes*

**no ipv6 mtu**

**Parameter Description**

| Parameter | Description |
|---|---|
| *bytes* | MTU of IPv6 packets, in bytes. The value ranges from 1280 to 1500. |

**Defaults** The default configuration is the same as the configuration of the **mtu** command.

**Command Mode** Interface configuration mode

**Usage Guide** If the size of an IPv6 packet exceeds the IPv6 MTU, the RGOS software segments the packet. For all devices in the same physical network segment, the IPv6 MTU of the interconnected interface must be

the same.

**Configuration Examples** The following example sets the IPv6 MTU of the FastEthernet 0/1 interface to 1400 bytes.

```
Ruijie(config)# interface fastEthernet 0/1
Ruijie(config-if)# ipv6 mtu 1400
```

**Related Commands**

| Command | Description |
|---|---|
| **mtu** | Sets the MTU of an interface. |

**Platform Description**

## 3.9 ipv6 nd cache interface-limit

Use this command to set the maximum number of neighbors learned on the interface. Use the **no** form of this command to restore the default setting.

**ipv6 nd cache interface-limit** *value*

**no ipv6 nd cache interface-limit**

**Parameter Description**

| Parameter | Description |
|---|---|
| *value* | Sets the maximum number of neighbors learned on the interface, including the static and dynamic neighbors, in the range from 0 to the number supported by the device. 0 indicates the number is not limited. |

**Defaults** The default is 0.

**Command Mode** Interface configuration mode

**Usage Guide** This function can prevent neighbor entries generated by malicious neighbor attacks from consuming memory. *limit* must be no smaller than the number of neighbors learned on the interface. Otherwise, the configuration does not take effect.

**Configuration Examples** The following example sets the number of neighbors learned on the interface to 100.

```
Ruijie(config)# interface GigabitEthernet 0/1
Ruijie(config-if-GigabitEthernet 0/1)# ipv6 nd cache interface-limit 100
```

**Related Commands**

| Command | Description |
|---|---|
| N/A | N/A |

**Platform** N/A

**Description**

## 3.10 ipv6 nd dad attempts

Use this command to set the number of the NS packets to be continuously sent for IPv6 address collision check on the interface. Use the **no** form of this command to restore it to the default setting.
**ipv6 nd dad attempts** value
**no ipv6 nd dad attempts** *value*

**Parameter Description**

| Parameter | Description |
|---|---|
| *value* | Number of the NS packets. If it is set to 0, it indicates that the IPv6 address collision check is disabled on the interface. The range is 0 to 600. |

**Defaults** The default is 1.

**Command Mode** Interface configuration mode.

**Usage Guide** When the interface is configured with a new IPv6 address, the address collision shall be checked before the address is assigned to the interface, and the address shall be in the "tentative" status. After the address collision check is completed, if no collision is detected, the address can be used normally; if collision is detected and the interface ID of the address is an EUI-64 ID, it indicates that the link-layer address is repeated, and the system will automatically shut down the interface (that is, to prohibit IPv6 operations on the interface). In this case, you shall modify and configure a new address manually, and restart address collision check for the **down/up** interface. Whenever the state of an interface changes from **down** to **up**, the address collision check function of the interface will be enabled.

**Configuration Examples** The following example continuously sends 3 NS packets for IPv6 address collision check on the interface, GigabitEthernet 0/1.

```
Ruijie(config-if)# ipv6 nd dad attempts 3
```

**Related Commands**

| Command | Description |
|---|---|
| **show ipv6 interface** | Displays the interface information. |

**Platform Description** N/A

## 3.11 Ipv6 nd dad retry

Use this command to set the interval for address conflict detection. Use the **no** form of this command to restore the default setting.
**ipv6 nd dad retry** *value*

**no ipv6 nd dad retry**

**Parameter Description**

| Parameter | Description |
|---|---|
| *value* | Sets the interval for address conflict detection, 60 seconds by default. Setting *value* to 0 indicates that the function is disabled. |

**Defaults** The default value is 1.

**Command Mode** Global configuration mode

**Usage Guide** Before configuring a new IPv6 address for an interface, enable address conflict detection on the interface. If a conflict address is detected, the device does not receive the IPv6 packet destined to the conflict address. This command is used to perform conflict detection again when the interval expires. If there is no conflict, the address can be used.

**Configuration Examples** The following example sets the interval for address conflict detection to 10s.

```
Ruijie(config)# ipv6 nd dad retry 10
```

**Related Commands**

| Command | Description |
|---|---|
| N/A | N/A |

**Platform Description** N/A

## 3.12 ipv6 nd managed-config-flag

Use this command to set the “managed address configuration” flag bit of the RA message. Use the **no** form of this command to restore the default setting.

**ipv6 nd managed-config-flag**

**no ipv6 nd managed-config-flag**

**Parameter Description**

| Parameter | Description |
|---|---|
| N/A | N/A |

**Defaults** N/A

**Command Mode** Interface configuration mode.

**Usage Guide** This flag determines whether the host that receives the RA message obtains an IP address through stateful auto configuration. If the flag is set, the host obtains an IP address through stateful auto

configuration, otherwise it does not be used.

**Configuration Examples** The following example sets the “managed address configuration” flag bit of the RA message.

```
Ruijie(config-if)# ipv6 nd managed-config-flag
```

**Related Commands**

| Command | Description |
| --- | --- |
| **show ipv6 interface** | Displays the interface information. |
| **ipv6 nd other-config-flag** | Sets the flag for obtaining all information except IP address through stateful auto configuration. |

**Platform Description** N/A

## 3.13 ipv6 nd ns-interval

Use this command to set the interval for the interface to retransmitting NS (Neighbor Solicitation). Use the **no** form of this command to restore the default setting.

**ipv6 nd ns-interval** *milliseconds*

**no ipv6 nd ns-interval**

**Parameter Description**

| Parameter | Description |
| --- | --- |
| *milliseconds* | Interval for retransmitting NS in the range of 1,000 to 429,467,295 milliseconds |

**Defaults** The default value in RA is 0 (unspecified); the interval for retransmitting NS is 1000 milliseconds (1 second).

**Command mode** Interface configuration mode.

**Usage Guide** The configured value will be advertised through RA and will be used by the device itself. It is not recommended to set a too short interval.

**Configuration Examples** The following example sets the interval for the interface to retransmitting NS to 2 seconds.

```
Ruijie(conifig-if)# ipv6 nd ns-interval 2000
```

**Related Commands**

| Command | Description |
| --- | --- |
| **show ipv6 interface** | Displays the interface information. |

**Platform Description** N/A

## 3.14 ipv6 nd other-config-flag

Use this command to set “other stateful configuration” flag bit of the RA message. Use the **no** form of this command to delete the flag bit.

**ipv6 nd other-config-flag**

**no ipv6 nd other-config-flag**

**Parameter Description**

| Parameter | Description |
|---|---|
| N/A | N/A |

**Defaults** The flag bit is not set by default.

**Command mode** Interface configuration mode.

**Usage Guide** With this flag bit set, the flag bit of the RA message sent by the device is set. After receiving this flag bit, the host uses the dhcpv6 to acquire the information excluding the IPv6 address for the purpose of automatic configuration. When the **managed address configuration** is set, the default **other stateful configuration** is also set

**Configuration Examples** The following example sets “other stateful configuration” flag bit of the RA message.

```
Ruijie(config-if)# ipv6 nd other-config-flag
```

**Related Commands**

| Command | Description |
|---|---|
| **show ipv6 interface** | Displays the interface information. |

**Platform Description** N/A

## 3.15 ipv6 nd prefix

Use this command to configure the address prefix included in the RA. Use the **no** form of this command to delete the set prefix or restore the default setting.

**ipv6 nd prefix** { *ipv6-prefix*/*prefix-length* | **default** } [ [ *valid-lifetime preferred-lifetime* ] | [ **at** *valid-date preferred-date* ] | [ **infinite** | *preferred-lifetime* ] ] [ **no-advertise**] | [ [ **off-link** ] [ **no-autoconfig** ] ]

**no ipv6 nd prefix** { *ipv6-prefix/prefix-length* | **default** }

**Parameter Description**

| Parameter | Description |
|---|---|
| *ipv6-prefix* | IPv6 network ID following the format defined in RFC4291 |
| *prefix-length* | Length of the IPv6 prefix. “/” shall be added in front of the prefix |
| *valid-lifetime* | Valid lifetime of the RA prefix received by the host |
| *preferred-lifetime* | Preferred lifetime of the RA prefix received by the host |
| *at valid-date preferred-date* | Sets the dead line for the valid lifetime and that of the preferred |

| | |
|---|---|
| | lifetime, in day, month, year, hour, minute. |
| **infinite** | Indicates that the prefix is always valid. |
| **default** | Sets the default prefix. |
| **no-advertise** | The prefix will not be advertised by the device. |
| **off-link** | When the host sends an IPv6 packet, if the prefix of the destination address matches the set prefix, it is considered that the destination is on-link and is directly reachable. If this option is set, it indicates that the prefix is not used for on-link judgment. |
| **no-autoconfig** | Indicates that the RA prefix received by the host cannot be used for auto address configuration. |

**Defaults** By default, the advertised prefix is the one set with **ipv6 address** on the interface. The default parameters of the prefix configured in the RA are as follows:
*valid-lifetime:* 2592000s (30 days)
preferred-lifetime: 604800s (7 days),
The prefix is advertised and is used for on-link judgment and auto address configuration.

**Command Mode** Interface configuration mode.

**Usage Guide** This command can be used to configure the parameters of each prefix, including whether to advertise the prefix. By default, the prefix advertised in RA is the one set with **ipv6 address** on the interface. To add other prefixes, use this command.

**ipv6 nd prefix default**

Set the default parameters to be used by the interface. If no parameter is specified for an added prefix, the parameters set with **ipv6 nd prefix default** will be used. Note that after a parameter is specified for the prefix, the default configuration will not be used. That is to say, the configuration of the prefix cannot be modified with **ipv6 nd prefix default**; only the prefix that uses all the default configurations can be modified with this command.

**at** *valid-date preferred-date*

The valid lifetime of a prefix can be specified in two ways. One way is to specify a fixed time for each prefix in the RA; the other way is to specify the end time (in this mode, the valid lifetime of the prefix sent in RA will be gradually reduced until the end time is 0).

**Configuration Examples** The following example adds a prefix for SVI 1.

```
Ruijie(config)# interface vlan 1
Ruijie(conifig-if)# ipv6 nd prefix 2001::/64 infinite 2592000
```

The following example sets the default prefix parameters for SVI 1 (they cannot be used for auto address configuration):

```
Ruijie(config)# interface vlan 1

Ruijie(config-if)# ipv6 prefix default no-autoconfig
```

If no parameter is specified, the default parameters will be used, and the prefix cannot be used for auto address configuration.

**Related Commands**

| Command | Description |
|---|---|
| **show ipv6 interface** | Displays the RA information of an interface. |

**Platform Description** N/A

## 3.16 ipv6 nd ra-hoplimit

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

**ipv6 nd ra-hoplimit** *value*

**no ipv6 nd ra-hoplimit**

**Parameter Description**

| Parameter | Description |
|---|---|
| *value* | Hopcount |

**Defaults** The default is 64.

**Command Mode** Interface configuration mode.

**Usage Guide**

**Configuration Examples** The following example sets the hopcount of the RA message to 110 on the interface, GigabitEthernet 0/1.

```
Ruijie(config-if-GigabitEthernet 0/1)# ipv6 nd ra-hoplimit 110
```

**Related Commands**

| Command | Description |
|---|---|
| **show ipv6 interface** | Displays the interface information. |
| **ipv6 nd ra-lifetime** | Sets the lifetime of the device. |

| | |
|---|---|
| **ipv6 nd ra-interval** | Sets the interval of sending the RA message. |
| **ipv6 nd ra-mtu** | Sets the MTU of the RA message. |

**Platform Description** N/A

## 3.17 ipv6 nd ra-interval

Use this command to set the interval of sending the RA. Use the **no** form of this command to restore the default setting.

**ipv6 nd ra-interval** { *seconds* | **min-max** *min_value max_value* }

**no ipv6 nd ra-interva** l

**Parameter Description**

| Parameter | Description |
|---|---|
| *seconds* | Interval of sending the RA message in seconds, 3-1800s. |
| **min-max** | Maximum and minimum interval sending the RA message in seconds |
| *min_value* | Minimum interval sending the RA message in seconds |
| *max_value* | Maximum interval sending the RA message in seconds |

**Defaults** 200s. The actual interval of sending the RA message will be fluctuated 20% based on 200s.

**Command Mode** Interface configuration mode.

**Usage Guide** If the device serves as the default device, the set interval shall not be longer than the lifetime of the device. Besides, to ensure other devices along the link occupies network bandwidth while sending the RA message, the actual interval for sending the RA message will be fluctuated 20% based on the set value.

If the key word **min-max** is specified, the actual interval for sending the packet will be chosen between the range of minimum value and maximum value.

**Configuration Examples** The following example sets the interval of sending the RA to 110 seconds.

```
Ruijie(conifig-if)# ipv6 nd ra-interval 110
```

The following example sets the interval of sending the RA from 110 to 120 seconds.

```
Ruijie(config-if)# ipv6 nd ra-interval min-max 110 120
```

**Related Commands**

| Command | Description |
|---|---|
| **show ipv6 interface** | Displays the interface information. |
| **ipv6 nd ra-lifetime** | Sets the lifetime of the device. |
| **ipv6 nd ra-hoplimit** | Sets the hopfcount of the RA message. |
| **ipv6 nd ra-mtu** | Sets the MTU of the RA message. |

**Platform Description** N/A

## 3.18 ipv6 nd ra-lifetime

Use this command to set the device lifetime of the RA sent on the interface. Use the **no** form of this command to restore the default setting.

**ipv6 nd ra-lifetime** *seconds*

**no ipv6 nd ra-lifetime**

**Parameter Description**

| Parameter | Description |
|---|---|
| *seconds* | Default life time of the device on the interface, in the range from 0 to 9000 in the unit of seconds. |

**Defaults** The default is 1800.

**Command Mode** Interface configuration mode.

**Usage Guide** The router lifetime field is available in each RA. It specifies the time during which the hosts along the link of the interface can select the device as the default device. If the value is set to 0, the device will not serve as the default device any longer. If it is not set to 0, it shall be larger than or equal to the interval of sending the RA (ra-interval)

**Configuration Examples** The following example sets the device lifetime of the RA sent on the interface to 2,000 seconds.

```
Ruijie(config-if-GigabitEthernet 0/1)# ipv6 nd ra-lifetime 2000
```

**Related Commands**

| Command | Description |
|---|---|
| **show ipv6 interface** | Displays the interface information. |
| **ipv6 nd ra-interval** | Sets the interval of sending the RA. |
| **ipv6 nd ra-hoplimit** | Sets the hopcount of the RA. |
| **ipv6 nd ra-mtu** | Sets the MTU of the RA. |

**Platform Description** N/A

## 3.19 ipv6 nd ra-mtu

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

**ipv6 nd ra-mtu** *value*

**no ipv6 nd ra-mtu**

| Parameter Description | Parameter | Description |
|---|---|---|
| | *value* | MTU value, in the range from 0 to 4294967295. |

**Defaults** IPv6 MTU value of the network interface.

**Command Mode** Interface configuration mode.

**Usage Guide** If it is specified as 0, the RA will not have the MTU option

**Configuration Examples** The following example sets the MTU of the RA message to 1,400 bytes.

```
Ruijie(config -if)# ipv6 nd ra-mtu 1400
```

| Related Commands | Command | Description |
|---|---|---|
| | **show ipv6 interface** | Displays the interface information. |
| | **ipv6 nd ra-lifetime** | Sets the lifetime of the device. |
| | **ipv6 nd ra-interval** | Sets the interval of sending the RA message. |
| | **ipv6 nd ra-hoplimit** | Sets the hopcount of the RA message. |

**Platform Description** N/A

## 3.20 ipv6 nd reachable-time

Use this command to set the reachable time after the interface checks the reachability of the neighbor dynamically learned through NDP. Use the **no** form of this command to restore the default setting.

**ipv6 nd reachable-time** *milliseconds*

**no ipv6 nd reachable-time**

| Parameter Description | Parameter | Description |
|---|---|---|
| | *milliseconds* | Reachable time for the neighbor in the range from 0 to 3,600,000 in the unit of milliseconds. |

**Defaults** The default value in RA is 0 (unspecified); the reachable time for the neighbor is 30000 milliseconds (30 seconds) when the device discovers the neighbor.

**Command Mode** Interface configuration mode.

**Usage Guide** The device checks the unreachable neighbor through the set time. A shorter time means that the device can check the neighbor failure more quickly, but more network bandwidth and device resource will be occupied. Therefore, it is not recommended to set a too short reachable time.

The configured value will be advertised through RA and will be used by the device itself. If the value is

set to 0, it indicates that the time is not specified, that is, the default value is used.
According to RFC4861, the actual time to reach neighbor is not consistent with the configured value, ranging from 0.5*configured value to 1.5*configured value.

**Configuration Examples** The following example sets the reachable time to 1,000 seconds.

```
Ruijie(config-if)# ipv6 nd reachable-time 1000000
```

**Related Commands**

| Command | Description |
|---|---|
| **show ipv6 interface** | Displays the interface information. |

**Platform Description** N/A

## 3.21 ipv6 nd state-time

Use this command to set the period for the neighbor to maintain the state. Use the **no** form of this command to restore the default setting.
**ipv6 nd stale-time** *seconds*
**no ipv6 nd stale-time**

**Parameter Description**

| Parameter | Description |
|---|---|
| *Seconds* | Sets the period for the neighbor to maintain the state, in the range from 0 to 86400 in the unit of seconds. |

**Defaults** The default is 3600.

**Command Mode** Global configuration mode

**Usage Guide** This command is used to set the period for the neighbor to maintain the state. After the period expires, neighbor unreachability detection is performed. The shorter the period, the faster the neighbor is found unreachable. On the other hand, more network bandwidth and device resources are consumed. Therefore, it is recommended to set a value not too small.

**Configuration Examples** The following example sets the period to 600 seconds for the neighbor to maintain the state.

```
Ruijie(config)# ipv6 nd stale-time 600
```

**Related Commands**

| Command | Description |
|---|---|
| N/A | N/A |

**Platform Description** N/A

## 3.22 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 **ipv6 nd suppress-ra** command is enabled by default.

**Command Mode** Interface configuration mode.

**Usage Guide**

**Configuration Examples** The following example disables the interface from sending the RA message.

```
Ruijie(config-if-GigabitEthernet 0/1)# ipv6 nd suppress-ra
```

**Related Commands**

| Command | Description |
|---|---|
| **show ipv6 interface** | Displays the interface information. |

**Platform Description** N/A

## 3.23 ipv6 nd unresolved

Use this command to set the maximum number of the unresolved neighbor table entries. Use the **no** form of this command to restore the default setting.

**ipv6 nd unresolved** *number*

**no ipv6 nd unresolved**

**Parameter Description**

| Parameter | Description |
|---|---|
| *number* | Sets the maximum number of the unresolved neighbor table entries, in the range from 1 to the neighbor table size supported by the device. |

**Defaults** The default is 0. (The maximum number is the neighbor table size supported by the device)

**Command Mode** Global configuration mode

**Usage Guide** This command is used to prevent unresolved ND table entries generated by malicious scan attacks

from consuming table entry resources,

**Configuration Examples** The following example sets the maximum number of the unresolved neighbor table entries to 200.

```
Ruijie(config)# ipv6 nd unresolved 200
```

**Related Commands**

| Command | Description |
| --- | --- |
| N/A | N/A |

**Platform Description** N/A

## 3.24 ipv6 neighbor

Use this command to configure a static neighbor. Use the **no** form of this command to delete a static neighbor.

**ipv6 neighbor** *ipv6-address interface-id hardware-address*

**no ipv6 neighbor** *ipv6-address interface-id*

**Parameter Description**

| Parameter | Description |
| --- | --- |
| *ipv6-address* | The neighbor IPv6 address, in the form as defined in RFC4291. |
| *interface-id* | Specifies the network interface where the neighbor is (including Router Port, L3 AP port and SVI interface). |
| *hardware-address* | The 48-bit MAC address, a dotted triple of four-digit hexadecimal numbers. |

**Defaults** No static neighbor is configured by default.

**Command Mode** Global configuration mode

**Usage Guide** This command can only be configured on the interface enabled with IPv6 protocol, similar to the ARP command.

If the neighbor to be configured has been learned through Neighbor Discovery Protocol (NDP) and stored in the NDP neighbor table, the dynamic neighbor turns to be static. If the static neighbor is valid, it is always reachable. An invalid static neighbor refers to the neighbor whose IPv6 address is not valid (not in the IPv6 network segment configured for the interface or interface address conflict). The packet is not forwarded to the MAC address as specified by the invalid static neighbor. The invalid static neighbor is in inactive state. Use the show ipv6 neighbor static command to display the state of the static neighbor.

Use the **clear ipv6 neighbors** command to clear all neighbors learned dynamically through NDP.

**Configuration** The following example configures a static neighbor on SVI 1.

**Examples**

```
Ruijie(config)# ipv6 neighbor 2001::1 vlan 1 00d0.f811.1111
```

**Related Commands**

| Command | Description |
| --- | --- |
| N/A | N/A |

**Platform Description** N/A

## 3.25 ipv6 ns-linklocal-src

Use this command to set the local address of the link as the source IP address to send neighbor requests. Use the **no** form of this command to use the global IP address as the source address to send neighbor requests.

**ipv6 ns-linklocal-src**

**no ipv6 ns-linklocal-src**

**Parameter Description**

| Parameter | Description |
| --- | --- |
| N/A | N/A |

**Defaults** The local address of the link is always used as the source address to send neighbor requests.

**Command Mode** Global configuration mode.

**Usage Guide** N/A

**Configuration Examples** The following example uses the global IP address as the source address to send neighbor requests.

```
Ruijie(config)# no ipv6 ns-linklocal-src
```

**Related Commands**

| Command | Description |
| --- | --- |
| N/A | N/A |

**Platform Description** N/A

## 3.26 ipv6 redirects

Use this command to control whether to send ICMPv6 redirect message when the switch receives and forwards an IPv6 packet through an interface. Use the **no** form of this command to restore the default setting.

**ipv6 redirects**

**no ipv6 redirects**

| Parameter Description | Parameter | Description |
|---|---|---|
| | N/A | N/A |

**Defaults** This function is enabled by default.

**Command Mode** Interface configuration mode.

**Usage Guide** The transmission rate of any ICMPv6 error message is limited. By default, it is 10pps.

**Configuration Examples** The following example enables ICMPv6 redirection on interface GigabitEthernet 0/1.

```
Ruijie(config-if-GigabitEthernet 0/1)# ipv6 redirects
```

| Related Commands | Command | Description |
|---|---|---|
| | **show ipv6 interface** | Displays the interface information. |

**Platform Description** N/A

## 3.27 ipv6 source-route

Use this command to forward the IPv6 packet with route header. Use the **no** form of this command to restore the default setting.

**ipv6 source-route**

**no ipv6 source-route**

| Parameter Description | Parameter | Description |
|---|---|---|
| | N/A | N/A |

**Defaults** The **ipv6 source-route** command is disabled by default.

**Command Mode** Global configuration mode.

**Usage Guide** Because of the potential security of the header of type 0 route, it's easy for the device to suffer from the denial service attack. Therefore, forwarding the IPv6 packet with route header is disabled by default. However, the IPv6 packet of route header with type 0 that destined to the local machine is processed.

**Configuration Examples** `The following example` forwards the IPv6 packet with route header.

```
Ruijie(config)# no ipv6 source-route
```

| Related | Command | Description |
|---|---|---|

| Commands | N/A | N/A |
|---|---|---|

**Platform Description** N/A

## 3.28 show ipv6 address

Use this command to display the IPv6 addresses.

**show ipv6 address** [ *interface-name* ]

**Parameter Description**

| Parameter | Description |
|---|---|
| *interface-name* | Interface name |

**Defaults** N/A

**Command Mode** Privileged EXEC mode.

**Usage Guide** N/A

**Configuration Examples** The following example displays all IPv6 address configured on the device.

```
Ruijie#show ipv6 address
Global unicast address limit: 1024, Global unicast address count: 3
Tentative address count: 2,Duplicate address count: 1
Preferred address count: 3,Deprecated address count: 0
Gi 0/5
  FE80::1/64                                  Preferred
    Preferred lifetime: INFINITE, Valid lifetime: INFINITE
  1000::1/64                                  Duplicate
    Preferred lifetime: INFINITE, Valid lifetime: INFINITE
Gi 0/6
  FE80::1/64                                  Tentative
    Preferred lifetime: INFINITE, Valid lifetime: INFINITE
  1111:1111:1111:1111:1111:1111:1111:1111/64   Tentative
    Preferred lifetime: INFINITE, Valid lifetime: INFINITE
Gi 0/7
  FE80::1/64                                  Preferred
    Preferred lifetime: INFINITE, Valid lifetime: INFINITE
  2000:1111:1111:1111:1111:1111:1111:1111/64   Preferred
    Preferred lifetime: INFINITE, Valid lifetime: INFINITE
```

The following example displays the IPv6 address configured on the GigabitEthernet 0/1.

```
Ruijie#show ipv6 address Gi 0/5
Global unicast address count: 3
Tentative address count: 0,Duplicate address count: 1
Preferred address count: 1,Deprecated address count: 0
FE80::1/64                                  Preferred
  Preferred lifetime: INFINITE, Valid lifetime: INFINITE
1000::1/64                                  Duplicate
  Preferred lifetime: INFINITE, Valid lifetime: INFINITE
```

| Related Commands | Command | Description |
|---|---|---|
| | N/A | N/A |

**Platform Description** N/A

## 3.29 show ipv6 general-prefix

Use this command to display the information of the general prefix.

**show ipv6 general-prefix**

| Parameter Description | Parameter | Description |
|---|---|---|
| | N/A | N/A |

**Defaults** N/A

**Command Mode** Privileged EXEC mode.

**Usage Guide** Use this command to display the information of the general prefix including the manually configured and learned from the DHCPv6 agent.

**Configuration Examples**

```
The following example displays the information of the general prefix.Ruijie#
show ipv6 general-prefix
There is 1 general prefix.
IPv6 general prefix my-prefix, acquired via Manual configuration
 2001:1111:2222::/48
 2001:1111:3333::/48
```

| Related Commands | Command | Description |
|---|---|---|
| | **ipv6 general-prefix** | Configures the general prefix. |

**Platform Description** N/A

## 3.30 show ipv6 interface

Use this command to display the IPv6 interface information.

**show ipv6 interface** [ *interface-id* ] [ **ra-info** ] ] [ *brief* [ interface-id ] ]

**Parameter Description**

| Parameter | Description |
|---|---|
| *interface-id* | Interface (including Ethernet interface, aggregate port, or SVI) |
| **ra-info** | Displays the RA information of the interface. |
| *brief* | Displays the brief information of the interface (interface status and address information). |

**Defaults** N/A

**Command Mode**

**Usage Guide** Use this command to display the address configuration, ND configuration and other information of an IPv6 interface.

**Configuration Examples** The following example displays the information of the IPv6 interface.

```
Ruijie# show ipv6 interface vlan 1
Interface vlan 1 is Up, ifindex: 2001
address(es):
Mac Address: 00:00:00:00:00:01
INET6: fe80::200:ff:fe00:1 , subnet is fe80::/64
Joined group address(es):
ff01:1::1
ff02:1::1
ff02:1::2
ff02:1::1:ff00:1
INET6: 2001::1 , subnet is 2001::/64 [TENTATIVE]
Joined group address(es):
ff01:1::1
ff02:1::1
ff02:1::2
ff02:1::1:ff00:1
MTU is 1500 bytes
ICMP error messages limited to one every 10 milliseconds
ICMP redirects are enabled
ND DAD is enabled, number of DAD attempts: 1
ND reachable time is 30000 milliseconds
ND advertised reachable time is 0 milliseconds
ND retransmit interval is 1000 milliseconds
ND advertised retransmit interval is 0 milliseconds
```

```
ND router advertisements are sent every 200 seconds<240--160>
ND device advertisements live for 1800 seconds
```

The following line is included in the above information: 2001::1, subnet is 2001::/64 [**TENTATIVE**]. The flag bit in the [ ] following the INET6 address is explained as follows:

| Flag | Meaning |
|---|---|
| ANYCAST | Indicate that the address is an anycast address. |
| TENTATIVE | Indicate that the DAD is underway. The address is a tentative before the DAD is completed. |
| DUPLICATED | Indicate that a duplicate address exists. |
| DEPRECATED | Indicate that the preferred lifetime of the address expires. |
| NODAD | Indicate that no DAD is implemented for the address. |
| AUTOIFID | Indicate that the interface ID of the address is automatically generated by the system, which is usually an EUI-64 ID. |
| PRE | Indicates the address automatically generated. |
| GEN | Indicates the address using the general prefix. |

```
The following example displays the RA information of the IPv6 interface.Ruijie#
show ipv6 interface vlan 1 ra-info
vlan 1: DOWN
RA timer is stopped
waits: 0, initcount: 3
statistics: RA(out/in/inconsistent): 4/0/0, RS(input): 0
Link-layer address: 00:00:00:00:00:01
Physical MTU: 1500
ND device advertisements live for 1800 seconds
ND device advertisements are sent every 200 seconds<240--160>
Flags: !M!O, Adv MTU: 1500
ND advertised reachable time is 0 milliseconds
ND advertised retransmit time is 0 milliseconds
ND advertised CurHopLimit is 64
Prefixes: (total: 1)
fec0:1:1:1::/64(Def,Auto,vltime: 2592000, pltime: 604800, flags: LA)
```

Description of the fields in **ra-info**:

| Field | Meaning |
|---|---|
| RA timer is stopped (on) | Indicate whether the RA timer is started. |
| waits | Indicate that the RS is received but the number of the responses is not available. |
| initcount | Indicate the number of the RAs when the RA timer is restarted. |

| | |
|---|---|
| RA(out/in/ inconsistent) | out: Indicate the number of the RAs that are sent.<br>In: Indicate the number of the RAs that are received.<br>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.<br>M: Conversely |
| !O \| O | !O indicates the other-config-flag bit in the RA is not set.<br>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.<br>!L: Indicate that the on-link in the prefix is not set. |
| A \| !A | A: Indicate that the auto-configure in the prefix is set. !A: It indicates that the auto-configure in the prefix is not set. |

The following example displays the brief information of the IPv6 interface.

```
Ruijie#show ipv6 interface brief

GigabitEthernet 0/1          [down/down]
       2222::2
       FE80::1614:4BFF:FE5C:ED3A
```

**Related Commands**

| Command | Description |
|---|---|
| N/A | N/A |

**Platform Description** N/A

## 3.31 show ipv6 neighbors

Use this command to display the IPv6 neighbors.

**show ipv6 neighbors** [ **verbose** ] [ *interface-id* ] [ *ipv6-address* ] **[static] [ oob ]**

**Parameter Description**

| Parameter | Description |
|---|---|
| **verbose** | Displays the neighbor details. |
| *interface-id* | Displays the neighbors of the specified interface. |
| *ipv6-addres* | Displays the neighbors of the specified IPv6 address. |
| **static** | Displays the validity status of static neighbors. |
| **oob** | Displays IPv6 neighbors leanred on the MGMT interface. |

**Defaults** N/A

**Command Mode** Privileged EXEC mode.

**Usage Guide**

**Configuration Examples** The following example displays the neighbors on the SVI 1 interface:

```
Ruijie# show ipv6 neighbors vlan 1
IPv6 Address Linklayer Addr Interface
fa::1 00d0.0000.0002 vlan 1
fe80::200:ff:fe00:2 00d0.0000.0002 vlan 1
```

Show the neighbor details:

```
Ruijie# show ipv6 neighbors verbose
IPv6 Address Linklayer Addr Interface
2001::1 00d0.f800.0001 vlan 1
 State: Reach/H Age: - asked: 0
fe80::200:ff:fe00:1 00d0.f800.0001 vlan 1
 State: Reach/H Age: - asked: 0
```

| Field | Meaning |
|---|---|
| IPv6 Address | IPv6 address of the Neighbor |
| Linklayer Addr | Link address, namely, MAC address. If it is not available, incomplete is displayed. |
| Interface | Interface the neighbor locates. |
| State | State of the neighbor: state/H(R)<br>The values of STATE are as below:<br>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.<br>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.<br>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.<br>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).<br>?: Unknown state.<br>/R—indicate the neighbor is considered as a device<br>/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. |

The following example displays status of static neighbors.

```
Ruijie# show ipv6 neighbors static
IPv6 Address    Linklayer Addr  Interface              State
2001:1::1        00d0.f822.33ab   GigabitEthernet 0/14   ACTIVE
2001:2::2        00d0.f822.33ac   VLAN 1                  INACTIVE
```

| Field | Meaning |
|---|---|
| IPv6 Address | IPv6 addresses of the static neighbors |
| Linklayer Addr | Link addresses, namely, MAC addresses. |
| Interface | Interfaces the neighbors locate. |
| State | States of the static neighbors:<br>The values of STATE are as below:<br>ACTIVE<br>INACTIVE |

**Related**

| Command | Description |
|---|---|

| Commands | ipv6 neighbor | Configures a neighbor. |
|---|---|---|

**Platform Description** N/A

## 3.32 show ipv6 neighbors statistics

Use the following commands to display the statistics of one IPv6 neighbors.

**show ipv6 neighbors statistics**

| Parameter Description | Parameter | Description |
|---|---|---|
| | N/A | N/A |

**Defaults** N/A

**Command Mode** Privileged EXEC mode.

**Usage Guide** N/A

**Configuration Examples** The following example displays the statistics of the global neighbors.

```
Ruijie#show ipv6 neighbor statistics

Memory: 0 bytes
Entries: 0
  Static: 0,Dynamic: 0,Local: 0
  Incomplete:0, Reachable:0, Stale:0, Delay:0, Probe:0
Ruijie#
```

The following example displays the statistics of all neighbors.

```
Ruijie#show ipv6 neighbor statistics all

IPv6 neighbor table count: 1
Static neighbor count: 0(0 active, 0 inactive)
Total
Memory: 0 bytes
Entries: 0
  Static: 0,Dynamic: 0,Local: 0
  Incomplete:0, Reachable:0, Stale:0, Delay:0, Probe:0;

Global
Memory: 0 bytes
Entries: 0
  Static: 0,Dynamic: 0,Local: 0
```

```
  Incomplete:0, Reachable:0, Stale:0, Delay:0, Probe:0;
Ruijie#
```

| Related Commands | Command | Description |
|---|---|---|
| | N/A | N/A |

**Platform Description**

## 3.33 show ipv6 packet statistics

Use this command to display the statistics of IPv6 packets.

**show ipv6 packet statistics** [ **total** | *interface-name* ]

| Parameter Description | Parameter | Description |
|---|---|---|
| | **total** | Displays total statistics of all interfaces. |
| | *interface-name* | Interface name |

**Defaults** N/A

**Command Mode** Privileged EXEC mode.

**Usage Guide** N/A

**Configuration Examples** The following example displays the total statistics of the Ipv6 packets and the statistics of each inerface.

```
Ruijie#show ipv6 packet statistics
Total
  Received 1000 packets, 1000000 bytes
    Unicast:1000,Multicast:0
    Discards:0
      HdrErrors:0(HoplimitExceeded:0,Others:0)
      NoRoutes:0
      Others:0
  Sent 100 packets, 6000 bytes
    Unicast:50,Multicast:50

VLAN 1
  Received 1000 packets, 1000000 bytes
    Unicast:1000,Multicast:0
    Discards:0
      HdrErrors:0(HoplimitExceeded:0,Others:0)
      NoRoutes:0
      Others:0
  Sent 100 packets, 6000 bytes
    Unicast:50,Multicast:50
```

The following example displays the total statistics of the Ipv6 packets.

```
Ruijie#show ipv6 packet statistics total
Received 1000 packets, 1000000 bytes
  Unicast:1000,Multicast:0
  Discards:0
    HdrErrors:0(HoplimitExceeded:0,Others:0)
    NoRoutes:0
    Others:0
Sent 100 packets, 6000 bytes
  Unicast:50,Multicast:50
```

| Related Commands | Command | Description |
|---|---|---|
| | N/A | N/A |

**Platform Description**

## 3.34 show ipv6 raw-socket

Use this command to display all IPv6 raw sockets.

**show ipv6 raw-socket** [ *num* ]

| Parameter Description | Parameter | Description |
|---|---|---|
| | *num* | Protocol. |

**Defaults** N/A

**Command Mode** Privileged EXEC mode.

**Usage Guide** N/A

**Configuration Examples** The following example displays all IPv6 raw sockets.

```
Ruijie# show ipv6 raw-socket
Number Protocol Process name
1      ICMPv6   vrrp.elf
2      ICMPv6   tcpip.elf
3      VRRP     vrrp.elf
Total: 3
```

| Field | Description |
|---|---|
| Number | Number. |
| Protocol | Protocol. |
| Process name | Process number. |
| Total | Total number of IPv6 raw sockets. |

**Related Commands**

| Command | Description |
|---|---|
| N/A | N/A |

**Platform Description** N/A

## 3.35 show ipv6 sockets

Use this command to display all IPv6 sockets.

**show ipv6 sockets**

**Parameter Description**

| Parameter | Description |
|---|---|
| N/A | N/A |

**Defaults** N/A

**Command Mode** Privileged EXEC mode.

**Usage Guide** N/A

**Configuration Examples** The following example displays all IPv6 sockets.

```
Ruijie# show ipv6 sockets
Number Process name    Type   Protocol  LocalIP:Port  ForeignIP:Port  State
1      vrrp.elf        RAW    ICMPv6    :::58         :::0            *
2      tcpip.elf       RAW    ICMPv6    :::58         :::0            *
```

```
3     vrrp.elf        RAW    VRRP     :::112        :::0          *
4     rg-snmpd        DGRAM  UDP      :::161        :::0          *
5     rg-snmpd        DGRAM  UDP      :::162        :::0          *
6     dhcp6.elf       DGRAM  UDP      :::547        :::0          *
7     rg-sshd         STREAM TCP      :::22         :::0          LISTEN
8     rg-telnetd      STREAM TCP      :::23         :::0          LISTEN
Total: 8
```

| Field | Description |
|---|---|
| Number | Number. |
| Process name | Process name. |
| Type | Socket type. RAW indicates the raw socket. DGRAM indicates data packet type. STREAM indicates traffic type. |
| Protocol | Protocol number |
| LocalIP:Port | Local IPv6 address and port. |
| ForeignIP:Port | Peer IPv6 address and port. |
| State | State (for IPv6 TCP sockets). |
| Total | Total number of sockets. |

**Related Commands**

| Command | Description |
|---|---|
| N/A | N/A |

**Platform Description** N/A

## 3.36 show ipv6 udp

Use this command to display all IPv6 UDP sockets.

**show ipv6 udp** [ **local-port** *num* ] [ **peer-port** *num* ]

Use this command to display IPv6 UDP socket statistics.

**show ipv6 udp statistics**

**Parameter Description**

| Parameter | Description |
|---|---|
| **local-port** *num* | Local port number. |
| **peer-port** *num* | Peer port number. |

**Defaults** N/A

**Command Mode** Privileged EXEC mode

**Usage Guide** N/A

**Configuration Examples** The following example displays all IPv6 UDP sockets.

```
Ruijie# show ipv6 udp
Number Local Address   Peer Address   Process name
1     :::161          :::0         rg-snmpd
2     :::162          :::0         rg-snmpd
3      :::547           :::0          dhcp6.elf
```

| Filed | Description |
|---|---|
| Number | Number. |
| Local Address | Local IPv6 address and port. |
| Peer Address | Peer IPv6 address and port. |
| Process name | Process name. |

**Related Commands**

| Command | Description |
|---|---|
| N/A | N/A |

**Platform Description** N/A

# 4 DHCP Commands

## 4.1 address range

Use this command to specify the network segment range of the addresses that can be allocated by CLASS associated with DHCP address pool. Use the **no** form of this command to restore the default setting.

**address range** *low-ip-address high-ip-address*

**no address range**

**Parameter Description**

| Parameter | Description |
|---|---|
| *low-ip-address* | Start address in the network segment range. |
| *high-ip-address* | End address in the network segment range. |

**Defaults** By default, the associated CLASS is not configured with the network segment range. The default is the address pool range.

**Command Mode** Address pool CLASS configuration mode.

**Usage Guide** Each CLASS corresponds to one network range which must be from low address to high address, so as to allow the duplication of network segment range between multiple CLASSes. If the CLASS associated with the address pool is specified without configuring the corresponding network segment range, the default network segment range of this CLASS is same as the range of the address pool where this CLASS is.

**Configuration Examples** The following example configures the network segment of class1 associated with address pool mypool0 ranging from 172.16.1.1 to 172.16.1.8.

```
Ruijie(config)# ip dhcp pool mypool0
Ruijie(dhcp-config)# class class1
Ruijie (config-dhcp-pool-class)# address range 172.16.1.1 172.16.1.8
```

**Related Commands**

| Command | Description |
|---|---|
| **ip dhcp pool** | Defines the name of the DHCP address pool and enters the DHCP address pool configuration mode. |
| **class** | Configures the CLASS associated with the DHCP address pool and enters the address pool CLASS configuration mode. |

**Platform Description** N/A

## 4.2 address-manage

Use this command to enter the AM rule configuration mode.

**address-manage**

| Parameter Description | Parameter | Description |
|---|---|---|
| | N/A | N/A |

**Defaults** N/A

**Command Mode** Global configuration mode

**Usage Guide** This command is configured on the DHCP server and used in combination with Super VLAN.

**Configuration Examples** The following example enters the AM rule configuration mode.

```
Ruijie(config)#address-manage
```

| Related Commands | Command | Description |
|---|---|---|
| | N/A | N/A |

**Platform Description** N/A

## 4.3 bootfile

Use this command to define the startup mapping file name of the DHCP client. Use the **no** or **default** form of this command to restore the default setting.

**bootfile** *file-name*

**no bootfile**

**default bootfile**

| Parameter Description | Parameter | Description |
|---|---|---|
| | *file-name* | Startup file name. |

**Defaults** No startup file name is defined by default.

**Command Mode** DHCP address pool configuration mode

**Usage Guide** Some DHCP clients need to download the operating system and configure the file during the startup. The DHCP server should provide the mapping file name required for the startup, so that DHCP clients

can download the file from the corresponding server (such as TFTP). Other servers are defined by the **next-server** command.

**Configuration Examples** The following example defines the device.conf as the startup file name.

```
bootfile device.conf
```

**Related Commands**

| Command | Description |
|---|---|
| **ip dhcp pool** | Defines the name of the DHCP address pool and enter the DHCP address pool configuration mode. |
| **next-server** | Configures the next server IP address of the DHCP client startup process. |

**Platform Description** N/A

## 4.4 class

Use this command to configure the associated CLASS in the DHCP address pool. Use the **no** form of this command to restore the default setting.

**class** *class-name*

**no class**

**Parameter Description**

| Parameter | Description |
|---|---|
| *class-name* | Class name, which can be the character string or numeric such as myclass or 1. |

**Defaults** By default, no CLASS is associated with the address pool.

**Command Mode** DHCP address pool configuration mode

**Usage Guide** Each DHCP address pool performs the address assignment according to the Option82 matching information. We can divide this Option82 information into classes and specify the available network segment range for these classes in the DHCP address pool. These classes are called CLASS. One DHCP address pool can map to multiple CLASSes, and each CLASS can specify different network segment range.

During the address assignment, firstly, ensure the assignable address pool through the network segment where the client is, then according to the Option82 information further ensure the CLASS and assign the IP address from the network segment range corresponding to the CLASS. If one request packet matches multiple CLASSes in the address pool, perform the address assignment according to the sequencing of configuring the CLASS in the address pool. If this CLASS's assigned addresses have been to the upper limit, then continue to assign the address from the next CLASS, and so on. Each CLASS corresponds to one network segment range that must be from low addresses to high addresses and the duplicated network ranges between multiple CLASSes are allowed. If the CLASS corresponding to the address pool is specified and the network segment corresponding to the CLASS is not configured, this CLASS's default network segment range is same

as the range of address pool where the CLASS is.

**Configuration Examples** The following example configures the address *mypool0* to associate with class1.

```
Ruijie(config)# ip dhcp pool mypool0
Ruijie(dhcp-config)# class class1
```

**Related Commands**

| Command | Description |
|---|---|
| **ip dhcp pool** | Defines the name of the DHCP address pool and enters the DHCP address pool configuration mode. |

**Platform Description** N/A

## 4.5 clear ip dhcp binding

Use this command to clear the DHCP binding table in the privileged user mode.

**clear ip dhcp binding** { * | *ip-address* }

**Parameter Description**

| Parameter | Description |
|---|---|
| * | Deletes all DHCP bindings. |
| *ip-address* | Deletes the binding of the specified IP addresses. |

**Defaults** N/A.

**Command Mode** Privileged EXEC mode.

**Usage Guide** This command can only clear the automatic DHCP binding, but the manual DHCP binding can be deleted by the **no ip dhcp pool** command.

**Configuration Examples** The following example clears the DHCP binding with the IP address 192.168.12.100.

```
clear ip dhcp binding 192.168.12.100
```

**Related Commands**

| Command | Description |
|---|---|
| **show ip dhcp binding** | Displays the address binding of the DHCP server. |

**Platform Description** N/A

## 4.6 clear ip dhcp conflict

Use this command to clear the DHCP address conflict record.

**clear ip dhcp conflict** { * | *ip-address* }

**Parameter Description**

| Parameter | Description |
|---|---|
| * | Deletes all DHCP address conflict records. |
| *ip-address* | Deletes the conflict record of the specified IP addresses. |

**Defaults** N/A.

**Command Mode** Privileged EXEC mode.

**Usage Guide** The DHCP server uses the ping session to detect the address conflict, while the DHCP client uses the address resolution protocol (ARP) to detect the address conflict. The **clear ip dhcp conflict** command can be used to delete the history conflict record.

**Configuration Examples** The following example clears all address conflict records.

```
clear ip dhcp conflict *
```

**Related Commands**

| Command | Description |
|---|---|
| **ip dhcp ping packets** | Defines the number of the data packets sent by the ping operation for the detection of the address conflict when the DHCP server assigns an IP address. |
| **show ip dhcp conflict** | Displays the address conflict that the DHCP server detects when it assigns an IP address. |

**Platform Description** N/A

## 4.7 clear ip dhcp history

Use this command to clear the address assigned by the DHCP server.

**clear ip dhcp history**{ * | *mac-address* }

**Parameter Description**

| Parameter | Description |
|---|---|
| * | Clears all addresses assigned by the DHCP server. |
| *mac-address* | Clears the address assigned by the DHCP server corresponding to the specified MAC address. |

**Defaults** N/A

**Command Mode** Privileged EXEC mode

**Usage Guide** This command is configured on the DHCP server.

**Configuration Examples** The following example clears all addresses assigned by the DHCP server.

```
Ruijie# clear ip dhcp history *
```

**Related Commands**

| Command | Description |
| --- | --- |
| N/A | N/A |

**Platform Description** N/A

## 4.8 clear ip dhcp server detect

Use this command to clear statistics about the fake DHCP server.

**clear ip dhcp server detect** { * | *ip-address* }

**Parameter Description**

| Parameter | Description |
| --- | --- |
| * | Clears statistics about all fake DHCP servers. |
| *ip-address* | Clears statistics about the specified fake DHCP server. |

**Defaults** N/A

**Command Mode** Privileged EXEC mode

**Usage Guide** The detected fake DHCP server addresses are saved on the server. You can use the **clear ip dhcp server detect** command to clear statistics about the fake DHCP server.

**Configuration Examples** The following example clears statistics about all fake DHCP servers.

```
Ruijie# clear ip dhcp server detect *
```

**Related Commands**

| Command | Description |
| --- | --- |
| N/A | N/A |

**Platform Description** N/A

## 4.9 clear ip dhcp server rate

Use this command to clear statistics about the packet processing rate of every module.

**clear ip dhcp server rate**

**Parameter Description**

| Parameter | Description |
| --- | --- |
| N/A | N/A |

**Defaults** N/A

**Command Mode** Privileged EXEC mode

**Usage Guide** This command is used to clear statistics about the packet processing rate of every module, including arp, hot backup, lsm, and socket.

**Configuration Examples** The following example clears statistics about the packet processing rate of every module.

```
Ruijie# clear ip dhcp server rate
```

**Related Commands**

| Command | Description |
| --- | --- |
| N/A | N/A |

**Platform Description** N/A

## 4.10 clear ip dhcp server statistics

Use this command to reset the counter of the DHCP server in the privileged user mode.

**clear ip dhcp server statistics**

**Parameter Description**

| Parameter | Description |
| --- | --- |
| N/A | N/A |

**Defaults** N/A

**Command Mode** Privileged EXEC mode.

**Usage Guide** The DHCP server carries out the statistics counter, records the DHCP address pool, automatic binding, manual binding and expired binding. Furthermore, it also carries out the statistics to the number of sent and received DHCP messages. The **clear ip dhcp server statistics** command can be used to delete the history counter record and carry out the statistics starting from scratch.

**Configuration Examples** The following example clears the statistics record of the DHCP server.

```
clear ip dhcp server statistics
```

**Related Commands**

| Command | Description |
| --- | --- |
| **show ip dhcp server statistics** | Displays the statistics record of the DHCP server. |

**Platform** N/A

**Description**

## 4.11 clear ip dhcp relay statistics

Use this command to clear the DHCP relay statistics.
**clear ip dhcp relay statistics**

| **Parameter Description** | **Parameter** | **Description** |
|---|---|---|
| | N/A | N/A |

**Defaults** N/A

**Command Mode** Privileged EXEC mode

**Usage Guide** The DHCP relay is configured with the counter to count various packets received or transmitted by the relay. This command is used to clear the counters.

**Configuration Examples** The following example clears the DHCP relay statistics.

```
Ruijie# clear ip dhcp relay statistics
```

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

**Platform Description** N/A

## 4.12 client-identifier

Use this command to define the unique ID of the DHCP client (indicated in hex, separated by dot) in the DHCP address pool configuration mode. Use the **no** or **default** form of this command to restore the default setting.
**client-identifier** *unique-identifier*
**no client-identifier**
**default client-identifier**

| **Parameter Description** | **Parameter** | **Description** |
|---|---|---|
| | *unique-identifier* | The DHCP client ID is indicated in hex and separated by dot, for instance, 0100.d0f8.2233.b467.6967.6162.6974.4574.6865.726e.6574.302f.31. |

**Defaults** N/A.

**Command** DHCP address pool configuration mode.

**Mode**

**Usage Guide** When some DHCP clients request the DHCP server to assign IP addresses, they use their client IDs rather than their hardware addresses. The client ID consists of media type, MAC addresses and interface name. For instance, the MAC address is 00d0.f822.33b4, the interface name is GigabitEthernet 0/1, and the corresponding client ID is 0100.d0f8.2233.b467.6967.6162.6974.4574.6865.726e.6574.302f.31, where, 01 denotes the type of the Ethernet media.
The 67.6967.6162.6974.4574.6865.726e.6574.302f.31 is the hex code of GigabitEthernet0/1. For the definition of the media code, refer to the Address Resolution Protocol Parameters section in RFC1700.
This command is used only when the DHCP is defined by manual binding.

**Configuration Examples** The following example defines the client ID of the Ethernet DHCP client whose MAC address is 00d0.f822.33b4.

```
client-identifier
0100.d0f8.2233.b467.6967.6162.6974.4574.6865.726e.6574.302f.31
```

**Related Commands**

| Command | Description |
|---|---|
| **hardware-address** | Defines the hardware address of DHCP client. |
| **host** | Defines the IP address and network mask, which is used to configure the DHCP manual binding. |
| **ip dhcp pool** | Defines the name of the DHCP address pool and enters the DHCP address pool configuration mode. |

**Platform Description** N/A

## 4.13 client-name

Use this command to define the name of the DHCP client in the DHPC address pool configuration mode. Use the **no** or **default** form of this command to restore the default setting.
**client-name** *client-name*
**no client-name**
**default client-name**

**Parameter Description**

| Parameter | Description |
|---|---|
| client-name | Name of DHCP client, a set of standards-based ASCII characters. The name should not include the suffix domain name. For instance, you can define the name of the DHCP client as river, not river.i-net.com.cn. |

**Defaults** No client name is defined by default.

**Command Mode** DHCP address pool configuration mode.

**Usage Guide** This command can be used to define the name of the DHCP client only when the DHCP is defined by manual binding. This name should not include the suffix domain name.

**Configuration Examples** The following example defines a string river as the name of the client.

```
Ruijie(dhcp-config)# client-name river
```

**Related Commands**

| Command | Description |
|---|---|
| **host** | Defines the IP address and network mask, which is used to configure the DHCP manual binding. |
| **ip dhcp pool** | Defines the name of the DHCP address pool and enters the DHCP address pool configuration mode. |

**Platform Description** N/A

## 4.14 default-router

Use this command to define the default gateway of the DHCP client in the DHPC address pool configuration mode. Use the **no** or **default** form of this command to restore the default setting.

**default-router** *ip-address* [ *ip-address2…ip-address8* ]

**no default-router**

**default default-route**

**Parameter Description**

| Parameter | Description |
|---|---|
| *ip-address* | Defines the IP address of the equipment. It is required to configure one IP address at least. |
| *ip-address2…ip-address8* | (Optional) Up to 8 gateways can be configured. |

**Defaults** No gateway is defined by default.

**Command Mode** DHCP address pool configuration mode.

**Usage Guide** In general, the DHCP client should get the information of the default gateway from the DHCP server. The DHCP server should specify one gateway address for the client at least, and this address should be of the same network segment as the address assigned to the client.

**Configuration Examples** The following example defines 192.168.12.1 as the default gateway.

```
default-router 192.168.12.1
```

| Related Commands | Command | Description |
|---|---|---|
| | **ip dhcp pool** | Defines the name of the DHCP address pool and enters the DHCP address pool configuration mode. |

**Platform Description** N/A

## 4.15 dns-server

Use this command to define the DNS server of the DHCP client in the DHPC address pool configuration mode. Use the **no** or **default** form of this command to restore the default setting.

**dns-server** { *ip-address* [ *ip-address2…ip-address8* ]

**no dns-server**

**default dns-server**

| Parameter Description | Parameter | Description |
|---|---|---|
| | *ip-address* | Defines the IP address of the DNS server. At least one IP address should be configured. |
| | *ip-address2…ip-address8* | (Optional) Up to 8 DNS servers can be configured. |

**Defaults** No DNS server is defined by default.

**Command Mode** DHCP address pool configuration mode.

**Usage Guide** When more than one DNS server is defined, the former will possess higher priory, so the DHCP client will select the next DNS server only when its communication with the former DNS server fails.
If the RGOS software also acts as the DHCP client, the DNS server information obtained by the client can be transmitted to the DHCP client.

**Configuration Examples** The following example specifies the DNS server 192.168.12.3 for the DHCP client.

```
dns-server 192.168.12.3
```

| Related Commands | Command | Description |
|---|---|---|
| | **domain-name** | Defines the suffix domain name of the DHCP client. |
| | **ip address dhcp** | Enables the DHCP client on the interface to obtain the IP address information. |
| | **ip dhcp pool** | Defines the name of the DHCP address pool and enters the DHCP address pool configuration mode. |

**Platform Description** N/A

## 4.16 domain-name

Use this command to define the suffix domain name of the DHCP client in the DHPC address pool configuration mode. Use the **no** or **default** form of this command to restore the default setting.
**domain-name** *domain-name*
**no domain-name**
**default domain-name**

| Parameter Description | Parameter | Description |
|---|---|---|
| | *domain-name* | Defines the suffix domain name string of the DHCP client. |

**Defaults** No suffix domain name by default.

**Command Mode** DHCP address pool configuration mode.

**Usage Guide** After the DHCP client obtains specified suffix domain name, it can access a host with the same suffix domain name by the host name directly.

**Configuration Examples** The following example defines the suffix domain name i-net.com.cn for the DHCP client.

```
Ruijie(dhcp-config)#domain-name ruijie.com.cn
```

| Related Commands | Command | Description |
|---|---|---|
| | **dns-server** | Defines the DNS server of the DHCP client. |
| | **ip dhcp pool** | Defines the name of the DHCP address pool and enter the DHCP address pool configuration mode. |

**Platform Description** N/A

## 4.17 dynamic-pool

Use this command to enable the fit AP to calculate the network number and mask of the dynamic DHCP address pool according to the MAC address. Use the **no** form of this command to remove the setting.
**dynamic-pool**
**no dynamic-pool**

| Parameter Description | Parameter | Description |
|---|---|---|
| | N/A | N/A |

**Defaults** N/A

**Command Mode** ap-config/ap-group mode

**Usage Guide** This command is configured on the server of the AC.

**Configuration Examples** The following example enables the fit AP to calculate the network number and mask of the dynamic DHCP address pool according to the MAC address

```
Ruijie(config-group) # dynamic-pool
```

**Related Commands**

| Command | Description |
|---|---|
| N/A | N/A |

**Platform Description** N/A

## 4.18 hardware-address

Use this command to define the hardware address of the DHCP client in the DHPC address pool configuration mode. Use the **no** or **default** form of this command to restore the default setting.

**hardware-address** *hardware-address* [ *type* ]

**no hardware-address**

**default hardware-address**

**Parameter Description**

| Parameter | Description |
|---|---|
| *hardware-address* | Define the MAC address of the DHCP client. |
| *type* | To indicate the hardware platform protocol of the DHCP client, use the string definition or digits definition.<br>String option:<br>Ethernet<br>ieee802<br>Digits option:<br>1 (10M Ethernet)<br>6 (IEEE 802) |

**Defaults** No hardware address is defined by default.
If there is no option when the hardware address is defined, it is the Ethernet by default.

**Command Mode** DHCP address pool configuration mode.

**Usage Guide** This command can be used only when the DHCP is defined by manual binding.

**Configuration Examples** The following example defines the MAC address 00d0.f838.bf3d with the type ethernet.

```
hardware-address 00d0.f838.bf3d
```

**Related Commands**

| Command | Description |
|---|---|
| **client-identifier** | Defines the unique ID of the DHCP client (Indicated by the hexadecimal numeral, separated by dot). |
| **host** | Defines the IP address and network mask, which is used to configure the DHCP manual binding. |
| **ip dhcp pool** | Defines the name of the DHCP address pool and enter the DHCP address pool configuration mode. |
| **default-router** | Defines the default route of the DHCP client. |

**Platform Description** N/A

## 4.19 host

Use this command to define the IP address and network mask of the DHCP client host in the DHCP address pool configuration mode. Use the **no** or **default** form of this command to restore the default setting.

**host** *ip-address* [ *netmask* ]

**no host**

**default host**

**Parameter Description**

| Parameter | Description |
|---|---|
| *ip-address* | Defines the IP address of DHCP client. |
| *netmask* | Defines the network mask of DHCP client. |

**Defaults** No IP address or network mask of the host is defined.

**Command Mode** DHCP address pool configuration mode.

**Usage Guide** If the network mask is not defined definitely, the DHCP server will use the natural network mask of this IP address: 255.0.0.0 for class A IP address, 255.255.0 for class B IP address, and 255.255.255.0 for class C IP address.

This command can be used only when the DHCP is defined by manual binding.

**Configuration Examples** The following example sets the client IP address as 192.168.12.91, and the network mask as 255.255.255.240.

```
host 192.168.12.91 255.255.255.240
```

**Related Commands**

| Command | Description |
|---|---|
| **client-identifier** | Defines the unique ID of the DHCP client (Indicated in hex and separated by dot). |

| | | |
|---|---|---|
| | **hardware-address** | Defines the hardware address of DHCP client. |
| | **ip dhcp pool** | Defines the name of the DHCP address pool and enters the DHCP address pool configuration mode. |
| **default-router** | Define the default route of the DHCP client. | **default-router** |

**Platform Description** N/A

## 4.20 ip address dhcp

Use this command to make the Ethernet interface or the PPP, HDLC and FR encapsulated interface obtain the IP address information by the DHCP in the interface configuration mode. Use the **no** or **default** form of this command to restore the default setting.

**ip address dhcp**

**no ip address dhcp**

**defaut ip address dhcp**

| **Parameter Description** | **Parameter** | **Description** |
|---|---|---|
| | N/A | N/A |

**Defaults** The interface cannot obtain the ID address by the DHCP by default.

**Command Mode** Interface configuration mode.

**Usage Guide** When requesting the IP address, the DHCP client of the RGOS software also requires the DHCP server provide 5 configuration parameter information: 1) DHCP option 1, client subnet mask, 2) DHCP option 3, it is the same as the gateway information of the same subnet, 3) DHCP option 6, the DNS server information, 4) DHCP option 15, the host suffix domain name, and 5) DHCP option 44, the WINS server information (optional).

The client of the RGOS software is allowed to obtain the address on the PPP, FR or HDL link by the DHCP, which should be supported by the server. At present, our server can support this function.

**Configuration Examples** The following example makes the FastEthernet 0 port obtain the IP address automatically.

```
Ruijie(config)# interface GigabitEthernet 0/1
Ruijie(config-if-GigabitEthernet 0/1) ip address dhcp
```

| **Related Commands** | **Command** | **Description** |
|---|---|---|
| | **dns-server** | Defines the DNS server of DHCP client. |
| | **ip dhcp pool** | Defines the name of the DHCP address pool and enters the DHCP address pool configuration mode. |

**Platform Description** N/A

## 4.21 ip dhcp class

Use this command to define a CLASS and enter the global CLASS configuration mode. Use the **no** form of this command to restore the default setting.

**ip dhcp class** *class-name*

**no ip dhcp class** *class-name*

**Parameter Description**

| Parameter | Description |
|---|---|
| *class-name* | Class name, which can be character string or numeric such as myclass or 1. |

**Defaults** By default, the class is not configured.

**Command Mode** Global configuration mode.

**Usage Guide** After executing this command, it enters the global CLASS configuration mode which is shown as “Ruijie (config-dhcp-class)#”. In this configuration mode, user can configure the Option82 information that matches the CLASS and the CLASS identification information.

**Configuration Examples** The following example configures a global CLASS.

```
Ruijie(config)# ip dhcp class myclass
```

**Related Commands**

| Command | Description |
|---|---|
| N/A | N/A |

**Platform Description** N/A

## 4.22 ip dhcp excluded-address

Use this command to define some IP addresses and make the DHCP server not assign them to the DHCP client in the global configuration mode. Use the **no** or **default** form of this command to restore the default setting.

**ip dhcp excluded-address** *low-ip-address* [ *high-ip-address* ]

**no ip dhcp excluded-address** *low-ip-address* [ *high-ip-address* ]

**default ip dhcp excluded-address** *low-ip-address* [*high-ip-address*]

**Parameter Description**

| Parameter | Description |
|---|---|
| *low-ip-address* | Excludes the IP address, or excludes the start IP address within the range of the IP address. |

| | |
|---|---|
| *high-ip-address* | Excludes the end IP address within the range of the IP address. |

**Defaults** The DHCP server assigns the IP addresses of the whole address pool by default.

**Command Mode** Global configuration mode.

**Usage Guide** If the excluded IP address is not configured, the DHCP server attempts to assign all IP addresses in the DHCP address pool. This command can reserve some IP addresses for specific hosts to prevent these addresses are assigned to the DHCP client, and define the excluded IP address accurately to reduce the conflict detecting time when the DHCP server assigns the address.

**Configuration Examples** In the following example, the DHCP server will not attempt to assign the IP addresses within 192.168.12.100~150.

```
ip dhcp excluded-address 192.168.12.100 192.168.12.150
```

The following example restores the default setting.

```
Ruijie(config)#no ip dhcp excluded-address 192.168.12.100 192.168.12.150
```

**Related Commands**

| Command | Description |
|---|---|
| **ip dhcp pool** | Defines the name of the DHCP address pool and enters the DHCP address pool configuration mode. |
| **network (DHCP)** | Defines the network number and network mask of the DHCP address pool. |

**Platform Description** N/A

## 4.23 ip dhcp force-send-nak

Use this command to configure the forcible NAK packet sending function. Use the **no** or **default** form of this command to restore the default setting.

**ip dhcp force-send-nak**

**no ip dhcp force-send-nak**

**default ip dhcp force-send-nak**

**Parameter Description**

| Parameter | Description |
|---|---|
| N/A | N/A |

**Defaults** This function is disabled by default.

**Command** Global configuration mode.

**Mode**

**Usage Guide** The DHCP client checks the previously used IP address every time it is started and sends a DHCPREQUEST packet to continue leasing this IP address. If the address is not available, the DHCP server sends an NAK packet to let the client resend a DHCPDISCOVER packet to apply for a new IP address. If no corresponding lease record can be found on the server, the client keeps sending DHCPDISCOVER packets. The forcible NAK packet sending function is added to shorten the interval at which the client sends DHCPDISCOVER packets.

**Configuration Examples** The following example enables the forcible NAK packet sending function in global configuration mode.

```
Ruijie(config)# ip dhcp force-send-nak
```

**Related Commands**

| Command | Description |
|---|---|
| N/A | N/A |

**Platform Description** N/A

## 4.24 ip dhcp monitor-vrrp-state

Use this command in layer-3 configuration mode to enable the DHCP Server to monitor the status of VRRP interfaces so that the DHCP Server processes only those packets sent from a VRRP interface in the Master state. Use the **no** or **default** form of this command to restore the default setting. If it is canceled, the DHCP Server processes packets from VRRP interfaces in the Master or Backup state.

**ip dhcp monitor-vrrp-state**

**no ip dhcp monitor-vrrp-state**

**default ip dhcp monitor-vrrp-state**

**Parameter Description**

| Parameter | Description |
|---|---|
| N/A | N/A |

**Defaults** The **ip dhcp monitor-vrrp-state** command is disabled by default. .

**Command Mode** Layer-3 interface configuration mode.

**Usage Guide** If a VRRP address is configured for an interface, the DHCP Server processes packets sent from the master interface and discards packets sent from the backup interface. If no VRRP address is configured, the DHCP Server does not monitor the status of VRRP interfaces. All DHCP packets will be processed.

**Configuration Examples** The following example enables the DHCP Server to monitor the status of VRRP interfaces.

```
Ruijie(config-if)# ip dhcp monitor-vrrp-state
```

| Related Commands | Command | Description |
|---|---|---|
| | N/A | N/A |

**Platform Description** N/A

## 4.25 ip dhcp ping packets

Use this command to configure the times of pinging the IP address when the DHCP server detects address conflict in the global configuration mode. Use the **no** or **default** form of this command to restore the default setting.

**ip dhcp ping packets** [ *number* ]

**no ip dhcp ping packets**

**default ip dhcp ping packets**

| Parameter Description | Parameter | Description |
|---|---|---|
| | *number* | (Optional) Number of packets in the range of 0 to 10, where 0 indicates disabling the ping operation. The Ping operation sends two packets by default. |

**Defaults** The Ping operation sends two packets by default.

**Command Mode** Global configuration mode.

**Usage Guide** When the DHCP server attempts to assign the IP address from the DHCP address pool, use the ping operation to check whether this address is occupied by other hosts. Record it if the address is occupied, otherwise, assign it to the DHCP client. The Ping operation will send up to 10 packets, two packets by default.

**Configuration Examples** The following example sets the number of the packets sent by the ping operation as 3.

```
ip dhcp ping packets 3
```

| Related Commands | Command | Description |
|---|---|---|
| | **clear ip dhcp conflict** | Clears the DHCP history conflict record. |
| | **ip dhcp ping packet** | Configures the timeout time that the DHCP server waits for the Ping response. If all the ping packets are not responded within the specified time, it indicates that this IP address can be assigned. Otherwise, it will record the address conflict. |
| | **show ip dhcp conflict** | Displays the DHCP server detects address conflict when it assigns an IP address. |

**Platform** N/A

**Description**

## 4.26 ip dhcp ping timeout

Use this command to configure the timeout that the DHCP server waits for response when it uses the ping operation to detect the address conflict in the global configuration mode. Use the **no** or **default** form of this command to restore the default setting.

**ip dhcp ping timeout** *milli-seconds*

**no ip dhcp ping timeout**

**default ip dhcp ping timeout**

**Parameter Description**

| Parameter | Description |
|---|---|
| *milli-seconds* | Time that the DHCP server waits for ping response in the range 100 to 10000 milliseconds. |

**Defaults** The default is 500 seconds.

**Command Mode** Global configuration mode.

**Usage Guide** This command defines the time that the DHCP server waits for a ping response packet.

**Configuration Examples** The following example configures the waiting time of the ping response packet to 600ms.

```
ip dhcp ping timeout 600
```

**Related Commands**

| Command | Description |
|---|---|
| **clear ip dhcp conflict** | Clears the DHCP history conflict record. |
| **ip dhcp ping packets** | Defines the number of the data packets sent by the ping operation for the detection of the address conflict when the DHCP server assigns an IP address. |
| **show ip dhcp conflict** | Displays the address conflict the DHCP server detects when it assigns an IP address. |

**Platform Description** N/A

## 4.27 ip dhcp pool

Use this command to define a name of the DHCP address pool and enter the DHCP address pool configuration mode in the global configuration mode. Use the **no** or **default** form of this command to restore the default setting.

**ip dhcp pool** *pool-name*

**no ip dhcp pool** *pool-name*

**default ip dhcp pool** *pool-name*

**Parameter Description**

| Parameter | Description |
|---|---|
| *pool-name* | A string of characters and positive integers, for instance, mypool or 1. |

**Defaults** No DHCP address pool is defined by default.

**Command Mode** Global configuration mode.

**Usage Guide** Execute the command to enter the DHCP address pool configuration mode:

```
Ruijie(dhcp-config)#
```

In this configuration mode, configure the IP address range, the DNS server and the default gateway.

**Configuration Examples** The following example defines a DHCP address pool named mypool0.

```
ip dhcp pool mypool0
```

**Related Commands**

| Command | Description |
|---|---|
| **host** | Defines the IP address and network mask, which is used to configure the DHCP manual binding. |
| **ip dhcp excluded-address** | Defines the IP addresses that the DHCP server cannot assign to the clients. |
| **network (DHCP)** | Defines the network number and network mask of the DHCP address pool. |

**Platform Description** N/A

## 4.28 ip dhcp refresh arp

Use this command to refreshes the trusted ARP allocation.

**ip dhcp refresh arp**

**Parameter Description**

| Parameter | Description |
|---|---|
| N/A | N/A |

**Defaults** N/A

**Command Mode** Global configuration mode

**Usage Guide** This command is configured on the DHCP server.

**Configuration Examples** The following example refreshes the trusted ARP allocation.

```
Ruijie(config)#ip dhcp refresh arp
```

**Related Commands**

| Command | Description |
| --- | --- |
| N/A | N/A |

**Platform Description** N/A

## 4.29 ip dhcp relay check server-id

Use this command to enable the **ip dhcp relay check** *server-id* function. Use the **no** form of this command to restore the default setting.

**ip dhcp relay check server-id**

**no ip dhcp relay check server-id**

**Parameter Description**

| Parameter | Description |
| --- | --- |
| N/A | N/A |

**Defaults** The **ip dhcp relay check server-id** command is disabled.

**Command Mode** Global configuration mode.

**Usage Guide** Switch will select the server to be sent according to server-id option when forwarding DHCP REQUEST via this command. Without this command configured, the switch forwards the DHCP REQUEST to all configured DHCP servers.

**Configuration Examples** The following example enables the ip dhcp relay check server-id function.

```
Ruijie# configure terminal
Ruijie(config)# ip dhcp relay check server-id
```

The following example disables the ip dhcp relay check server-id function.

```
Ruijie(config)# no ip dhcp relay check server-id
```

**Related Commands**

| Command | Description |
| --- | --- |
| **service dhcp** | Enables the DHCP Relay. |

**Platform Description** N/A

## 4.30 ip dhcp relay information option82

Use this command to enable the **ip dhcp relay information option82** function. Use the **no** form of this command to restore the default setting.

**ip dhcp relay information option82**

**no ip dhcp relay information option82**

| **Parameter Description** | **Parameter** | **Description** |
|---|---|---|
| | N/A | N/A |

**Defaults** The **ip dhcp relay information option82** command is disabled.

**Command Mode** Global configuration mode.

**Usage Guide** 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
```

The following example disables the option82 function on the DHCP relay.

```
Ruijie(config)# no ip dhcp relay information option82
```

| **Related Commands** | **Command** | **Description** |
|---|---|---|
| | **service dhcp** | Enables the DHCP Relay. |

**Platform Description** N/A

## 4.31 ip dhcp relay suppression

Use this command to enable the DHCP binding globally. Use the **no** form of this command to disable the DHCP binding globally and enable the **DHCP relay** suppression on the port.

**ip dhcp relay suppression**

**no ip dhcp relay suppression**

| **Parameter Description** | **Parameter** | **Description** |
|---|---|---|
| | N/A | N/A |

**Defaults** The **ip dhcp relay suppression** command is disabled.

**Command** Interface configuration mode.

**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.

```
Ruijie(config-if)# ip dhcp relay suppression
```

The following example disables the relay suppression function.

```
Ruijie(config-if)# no ip dhcp relay suppression
```

**Related Commands**

| Command | Description |
|---|---|
| **service dhcp** | Enables the DHCP Relay. |

**Platform Description** N/A

## 4.32 ip dhcp server detect

Use this command to enable the fake DHCP server detection. Use the **no** or **default** form of this command to restore the default setting.

**ip dhcp server detect**

**no ip dhcp server detect**

**default ip dhcp server detect**

**Parameter Description**

| Parameter | Description |
|---|---|
| N/A | N/A |

**Defaults** This function is disabled by default.

**Command Mode** Global configuration mode

**Usage Guide** After this function is enabled, any fake DHCP server detected is logged.

**Configuration Examples** The following example enables the fake DHCP server detection.

```
Ruijie(config)# ip dhcp server detect
```

**Related Commands**

| Command | Description |
|---|---|
| N/A | N/A |

**Platform Description** N/A

## 4.33 ip dhcp use class

Use this command to enable the CLASS to allocate addresses in the global configuration mode. Use the **no** form of this command can be used to disable the CLASS.

**ip dhcp use class**

**no ip dhcp use class**

| **Parameter Description** | **Parameter** | **Description** |
|---|---|---|
| | N/A | N/A |

**Defaults** Enabled

**Command Mode** Global configuration mode

**Usage Guide** This command is configured on the DHCP server.

**Configuration Examples** The following example enables the CLASS to allocate addresses.

```
Ruijie(config)# ip dhcp use class
```

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

**Platform Description** N/A

## 4.34 ip helper-address

Use this command to add an IP address of the DHCP server. Use the **no** form of this command to delete an IP address of the DHCP server.

The server address can be configured globally or on a specific interface. Therefore, this command can run in the global configuration mode or the interface configuration mode to add the DHCP server information.

**ip helper-address { cycle-mode |** *A.B.C.D* **}**

**no ip helper-address { cycle-mode |** *A.B.C.D* **}**

| **Parameter Description** | **Parameter** | **Description** |
|---|---|---|
| | **cycle-mode** | Forwards DHCP request packets to all DHCP servers. |
| | *A.B.C.D* | The IP address of the specified DHCP server. |

**Defaults** N/A

**Command** Global configuration mode

**Mode**

**Usage Guide** Up to 20 DHCP server IP addresses can be configured globally.

**Configuration Examples** The following example sets the IP address for the global server to 192.168.100.1

```
Ruijie# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Ruijie(config)# ip helper-address 192.168.100.1
```

The following example deletes the set IP address for the global server, 192.168.100.1.

```
Ruijie(config)# no ip helper-address 192.168.100.1
```

The following example enables forwarding DHCP request packets to all DHCP servers.

```
Ruijie(config)# ip helper-address cycle-mode
```

The following example disables forwarding DHCP request packets to all DHCP servers.

```
Ruijie(config)# no ip helper-address cycle-mode
```

**Related Commands**

| Command | Description |
|---|---|
| **service dhcp** | Enables the DHCP relay. |

**Platform Description** N/A

## 4.35 lease

Use this command to define the lease time of the IP address that the DHCP server assigns to the client in the DHCP address pool configuration mode. Use the **no** or **default** form of this command to restore the default setting. A limited lease time ranges from 1 minute to 23 hours and 59 minutes.

**lease** { *days* [ *hours* ] [ *minutes* ] | **infinite** }

**no lease**

**default lease**

**Parameter Description**

| Parameter | Description |
|---|---|
| *days* | Lease time in days |
| *hours* | (Optional) Lease time in hours. It is necessary to define the days before defining the hours. |
| *minutes* | (Optional) Lease time in minutes. It is necessary to define the days and hours before defining the minutes. |
| **infinite** | Infinite lease time. |

**Defaults** The lease time for a static address pool is infinite. The lease time for other address pools is 1 day.

**Command Mode** DHCP address pool configuration mode.

**Usage Guide** When the lease is getting near to expire, the DHCP client will send the request of renewal of lease. In general, the DHCP server will allow the renewal of lease of the original IP address.

**Configuration Examples** The following example sets the DHCP lease to 1 hour.

```
lease 0 1
```

The following example sets the DHCP lease to 1 minute.

```
lease 0 0 1
```

**Related Commands**

| Command | Description |
|---|---|
| **ip dhcp pool** | Defines the name of the DHCP address pool and enters the DHCP address pool configuration mode. |

**Platform Description** N/A

## 4.36 lease-threshold

Use this command in DHCP address pool configuration mode to define the DHCP alarm threshold. Use the **default** or **no** form of this command to restore the default setting.

**lease-threshold** *percentage*

**defaut lease-threshold**

**no lease-threshold**

**Parameter Description**

| Parameter | Description |
|---|---|
| *percentage* | Usage of the address pool, ranging from 60 to 100 in percentage. |

**Defaults** 90

**Command Mode** DHCP address pool configuration mode.

**Usage Guide** If the maximum IP usage of the address pool reaches the threshold, the DHCP Server generates a SYSLOG alarm. The IP usage indicates the ratio of the number of assigned address pools to the total number of assignable address pools. If the number of assigned pools stays above the alarm threshold, an alarm is generated every 5 minutes.

**Configuration Examples** The following example sets the alarm threshold to 80%.

```
lease-threshold 80
```

The following example restores the default alarm threshold.

```
default lease-threshold
```

**Related Commands**

| Command | Description |
| --- | --- |
| **ip dhcp pool** | Defines the name of the DHCP address pool and enters the DHCP address pool configuration mode. |

**Platform Description** N/A

## 4.37 match ip

Use this command to define an AM matching rule.
Use the **no** form of this command to remove the configuration.
Use the clear form of this command to clear all configurations.
**match ip** *ip-address netmask* [*interface*] [**add/remove**] **vlan** *vlan-list*
**no match ip** *ip-address netmask* [*interface*] [**add/remove**] **vlan** *vlan-list*

**Parameter Description**

| Parameter | Description |
| --- | --- |
| *ip-address* | IP address |
| *netmask* | Subnet mask |
| *interface* | Interface ID |
| *add/remove* | Adds or removes the specified VLAN. |
| *vlan-list* | VLAN ID |

**Defaults** N/A

**Command Mode** AM rule configuration mode

**Usage Guide** With this function enabled, all DHCP clients with specified *vlan-list* and *interface* obtain addresses in the rule.
If a DHCP client obtains a static address, it is not subject to AM matching rules in whichever Sub VLAN unless the AM rule configuration is based on VLAN instead of Sub VLAN. This type of matching rules applies to only static addresses.

**Configuration Examples** The following example defines an AM matching rule.

```
Ruijie(config-address-manage)#match ip 192.168.11.0 255.255.255.0
GigabitEthernet 0/10 vlan 10
```

**Related Commands**

| Command | Description |
| --- | --- |
| N/A | N/A |

**Platform** N/A

**Description**

## 4.38 match ip default

Use this command to define a default AM matching rule.
Use the **no** form of this command to remove the configuration,
**match ip default** *ip-address netmask*
**no match ip default** *ip-address netmask*

**Parameter Description**

| Parameter | Description |
|---|---|
| *ip-address* | IP address |
| *netmask* | Subnet mask |

**Defaults** N/A

**Command Mode** AM rule configuration mode

**Usage Guide** With this function enabled, all DHCP clients with specified *vlan-list* and *interface* obtain addresses in the default rule.

**Configuration Examples** The following example defines a default AM matching rule.

```
Ruijie(config-address-manage)#match ip default 192.168.12.0 255.255.255.0
```

**Related Commands**

| Command | Description |
|---|---|
| N/A | N/A |

**Platform Description** N/A

## 4.39 netbios-name-server

Use this command to configure the WINS name server of the Microsoft DHCP client NETBIOS in the DHCP address pool configuration mode. The **no** or **default** form of this command can be used to restore the default setting.
**netbios-name-server** *ip-address* [ *ip-address2…ip-address8* ]
**no netbios-name-server**
**defaut netbios-name-server**

**Parameter Description**

| Parameter | Description |
|---|---|
| *ip-address* | IP address of the WINS server. It is required to configure one IP address at least. |
| *ip-address2…ip-address8* | (Optional) IP addresses of WINS servers. Up to 8 WINS servers can |

| | |
|---|---|
| | be configured. |

**Defaults** No WINS server is defined by default.

**Command Mode** DHCP address pool configuration mode.

**Usage Guide** When more than one WINS server is defined, the former has higher priory. The DHCP client will select the next WINS server only when its communication with the former WINS server fails.

**Configuration Examples** The following example specifies the WINS server 192.168.12.3 for the DHCP client.

```
netbios-name-server 192.168.12.3
```

**Related Commands**

| Command | Description |
|---|---|
| **ip address dhcp** | Enables the DHCP client on the interface to obtain the IP address. |
| **ip dhcp pool** | Defines the name of the DHCP address pool and enter the DHCP address pool configuration mode. |
| **netbios-node-type** | Defines the netbios node type of the client host. |

**Platform Description** N/A

## 4.40 netbios-node-type

Use this command to define the node type of the master NetBIOS of the Microsoft DHCP client in the DHCP address configuration mode. Use the **no** or **default** form of this command to restore the default setting.

**netbios-node-type** *type*

**no netbios-node-type**

**defaut netbios-node-type**

**Parameter Description**

| Parameter | Description |
|---|---|
| *type* | Type of node in two modes:<br>Digit in hexadecimal form in the range of 0 to FF. Only the following numerals are available:<br>1: b-node.<br>2: p-node.<br>4: m-node.<br>8: h-node.<br>String:<br>b-node: broadcast node<br>p-node: peer-to-peer node<br>m-node: mixed node |

| | |
|---|---|
| | h-node: hybrid node |

**Defaults** No type of the NetBIOS node is defined by default.

**Command Mode** DHCP address pool configuration mode.

**Usage Guide** There are 4 types of the NetBIOS nodes of the Microsoft DHCP client: 1) Broadcast, which carries out the NetBIOS name resolution by the broadcast method, 2) Peer-to-peer, which directly requests the WINS server to carry out the NetBIOS name resolution, 3) Mixed, which requests the name resolution by the broadcast method firstly, and then carry out the name resolution by the WINS server connection, 4) Hybrid, which requests the WINS server to carry out the NetBIOS name resolution firstly, and it will carry out the NetBIOS name resolution by the broadcast method if the response is not received.
By default, the node type for Microsoft operating system is broadcast or hybrid. If the WINS server is not configured, broadcast node is used. Otherwise, hybrid node is used. It is recommended to set the type of the NetBIOS node as Hybrid.

**Configuration Examples** The following example sets the NetBIOS node of Microsoft DHCP client as Hybrid.

```
netbios-node-type h-node
```

**Related Commands**

| Command | Description |
|---|---|
| **ip dhcp pool** | Defines the name of DHCP address pool and enters the DHCP address pool configuration mode. |
| **netbios-name-server** | Configures the WINS name server of the Microsoft DHCP client NETBIOS. |

**Platform Description** N/A

## 4.41 network

Use this command to define the network number and network mask of the DHCP address pool in the DHCP address pool configuration mode. Use the **no** or **default** form of this command to restore the default setting.
**network** *net-number net-mask* [ *low-ip-address high-ip-address* ]
**no network**
**defaut network**

**Parameter Description**

| Parameter | Description |
|---|---|
| *net-number* | Network number of the DHCP address pool |
| *net-mask* | Network mask of the DHCP address pool. If the network mask is not defined, the natural network mask will be used by default. |

| | |
|---|---|
| *low-ip-address* | Start IP address. |
| *high-ip-address* | End IP address. |

**Defaults** No network number or network mask is defined by default.

**Command Mode** DHCP address pool configuration mode.

**Usage Guide** This command defines the subnet and subnet mask of a DHCP address pool, and provides the DHCP server with an address space which can be assigned to the clients. Unless excluded addresses are configured, all the addresses of the DHCP address pool can be assigned to the clients. The DHCP server assigns the addresses in the address pool orderly. If the DHCP server found an IP address is in the DHCP binding table or in the network segment, it checks the next until it assigns an effective IP address.

The **show ip dhcp binding** command can be used to view the address assignment, and the **show ip dhcp conflict** command can be used to view the address conflict detection configuration.

**Configuration Examples** The following example defines the network number of the DHCP address pool as 192.168.12.0, and the network mask as 255.255.255.240.

```
network 192.168.12.0 255.255.255.240
```

**Related Commands**

| Command | Description |
|---|---|
| **ip dhcp excluded-address** | Defines the IP addresses that the DHCP server cannot assign to the clients. |
| **ip dhcp pool** | Defines the name of the DHCP address pool and enters the DHCP address pool configuration mode. |

**Platform Description** N/A

## 4.42 next-server

Use this command to define the startup sever list that the DHCP client accesses during startup in the DHCP address configuration mode. Use the **no** or **default** form of this command to restore the default setting.

**next-server** *ip-address* [ *ip-address2…ip-address8* ]

**no next-server**

**defaut next-server**

**Parameter Description**

| Parameter | Description |
|---|---|
| *ip-address* | Defines the IP address of the startup server, which is usually the TFTP server. It is required to configure one IP address at least. |
| *ip-address2…ip-address8* | (Optional) Up to 8 startup servers can be configured. |

**Defaults** N/A

**Command Mode** DHCP address pool configuration mode.

**Usage Guide** When more than one startup server is defined, the former will possess higher priory. The DHCP client will select the next startup server only when its communication with the former startup server fails.

**Configuration Examples** The following example specifies the startup server 192.168.12.4 for the DHCP client.

```
next-server 192.168.12.4
```

**Related Commands**

| Command | Description |
|---|---|
| **bootfile** | Defines the default startup mapping file name of the DHCP client. |
| **ip dhcp pool** | Defines the name of the DHCP address pool and enter the DHCP address pool configuration mode. |
| **ip help-address** | Defines the Helper address on the interface. |
| **option** | Configures the option of the RGOS software DHCP server. |

**Platform Description** N/A

## 4.43 option

Use this command to configure the option of the DHCP server in the DHCP address pool configuration mode. Use the **no** or **default** form of this command to restore the default setting.

**option** *code* { **ascii** *string* | **hex** *string* | **ip** *ip-address* }

**no option**

**defaut option**

**Parameter Description**

| Parameter | Description |
|---|---|
| *code* | Defines the DHCP option codes. |
| **ascii** *string* | Defines an ASCII string. |
| **hex** *string* | Defines a hex string. |
| **ip** *ip-address* | Defines an IP address list. |

**Defaults** N/A

**Command Mode** Global configuration mode

**Usage Guide** The DHCP provides a mechanism to transmit the configuration information to the host in the TCP/IP

network. The DHCP message has a variable option field that can be defined according to the actual requirement. The DHCP client needs to carry the DHCP message with 32 bytes of option information at least. Furthermore, the fixed data field in the DHCP message is also referred to as an option. For the definition of current DHCP option, refer to RFC 2131.

**Configuration Examples** The following example defines the option code 19, which determines whether the DHCP client can enable the IP packet forwarding. 0 indicates to disable the IP packet forwarding, and 1 indicates to enable the IP packet forwarding. The configuration below enable the IP packet forwarding on the DHCP client.

```
Ruijie(dhcp-config)# option 19 hex 1
```

The following example defines the option code 33, which provides the DHCP client with the static route information. The DHCP client will install two static routes: 1) the destination network 172.16.12.0 and the gateway 192.168.12.12, 2) the destination network 172.16.16.0 and the gateway 192.168.12.16.

```
option 33 ip 172.16.12.0 192.168.12.12 172.16.16.0 192.168.12.16
```

**Related Commands**

| Command | Description |
|---|---|
| **ip dhcp pool** | Defines the name of the DHCP address pool and enters the DHCP address pool configuration mode. |

**Platform Description** N/A

## 4.44 pool-status

Use this command to enable or disable the DHCP address pool.

**pool-status** { **enable** | **disable** }

**Parameter Description**

| Parameter | Description |
|---|---|
| **enable** | Enables the address pool. |
| **disable** | Disables the address pool. |

**Defaults** By default, the address pool is enabled after it is configured.

**Command Mode** DHCP address pool configuration mode

**Usage Guide** This command is configured on the DHCP server.

**Configuration Examples** The following example disables the address pool.

```
Ruijie(dhcp-config)# pool-status disable
```

| Related Commands | Command | Description |
|---|---|---|
| | N/A | N/A |

**Platform Description** N/A

## 4.45 relay agent information

Use this command to enter the Option82 matching information configuration mode in the global CLASS configuration mode. Use the **no** form of this command to delete the Option82 matching information of the CLASS.

**relay agent information**

**no relay agent information**

| Parameter Description | Parameter | Description |
|---|---|---|
| | N/A | N/A |

**Defaults** N/A

**Command Mode** Global CLASS configuration mode

**Usage Guide** After executing this command, it enters the Option82 matching information configuration mode which is shown as “Ruijie (config-dhcp-class-relayinfo)#”.
In this configuration mode, user can configure the class matching multiple Option82 information.

**Configuration Examples** The following example configures a global CLASS and enters the Option82 matching information configuration mode.

```
Ruijie(config)# ip dhcp class myclass
Ruijie(config-dhcp-class)# relay agent information
Ruijie(config-dhcp-class-relayinfo)#
```

| Related Commands | Command | Description |
|---|---|---|
| | **ip dhcp class** | Defines a CLASS and enters the global CLASS configuration mode. |

**Platform Description** N/A

## 4.46 relay-information hex

Use this command to enter the Option82 matching information configuration mode. Use the **no** form of this command to delete a piece of matching information.

**relay-information hex** *aabb.ccdd.eeff…* [ * ]

**no relay-information hex** *aabb.ccdd.eeff…* [ * ]

**Parameter Description**

| Parameter | Description |
|---|---|
| *aabb.ccdd.eeff…[*]* | Hexadecimal Option82 matching information. The '*' symbol means partial matching which needs the front part matching only. Without the '*' means needing full matching. |

**Defaults** N/A

**Command Mode** Global CLASS configuration mode

**Usage Guide** This command is configured on the DHCP server.

**Configuration Examples** The following example configures a global CLASS which can match multiple Option82 information.

```
Ruijie(config)# ip dhcp class myclass
Ruijie(config-dhcp-class)# relay agent information
Ruijie(config-dhcp-class-relayinfo)# relay-information
 hex 0102256535
Ruijie(config-dhcp-class-relayinfo)# relay-information
 hex 010225654565
Ruijie(config-dhcp-class-relayinfo)# relay-information
 hex 060225654565
Ruijie(config-dhcp-class-relayinfo)# relay-information
 hex 060223*
```

**Related Commands**

| Command | Description |
|---|---|
| **ip dhcp class** | Defines a CLASS and enter the global CLASS configuration mode. |
| **relay agent information** | Enters the Option82 matching information configuration mode. |

**Platform Description** N/A

## 4.47 remark

Use this command to configure the identification which is used to describe the CLASS in this global CLASS configuration mode. Use the **no** form of this command to delete the identification.

**remark** *class-remark*

**no remark**

**Parameter Description**

| Parameter | Description |
|---|---|
| class-remark | Information used to identify the CLASS, which can be the character strings with space in them. |

**Defaults** N/A.

**Command Mode** Global CLASS configuration mode.

**Usage Guide** This command is configured on the DHCP server.

**Configuration Examples** The following example configures the identification information for a global CLASS.

```
Ruijie(config)# ip dhcp class myclass
Ruijie(config-dhcp-class)# remark used in #1 build
```

**Related Commands**

| Command | Description |
| --- | --- |
| **ip dhcp class** | Defines a CLASS and enter the global CLASS configuration mode. |

**Platform Description** N/A

## 4.48 service dhcp

Use this command to enable the DHCP server and the DHCP relay on the device in global configuration mode. Use the **no** or **default** form of this command to restore the default setting.
**service dhcp**
**no service dhcp**
**defaut service dhcp**

**Parameter Description**

| Parameter | Description |
| --- | --- |
| N/A | N/A |

**Defaults** The **service dhcp** command is disabled.

**Command Mode** Global configuration mode, ap-config/ap-group mode

**Usage Guide** The DHCP server can assign the IP addresses to the clients automatically, and provide them with the network configuration information such as DNS server and default gateway. The DHCP relay can forward the DHCP requests to other servers, and the returned DHCP responses to the DHCP client, serving as the relay for DHCP packets.

**Configuration Examples** The following example enables the DHCP server and the DHCP relay feature.

```
service dhcp
```

**Related**

| Command | Description |
| --- | --- |

| Commands | | |
|---|---|---|
| | **show ip dhcp server statistics** | Displays various statistics information of the DHCP server. |
| | **ip helper-address** [ **vrf** ] *A.B.C.D* | Adds an IP address of the DHCP server. |

**Platform Description** N/A

## 4.49 show dhcp lease

Use this command to display the lease information of the IP address obtained by the DHCP client.

**show dhcp lease**

| Parameter Description | Parameter | Description |
|---|---|---|
| | N/A | N/A |

**Defaults** N/A

**Command Mode** Privileged EXEC mode.

**Usage Guide** If the IP address is not defined, display the binding condition of all addresses. If the IP address is defined, display the binding condition of this IP address.

**Configuration Examples** The following example displays the result of the show dhcp lease.

```
Ruijie# show dhcp lease
Temp IP addr: 192.168.5.71 for peer on Interface: FastEthernet0/0
Temp sub net mask: 255.255.255.0
 DHCP Lease server: 192.168.5.70, state: 3 Bound
 DHCP transaction id: 168F
 Lease: 600 secs, Renewal: 300 secs, Rebind: 525 secs
Temp default-gateway addr: 192.168.5.1
 Next timer fires after: 00:04:29
 Retry count: 0 Client-ID: redgaint-00d0.f8fb.5740-Fa0/0
```

| Related Commands | Command | Description |
|---|---|---|
| | N/A | N/A |

**Platform Description** N/A

## 4.50 show ip dhcp binding

Use this command to display the binding condition of the DHCP address.

**show ip dhcp binding** [ *ip-address* ]

**Parameter Description**

| Parameter | Description |
| --- | --- |
| *ip-address* | (Optional) Only displays the binding condition of the specified IP addresses. |

**Defaults** N/A

**Command Mode** Privileged EXEC mode.

**Usage Guide** If the IP address is not defined, show the binding condition of all addresses. If the IP address is defined, show the binding condition of this IP address

**Configuration Examples** The following is the result of the show ip dhcp binding.

```
Ruijie# show ip dhcp binding
Total number of clients   : 4
Expired clients          : 3
Running clients          : 1

IP address       Hardware address      Lease expiration          Type
20.1.1.1         2000.0000.2011        000 days 23 hours 59 mins   Automatic
```

The meaning of various fields in the show result is described as follows.

| Field | Description |
| --- | --- |
| IP address | The IP address to be assigned to the DHCP client. |
| Client-Identifier /Hardware address | The client identifier or hardware address of the DHCP client. |
| Lease expiration | The expiration date of the lease. The Infinite indicates it is not limited by the time. The IDLE indicates the address is in the free status currently for it is not renewed or the DHCP client releases it actively. |
| Type | The type of the address binding. The Automatic indicates an IP address is assigned automatically, and the Manual indicates an IP address is assigned by manual. |

**Related Commands**

| Command | Description |
| --- | --- |
| **clear ip dhcp binding** | Clears the DHCP address binding table. |

**Platform Description** N/A

## 4.51 show ip dhcp conflict

Use this command to show the conflict history record of the DHCP sever.

**show ip dhcp conflict**

**Parameter Description**

| Parameter | Description |
|---|---|
| N/A | N/A |

**Defaults** N/A

**Command Mode** Privileged EXEC mode.

**Usage Guide** This command can display the conflict address list detected by the DHCP server.

**Configuration Examples** The following example displays the output result of the **show ip dhcp conflict** command.

```
Ruijie# show ip dhcp conflict
IP address  Detection Method
 192.168.12.1  Ping
```

The meaning of various fields in the show result is described as follows.

| Field | Description |
|---|---|
| IP address | The IP addresses which cannot be assigned to the DHCP client. |
| Detection Method | The conflict detection method. |

**Related Commands**

| Command | Description |
|---|---|
| **clear ip dhcp conflict** | Clears the DHCP conflict record. |

**Platform Description** N/A

## 4.52 show ip dhcp pool

Use this command to display the address statistics of an address pool.

**show ip dhcp pool** [ *poolname* ]

**Parameter Description**

| Parameter | Description |
|---|---|
| *poolname* | (Optional) Address pool whose address statistics are to be displayed. |

**Defaults**

**Command Mode** Privileged EXEC mode.

**Usage Guide** This command is configured on the DHCP server. Use this command to show the address statistics of an address pool.

**Configuration Examples** The following example displays the output result of the **show ip dhcp pool** *poolname* command.

```
Ruijie# show ip dhcp poolname
Pool poolname:
 Address range    192.168.0.1 - 192.168.0.254
 Class range     192.168.0.1 - 192.168.0.254
 Total address    252
Excluded     2
Distributed    30
Conflict     10
Remained     212
Usage percentage    84.12698%
Lease threshold    90%
```

The meaning of various fields in the show result is described as follows.

| Field | Description |
|---|---|
| Address range | Address range of the address pool. |
| Class range | Class address range. By default, the address range for the same address pool is not configured. Otherwise, the class range is displayed. |
| Total address | Total number of addresses that can be assigned in the address pool. |
| Excluded | Number of excluded addresses. |
| Distributed | Number of assigned addresses. |
| Conflict | Number of conflicting addresses in the address pool. |
| Remained | Number of remaining addresses that have not been assigned or can be reused. |
| Usage percentage | Address pool usage. |
| Lease threshold | Lease threshold. |

**Related Commands**

| Command | Description |
|---|---|
| ip dhcp pool | Defines the name of the DHCP address pool and enters the DHCP address pool configuration mode. |

**Platform Description** N/A

# 4.53 show ip dhcp relay-statistics

Use this command to display the statistics of the DHCP relay.

**show ip dhcp relay-statistics**

**Parameter Description**

| Parameter | Description |
|---|---|
| N/A | N/A |

**Defaults** N/A

**Command Mode** Privileged EXEC mode

**Usage Guide** This command is used to display the statistics of the DHCP relay.

**Configuration Examples** The following example displays the statistics of the DHCP relay.

```
Ruijie# show ip dhcp relay-statistics
Cycle mode              0

Message                 Count
Discover                0
Offer                   0
Request                 0
Ack                     0
Nak                     0
Decline                 0
Release                 0
Info                    0
Bad                     0

Direction               Count
Rx client               0
Rx client uni           0
Rx client bro           0
Tx client               0
Tx client uni           0
Tx client bro           0
Rx server               0
Tx server               0
```

The meaning of various fields in the show result is described as follows.

| Field | Description |
|---|---|
| Cycle mode | Whether to allow packets to be sent to multiple DHCP servers. |

| | |
|---|---|
| Discover | The number of Discover packets. |
| Offer | The number of Offer packets. |
| Request | The number of Request packets. |
| Ack | The number of Ack packets. |
| Nak | The number of Nak packets. |
| Decline | The number of Decline packets. |
| Release | The number of Release packets. |
| Info | The number of Info packets. |
| Bad | The number of error packets. |
| Rx client | The number of packets received from the client. |
| Rx client uni | The number of unicast packets received from the client. |
| Rx client bro | The number of broadcast packets received from the client. |
| Tx client | The number of packets transmitted to the client. |
| Tx client uni | The number of unicast packets transmitted to the client |
| Tx client bro | The number of multicast packets transmitted to the client |
| Rx server | The number of packets received from the server. |
| Tx server | The number of packets transmitted to the server. |

**Related Commands**

| Command | Description |
|---|---|
| N/A | N/A |

**Platform Description** N/A

## 4.54 show ip dhcp server detect

Use this command to display the fake DHCP server detected.

**show ip dhcp server detect**

**Parameter Description**

| Parameter | Description |
|---|---|
| N/A | N/A |

**Defaults** N/A

**Command Mode** Privileged EXEC mode

**Usage Guide** This command is configured on the DHCP server.

**Configuration Examples** The following example displays the fake DHCP server detected.

```
Ruijie#show ip dhcp server detect
The DHCP Server information:
Server IP = 10.1.10.40, DHCP server interface = GigabitEthernet 0/1
```

**Related Commands**

| Command | Description |
| --- | --- |
| N/A | N/A |

**Platform Description** N/A

## 4.55 show ip dhcp server statistics

Use this command to display the statistics of the DHCP server.

**show ip dhcp server statistics**

**Parameter Description**

| Parameter | Description |
| --- | --- |
| N/A | N/A |

**Defaults** N/A

**Command Mode** Privileged EXEC mode

**Usage Guide** This command displays the statistics of the DHCP server.

**Configuration Examples** The following example displays the output result of the **show ip dhcp server statistics** command.

```
Ruijie# show ip dhcp server statistics
Address pools           2
Lease counter           4
Active  Lease Counter    0
Expired Lease Counter    4
Malformed messages       0
Dropped messages         0

Message                 Received
BOOTREQUEST           216
DHCPDISCOVER           33
DHCPREQUEST           25
DHCPDECLINE            0
DHCPRELEASE            1
DHCPINFORM            150
```

```
Message                  Sent
BOOTREPLY               16
DHCPOFFER               9
DHCPACK                  7
DHCPNAK                  0
DHCPREQTIMES             0
DHCPREQSUCTIMES         0
DISCOVER-PROCESS-ERROR 0
LEASE-IN-PINGSTATE        0
NO-LEASE-RESOURCE       0
SERVERID-NO-MATCH        0
---------------------------------------------
recv                       0
send                       0
```

The meaning of various fields in the show result is described as follows.

| Field | Description |
|---|---|
| Address pools | Number of address pools. |
| Automatic bindings | Number of automatic address bindings. |
| Manual bindings | Number of manual address bindings. |
| Expired bindings | Number of expired address bindings. |
| Malformed messages | Number of malformed messages received by the DHCP. |
| Message Received or Sent | Number of the messages received and sent by the DHCP server respectively. |

**Related Commands**

| Command | Description |
|---|---|
| **clear ip dhcp server statistics** | Clears the DHCP server statistics. |

**Platform Description** N/A

## 4.56 show ip dhcp socket

Use this command to display the socket used by the DHCP server.

**show ip dhcp socket**

**Parameter Description**

| Parameter | Description |
|---|---|
| N/A | N/A |

**Defaults** N/A

**Command Mode** Privileged EXEC mode

**Usage Guide** N/A

**Configuration Examples** The following example displays the socket used by the DHCP server.

```
ruijie#show ip dhcp socket
dhcp socket = 47.
```

**Related Commands**

| Command | Description |
| --- | --- |
| N/A | N/A |

**Platform Description** N/A

## 4.57 update arp

Use this command to enable DHCP to add trusted ARP when allocating addresses. Use the **no** or **default** form of this command to restore the default setting.

**update arp**

**no update arp**

**defaut update arp**

**Parameter Description**

| Parameter | Description |
| --- | --- |
| N/A | N/A |

**Defaults** This function is disabled by default.

**Command Mode** DHCP address pool configuration mode

**Usage Guide** This command is configured on the DHCP server. The trusted ARP has a higher priority than the dynamic ARP and cannot be overwritten.

**Configuration Examples** The following example enables DHCP to add trusted ARP when allocating addresses.

```
Ruijie(dhcp-config)# update arp
```

**Related Commands**

| Command | Description |
| --- | --- |
| N/A | N/A |

**Platform** N/A

**Description**

# 5 DNS Commands

## 5.1 clear host

Use this command to clear the dynamically learned host name.

**clear host** [ * | *host-name* ]

**Parameter Description**

| Parameter | Description |
|---|---|
| *host-name* | Deletes the specified dynamic domain name buffer. |
| * | Deletes all dynamic domain name buffer. |

**Defaults** N/A

**Command Mode** Privileged EXEC mode.

**Usage Guide** You can obtain the mapping record of the host name buffer table in two ways: 1) the **ip host** static configuration, 2) the DNS dynamic learning. Execute this command to delete the host name records learned by the DNS dynamically.

**Configuration Examples** The following configuration deletes the dynamically learned mapping records from the host name-IP address buffer table.

```
Ruijie(config)#clear host *
```

**Related Commands**

| Command | Description |
|---|---|
| **show hosts** | Displays the host name buffer table. |

**Platform Description** N/A

## 5.2 ip domain-lookup

Use this command to enable DNS domain name resolution. Use the **no** form of this command to disable the DNS domain name resolution function.

**ip domain-lookup**

**no ip domain-lookup**

**Parameter Description**

| Parameter | Description |
|---|---|

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

**Defaults** This function is enabled by default.

**Command Mode** Global configuration mode.

**Usage Guide** This command enables the domain name resolution function.

**Configuration Examples** The following example disables the DNS domain name resolution function.

```
Ruijie(config)# no ip domain-lookup
```

**Related Commands**

| Command | Description |
|---|---|
| **show hosts** | Displays the DNS related configuration information. |

**Platform Description** N/A

## 5.3 ip host

Use this command to configure the mapping of the host name and the IP address. Use the **no** form of the command to remove the host list.

**ip host** *host-name ip-address*

**no ip host** *host*-name *ip-address*

**Parameter Description**

| Parameter | Description |
|---|---|
| *host-name* | The host name of the equipment |
| *ip-address* | The IP address of the equipment |

**Defaults** N/A

**Command Mode** Global configuration mode.

**Usage Guide** N/A

**Configuration Examples** The following example configures IPv4 address 192.168.5.243 for domain name www .test.com.

```
Ruijie(config)# ip host www.test.com 192.168.5.243
```

**Related**

| Command | Description |
|---|---|

**Commands**

| | |
|---|---|
| **show hosts** | Show the DNS related configuration information. |

**Platform Description** N/A

## 5.4 ip name-server

Use this command to configure the IP address of the domain name server. Use the **no** form of this command to delete the configured domain name server.

**ip name-server** { *ip-address* | *ipv6-address* }

**no ip name-server** [ *ip-address* | *ipv6-address* ]

**Parameter Description**

| Parameter | Description |
|---|---|
| *ip-address* | The IP address of the domain name server. |
| *ipv6-address* | The IPv6 address of the domain name server. |

**Defaults** No domain name server is configured by default.

**Command Mode** Global configuration mode.

**Usage Guide** Add the IP address of the DNS server. Once this command is executed, the equipment will add a DNS server. When the device cannot obtain the domain name from a DNS server, it will attempt to send the DNS request to subsequent servers until it receives a response.

Up to 6 DNS servers are supported. You can delete a DNS server with the *ip-address* option or all the DNS servers.

**Configuration Examples** The following example configures the IPv4 domain name server and IPv6 domain name server.

```
Ruijie(config)# ip name-server 192.168.5.134
Ruijie(config)# ip name-server 2001:0DB8::250:8bff:fee8:f800
2001:0DB8:0:f004::1
```

**Related Commands**

| Command | Description |
|---|---|
| **show hosts** | Displays the DNS related configuration information. |

**Platform Description** N/A

## 5.5 ipv6 host

Use this command to configure the mapping of the host name and the IPv6 address by manual. Use the **no** form of the command to remove the host list.

**ipv6 host** *host-name ipv6-address*

**no ipv6 host** *host*-name *ipv6-address*

**Parameter Description**

| Parameter | Description |
|---|---|
| *host-name* | The host name of the equipment |
| *ipv6-address* | The IPv6 address of the equipment |

**Defaults** N/A

**Command Mode** Global configuration mode.

**Usage Guide**

**Configuration Examples** The following example configures the IPv6 address for the domain name.

```
Ruijie(config)# ipv6 host switch 2001:0DB8:700:20:1::12
```

**Related Commands**

| Command | Description |
|---|---|
| **show hosts** | Displays the DNS related configuration information. |

**Platform Description** N/A

## 5.6 show hosts

Use this command to display DNS configuration.

**show hosts** [ *hostname* ]

**Parameter Description**

| Parameter | Description |
|---|---|
| *hostname* | Displays the specified domain name information, |

**Defaults** N/A

**Command Mode** Global configuration mode

**Usage Guide** This command is used to display the DNS related configuration information.

**Configuration Examples**

```
Ruijie# show hosts
Name servers are:
192.168.5.134 static

Host             type         Address             TTL(sec)
switch           static       192.168.5.243          ---
www.ruijie.com   dynamic      192.168.5.123          126
```

| Field | Description |
|---|---|
| Name servers | Domain name server |
| Host | Domain name |
| type | Resolution type:<br>Static resolution and dynamic resolution. |
| Address | IP address corresponding to the domain name |
| TTL | TTL of entries corresponding to the domain name/IP address. |

**Related Commands**

| Command | Description |
|---|---|
| **ip host** | Configures the host name and IP address mapping by manual. |
| **ipv6 host** | Configures the host name and IPv6 address mapping by manual. |
| **ip name-server** | Configures the DNS server. |

**Platform Description** N/A

# 6 Network Connectivity Test Tool Commands

## 6.1 clear rping table all

Use this command to clear Rping entries.

**clear rping table** [**all |** [**ping-object** *owner test-name*] | [**trace-object** *owner test-name*]]

**Parameter Description**

| Parameter | Description |
|---|---|
| *owner* | User index |
| *test-name* | Test index |

**Defaults** N/A

**Command Mode** Privileged EXEC mode

**Usage Guide** N/A

**Configuration Examples** The following example clears all Rping entries.

```
Ruijie# clear rping table all
```

The following example clears the specified Rping entry.

```
Ruijie# clear rping table user ruijie
```

**Related Commands**

| Command | Description |
|---|---|
| N/A | N/A |

**Platform Description** N/A

## 6.2 ping

Use this command to test the connectivity of a network to locate the network connectivity problem. The command format is as follows:

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

**Parameter Description**

| Parameter | Description |
|---|---|

| | |
|---|---|
| *address* | Specifies an IPv4 address. |
| *length* | Specifies the length of the packet to be sent (range: 36-18024, default: 100). |
| *times* | Specifies the number of packets to be sent (range:1-4294967295). |
| *seconds* | Specifies the timeout time (range: 1-10 seconds). |
| *data* | Specifies the data to fill in. |
| *source* | Specifies the source IPv4 address or the source interface. The loopback interface address (for example: 127.0.0.1) is not allowed to be the source address. |
| **df-bit** | Sets the DF bit for the IP address. DF bit=1 indicates not to segment the datagrams. By default, the DF bit is 0. |
| **validate** | Sets whether to validate the reply packets or not. |
| **detail** | Sets whether to contain details in the echoed message. By default, only "!" and "." are displayed. |

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

**Command Mode** Privileged EXEC mode: enables extended functions.
User EXEC mode: enables basic functions.

**Usage Guide** If the device can be pinged, the response information is displayed, and the statistics is listed at the end. For the extension functions of ping, the number, quantity and timeout time of the packets to be sent can be specified, and the statistics is also displayed in the end. To use the domain name function, configure the domain name server firstly. For the concrete configuration, refer to the DNS Configuration section.

**Configuration Examples** The following example tests the connectivity of a network to locate the network connectivity problem.

```
(regular ping).Ruijie# ping 192.168.21.26
Sending 5, 100-byte ICMP Echoes to 192.168.21.26, timeout is 2 seconds:
  < press Ctrl+C to break >
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/10 ms
```

The following example displays details.

```
Ruijie#ping 192.168.21.26 detail
Sending 5, 100-byte ICMP Echoes to 192.168.21.26, timeout is 2 seconds:
  < press Ctrl+C to break >
Reply from 192.168.21.26: bytes=100 time=4ms TTL=64
Reply from 192.168.21.26: bytes=100 time=3ms TTL=64
Reply from 192.168.21.26: bytes=100 time=1ms TTL=64
Reply from 192.168.21.26: bytes=100 time=1ms TTL=64
Reply from 192.168.21.26: bytes=100 time=1ms TTL=64
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms.2
```

The following example tests the connectivity of a network to locate the network connectivity problem

(extension ping).

```
Ruijie# ping 192.168.21.26 length 1500 ntimes 100 data ffff source 192.168.21.99
timeout 3
Sending 100, 1500-byte ICMP Echoes to 192.168.21.26, timeout is 3 seconds:
  < press Ctrl+C to break >
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!
Success rate is 100 percent (100/100), round-trip min/avg/max = 2/2/3 ms
```

The following example displays the details.

```
ping 192.168.21.26 length 1500 ntimes 20 data ffff source 192.168.21.99 timeout 3
detail
Sending 20, 1500-byte ICMP Echoes to 192.168.21.26, timeout is 3 seconds:
  < press Ctrl+C to break >
Reply from 192.168.21.26: bytes=1500 time=1ms TTL=64
Reply from 192.168.21.26: bytes=1500 time=1ms TTL=64
Reply from 192.168.21.26: bytes=1500 time=1ms TTL=64
Reply from 192.168.21.26: bytes=1500 time=1ms TTL=64
Reply from 192.168.21.26: bytes=1500 time=1ms TTL=64
Reply from 192.168.21.26: bytes=1500 time=1ms TTL=64
Reply from 192.168.21.26: bytes=1500 time=1ms TTL=64
Reply from 192.168.21.26: bytes=1500 time=2ms TTL=64
Reply from 192.168.21.26: bytes=1500 time=1ms TTL=64
Reply from 192.168.21.26: bytes=1500 time=1ms TTL=64
Reply from 192.168.21.26: bytes=1500 time=1ms TTL=64
Reply from 192.168.21.26: bytes=1500 time=1ms TTL=64
Reply from 192.168.21.26: bytes=1500 time=1ms TTL=64
Reply from 192.168.21.26: bytes=1500 time=1ms TTL=64
Reply from 192.168.21.26: bytes=1500 time=1ms TTL=64
Reply from 192.168.21.26: bytes=1500 time=1ms TTL=64
Reply from 192.168.21.26: bytes=1500 time=1ms TTL=64
Reply from 192.168.21.26: bytes=1500 time=3ms TTL=64
Reply from 192.168.21.26: bytes=1500 time=1ms TTL=64
Reply from 192.168.21.26: bytes=1500 time=1ms TTL=64

Success rate is 100 percent (20/20), round-trip min/avg/max = 1/1/3 ms
```

**Related Commands**

| Command | Description |
|---|---|
| N/A | N/A |

**Platform Description** N/A

## 6.3 ping ipv6

Use this command to test the connectivity of a network to locate the network connectivity problem. The command format is as follows:

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

**Parameter Description**

| Parameter | Description |
|---|---|
| *Ip-address* | Specifies an IPv6 address. |
| *length* | Specifies the length of the packet to be sent (range: 36-18024, default: 100). |
| *times* | Specifies the number of packets to be sent (range:1-4294967295). |
| *seconds* | Specifies the timeout time (range: 1-10 seconds). |
| *data* | Specifies the data to fill in. |
| *source* | Specifies the source IPv6 address or the source interface. The loopback interface address (for example: 127.0.0.1) is not allowed to be the source address. |
| **detail** | Sets whether to contain details in the echoed message. By default, only “!” and “.” are displayed. |

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

**Command Mode** Privileged EXEC mode: enables extended functions.
User EXEC mode: enables basic functions.

**Usage Guide** If the device can be pinged, the response information is displayed, and the statistics is listed at the end. If the response data does not match the request data, a ‘Request receive error.’ message is displayed and the statistics is listed in the end. For the extension functions of ping ipv6, the number, quantity and timeout time of the packets to be sent can be specified, and the statistics is also displayed in the end. To use the domain name function, configure the domain name server firstly. For the concrete configuration, refer to the DNS Configuration section.

**Configuration Examples** The following example tests the connectivity of a network to locate the network connectivity problem.

```
(regular ping) Ruijie# ping ipv6 2001::5
Sending 5, 100-byte ICMP Echoes to 2001::5, timeout is 2 seconds:
< press Ctrl+C to break >
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/10 ms
```

The following example displays details.

```
Ruijie#ping 2001::1 detail
```

```
Sending 5, 100-byte ICMP Echoes to 2001::1, timeout is 2 seconds:
  < press Ctrl+C to break >
Reply from 2001::1: bytes=100 time=1ms
Reply from 2001::1: bytes=100 time=1ms
Reply from 2001::1: bytes=100 time=1ms
Reply from 2001::1: bytes=100 time=1ms
Reply from 2001::1: bytes=100 time=1ms

Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms.
```

The following example tests the connectivity of a network to locate the network connectivity problem (extension ping).

```
Ruijie# ping ipv6 2001::5  length 1500 ntimes 100 data ffff source 2001::9 timeout
3
Sending 100, 1500-byte ICMP Echoes to 2000::1, timeout is 3 seconds:
  < press Ctrl+C to break >
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!
Success rate is 100 percent (100/100), round-trip min/avg/max = 2/2/3 ms
```

The following example displays the details.

```
Ruijie#ping 2001::5 length 1500 ntimes 10 data ffff source 2001::9 timeout 3
Sending 10, 1500-byte ICMP Echoes to 2001::5, timeout is 3 seconds:
  < press Ctrl+C to break >
Reply from 2001::5: bytes=1500 time=1ms
Reply from 2001::5: bytes=1500 time=1ms
Reply from 2001::5: bytes=1500 time=1ms
Reply from 2001::5: bytes=1500 time=1ms
Reply from 2001::5: bytes=1500 time=1ms
Reply from 2001::5: bytes=1500 time=1ms
Reply from 2001::5: bytes=1500 time=1ms
Reply from 2001::5: bytes=1500 time=1ms
Reply from 2001::5: bytes=1500 time=1ms
Reply from 2001::5: bytes=1500 time=1ms

Success rate is 100 percent (10/10), round-trip min/avg/max = 1/1/1 ms.
```

**Related Commands**

| Command | Description |
| --- | --- |
| N/A | N/A |

**Platform Description** N/A

## 6.4 show rping detail

Use this command to display Rping information.

**show rping detail**

**Parameter Description**

| Parameter | Description |
|---|---|
| N/A | N/A |

**Defaults** N/A

**Command Mode** Privileged EXEC mode/Global configuration mode/Interface configuration mode

**Usage Guide** This command is used to display the Rping information such as numbers of test accounts and users.

**Configuration Examples** The following example displays Rping information.

```
Ruijie#show rping detail
Total owner number: 2
Total test number: 4
owner: user1
  test name: taget_1       storage type: volatile
test name: taget_2       storage type: nonVolatile
owner: user2
  test name: taget_1       storage type: permanent
test name: taget_2       storage type: readOnly
```

| Field | Description |
|---|---|
| Total owner number | The number of users |
| Total test number | The number of Rping accounts |
| owner | Username |
| test name | Test name |
| storage type | Storage type |

**Related Commands**

| Command | Description |
|---|---|
| N/A | N/A |

**Platform Description** N/A

## 6.5 traceroute

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

**traceroute** [**ip**] [*adress* [**probe** *number* ] [ **source** *source* ] [ **timeout** *seconds* ] [ **ttl** *minimum maximum* ] ]

**Parameter Description**

| Parameter | Description |
|---|---|
| *address* | Specifies an IPv4 address. |
| *number* | Specifies the number of probe packets to be sent (range: 1-255). |
| *source* | Specifies the source IPv4 address or the source interface. The loopback interface address (for example: 127.0.0.1) is not allowed to be the source address. |
| *seconds* | Specifies the timeout time (range: 1-10 seconds). |
| *minimum maximum* | Specifies the minimum and maximum TTL values (range:1-255). |

**Defaults** By default, *seconds* is 3 seconds, *number* is 3, *minimum* and *maximum* are 1 and 255.

**Command Mode** Privileged EXEC mode: enables extended functions.
User EXEC mode: enables basic functions.

**Usage Guide** Use the **traceroute** command to test the connectivity of a network to exactly locate the network connectivity problem when the network failure occurs. To use the function domain name, configure the domain name server. For the concrete configuration, refer to the DNS Configuration part.

**Configuration Examples** The following is two examples of the application bout traceroute, the one is of the smooth network, and the other is the network in which some gateways aren't connected successfully.

1. When the network is connected smoothly:

```
Ruijie# traceroute 61.154.22.36
  < press Ctrl+C to break >
Tracing the route to 61.154.22.36

1     192.168.12.1      0 msec   0 msec   0 msec
2     192.168.9.2       4 msec   4 msec   4 msec
3     192.168.9.1       8 msec   8 msec   4 msec
4      192.168.0.10     4 msec   28 msec  12 msec
5      192.168.9.2      4 msec   4 msec   4 msec
6      202.101.143.154      12 msec  8 msec   24 msec
7      61.154.22.36     12 msec  8 msec   22 msec
```

From above result, it's clear to know that the gateways passed by the packets sent to the host with an IP address of 61.154.22.36 (gateways 1~6) and the spent time are displayed. Such information is helpful for network analysis.

2. When some gateways in the network fail:

```
Ruijie# traceroute 202.108.37.42
  < press Ctrl+C to break >
Tracing the route to 202.108.37.42

1     192.168.12.1      0 msec    0 msec  0 msec
2     192.168.9.2       0 msec    4 msec  4 msec
3     192.168.110.1     16 msec  12 msec  16 msec
4     *  *  *
5     61.154.8.129      12 msec   28 msec  12 msec
6     61.154.8.17       8 msec    12 msec  16 msec
7     61.154.8.250      12 msec   12 msec  12 msec
8     218.85.157.222    12 msec   12 msec  12 msec
9      218.85.157.130   16 msec   16 msec  16 msec
10     218.85.157.77    16 msec   48 msec  16 msec
11     202.97.40.65     76 msec   24 msec  24 msec
12     202.97.37.65     32 msec   24 msec  24 msec
13     202.97.38.162    52 msec   52 msec  224 msec
14     202.96.12.38     84 msec   52 msec  52 msec
15     202.106.192.226  88 msec   52 msec  52 msec
16     202.106.192.174      52 msec   52 msec  88 msec
17     210.74.176.158   100 msec  52 msec  84 msec
18     202.108.37.42    48 msec   48 msec  52 msec
```

The above result clearly shown that the gateways passed by the packets sent to the host with an IP address of 202.108.37.42 (gateways 1~17) and the spent time are displayed, and gateway 4 fails.

```
Ruijie# traceroute www.ietf.org

Translating "www.ietf.org"...[OK]
  < press Ctrl+C to break >
Tracing the route to 64.170.98.32

 1     192.168.217.1    0 msec  0 msec  0 msec
 2     10.10.25.1       0 msec  0 msec  0 msec
 3     10.10.24.1       0 msec  0 msec  0 msec
 4     10.10.30.1       10 msec 0 msec  0 msec
 5     218.5.3.254      0 msec  0 msec  0 msec
 6     61.154.8.49      10 msec 0 msec  0 msec
 7     202.109.204.210  0 msec  0 msec  0 msec
 8     202.97.41.69     20 msec 10 msec 20 msec
 9     202.97.34.65     40 msec 40 msec 50 msec
 10    202.97.57.222    50 msec 40 msec 40 msec
 11    219.141.130.122  40 msec 50 msec 40 msec
 12    219.142.11.10    40 msec 50 msec 30 msec
 13    211.157.37.14    50 msec 40 msec 50 msec
 14    222.35.65.1      40 msec 50 msec 40 msec
```

```
15    222.35.65.18     40 msec 40 msec 40 msec
16    222.35.15.109    50 msec 50 msec 50 msec
17    *      *      *
18    64.170.98.32    40 msec 40 msec 40 msec
```

**Related Commands**

| Command | Description |
|---|---|
| N/A | N/A |

**Platform Description** N/A

## 6.6 traceroute ipv6

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

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

**Parameter Description**

| Parameter | Description |
|---|---|
| *address* | Specifies an IPv6 address. |
| *number* | Specifies the number of probe packets to be sent. |
| *seconds* | Specifies the timeout time. |
| *minimum maximum* | Specifies the minimum and maximum TTL values. |

**Defaults** By default, *seconds* is 3 seconds, *number* is 3, *minimum* and *maximum* are 1 and 255.

**Command Mode** Privileged EXEC mode: enables extended functions.
User EXEC mode: enables basic functions.

**Usage Guide** Use the **traceroute ipv6** command to test the connectivity of a network to exactly locate the network connectivity problem when the network failure occurs. To use the function domain name, configure the domain name server. For the concrete configuration, refer to the DNS Configuration part.

**Configuration Examples** The following is two examples of the application bout traceroute ipv6, the one is of the smooth network, and the other is the network in which some gateways aren't connected successfully.
1. When the network is connected smoothly:

```
Ruijie# traceroute ipv6 3004::1
  < press Ctrl+C to break >
Tracing the route to 3004::1
1     3000::1        0 msec  0 msec  0 msec
2     3001::1        4 msec  4 msec 4 msec
3     3002::1        8 msec  8 msec  4 msec
```

```
4     3004::1        4 msec  28 msec  12 msec
```

From above result, it's clear to know that the gateways passed by the packets sent to the host with an IP address of 3004::1 (gateways 1~4) and the spent time are displayed. Such information is helpful for network analysis.

2. When some gateways in the network fail:

```
Ruijie# traceroute ipv6 3004::1
 < press Ctrl+C to break >
Tracing the route to 3004::1
1     3000::1        0 msec  0 msec  0 msec
2     3001::1        4 msec  4 msec 4 msec
3     3002::1        8 msec  8 msec  4 msec
4     * * *
5     3004::1        4 msec  28 msec  12 msec
```

The above result clearly shown that the gateways passed by the packets sent to the host with an IP address of 3004::1 (gateways 1~5) and the spent time are displayed, and gateway 4 fails.

**Related Commands**

| Command | Description |
| --- | --- |
| N/A | N/A |

**Platform Description** N/A

# 7 TCP Commands

## 7.1 ip tcp adjust-mss

Use this command to change the Maximum Segment Size (MSS) option value of SYN packets sent and received on an interface. Use the **no** form of this command to restore the default setting.

**ip tcp adjust-mss** *max-segment-size*

**no ip tcp adjust-mss**

**Parameter Description**

| Parameter | Description |
|---|---|
| *max-segment-size* | Maximum segment size in the range from 500 to 1460 bytes |

**Defaults** The MSS option value of SYN packets is not changed by default.

**Command Mode** Interface configuration mode

**Usage Guide** MSS refers to the maximum size of the payload of a TCP packet.

The TCP Path MTU (PMTU) is implemented as per RFC1191. This feature can improve the network bandwidth utilization ratio. When the user uses TCP to transmit mass data, this feature can substantially enhance the transmission performance.

When the client initiates a TCP connection, it negotiates the maximum payload of TCP packets through the MSS option field of the TCP SYN packet. The MSS value of the client's SYN packet implies the maximum payload of TCP packets sent by the server, and vice versa.

Configuring this command on the interface will change the MSS option of SYN packets received or sent by the interface to the MSS value configured on the interface. If the MSS is configured on both the inbound interface and the outbound interface of the SYN packet, the smaller of the two applies. It is recommended that you configure the same value on the inbound interface and outbound interface.

This command actually changes the SYN packet exchanged during TCP connection establishment. For some versions, this command may also change the SYN+ACK packet.

This command takes effect on the subsequent TCP connections to be established instead of established TCP connections.

**Configuration Examples** The following example changes the MSS option value of the TCPv4 SYN packet to 1000 bytes on port GigabitEthernet 0/0.

```
Ruijie(config-if-GigabitEthernet 0/0)# ip tcp adjust-mss 1000
```

**Related Commands**

| Command | Description |
|---|---|
| N/A | N/A |

**Platform Description** N/A

## 7.2 ip tcp keepalive

Use this command to enable the TCP keepalive function.
**ip tcp keepalive** [ **interval** *num1* ] [ **times** *num2* ] [ **idle-period** *num3* ]

**Parameter Description**

| Parameter | Description |
|---|---|
| **interval** *num1* | The interval of sending the keepalive packet, in the range from1 to 120 in the unit of seconds, The default is 75. |
| **times** *num2* | Keepalive packet sending times, in the range from 1 to 10. The default is 6. |
| **idle-period** *num3* | Idle time, the time period during which the peer end does not send any packet to the local end, in the range from 60 to 1800 in the unit of seconds. The default is 900. |

**Defaults** The function is disabled by default.

**Command Mode** Global configuration mode

**Usage Guide** The keepalive function enables TCP to detect whether the peer end is operating properly. Suppose the keepalive function is enabled together with default **interval**, **times** and **idle-period** settings. TCP begins to send the keepalive packet at an interval of 75 seconds if it does not receive any packet from the peer end in 900 seconds. The TCP connection is considered invalid and then disconnected automatically if the device sends the keepalive packet for six consecutive times without receiving any TCP packet from the peer end. This command applies to both IPv4 and IPv6 TCP.

**Configuration Examples** The following example enables the TCP keepalive function on the device and sets the **idle-period** and **interval** to180 and 60 respectively. If the device sends the keepalive packet for four consecutive times without receiving any TCP packet from the peer end, the TCP connection is considered invalid.

```
Ruijie(config)# ip tcp keepalive interval 60 times 4 idle-period 180
```

**Related Commands**

| Command | Description |
|---|---|
| N/A | N/A |

**Platform Description** When you run the RGOS 10.x command **service tcp-keepalives-in** or **service tcp-keepalives-out**, it is converted to this command automatically in RGOS 11.0.

## 7.3 ip tcp mss

Use this command to set the upper limit of the MSS value. Use the **no** form of this command to restore the default setting.

**ip tcp mss** *max-segment-size*

**no ip tcp mss**

**Parameter Description**

| Parameter | Description |
|---|---|
| *max-segment-size* | Upper limit of the MSS value in the range from 68 to 10000 bytes |

**Defaults** N/A

**Command Mode** Global configuration mode

**Usage Guide** This command is used to limit the maximum value of MSS for the TCP connection to be created. The negotiated MSS cannot exceed the configured value. You can use this command to reduce the maximum value of MSS. However, this configuration is not needed in general.

**Configuration Examples** The following example sets the upper limit of the MSS value to 1300 bytes.

```
Ruijie(config)# ip tcp mss 1300
```

**Related Commands**

| Command | Description |
|---|---|
| N/A | N/A |

**Platform Description** In versions 10.X, this command only applies to IPv4 TCP. In version 11.0 or later, this command applies to both IPv4 and IPv6 TCP.

## 7.4 ip tcp path-mtu-discovery

Use this command to enable Path Maximum Transmission Unit (PMTU) discovery function for TCP in global configuration mode. Use the **no** form of this command to restore the default setting.

**ip tcp path-mtu-discovery** [ **age-timer** *minutes* **| age-timer infinite** ]

**no ip tcp path-mtu-discovery**

**Parameter Description**

| Parameter | Description |
|---|---|
| **age-timer** *minutes* | The time interval for further discovery after discovering PMTU. Its value ranges from 10 to 30 minutes. The default value is 10. |
| **age-timer infinite** | No further discovery after discovering PMTU |

**Defaults** This function is disabled by default.

**Command Mode** Global configuration mode

**Usage Guide** Based on RFC1191, the TCP path MTU function improves the network bandwidth utilization and data transmission when the user uses TCP to transmit the data in batch.
Enabling or disabling this function takes no effect for existent TCP connections and is only effective for TCP connections to be created. This command applies to only IPv4 TCP. This function is enabled for IPv6 TCP constantly and cannot be disabled.
According to RFC1191, after discovering the PMTU, the TCP uses a greater MSS to detect the new PMTU at a certain interval, which is specified by the parameter **age-timer**. If the PMTU discovered is smaller than the MSS negotiated between two ends of the TCP connection, the device will be trying to discover the greater PMTU at the specified interval untill the PMTU value reaches the MSS or the user stops this timer. Use the parameter **age-timer infinite** to stop this timer.

**Configuration Examples** The following example enables PMTU discovery.

```
Ruijie(config)# ip tcp path-mtu-discovery
```

**Related Commands**

| Command | Description |
| --- | --- |
| **show tcp pmtu** | Shows the PMTU value for the TCP connection. |

**Platform Description** In versions 10.X, this command applies to both IPv4 and IPv6 TCP. In version 11.0 or later, this command only applies to IPv4 TCP, and PMTU discovery function is always enabled and cannot be disabled.

## 7.5 ip tcp send-reset

Use this command to enable the device to send the reset packet when receiving the TCP port unreachable packet. Use the **no** form of this command to disable this function,
**ip tcp send-reset**
**no ip tcp send-reset**

**Parameter Description**

| Parameter | Description |
| --- | --- |
| N/A | N/A |

**Defaults** This function is enabled by default.

**Command Mode** Global configuration mode

**Usage Guide** In general, when dispatching the TCP packet, the TCP module replies a reset packet automatically to disconnect the TCP connection with the peer end if the TCP connection that this packet belongs to is not found, However, flooding TCP port unreachable packets pose an attack threat to the device, This command can be used to disable the device from sending the reset packet when receiving the TCP port unreachable packet. This command applies to both IPv4 and IPv6 TCP.

**Configuration Examples** The following example disables the device from sending the reset packet when receiving the TCP port unreachable packet.

```
Ruijie(config)# no ip tcp send-reset
```

**Related Commands**

| Command | Description |
| --- | --- |
| N/A | N/A |

**Platform Description** The **ip tcp not-send-rst** command in RGOS 10.x is compatible in RGOS 11.0. When you run this command, it is converted to the **no ip tcp send-reset** command automatically.

## 7.6 ip tcp synwait-time

Use this command to set the timeout value for SYN packets (the maximum time from SYN transmission to successful three-way handshake). Use the **no** form of this command to restore the default setting.

**ip tcp synwait-time** *seconds*

**no ip tcp synwait-time** *seconds*

**Parameter Description**

| Parameter | Description |
| --- | --- |
| *seconds* | Timeout value for SYN packets in the range from 5 to 300 in the unit of seconds. |

**Defaults** The default is 20.

**Command Mode** Global configuration mode

**Usage Guide** If there is an SYN attack in the network, reducing the SYN timeout value can prevent resource consumption, but it takes no effect for successive SYN attacks. When the device actively requests a connection with an external device, reducing the SYN timeout value can shorten the time for the user to wait, such as telnet login. For poor network conditions, the timeout value can be increased properly. This command applies to both IPv4 and IPv6 TCP.

**Configuration Examples** The following example set the timeout value for SYN packets to 10 seconds.

```
Ruijie(config)# ip tcp syntime-out 10
```

**Related Commands**

| Command | Description |
| --- | --- |
| N/A | N/A |

**Platform Description** In versions 10.X, this command only applies to IPv4 TCP. In version 11.0 or later, this command applies to both IPv4 and IPv6 TCP.

## 7.7 ip tcp window-size

Use this command to change the size of receiving buffer and sending buffer for TCP connections. Use the **no** form of this command to restore the default setting.

**ip tcp window-size** *size*

**no ip tcp window-size**

**Parameter Description**

| Parameter | Description |
| --- | --- |
| *size* | Size of receiving buffer and sending buffer for TCP connections in the range from 128 to 65535 << 14 bytes. |

**Defaults** The default is 65535.

**Command Mode** Global configuration mode

**Usage Guide** The TCP receiving buffer is used to buffer the data received from the peer end. These data will be subsequently read by application programs. Generally, the window size of TCP packets implies the size of free space in the receiving buffer. For connections involving a large bandwidth and mass data, increasing the size of receiving buffer will remarkably improve TCP transmission performance.

When the window size exceeds 65,535 bytes, the size of receiving buffer is increased automatically.

**Configuration Examples** The following example sets the TCP window size to 16,386 bytes.

```
Ruijie(config)# ip tcp window-size 16386
```

**Related Commands**

| Command | Description |
| --- | --- |
| N/A | N/A |

**Platform Description** In versions 10.X, this command only applies to IPv4 TCP. In version 11.0 or later, this command applies to both IPv4 and IPv6 TCP.

## 7.8 ipv6 tcp adjust-mss

Use this command to set the MSS option value of the TCPv6 SYN packet. Use the **no** form of this command to restore the default setting.

**ipv6 tcp adjust-mss** *max-segment-size*

**no ipv6 tcp adjust-mss**

**Parameter Description**

| Parameter | Description |
|---|---|
| *max-segment-size* | The maximum segment size (MSS), in the range from 1220 to 1440 in the unit of bytes. |

**Defaults** The MSS option value of the TCPv6 SYN packet is not changed by default.

**Command Mode** Interface configuration mode

**Usage Guide** TCP negotiates MSS at 3-way handshake. If the IPv6 MTU of one link for TCPv6 packet transmission is too small and packet segmentation is not allowed during forwarding, the router changes the MSS option value of the TCPv6 SYN packet to prevent transmitting the TCPv6 packet surpassing MTU.

This configuration is not applicable to established TCPv6 connections.

**Configuration Examples** The following example sets the MSS option value of the TCPv6 SYN packet to 1300 bytes on port GigabitEthernet 0/0.

```
Ruijie(config-if-GigabitEthernet 0/0)# ipv6 tcp adjust-mss 1300
```

**Related Commands**

| Command | Description |
|---|---|
| N/A | N/A |

**Platform Description** N/A

## 7.9 service tcp-keepalives-in

Use this command to enable the keepalive function for the TCP server. Use the no form of this command to restore the default setting.

**service tcp-keepalives-in** [ *interval* ] [ **garbage** ]

**no service tcp-keepalives-in**

**Parameter Description**

| Parameter | Description |
|---|---|
| *interval* | The interval of sending keepalive packets, in the range from 1 to |

| | |
|---|---|
| | 65535 in the unit of seconds. The default is 60. |
| **garbage** | The keepalive packet contains one-byte invalid data. The invalid data is not contained by default. |

**Defaults** This function is disabled by default.

**Command Mode** Global configuration mode

**Usage Guide** The keepalive function enables the TCP server to detect whether the client is operating properly. If the TCP server sends the keepalive packet for four consecutive times without receiving any TCP packet from the client, the TCP connection is considered invalid and then is disconnected automatically.

**Configuration Examples** The following example enables the keepalive function for the TCP server and sets the interval of sending the keepalive packet to 10 seconds. The keepalive packet contains one-byte invalid data.

```
Ruijie(config)# service tcp-keepalives-in 10 garbage
```

**Related Commands**

| Command | Description |
|---|---|
| N/A | N/A |

**Platform Description** When you run this RGOS 10.x command, it is converted to the **ip tcp keepalive** command automatically in RGOS 11.0.

## 7.10 service tcp-keepalives-out

Use this command to enable the keepalive function for the TCP client.

**service tcp-keepalives-out** [ *interval* ] [ **garbage** ]

**Parameter Description**

| Parameter | Description |
|---|---|
| *interval* | The interval of sending keepalive packets, in the range from 1 to 65535 in the unit of seconds. The default is 60. |
| **garbage** | The keepalive packet contains one-byte invalid data. The invalid data is not contained by default. |

**Defaults** This function is disabled by default.

**Command Mode** Global configuration mode

**Usage Guide** The keepalive function enables the TCP client to detect whether the server is operating properly.

If the TCP client sends the keepalive packet for four consecutive times without receiving any TCP packet from the server, the TCP connection is considered invalid and then is disconnected automatically.

**Configuration Examples** The following example enables the keepalive function for the TCP client and sets the interval of sending the keepalive packet to 10 seconds. The keepalive packet contains one-byte invalid data

```
Ruijie(config)# service tcp-keepalives-out 10 garbage
```

**Related Commands**

| Command | Description |
| --- | --- |
| N/A | N/A |

**Platform Description** When you run this RGOS 10.x command, it is converted to the **ip tcp keepalive** command automatically in RGOS 11.0.

## 7.11 show ipv6 tcp connect

Use this command to display the current IPv6 TCP connection information.
**show ipv6 tcp connect** [ **local-ipv6** *X:X:X:X::X* ] [ **local-port** *num* ] [ **peer-ipv6** *X:X:X:X::X* ] [ **peer-port** *num* ]
Use this command to display the current IPv6 TCP connection statistics.
**show ipv6 tcp connect statistics**

**Parameter Description**

| Parameter | Description |
| --- | --- |
| **local-ipv6** *X:X:X:X::X* | Local IPv6 address |
| **local-port** *num* | Local port |
| **peer-ipv6** *X:X:X:X::X* | Peer IPv6 address |
| **peer-port** *num* | Peer port |
| **statistics** | Displays IPv6 TCP connection statistics |

**Defaults** N/A

**Command Mode** Privileged EXEC mode

**Usage Guide** N/A

**Configuration Examples** The following example displays the current IPv6 TCP connection information.

```
Ruijie#show ipv6 tcp connect
Number Local Address    Foreign Address        State       Process name
1     :::22           :::0                LISTEN      rg-sshd
```

```
2     :::23           :::0                 LISTEN      rg-telnetd
3     1000::1:23       1000::2:64201          ESTABLISHED  rg-telnetd
```

The following example displays the current IPv6 TCP connection statistics.

```
Ruijie#show ipv6 tcp connect statistics
State         Count
-----      -----
ESTABLISHED 1
SYN_SENT     0
SYN_RECV     0
FIN_WAIT1    0
FIN_WAIT2    0
TIME_WAIT    0
CLOSED        0
CLOSE_WAIT   0
LAST_ACK     0
LISTEN        1
CLOSING       0
Total: 2
```

**Related Commands**

| Command | Description |
|---|---|
| N/A | N/A |

**Platform Description** N/A

## 7.12 show ipv6 tcp pmtu

Use this command to display information about IPv6 TCP PMTU.

**show ipv6 tcp pmtu** [ **local-ipv6** *X:X:X:X::X* ] [ **local-port** *num* ] [ **peer-ipv6** *X:X:X:X::X* ] [ **peer-port** *num* ]

**Parameter Description**

| Parameter | Description |
|---|---|
| **local-ipv6** *X:X:X:X::X* | Local IPv6 address |
| **local-port** *num* | Local port |
| **peer-ipv6** *X:X:X:X::X* | Peer IPv6 address |
| **peer-port** *num* | Peer port |

**Defaults** N/A

**Command Mode** Privileged EXEC mode

**Usage Guide** N/A

**Configuration Examples** The following example information about IPv6 TCP PMTU.

```
Ruijie# show ipv6 tcp pmtu
Number  Local Address          Foreign Address       PMTU
1       1000::1:23             1000::2.13560
```

| Field | Description |
|---|---|
| Number | Number |
| Local Address | Local address and port number. The number after the last colon is the port number. |
| Foreign Address | Remote address and port number. The number after the last colon is the port number. |
| PMTU | Path MTU. |

**Related Commands**

| Command | Description |
|---|---|
| N/A | N/A |

**Platform Description** N/A

## 7.13 show ipv6 tcp port

Use this command to display the current IPv6 TCP port status.

**show ipv6 tcp port** [ *num* ]

**Parameter Description**

| Parameter | Description |
|---|---|
| *num* | Port number |

**Defaults** N/A

**Command Mode** Privileged EXEC mode

**Usage Guide** N/A

**Configuration Examples** The following example displays the current IPv6 TCP port status.

```
Ruijie#show ipv6 tcp port
TCP connections on port 23:
Number  Local Address Foreign Address   State
```

```
1      1000::1:23    1000::2:64571     ESTABLISHED
Total: 1

TCP connections on port 2650:
Number  Local Address Foreign Address   State
Total: 0
```

| Field | Description |
|---|---|
| Number | Number |
| Local Address | Local address and port number. |
| Foreign Address | Remote address and port number. |
| State | Current status of the TCP connection. There are eleven possible states:<br>CLOSED: The connection has been closed.<br>LISTEN: Listening state<br>SYNSENT: In the three-way handshake phase when the SYN packet has been sent out.<br>SYNRCVD: In the three-way handshake phase when the SYN packet has been received.<br>ESTABLISHED: The connection has been established.<br>FINWAIT1: The local end has sent the FIN packet.<br>FINWAIT2: The FIN packet sent by the local end has been acknowledged.<br>CLOSEWAIT: The local end has received the FIN packet from the peer end.<br>LASTACK: The local end has received the FIN packet from the peer end, and then sent its own FIN packet.<br>CLOSING: The local end has sent the FIN packet from the peer end, and received the FIN packet from the peer end before the ACK packet for the peer end to respond with this FIN packet is received.<br>TIMEWAIT: The FIN packet sent by the local end has been acknowledged, and the local end has also acknowledged the FIN packet. |
| Process Name | Process name |

**Related Commands**

| Command | Description |
|---|---|
| N/A | N/A |

**Platform Description** N/A

# 7.14 show tcp connect

Use this command to display basic information about the current TCP connections.

**show tcp connect** [ **local-ip** *a.b.c.d* ] [ **local-port** *num* ] [ **peer-ip** *a.b.c.d* ] [ **peer-port** *num* ]

Use this command to display the current IPv4 TCP connection statistics.

**show tcp connect statistics**

**Parameter Description**

| Parameter | Description |
|---|---|
| **local-ip** *a.b.c.d* | Local IP address. |
| **local-port** *num* | Local port. |
| **peer-ip** *a.b.c.d* | Peer IP address. |
| **peer-port** *num* | Peer port. |
| **statistics** | Displays IPv4 TCP connection statistics. |

**Defaults** N/A

**Command Mode** Privileged EXEC mode

**Usage Guide** N/A

**Configuration Examples** The following example displays the current IPv4 TCP connection information.

```
Ruijie#show tcp connect
Number Local Address    Foreign Address         State      Process name
1      0.0.0.0:22       0.0.0.0:0              LISTEN     rg-sshd
2      0.0.0.0:23       0.0.0.0:0              LISTEN     rg-telnetd
3      1.1.1.1:23       1.1.1.2:64201           ESTABLISHED rg-telnetd
```

| Field | Description |
|---|---|
| Number | Sequence number. |
| Local Address | The Local address and port number. The number after the last “.” is the port number. For example, in “2002::2.23” and “192.168.195.212.23” , “23” is the port number. |
| Foreign Address | The remote address and port number. The number after the last “.” is the port number. For example, in “2002::2.23” and “192.168.195.212.23” , “23” is the port number. |
| State | Current status of the TCP connection. There are eleven possible states:<br>CLOSED: The connection has been closed.<br>LISTEN: Listening state<br>SYNSENT: In the three-way handshake phase when the SYN packet has been sent out.<br>SYNRCVD: In the three-way handshake phase when the SYN |

| | |
|---|---|
| | packet has been received.<br>ESTABLISHED: The connection has been established.<br>FINWAIT1: The local end has sent the FIN packet.<br>FINWAIT2: The FIN packet sent by the local end has been acknowledged.<br>CLOSEWAIT: The local end has received the FIN packet from the peer end.<br>LASTACK: The local end has received the FIN packet from the peer end, and then sent its own FIN packet.<br>CLOSING: The local end has sent the FIN packet from the peer end, and received the FIN packet from the peer end before the ACK packet for the peer end to respond with this FIN packet is received.<br>TIMEWAIT: The FIN packet sent by the local end has been acknowledged, and the local end has also acknowledged the FIN packet. |
| Process name | Process name. |

The following example displays the current IPv4 TCP connection statistics.

```
Ruijie#show tcp connect statistics
State         Count
-----      -----
ESTABLISHED 1
SYN_SENT     0
SYN_RECV     0
FIN_WAIT1    0
FIN_WAIT2    0
TIME_WAIT    0
CLOSED        0
CLOSE_WAIT   0
LAST_ACK     0
LISTEN        1
CLOSING       0
Total: 2
```

**Related Commands**

| Command | Description |
|---|---|
| N/A | N/A |

**Platform Description** N/A

# 7.15 show tcp pmtu

Use this command to display information about TCP PMTU.

**show tcp pmtu** [ **local-ip** *a.b.c.d* ] [ **local-port** *num* ] [ **peer-ip** *a.b.c.d* ] [ **peer-port** *num* ]

**Parameter Description**

| Parameter | Description |
|---|---|
| **local-ip** *a.b.c.d* | Local IP address. |
| **local-port** *num* | Local port. |
| **peer-ip** *a.b.c.d* | Peer IP address. |
| **peer-port** *num* | Peer port. |

**Defaults** N/A

**Command Mode** Privileged EXEC mode

**Usage Guide** N/A

**Configuration Examples** The following example displays PMTU of IPv4 TCP connection.

```
Ruijie# show tcp pmtu
Number  Local Address          Foreign Address       PMTU
1      192.168.195.212.23     192.168.195.112.13560  1440
```

| Field | Description |
|---|---|
| Number | Sequence number. |
| Local Address | The local address and the port number. The number after the last “.” is the port number. For example, in “2002::2.23” and “192.168.195.212.23” , “23” is the port number. |
| Foreign Address | The remote address and the port number. The number after the last "." is the port number. For example, in “2002::2.23” and “192.168.195.212.23” , “23” is the port number. |
| PMTU | PMTU value. |

**Related Commands**

| Command | Description |
|---|---|
| **ip tcp path-mtu-discovery** | Enables the TCP PMTU discovery function. |

**Platform Description** N/A

## 7.16 show tcp port

Use this command to display information about the current TCP port.

**show tcp port** [ *num* ]

**Parameter Description**

| Parameter | Description |
|---|---|
| *num* | Port number |

**Defaults** N/A

**Command Mode** Privileged EXEC mode

**Usage Guide** N/A

**Configuration Examples** The following example displays the current IPv4 TCP port status.

```
Ruijie#show tcp port
TCP connections on port 23:
Number  Local Address Foreign Address    State
1      1.1.1.1:23    1.1.1.2:64571    ESTABLISHED
Total: 1

TCP connections on port 2650:
Number  Local Address Foreign Address    State
Total: 0
```

Tcpv6 listen on 23 have total 1 connections.

| Field | Description |
|---|---|
| Number | Port number |
| Local Address | Local address |
| Foreign Address | Remote address |
| State | Status of the current TCP connection. There are eleven possible states:<br>CLOSED: The connection has been closed.<br>LISTEN: Listening state<br>SYNSENT: In the three-way handshake phase when the SYN packet has been sent.<br>SYNRCVD: In the three-way handshake phase when the SYN packet has been received.<br>ESTABLISHED: The connection has been established.<br>FINWAIT1: The local end has sent the FIN packet.<br>FINWAIT2: The FIN packet sent by the local end has been |

| | |
|---|---|
| | acknowledged.<br>CLOSEWAIT: The local end has received the FIN packet from the peer end.<br>LASTACK: The local end has received the FIN packet from the peer end, and then sent its own FIN packet.<br>CLOSING: The local end has sent the FIN packet from the peer end, and received the FIN packet from the peer end before the ACK packet for the peer end to respond with this FIN packet is received.<br>TIMEWAIT: The FIN packet sent by the local end has been acknowledged, and the local end has also acknowledged the FIN packet. |

**Related Commands**

| Command | Description |
|---|---|
| N/A | N/A |

**Platform Description** N/A

# 8 IPv4/IPv6 REF Commands

## 8.1 clear ip ref packet statistics

Use this command to clear IPv4 Ruijie Express Forwarding (REF) packet statistics.

**clear ip ref packet statistics**

**Parameter Description**

| Parameter | Description |
|---|---|
| N/A | N/A |

**Defaults** N/A

**Command Mode** Privileged EXEC mode

**Usage Guide** N/A

**Configuration Examples** The following example clears IPv4 REF packet statistics.

```
Ruijie #clear ip ref packet statistics
```

**Related Commands**

| Command | Description |
|---|---|
| N/A | N/A |

**Platform Description** N/A

## 8.2 clear ipv6 ref packet statistics

Use this command to clear IPv6 REF packet statistics.

**clear ipv6 ref packet statistics**

**Parameter Description**

| Parameter | Description |
|---|---|
| N/A | N/A |

**Defaults** N/A

**Command Mode** Privileged EXEC mode

**Usage Guide** N/A

**Configuration Examples** The following example clears IPv6 REF packet statistics.

```
Ruijie #clear ipv6 ref packet statistics
```

**Related Commands**

| Command | Description |
| --- | --- |
| N/A | N/A |

**Platform Description** N/A

## 8.3 ip ref load-sharing original

Use this command to configure the algorithm that is used for load balancing during forwarding based on the source and destination IPv4 addresses. Use the **no** form of this command to restore the default setting.

**ip ref load-sharing original**

**no ip ref load-sharing original**

**Parameter Description**

| Parameter | Description |
| --- | --- |
| N/A | N/A |

**Defaults** The default algorithm is based on the destination IPv4 address.

**Command Mode** Global configuration mode

**Usage Guide** The REF is responsible for data forwarding and supports two load balancing algorithms. One is based on destination IP addresses and the other is based on the source and destination IP addresses. When IP packets are forwarded on multiple paths, for example, when load balancing based on destination IP addresses is configured, the REF forwards packets based on a path matching the destination IP address of packets. By default, load balancing based on destination IP addresses is used.

**Configuration Examples** The following example configures the load balancing algorithm based on source and destination IP addresses.

```
Ruijie(config)# ip ref load-sharing original
```

The following example configures the load balancing algorithm based on destination IP addresses of packets.

```
Ruijie(config)# no ip ref load-sharing original
```

**Related Commands**

| Command | Description |
| --- | --- |
| N/A | N/A |

**Platform Description** N/A

## 8.4 ipv6 ref load-sharing original

Use this command to configure the algorithm that is used for load balancing during forwarding based on the source and destination IPv6 addresses. Use the **no** form of this command to restore the default setting.

**ipv6 ref load-sharing original**

**no ipv6 ref load-sharing original**

**Parameter Description**

| Parameter | Description |
|---|---|
| N/A | N/A |

**Defaults** The default algorithm is based on the destination IPv6 address.

**Command Mode** Global configuration mode

**Usage Guide** N/A

**Configuration Examples** The following example restores the algorithm that is used for load balancing during forwarding to the default setting.

```
Ruijie(config)#no ipv6 ref load-sharing original
```

**Related Commands**

| Command | Description |
|---|---|
| N/A | N/A |

**Platform Description** N/A.

## 8.5 show ip ref adjacency

Use this command to display the information about the specified adjacent node or all adjacent nodes.

**show ip ref adjacency** [ **glean** | **local** | *ip-address* | **interface** *interface_type interface_number* | **discard** | **statistics** ]

**Parameter Description**

| Parameter | Description |
|---|---|
| **glean** | Aggregate adjacent node, which is used for a direct route |
| **local** | Local adjacent node, which is used by the local host |
| *ip* | Next-hop IP address |
| *interface_type* | Interface type |
| *interface_number* | Interface number |

| | |
|---|---|
| **discard** | Displays discarded adjacent nodes. |
| **statistics** | Statistics |

**Defaults** N/A

**Command Mode** Privileged EXEC mode

**Usage Guide** This command can be used to display the information about the adjacent node table in the current REF module. By specifying parameters, the information about the aggregate adjacent node, local adjacent node, adjacent node of the specified IP address, adjacent node associated with the specified interface, and all adjacent nodes can be displayed.

**Configuration Examples** The following example displays the information about all adjacent nodes in the adjacent node table.

```
Ruijie#show ip ref adjacency
id state     type    rfct chg  ip          interface        linklayer(header
data)
1  unresolved mcast   1    0   224.0.0.0
9  resolved   forward 1    0   192.168.50.78   GigabitEthernet 0/0  00 25 64 C5
9D 6A 00 D0 F8 98 76 54 08 00
7  resolved   forward 1    0   192.168.50.200  GigabitEthernet 0/0  00 04 5F 87
69 66 00 D0 F8 98 76 54 08 00
6  unresolved  glean  1    0   0.0.0.0        GigabitEthernet 0/0
4  unresolved  local  3    0   0.0.0.0        Local 1
```

Description of fields:

| Field | Description |
|---|---|
| id | Adjacent node ID |
| state | Adjacent node state:<br>Unresolved<br>Resolved |
| type | Adjacent node type<br>Local: local adjacency<br>Forward: forward adjacency<br>Discard: discard adjacency<br>Glean: glean adjacency<br>Mcast: multicast adjacency |
| rfct | Reference count of the adjacent node |
| chg | Whether the adjacent node is on the changing link. |
| ip | IP address of the adjacent node |
| interface | Interface |
| linklayer | Layer 2 head |

| Related Commands | Command | Description |
|---|---|---|
| | **show ip ref route** | Displays all route information in the current REF module. |

**Platform Description** N/A

## 8.6 show ip ref exact-route

This command is used to display the IPv4 REF exact route.

**show ip ref exact-rout** *source_ipaddress dest_ipaddress*

| Parameter Description | Parameter | Description |
|---|---|---|
| | *source_ipaddress* | Source IP address of the packet |
| | *dest_ipaddress* | Destination IP address of the packet |

**Defaults** N/A

**Command Mode** Privileged EXEC mode

**Usage Guide** This command is used to specify the source and the destination IP address of the IP packets, and to display the path of forwarding the current packet with REF

**Configuration Examples** The following example displays the IPv4 REF exact route from 192.168.217.74 to 192.168.13.1.

```
Ruijie# show ip ref exact-route 192.168.217.74 192.168.13.1
192.168.217.74  --> 192.168.13.1 (vrf index:0):
id state   type   rfct chg  ip          interface        linklayer(header
data)
9  resolved forward 1    0   192.168.17.1  GigabitEthernet 0/0 00 25 64 C5 9D
6A 00 D0 F8 98 76 54 08 00
```

Description of fields:

| Field | Description |
|---|---|
| id | Adjacency ID |
| state | Adjacency state:<br>Unresolved<br>Resolved |

| | |
|---|---|
| type | Adjacency type<br>Local: local adjacency<br>Forward: forward adjacency<br>Discard: discard adjacency<br>Glean: glean adjacency<br>Mcast: multicast adjacency |
| rfct | Reference count of the adjacency |
| chg | Whether the adjacency is on the changing link. |
| ip | Adjacency IP address |
| interface | Interface |
| linklayer | Layer 2 head |

**Related Commands**

| Command | Description |
|---|---|
| **show ip ref route** | Displays all routing information in the current REF module. |

**Platform Description** N/A

## 8.7 show ip ref packet statistics

Use this command to display IPv4 REF packet statistics.

**show ip ref packet statistics**

**Parameter Description**

| Parameter | Description |
|---|---|
| N/A | N/A |

**Defaults** N/A

**Command Mode** Privileged EXEC mode

**Usage Guide** N/A

**Configuration Examples** The following example displays IPv4 REF packet statistics.

```
Ruijie #show ip ref pkt-statistic
ref packet statistic:
   bad head       : 0
   lookup fib fail : 0
   local adj      : 0
   glean adj      : 0
   forward        : 0
```

```
redirect       : 0
punt adj       : 0
outif not in ef : 0
ttl expiration  : 0
no ip routing   : 0
```

| Field | Description |
|---|---|
| total recved | Number of total packets received by REF |
| bad head | Number of the packets with false header |
| lookup fib fail | Number of the packets with failed REF routing |
| drop adj | Number of the packets matching the dropped adjacency |
| local adj | Number of the packets matching the local adjacency |
| glean adj | Number of the packets matching the gleaned adjacency |
| forward | Number of the packets matching the forwarded adjacency |
| no ip routing | Number of the packets not allowed to be forwarded and sent to local. |

**Related Commands**

| Command | Description |
|---|---|
| N/A | N/A |

**Platform Description** N/A

## 8.8 show ip ref resolve-list

Use this command to display the IPv4 REF resolution information.

**show ip ref resolve-list**

**Parameter Description**

| Parameter | Description |
|---|---|
| N/A | N/A |

**Defaults** N/A

**Command Mode** Privileged EXEC mode

**Usage Guide** N/A

**Configuration Examples** The following example displays IPv4 REF resolution information.

```
Ruijie#show ip ref resolve-list
IP               res_state flags interface
1.1.1.1           unres    1     GigabitEthernet 0/0
```

| Field | Description |
|---|---|
| IP | IP address |
| res_state | unres: unresolved<br>res: resolved |
| flags | 0: related to adjacency<br>1: unrelated to adjacency |
| interface | Interface |

**Related Commands**

| Command | Description |
|---|---|
| N/A | N/A |

**Platform Description** N/A

## 8.9 show ip ref route

Use this command to display all the routing information in the IPv4 REF table.

**show ip ref route** [ **default** | *ip mask* | **statistics** ]

**Parameter Description**

| Parameter | Description |
|---|---|
| **default** | Specifies the default route. |
| *ip* | Specifies the destination IP address of the route |
| *mask* | Specifies the mask of the route. |
| **statistics** | Statistics |

**Defaults** N/A

**Command Mode** Privileged EXEC mode

**Usage Guide** This command is used to display the related routing information on the current REF table, and specify the default route and all the routing information matching IP/MASK.

**Configuration Examples** The following example displays all the routing information in the IPv4 REF table.

```
Ruijie#show ip ref route
Codes: * - default route
       # - zero route
```

```
ip     mask    weight  path-id     next-hop       interface
255.255.255.255 255.255.255.255 1  4   0.0.0.0    Local 0
224.0.0.0       240.0.0.0        1  1   224.0.0.0
224.0.0.0     255.255.255.0    1  4    0.0.0.0    Local 0
192.168.50.0  255.255.255.0     1  6   0.0.0.0 FastEthernet 0/0
192.168.50.255  255.255.255.255 1  2      0.0.0.0
192.168.50.200 255.255.255.255 1 7 192.168.50.200 FastEthernet 0/0
192.168.50.122  255.255.255.255 1 4 0.0.0.0        Local 0
192.168.50.78  255.255.255.255 1 9 192.168.50.78  FastEthernet 0/0
```

| Field | Description |
|---|---|
| ip | Destination IP address |
| mask | Mask |
| path-id | Adjacent identity |
| next-hop | Address of next hop |
| weight | Routing weight |
| interface | Egress |

**Related Commands**

| Command | Description |
|---|---|
| show ip ref exact-route | Displays the accurate REF forwarding path of an IP packet. |

**Platform Description** N/A

## 8.10 show ipv6 ref adjacency

Use this command to display the information about the IPv6 adjacent node.

**show ipv6 ref adjacency** [**glean** | **local** | *ipv6-address* | **interface** *interface_type interface_number* | **discard** | **statistics** ]

**Parameter Description**

| Parameter | Description |
|---|---|
| **glean** | Aggregate adjacent node, which is used for a direct route |
| **local** | Local adjacent node, which is used by the local host |
| *ipv6-address* | Next-hop IP address |
| *interface_type* | Interface type |
| *interface_number* | Interface number |
| **discard** | Displays discarded adjacent nodes. |
| **statistics** | Statistics |

**Defaults** N/A

**Command Mode** Privileged EXEC mode

**Usage Guide** This command can be used to display the information about the adjacent node table in the privileged EXEC mode and global configuration mode.

**Configuration Examples** The following example displays the information about the IPv6 adjacent node..

```
Ruijie#show ipv6 ref adjacency
id    state      type    rfct chg ip    interface           linklayer(header
data)
1     unresolved  glean   1    0   ::    GigabitEthernet 0/0
2     unresolved  local   2    0   ::1   Local 1
```

Description of fields:

| Field | Description |
|---|---|
| id | Adjacent node ID |
| state | Adjacent node state:<br>Unresolved<br>Resolved |
| type | Adjacent node type<br>Local: local adjacency<br>Forward: forward adjacency<br>Discard: discard adjacency<br>Glean: glean adjacency<br>Mcast: multicast adjacency |
| rfct | Reference count of the adjacent node |
| chg | Whether the adjacent node is on the changing link. |
| ip | IP address of the adjacent node |
| interface | Interface |
| linklayer | Layer 2 head |

**Related Commands**

| Command | Description |
|---|---|
| N/A | N/A |

**Platform Description** N/A

## 8.11 show ipv6 ref exact-route

This command is used to display the IPv6 REF exact route.

**show ipv6 ref exact-route** *source-ipv6-address destination-ipv6-address*

**Parameter Description**

| Parameter | Description |
| --- | --- |
| *source-ipv6-address* | Source IP address of the packet |
| *destination-ipv6-address* | Destination IP address of the packet |

**Defaults** N/A

**Command Mode** Privileged EXEC mode

**Usage Guide** N/A

**Configuration Examples** The following example displays the IPv4 REF exact route from 2001:db8:1::1 to 3001:db8:2::2.

```
Ruijie#show ipv6 exact-route 2001:db8:1::1 3001:db8:2::2
2001:db8:1::1 --> 3001:db8:2::2 (vrf index:0):
ID  state      type    rfct chg ip interface           linklayer(header data)
3   unresolve   glean   1    0   :: GigabitEthernet 0/0
```

Description of fields:

| Field | Description |
| --- | --- |
| id | Adjacent node ID |
| state | Adjacent node state:<br>Unresolved<br>Resolved |
| type | Adjacent node type<br>Local: local adjacency<br>Forward: forward adjacency<br>Discard: discard adjacency<br>Glean: glean adjacency<br>Mcast: multicast adjacency |
| rfct | Reference count of the adjacent node |
| chg | Whether the adjacent node is on the changing link. |
| ip | IP address of the adjacent node |
| interface | Interface |
| linklayer | Layer 2 head |

**Related Commands**

| Command | Description |
| --- | --- |
| N/A | N/A |

**Platform** N/A

**Description**

## 8.12 show ipv6 ref packet statistics

Use this command to display IPv6 REF packet statistics.

**show ipv6 ref packet statistics**

**Parameter Description**

| Parameter | Description |
|---|---|
| N/A | N/A |

**Defaults** N/A

**Command Mode** Privileged EXEC mode

**Usage Guide** N/A

**Configuration Examples** The following example displays IPv6 REF packet statistics.

```
Ruijie#show ipv6 ref packet statistics
ref packet statistic:
   bad head       : 0
   lookup fib fail : 0
   local adj      : 0
   glean adj      : 0
   forward        : 0
   redirect       : 0
   hop-limit expiration  : 0
   no ipv6 unicast-routing   : 0
```

| Field | Description |
|---|---|
| total recved | Number of total packets received by REF |
| bad head | Number of the packets with false header |
| lookup fib fail | Number of the packets with failed REF routing |
| drop adj | Number of the packets matching the dropped adjacency |
| local adj | Number of the packets matching the local adjacency |
| glean adj | Number of the packets matching the gleaned adjacency |
| forward | Number of the packets matching the forwarded adjacency |

| | |
|---|---|
| no ip routing | Number of the packets not allowed to be forwarded and sent to local. |

**Related Commands**

| Command | Description |
|---|---|
| N/A | N/A |

**Platform Description** N/A

## 8.13 show ipv6 ref resolve-list

This command is used to display the IPv6 REF resolution information.

**show ipv6 ref resolve-list**

**Parameter Description**

| Parameter | Description |
|---|---|
| N/A | N/A |

**Defaults** N/A

**Command Mode** Privileged EXEC mode

**Usage Guide** N/A

**Configuration Examples** The following example displays IPv6 REF resolution information.

```
Ruijie#show ipv6 ref resolve-list
IP              res_state flags interface
1000::1          unres    1     GigabitEthernet 0/0
```

| Field | Description |
|---|---|
| IP | IPv6 address |
| res_state | unres: unresolved<br>res: resolved |
| flags | 0: related to adjacency<br>1: unrelated to adjacency |
| interface | Interface |

**Related Commands**

| Command | Description |
|---|---|
| N/A | N/A |

**Platform Description** N/A

## 8.14 show ipv6 ref route

Use this command to display all the routing information in the IPv6 REF table.

**show ipv6 ref route** [ **default** | **statistics** | **prefix/len** ]

**Parameter Description**

| Parameter | Description |
|---|---|
| **default** | Specifies the default route. |
| **statistics** | Statistics |
| **prefix/len** | Displays the route with the specified prefix (X:X:X:X::X/<0-128>). |

**Defaults** N/A

**Command Mode** Privileged EXEC mode

**Usage Guide** The command can also be used to display information about the default route, the route with the specified prefix, and statistics of all types of routes.

**Configuration Examples** The following example displays all the routing information in the REF IPv6 table.

```
Ruijie#show ipv6 ref route
Codes: * - default route
 prefix/len                  weight path_id  next_hop interface
 2001:da8:ffe:2::/64           1       3      ::     GigabitEthernet 0/0
 2001:da8:ffe:2::3/128         1       2      ::1    Local 1
 fe80::/10                    1       6       ::    Null 0
 fe80::21a:a9ff:fe3b:fa41/128   1       2       ::1   Local 1
```

| Field | Description |
|---|---|
| prefix/len | IPv6 prefix and prefix length. |
| path-id | Adjacent identity |
| next-hop | Address of next hop |
| weight | Routing weight |
| interface | Interface |

**Related Commands**

| Command | Description |
| --- | --- |
| N/A | N/A |

**Platform Description** N/A

# 9 NAT Commands

## 9.1 address

Use this command to configure the address range of an empty NAT address pool.
Use the **no** form of this command to delete the address range of an address pool.
**address** *start-ip end-ip* [ **match interface** *interface* ]
**no address** *start-ip end-ip* [ **match interface** *interface*]
**address interface** *interface* [ **match interface** *interface* ]
**no address interface** *interface* [ **match interface** *interface*]

**Parameter Description**

| Parameter | Description |
|---|---|
| *start-ip* | Start IP address of an address block |
| *end-ip* | End IP address of an address block |
| **interface** *interface* | Sets the interface used when NAT has multiple outside interfaces. The addresses defined in a pool use interface addresses and are used when the interface addresses are unknown and will be negotiated.<br>Note that this parameter must be used with the **match interface** *interface* parameter, and the two interfaces must be consistent. Otherwise, NAT may fail. |
| **match interface** *interface* | Sets the interface used when NAT has multiple outside interfaces. When the router determines the egress of packets, NAT uses this egress to select an address that matches it from the pool. |

**Defaults** No address range is defined by default.

**Command Mode** NAT address pool configuration mode

**Usage Guide** If you need to define multiple address ranges for an address pool, first enter NAT address pool configuration mode, and then define the NAT address ranges. These commands are not supported on aggregate ports.

**Configuration Examples** The following example creates a mulnets address pool and defines two address blocks.

```
Ruijie(config)# ip nat pool mulnets netmask 255.255.255.0
Ruijie(config-nat)# address 172.16.10.1 172.16.10.254
Ruijie(config-nat)# address 192.168.100.1 192.168.100.50
```

**Related**

| Command | Description |
|---|---|

| Commands | ip nat pool | Defines the IP NAT address pool. |
|---|---|---|

**Platform Description** N/A

## 9.2 ip nat

Use this command to perform NAT on an interface.

Use the **no** form of this command to disable NAT on an interface.

**ip nat** { **inside** | **outside** }

**no ip nat** { **inside** | **outside** }

**Parameter Description**

| Parameter | Description |
|---|---|
| **inside** | Perfoms NAT on incoming packets. |
| **outside** | Performs NAT on outgoing packets. |

**Defaults** NAT is not enabledby default.

**Command Mode** Interface configuration mode

**Usage Guide** NAT is performed only when packets are routed between outside and inside interfaces and meet a certain rule. Therefore, at least an inside interface and an outside interface must be configured.

**Configuration Examples** The following example dynamically translates the internal host 192.168.12.0/24 to the network segment with the global address 200.168.12.0/28. NAT is not allowed for the hosts in other network segments of the internal network.

```
Ruijie#configure terminal
Ruijie(config)# interface GigabitEthernet 0/0
Ruijie(config-if-GigabitEthernet 0/0)# ip address 192.168.12.6 255.255.255.0
Ruijie(config-if-GigabitEthernet 0/0)# ip nat inside
Ruijie(config-if-GigabitEthernet 0/0)# exit
Ruijie(config)# interface GigabitEthernet 0/1
Ruijie(config-if-GigabitEthernet 0/1)# ip address 200.168.12.17
255.255.255.0
Ruijie(config-if-GigabitEthernet 0/1)# ip nat outside
Ruijie(config-if-GigabitEthernet 0/1)# exit
Ruijie(config)# ip nat pool net200 200.168.12.1 200.168.12.15 netmask
255.255.255.0
Ruijie(config)# ip nat inside source list 1 pool net200
Ruijie(config)# access-list 1 permit 192.168.12.0 0.0.0.255
```

**Related Commands**

| Command | Description |
|---|---|
| **clear ip nat translation** | Clears the NAT entry table. |
| **ip nat inside destination** | Enables NAT for the internal destination address. |
| **ip nat inside source** | Enables NAT for internal source addresses. |
| **ip nat outside source** | Enables NAT for external source addresses. |
| **ip nat pool** | Defines the IP NAT address pool. |
| **show ip nat translations** | Displays IP NAT entries. |

**Platform Description**

N/A

## 9.3 ip nat application

Use this command to implement special application of NAT.

Use the **no** form of this command to cancel this special application.

**ip nat application source list** *list-num* **destination** *dest-ip* { **dest-change** | **src-change** } *ip-addr*

**ip nat application source list** *list-num* **destination** { **tcp** | **udp** *dest-ip port-num*} { **dest-change** *ip-addr port-num* | **src-change** *ip-addr* }

**no ip nat application source list** *list-num* **destination** *dest-ip* { **dest-change** | **src-change** } *ip-addr*

**no ip nat application source list** *list-num* **destination** { **tcp** | **udp** *dest-ip port-num*} { **dest-change** *ip-addr port-num* | **src-change** *ip-addr* }

**Parameter Description**

| Parameter | Description |
|---|---|
| *list-num* | Access list of internal local addresses, that is, match criteria of the source addresses of packets |
| *dest-ip* | Internal global address match, that is, match criteria of the destination addresses of packets. NAT entries are created only when the destination IP address matches this address and the source IP address matches the previously defined access list. |
| **tcp** *dest-ip port-num* | Matches the internal global address and the destination port. NAT entries are created only when the destination address and port of the TCP packet match the criteria defined here and the source address matches the previously defined access list. |
| **udp** *dest-ip port-num* | Matches the internal global address and the destination port. NAT entries are created only when the destination address and port of the UDP packet match the criteria |

| | |
|---|---|
| | defined here and the source address matches the previously defined access list. |
| **dest-change** *ip-addr port-num* | Changes the destination address and port of the packet that meets criteria. |
| **src-change** *ip-addr* | Changes the source address of the packet that meets criteria. |

**Defaults** This rule is not defined by default.

**Command Mode** Global configuration mode

**Usage Guide** In some advanced applications of NAT, it is necessary to change the source or destination addresses of some particular IP packets. This command can be used to perform this operation. The following example uses this command to implement the domain name resolution relay service (DNS relay).

**Configuration Examples** The following example allows the host in the network segment 192.168.1.0 in the internal network to point the DNS server to the IP address 192.168.1.1 of the NAT inside interface. The NAT function of the router forwards the DNS request from the host in the internal network to the true DNS server 202.101.98.55, and forwards the DNS response packet to the host in the internal network. Implement this function with the **ip nat application** command. The semantics is: If there is a UDP packet whose source address meets the criteria of access-list 1, destination address is 192.168.1.1, and destination port is 53, and then change the destination address of this IP packet to 202.101.98.55 and the destination port to 53.

```
Ruijie#configure terminal
Ruijie(config)# interface GigabitEthernet 0/0
Ruijie(config-if-GigabitEthernet 0/0)# ip address 192.168.1.1 255.255.255.0
Ruijie(config-if-GigabitEthernet 0/0)# ip nat inside
Ruijie(config-if-GigabitEthernet 0/0)# exit
Ruijie(config)# interface GigabitEthernet 0/1
Ruijie(config-if-GigabitEthernet 0/1)# ip address 200.168.12.1 255.255.255.0
Ruijie(config-if-GigabitEthernet 0/1)# ip nat outside
Ruijie(config-if-GigabitEthernet 0/1.)# exit
Ruijie(config)# ip nat pool net200 200.168.12.2 200.168.12.10 netmask
255.255.255.0
Ruijie(config)# ip nat inside source list 1 pool net200
Ruijie(config)# access-list 1 permit 192.168.12.0 0.0.0.255
Ruijie(config)# ip nat application source list 1 destination udp 192.168.1.1
53 dest-change 202.101.98.55 53
Ruijie(config)# access-list 1 permit 192.168.1.0 0.0.0.255
```

**Related**

| Command | Description |
|---|---|

| Commands | | |
|---|---|---|
| | **address** | Defines the address block range of an address pool. |
| | **clear ip nat translation** | Clears the NAT entry table. |
| | **ip nat** | Specifies that NAT should be performed on the traffic that passes this interface. |
| | **ip nat inside destination** | Enables NAT for the internal destination address. |
| | **ip nat inside source** | Enables NAT for internal source addresses. |
| | **ip nat outside source** | Enables NAT for external source addresses. |
| | **show ip nat translations** | Displays IP NAT entries. |

**Platform Description** N/A

## 9.4 ip nat inside destination

Use this command to enable NAT for the internal destination address.

Use the **no** form of this command to disable NAT for the internal destination address.

**ip nat inside destination list** *access-list-number* **pool** *pool-name*

**no ip nat inside destination list** *access-list-number*

**Parameter Description**

| Parameter | Description |
|---|---|
| **list** *access-list-number* | Internal global addresses are defined in the access list. If the external network accesses the address in the access list, the internal global address will be translated into the internal local address defined in the pool. Note that here you should use the extended ACL in the range from 100 to 199 whose destination IP address is a virtual IP address. |
| **pool** *pool-name* | A space in the address pool that defines the internal local address. An internal local address will be assigned from this space during destination address translation. |

**Defaults** NAT for the internal source address is disabled by default.

**Command Mode** Global configuration mode

**Usage Guide** Translation of internal destination addresses can be performed to realize load balance of TCP traffic. When a host in the internal network is overloaded with TCP traffic, multiple hosts may be required to balance the load of TCP traffic. In this case, you can use NAT to realize load balance of TCP traffic. NAT will create a virtual host to provide the TCP service. This virtual host corresponds to multiple real internal hosts. Then, NAT polls and replaces the destination address, so as to distribute the load. However, no change is made to other IP traffic, unless NAT is configured otherwise.

When NAT is configured to realize TCP load balance, the address of the internal network can be either a valid global address or a private network address. However, the address of the virtual host must be a valid global address.

**Configuration Examples** The following example configures the internal network to provide a virtual host address 10.10.10.100 externally. The external network uses this address to access the WWW service. The hosts that provide services in the internal LAN are actually two hosts with the addresses 10.10.10.1 and 10.10.10.2. During NAT, load balance is realized in polling mode.

```
Ruijie#configure terminal
Ruijie(config)# interface GigabitEthernet 0/0
Ruijie(config-if-GigabitEthernet 0/0)# ip address 10.10.10.254 255.255.255.0
Ruijie(config-if-GigabitEthernet 0/0)# ip nat inside
Ruijie(config-if-GigabitEthernet 0/0)# exit
Ruijie(config)# interface GigabitEthernet 0/1
Ruijie(config-if-GigabitEthernet 0/1)# ip address 200.168.12.17
255.255.255.0
Ruijie(config-if-GigabitEthernet 0/1)# ip nat outside
Ruijie(config-if-GigabitEthernet 0/1)# exit
Ruijie(config)# ip nat pool net10 10.10.10.1 10.10.10.2 prefix-length 24 type
rotary
Ruijie(config)# ip nat inside destination list 100 pool net10
Ruijie(config)# access-list 100 permit ip any host 10.10.10.100
```

**Related Commands**

| Command | Description |
|---|---|
| **clear ip nat translation** | Clears the NAT entry table. |
| **ip nat** | Specifies that NAT should be performed on the traffic that passes this interface. |
| **ip nat inside source** | Enables NAT for internal source addresses. |
| **ip nat outside source** | Enable NAT for external source addresses. |
| **ip nat pool** | Defines the IP NAT address pool |
| **show ip nat translations** | Displays IP NAT entries. |

**Platform Description** N/A

## 9.5 ip nat inside source

Use this command to enable NAT for internal source addresses in interface configuration mode.
Use the **no** form of this command to disable static or dynamic NAT.

**ip nat inside source list** *access-list-number* { **interface** *interface-type interface-number* | **pool**

*pool-name* } [ **overload** ]

**ip nat inside source static** *local-ip global-ip* [ **match** *interface-type interface-number* | **netmask** *mask* ][ **permit-inside** ]

**ip nat inside source static** *local-ip* **interface** *interface-type interface-number* [**permit-inside**]

**ip nat inside source static** { **tcp** *local-ip local-port* | **udp** *local-ip local-port* } *global-ip global-port* [ **match** *interface-type interface-number* | **netmask** *mask* ] [ **permit-inside** ]

**ip nat inside source static** { **tcp** *local-ip local-port* | **udp** *local-ip local-port* } **interface** *interface-type interface-number global-port* [ **permit-inside** ]

**no ip nat inside source list** *access-list-number*

**no ip nat inside source static** *local-ip global-ip*

**no ip nat inside source static** *local-ip* **interface** *interface-type interface-number*

**no ip nat inside source static** { **tcp** *local-ip local-port* | **udp** *local-ip local-port* } *global-ip global-port*

**no ip nat inside source static** { **tcp** *local-ip local-port* | **udp** *local-ip local-port* } **interface** *interface-type interface-number global-port*

**Parameter Description**

| Parameter | Description |
|---|---|
| **list** *access-list-number* | Specifies the access list of local addresses. NAT entries will be created only for the traffic with the source address that matches this access list. |
| **interface** *interface-type interface-number* | Uses the global address of the outside interface to perform Network Address Port Translation (NAPT), also called extended NAT. |
| **pool** *pool-name* | Uses a global address in the address pool to perform NAT. |
| **overload** | (Optional) Every global address in the pool can be reused for translation, namely, NAPT. Currently, this parameter is not set, and global addresses are reusable. This parameter is added in order to be compatible with the command of Cisco. |
| **static** *local-ip global-ip* | Defines the simple static NAT. local-ip is a local address, and global-ip is a global address.<br>The **no** form of this command does not check the validity of global-ip. |
| **static** *protocol* | Defines the extended static NAT. protocol can be either TCP or UDP. |
| *local-port* | Service port number (TCP or UDP) of the local address. Each service typically corresponds to a service port. |
| *global-port* | Service port number of the global address. The external network accesses the services of hosts in the internal network through this port. This port number can be different from local-port. |
| **permit-inside** | Allows users in the internal network to access the |

| | |
|---|---|
| | host with the IP address indicated by local-ip through global-ip. This keyword appears only in the **ip nat inside source static** command is applicable only on routers. |
| **match** *interface-type interface-number* | Specifies the outside interface (used in smart DNS). |
| **netmask** *mask* | Network mask |

**Defaults** NAT for internal source addresses is disabled by default.

**Command Mode** Global configuration mode

**Usage Guide** When the IP address of the internal network is a private address and the internal network needs to communicate with the external network, NAT must be configured to translate the internal private IP address into the globally unique IP address.

If organizations, such as net bars or enterprises, access the network only for obtaining resources in the external network, such as browsing Web pages, receiving and sending emails, and downloading files, but not for providing network services for the external network, the IP address of the outside interface can be used directly as the global address and the address is translated in NAPT mode. If NAT is not configured, the internal network with the private address, even if physically interconnected with the external network, is unable to interwork with the external network, because the external network does not provide network routing for the private address.

Static NAT or NAPT should be configured for the internal hosts that provide services. To ensure continuous service provisioning, do not use the address of the outside interface to perform NAPT because this address is interconnected with ISP and is very likely to be translated. Generally, users in the internal network can access the services provided by these internal hosts simply by using the IP address of the internal network. However, some special application services can only be accessed by users in the internal network using the global IP address. In this case, you need to add the keyword **permit-inside** when configuring static NAT or static NAPT for internal source addresses. Moreover, it is advisable to run the **no ip redirects** command on the inside interface to prevent the inside interface from sending redirection packets.

**Configuration Examples** The following example dynamically translates the internal host 192.168.12.0/24 to the network segment with the global address 200.168.12.0/28. NAT is not allowed for the hosts in other network segments of the internal network.

```
Ruijie#configure terminal
Ruijie(config)# interface GigabitEthernet 0/0
Ruijie(config-if-GigabitEthernet 0/0)# ip address 192.168.12.6 255.255.255.0
Ruijie(config-if-GigabitEthernet 0/0)# ip nat inside
Ruijie(config-if-GigabitEthernet 0/0)# exit
Ruijie(config)# interface GigabitEthernet 0/1
Ruijie(config-if-GigabitEthernet 0/1)# ip address 200.168.12.17
255.255.255.0
```

```
Ruijie(config-if-GigabitEthernet 0/1)# ip nat outside
Ruijie(config-if-GigabitEthernet 0/1)# exit
Ruijie(config)# ip nat pool net200 200.168.12.1 200.168.12.15 prefix-length
28
Ruijie(config)# ip nat inside source list 1 pool net200
Ruijie(config)# access-list 1 permit 192.168.12.0 0.0.0.255
```

**Related Commands**

| Command | Description |
|---|---|
| **clear ip nat translation** | Clears the NAT entry table. |
| **ip nat** | Specifies that the NAT should be performed on the traffic that passes this interface. |
| **ip nat inside destination** | Enables NAT for the inside destination address. |
| **ip nat outside source** | Enable NAT for external source addresses. |
| **ip nat pool** | Defines the IP NAT address pool. |
| **show ip nat translations** | Displays IP NAT entries. |

**Platform Description** N/A

## 9.6 ip nat outside source

Use this command to enable NAT for the external source addresses.

Use the **no** form of this command is used to disable NAT for external source addresses.

**ip nat outside source list** *access-list-number* **pool** *pool-name*

**no ip nat outside source list** *access-list-number*

**ip nat outside source static** *global-ip local-ip*

**no ip nat outside source static** *global-ip local-ip*

**ip nat outside source static** *protocol global-ip global-port local-ip local-port*

**no ip nat outside source static** *protocol global-ip global-port local-ip local-port*

**Parameter Description**

| Parameter | Description |
|---|---|
| **list** *access-list-number* | Global address access list. NAT entries will be created only for the traffic with the source address that matches this access list. |
| **pool** *pool-name* | Uses a local address in the address pool to perform NAT. |
| **static** *global-ip local-ip* | Defines the simple static NAT. *local-ip* is a local address, and *global-ip* is a global address. |
| **static** *protocol* | Defines the extended static NAT. *protocol* can be either TCP or UDP. |
| *local-port* | Service port number (TCP or UDP) of the local address. Each service typically corresponds to a |

| | |
|---|---|
| | service port. This port number can be different from *global-port*. |
| *global-port* | Service port number of the global address |

**Defaults** NAT for external source addresses is disabled by default.

**Command Mode** Global configuration mode

**Usage Guide** NAT for external source addresses is mainly used for the overlapped address space. Two private networks to be interconnected are assigned with the same IP address, or a private network and a public network are assigned with the same global IP address, which is called address overlap. Two network hosts with the overlapped address cannot communicate with each other because they both determine that the remote host is located in the local network. Overlapped address NAT is configured to resolve the problem of communication between networks with the overlapped address. With overlapped address NAT configured, the external network host address behaves like another network host address in the internal network, and vice versa.

Configuration of overlapped address NAT includes two steps: 1) Configure the internal source address NAT; 2) Configure the external source address NAT. The external source address translation can be configured only when the address of the external network is overlapped with that of the internal network. The external source address translation can be configured as static NAT or dynamic NAT.

Address overlap is inevitable when a non-registered global IP address is assigned to connect to the Internet during internal network construction. Because the internal network generally uses the domain name to access the external network host, routers must support NAT for DNS packets.

**Configuration Examples** In the following example, the address of the internal network 92.168.12.0/24 is overlapped with that of the external network. After translation, the internal host can access the host in the network segment 92.168.12.0/24 in the external network through the network address 192.168.12.0/24.

```
Ruijie#configure terminal
Ruijie(config)# interface GigabitEthernet 0/0
Ruijie(config-if-GigabitEthernet 0/0)# ip address 192.168.12.55 255.255.255.0
Ruijie(config-if-GigabitEthernet 0/0)# ip nat inside
Ruijie(config-if-GigabitEthernet 0/0)# exit
Ruijie(config)# interface Serial 10/1
Ruijie(config-if-GigabitEthernet 0/1)# ip address 192.168.10.1 255.255.255.0
Ruijie(config-if-GigabitEthernet 0/1)# ip nat outside
Ruijie(config-if-GigabitEthernet 0/1)# encapsulation ppp
Ruijie(config-if-GigabitEthernet 0/1)# exit
Ruijie(config)#ip nat pool net200 200.168.12.1 200.168.12.15 prefix-length 28
Ruijie(config)#ip nat pool net192 192.168.12.1 192.168.12.254 prefix-length 24
Ruijie(config)#ip nat inside source list  1 pool net200
Ruijie(config)#ip nat outside source list 1 pool net192
```

```
Ruijie(config)#access-list 1 permit 92.168.12.0 0.0.0.255
Ruijie(config)#ip route 192.168.12.0 255.255.255.0 192.168.100.2
```

**Related Commands**

| Command | Description |
|---|---|
| **clear ip nat translation** | Clears the NAT entry table. |
| **ip nat** | Specifies that NAT should be performed for the traffic that passes this interface. |
| **ip nat inside destination** | Enables NAT for internal destination address. |
| **ip nat inside source** | Enables NAT for internal source address. |
| **ip nat pool** | Defines the IP NAT address pool. |
| **show ip nat translations** | Displays IP NAT entries. |

**Platform Description** N/A

## 9.7 ip nat pool

Use this command to define an address pool for NAT.

Use the **no** form of this command to delete the address pool.

**ip nat pool** *pool-name start-ip end-ip* { **netmask** *netmask* | **prefix-length** *prefix-length* } [ **type rotary** ]

**ip nat pool** *pool-name* { **netmask** *netmask* | **prefix-length** *prefix-length* } [ **type rotary** ]

**ip nat pool** *pool-name* { **netmask** *netmask* | **prefix-length** *prefix-length* } [ **type rotary** ] [ **hardware** ]

**no ip nat pool** *pool-name*

**Parameter Description**

| Parameter | Description |
|---|---|
| *pool-name* | Name of the NAT address pool |
| *start-ip* | Start IP address of the NAT address pool |
| *end-ip* | End IP address of the NAT address pool |
| **netmask** *netmask* | Net mask of an address in the NAT address pool |
| **type** | Type of the NAT address pool. **rotary** means round robin. That is, each address has the same probability of being assigned. The type is **rotary** no matter whether **rotary** is set. The **rotary** parameter is introduced in order to keep compatible with the command of Cisco. |

**Defaults** No address pool is defined by default.

**Command Mode** Global configuration mode

**Usage Guide** If multiple address blocks must be defined for an address pool, first create an empty address pool, and define the address range.

**Configuration Examples** The following example creates an address pool named **net192**, with the start address 192.168.12.1, end address 192.168.12.254, and a 24-bit net mask.

```
Ruijie#configure terminal
Ruijie(config)# ip nat pool net192 192.168.12.1 192.168.12.254 prefix-length 24
```

**Related Commands**

| Command | Description |
|---|---|
| **address** | Defines the address block range of an address pool. |
| **clear ip nat translation** | Clears the NAT entry table. |
| **ip nat** | Specifies that NAT should be performed for the traffic that passes this interface. |
| **ip nat inside destination** | Enables NAT for inside destination addresses. |
| **ip nat inside source** | Enables NAT for internal source addresses. |
| **ip nat outside source** | Enables NAT for external source addresses. |
| **show ip nat statistics** | Displays IP NAT statistics. |
| **show ip nat translations** | Displays IP NAT entries. |

**Platform Description** N/A

## 9.8 ip nat keepalive

Use this command to configure the interval of sending gratuitous ARP (GARP) packets with the local address.

**ip nat keepalive** [ *keealive_out* ]

**no ip nat keepalive**

**default ip nat keepalive**

**Parameter Description**

| Parameter | Description |
|---|---|
| *keealive_out* | Sending interval |

**Defaults** The interval of sending GARP packets with the local address is not configured by default.

**Command Mode** Global configuration mode

**Usage Guide** Some addresses in NAT rules should be taken as the local address. Sending GARP packets at

intervals avoids address conflicts.

**Configuration Examples**

The following example sets the interval of sending GARP packets with the local address to 10 seconds.

```
Ruijie#configure terminal
Ruijie(config)# ip nat keepalive 10
```

**Related Commands**

| Command | Description |
|---|---|
| N/A | N/A |

**Platform Description**

N/A

## 9.9 ip nat translation

Use this command to configure the NAT Application Layer Gateway (ALG).

**ip nat translation** { **dns** [ **ttl** *ttl_time* ] **| ftp** [ **port** *port_num* ] **| tftp | pptp | h323 | rtsp** }

**no ip nat translation** { **dns | ftp | tftp | pptp | h323 | rtsp** }

**Parameter Description**

| Parameter | Description |
|---|---|
| *ttl_time* | Defines the UDP TTL for DNS. The default is 0. |
| *port_num* | Defines the port for FTP. The default is 21. |

**Defaults**

All NAT ALGs are enabled by default.

**Command Mode**

Global configuration mode

**Usage Guide**

In NAT application, the IP addresses and ports of data packets are changed. However, the IP addresses and ports of certain special protocols are contained in the valid data of the application layer. To successfully perform NAT for such special protocols, the specific protocol gateway needs to be enabled.

**Configuration Examples**

The following example configures DNS TTL to 30 seconds.

```
Ruijie#configure terminal
Ruijie(config)# ip nat translation dns ttl 30
```

The following example configures Port 25 for FTP.

```
Ruijie#configure terminal
Ruijie(config)# ip nat translation ftp port 25
```

| Related Commands | Command | Description |
|---|---|---|
| | N/A | N/A |

**Platform Description** N/A

## 9.10 ip nat user-port-range user-type

Use this command to configure port-range-based QoS. Use the **no** form of this command to restore the default setting.

**ip nat user-port-range user-type {level0 | level1 | level2 | level3 | level4 | level5 | level6} port-range** *start-port end-port*

**no ip nat user-port-range user-type {level0 | level1 | level2 | level3 | level4 | level5 | level6}**

**Parameter Description**

| Parameter | Description |
|---|---|
| **user-type** | Indicates user type. Only one port range can be configured for each type. |
| **level0** | Indicates a user type. |
| **Level1** | Indicates a user type. |
| **Level2** | Indicates a user type. |
| **Level3** | Indicates a user type. |
| **Level4** | Indicates a user type. |
| **Level5** | Indicates a user type. |
| **Level6** | Indicates a user type. |
| **port-range** | Indicates port range. |
| *start-port* | Specifies the start port number, which ranges from 1 to 65535. |
| *end-port* | Specifies the end port number, which ranges from 1 to 65535. |

**Defaults** By default, this function is disabled.

**Command Mode** Global configuration mode

**Usage Guide** The start port number cannot be smaller than the end port number.
Port ranges of user types cannot overlap.

**Configuration Examples** The following example configures the port range for Level 1 from 100 to 200..

```
Ruijie#configure terminal
```

```
Ruijie(config)# ip nat user-port-range user-type level1 port-range 100 200
```

**Related Commands**

| Command | Description |
| --- | --- |
| N/A | N/A |

**Platform Description** This command is supported on Fat APs.

## 9.11 show ip nat translations

Use this command to display NAT translations.

**show ip nat translations** [*dev_id*] [*slot_id*] [ *acl_num* ] [ **icmp** | **tcp** | **udp** ] [ **verbose** ]

**Parameter Description**

| Parameter | Description |
| --- | --- |
| **icmp** | Displays NAT entries only for ICMP. |
| **tcp** | Displays NAT entries only for TCP. |
| **udp** | Displays NAT entries only for UDP. |
| **gre** | Displays NAT entries only for GRE. |
| *acl_num* | ACL number, which supports only the extended ACL to filter the displayed content. |
| **verbose** | Displays more detailed NAT entries. |
| *dev_id* | Device ID |
| *slot_id* | Slot ID of service card |

**Defaults** N/A

**Command Mode** Privileged EXEC mode

**Usage Guide** This command can be used to display the summary of IP NAT entries, such as protocols, internal global addresses and port numbers, internal local addresses and port numbers, external local addresses and port numbers, and external global addresses and port numbers. Used with the **verbose** parameter, it displays more detailed information, including the timeout period configured for each entry, remaining time for this entry, and flag of the entry.

**Configuration Examples** The following example displays NAT translations.

```
Ruijie# show ip nat translations verbose
timeout for NAT TCP flows: 86400
timeout for NAT TCP flows after a FIN or RST: 60
timeout for NAT TCP flows after a SYN : 60
timeout for NAT UDP flows: 300
```

```
timeout for NAT DNS flows: 60
timeout for NAT ICMP flows: 60
Pro Inside global     Inside local      Outside local     Outside global timeout vrf
tcp 192.168.5.103:1987 192.168.211.21 :1987 211.67.71.7    :80    211.67.71.7:80
timeout=85139 1
udp 192.168.5.103:1041 192.168.211.183:1041 202.101.98.55  :53 202.101.98.55:53
timeout=38 1
```

Field Description

| Field | Description |
|---|---|
| Pro | Protocol type. **udp** indicates the UDP translation entry. **tcp** indicates the TCP translation entry. **icmp** indicates the ICMP translation entry. |
| Inside global | Internal global address and port number |
| Inside local | Internal local address and port number |
| Outside local | External local address and port number |
| Outside global | External global address and port number |
| timeout | Time (in seconds) left before this NAT entry times out |

**Related Commands**

| Command | Description |
|---|---|
| **clear ip nat translation** | Clears the NAT entry table. |
| **ip nat** | Performs NAT on the traffic that passes this interface. |
| **ip nat inside destination** | Enables NAT for internal destination addresses. |
| **ip nat inside source** | Enables NAT for internal source addresses. |
| **ip nat outside source** | Enables NAT for external source addresses. |
| **ip nat pool** | Defines the IP NAT address pool. |
| **show ip nat translations** | Displays IP NAT entries. |

**Platform Description**

N/A

## 9.12 show ip nat user-port-range

Use this command to display NAT information based on port range.

**show ip nat user-port-range{configuration | users | all}**

**Parameter Description**

| Parameter | Description |
|---|---|
| **configuration** | Displays NAT configuration based on port range. |
| **users** | Displays user information based on port range. |
| **all** | Displays all NAT information based on port range, including |

| | |
|---|---|
| | configuration and user information. |

**Defaults** N/A

**Command Mode** Privileged EXEC mode

**Usage Guide** This command can be used to display NAT information based on port range.

**Configuration Examples** The following example displays all port-range-based NAT information.

```
Ruijie# show ip nat user-port-range all
User port range NAT configuration:
Index User Level Begin Port End Port
----- ---------- ---------- --------
1    level0    ----      ----
2    level1    100       200
3    level2    201       300
4    level3    301       400
5    level4    ----      ----
6    level5    ----      ----
7    level6    ----      ----

User port range NAT users:
Index User Level User IP
----- ---------- ---------------
1    level1    10.10.10.1
2    level2    10.10.10.2
3    level3    10.10.10.3
```

**Related Commands**

| Command | Description |
|---|---|
| N/A | N/A |

**Platform Description** N/A

# IP Routing Commands

# 1 NSM Commands

## 1.1 clear ip route

Use this command to clear the route cache.

**clear ip route** { ***** **|** *network* [ *netmask* ] | }

**Parameter Description**

| Parameter | Description |
|---|---|
| * | Clears all route cache. |
| *network* | Specifies the route cache of the network or subnet. |
| *netmask* | (Optional) Subnet mask. If no subnet mask is specified, the longest match principle is used when you match *network* with the route. The cache of the longest match is cleared. |

**Command Mode** Privileged EXEC mode

**Usage Guide** Clearing route cache clears the corresponding routes and triggers the routing protocol relearning. Please note that clearing all route cache leads to temporary network disconnection.

**Examples** The following example clears the cache of the route which is the longest match with IP address 192.168.12.0.

```
clear ip route 192.168.12.0
```

**Related Commands**

| Command | Description |
|---|---|
| N/A | N/A |

**Platform Description**

## 1.2 ip default-network

Use this command to configure the default network globally. Use the **no** or **default** form of this command to restore the default setting.

**ip default-network** *network*

**no ip default-network** *network*

**default ip default-network** *network*

**Parameter Description**

| Parameter | Description |
|---|---|
| *network* | Default network |

**Defaults** The default is 0.0.0.0/0.

**Command Mode** Global configuration mode

**Usage Guide**
The goal of this command is to generate the default route. The default network must be reachable in the routing table, but not the directly connected network.
The default network always starts with an asterisk (“*”), indicating that it is the candidate of the default route. If there is connected route and the route without the next hop in the default network, the default route must be a static route.

**Examples**
The following example sets 192.168.100.0 as the default network. Since the static route to the network is configured, the device will automatically generate a default route.

```
ip route 192.168.100.0 255.255.255.0 serial 0/1
ip default-network 192.168.100.0
```

The following example sets 200.200.200.0 as the default network. The route becomes the default one only when it is available in the routing table.

```
ip default-network 200.200.200.0
```

**Related Commands**

| Command | Description |
|---|---|
| **show ip route** | Displays the routing table. |

## 1.3 ip route

Use this command to configure a static route. Use the **no** or **default** form of this command to restore the default setting.
**ip route** *network net-mask* { *ip-address* | *interface* [ *ip-address* ] } [ *distance* ] [ **tag** *tag* ] [ **permanent** ] [ **weight** *number* ] [**description** *description-text*] [ **disabled** | **enabled**] [ **global** ]
**no ip route** *network net-mask* { *ip-address* | *interface* [ *ip-address* ] } [ *distance* ]
**no ip route all**
**default ip route** *network net-mask* { *ip-address* | *interface* [ *ip-address* ] } [ *distance* ]

**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 administrative distance of the static route |
| *tag* | (Optional) The tag of the static route |
| **permanent** | (Optional) Permanent route ID |
| **weight** *number* | (Optional) Indicates the weight of the static route. The |

| | |
|---|---|
| | weight is 1 by default. |
| **description** *description-text* | (Optional) Indicates the description of the static route. By default, no description is configured. *description-text* is a string of one to 60 characters. |
| **disabled/enabled** | (Optional) Indicates the enable flag of the static route. The flag is enabled by default. |
| **global** | (Optional) Indicates that the next hop belongs to a global VRF. By default, the VRF of the next hop is the same as the VRF specified by *vrf name*. |
| **arp** | (Optional) Indicates that the next hop belongs to a global VRF. By default, the VRF of the next hop is the same as the VRF specified by *vrf name*. |

**Defaults** No static route is configured by default.

**Command Mode** Global configuration mode

**Usage Guide**

The default administrative distance of the static route is 1. Setting the administrative distance allows the learnt dynamic route to overwrite the static route. Setting the administrative distance of the static route can enable route backup, which is called floating route in this case. For example, the administrative distance of the OSPF is 110. You can set its administrative distance to 125. Then the data can switch over the static route when the route running OSPF fails.

The default weight of the static route is 1. To view the static route of non default weight, execute the show ip route weight command. The parameter weight is used to enable WCMP. When there are load-balanced routes to the destination, the device assigns data flows by their weights. The higher the weight of a route is, the more data flow the route carries.

Enablement/disablement shows the state of the static route. Disablement means the static route is not used for forwarding. The forwarding table used the permanent route until administrator deletes it.

When you configure the static route on an Ethernet interface, do not set the next hop as an interface, for example, ip route 0.0.0.0 0.0.0.0 Fastethernet 0/0. In this case, the switch may consider that all unknown destination networks are directly connected to the Fastethernet 0/0. So it sends an ARP request to every destination host, which occupies many CPU and memory resources. It is not recommended to set the static route to an Ethernet interface.

**Examples**

The following example adds a static route to the destination network of 172.16.100.0/24 whose next hop is 192.168.12.1 and administrative distance is 15.

```
ip route 172.16.199.0 255.255.255.0 192.168.12.1 155
```

If the static route has not a specific interface, data flows may be sent thought other interface in case of interface failure. The following example configures data flows to be sent through fastehternet 0/0 to the destination network of 172.16.100.0/24.

```
ip route 172.16.199.0 255.255.255.0 fastethernet 0/0 192.168.12.1
```

**Related** This command is not supported on 2-layer devices.

**Commands**

## 1.4 ip routing

Use this command to enable IP routing in the global configuration mode. Use the **no** or **default** form of this command to disable this function.

**ip routing**

**no ip routing**

**default ip routing**

**Defaults** This function is enabled by default.

**Command Mode** Global configuration mode

**Usage Guide**

IP routing is not necessary when the switch serves as bridge or VoIP gateway.

When a device functions only as a bridge or VoIP gateway, the IP routing function of the RGOS software is not required. In this case, the IP routing function of the RGOS software can be disabled.

After the IP routing function is disabled, the device functions as a common host. The device can send and receive packets but cannot forward packets. All route-related configurations will be deleted except the static route configuration. A large number of static routes may be configured. If a user runs the **no ip routing** command, the configuration of a large number of static routes may be lost. To prevent this situation, the static route configuration will be hidden temporarily when the **no ip routing** command is run. If the **ip routing** command is run again, the static route configuration can be restored.

Note that if the process or whole system restarts when the **no ip routing** command is run, the static route configuration will not be reserved.

**Examples**

The following example disables IP routing.

```
Ruijie(config)# no ip routing
```

**Related Commands** N/A

**Platform Description**

## 1.5 ip static route-limit

Use this command to set the upper threshold of the static route. Use the **no** or **default** form of this command to restore the default setting.

**ip static route-limit** *number*

**no ip static route-limit** *number*
**default ip static route-limit**

**Parameter Description**

| Parameter | Description |
|---|---|
| *number* | Upper threshold of static routes in the range from 1 to 10000 |

**Defaults** The default is 1024.

**Command Mode** Global configuration mode

**Usage Guide** The goal is to control the number of static routes. You can view the upper threshold of the configured non-default static routes with the **show running-config** command.

**Examples** The following example sets the upper threshold of the static routes to 900 and then restores the setting to the default value.

```
ip static route-limit 900
```

**Related Commands** N/A

**Platform Description**

## 1.6 ipv6 route

Use this command to configure an ipv6 static route. Use the **no** or **default** form of this command to restore the default setting.
**ipv6 route** *ipv6-prefix* / *prefix-length* { *ipv6-address* | *interface* [ *ipv6-address* ] } [ *distance* ] [ **tag** *tag* ] [ **weight** *number* ] [**description** *description-text*]
**no ipv6 route***ipv6-prefix* / *prefix-length* { *ipv6-address* | *interface* [ *ipv6-address* ] } [ *distance* ]
**no ipv6 route all**

**Parameter Description**

| Parameter | Description |
|---|---|
| *prefix-length* | Mask length of the destination |
| *ipv6-address* | The next hop IP address of the static route |
| *interface* | (Optional) The next hop egress of the static route |
| *distance* | (Optional) The administrative distance of the static route. The default is 1. |
| *tag* | (Optional) The tag value of the static route. The default is 0. |
| **weight** *number* | (Optional) Indicates the weight of the static route, which must be specified when you configure equal-cost routes. |

| | |
|---|---|
| | The weight ranges from 1 to 8. When the weights of all equal-cost routes of a route are summed up, the sum cannot exceed the maximum number of equal-cost routes that can be configured for the route. Weighting of equal-cost routes of a route indicates the traffic ratio of these routes. The weight is 1 by default. |
| **description***description-text* | (Optional) Indicates the description of the static route. By default, no description is configured. *description-text* is a string of one to 60 characters. |

**Defaults** No IPv6 static route is configured by default.

**Command Mode** Global configuration mode

**Usage Guide** The default administrative distance of the static route is 1. Setting the administrative distance allows the learnt dynamic route to overwrite the static route. Setting the administrative distance of the static route can enable route backup, which is called floating route in this case. For example, the administrative distance of the OSPF is 110. You can set its administrative distance to 125. Then the data can switch over the static route when the route running OSPF fails.

**Examples** The following example adds a static route to the destination network of 2001::/64 whose next hop is 2002::2 and administrative distance are 115.

```
ipv6 route 2001::/64 2002::2 115
```

If the static route has not a specific interface, data flows may be sent thought other interface in case of interface failure. The following example configures that data flows are sent through fastehternet 0/0 to the destination network of 2001::/64.

```
ipv6 route 2001::/64 fastethernet 0/0 2002::2
```

**Related Commands**

| Command | Description |
|---|---|
| show ipv6 route | Displays IPv6 routing table. |

**Platform Description**

## 1.7 ipv6 static route-limit

Use this command to set the upper threshold of the static route. Use the **no** or **default** form of this command to restore the default setting.

**Ipv6 static route-limit** *number*

**no ipv6 static route-limit** *number*

**default ipv6 static route-limit**

**Parameter Description**

| Parameter | Description |
| --- | --- |
| *number* | Upper threshold of static routes in the range from 1 to 10000. |

**Defaults** The default is 1000.

**Command Mode** Global configuration mode

**Usage Guide** The goal is to control the number of static routes. You can view the upper threshold of the configured non-default static routes with the show running config command.

**Examples** The following example sets the upper threshold of the ipv6 static routes to 900 and then restores the setting to the default value.

```
Ruijie# ipv6 static route-limit 900
Ruijie# no ipv6 static route-limit
```

**Related Commands**

| Command | Description |
| --- | --- |
| ipv6 route | Configures the IPv6 static route. |
| show ipv6 route | Displays the IPv6 routing table. |

**Platform Description**

## 1.8 ipv6 unicast-routing

Use this command to enable the IPv6 route function of the RGOS. Use the **no** or **default** form of this command to disable this function.

**ipv6 unicast-routing**

**no ipv6 unicast-routing**

**default ipv6 unicast-routing**

**Parameter Description** N/A

**Defaults** This function is enabled by default.

**Command Mode** Global configuration mode

**Usage Guide** This function can be disabled if the device is just used as the bridge-connection device or the VOIP gateway device.

**Examples** The example disables the IPv6 route function of RGOS.

```
Ruijie# no ipv6 unicast-routing
```

**Related Commands**

| Command | Description |
|---|---|
| ipv6 route | Configure the IPv6 static route. |
| show ipv6 route | Displays the IPv6 routing table. |

**Platform Description**

## 1.9 maximum-paths

Use this command to specify the number of equivalent routes. Use the **no** or **default** form of this command is used to restore the default setting.

**maximum-paths** *number*

**no maximum-paths** *number*

**default maximum-paths**

**Parameter Description**

| Parameter | Description |
|---|---|
| *number* | Number of equivalent routes in the range from 1 to 64. |

**Defaults** The default value varies from products.

**Command Mode** Global configuration mode

**Usage Guide**

The number of equivalent routes is configured to control the number of equivalent routes. After the number of equivalent routes is configured by running the **maximum-paths** command, the number of load-sharing channels in load-sharing mode will not exceed the number of configured static routes. You can run the **show running config** command to query the number of configured static routes. This command takes effect both to IPv4 and IPv6 addresses. After this command is configured, the maximum number of equivalent routes to an IPv4 or IPv6 destination is equal to the configured value.

S8600/S5750/S7600 supports 64 groups of equivalent routes. Each group supports a maximum of 32 equivalent routes. The maximum number of equivalent routes on S3760/S5760 is 8. The number of static route groups is not restricted, that is, each route supports equivalent routes. An equivalent route group includes multiple equivalent next hops of the same prefix. On S8600/S5750/S7600, when 64 groups of equivalent routes are configured and an equivalent route needs to be configured for a prefix, the configuration is successful if the equivalent route exists in the 64 groups. Otherwise, the configuration fails.

**Examples** The following example sets the number of equivalent routes to 10 and then restores the default

setting.

```
maximum-paths 10
no maximum-paths 10
```

## 1.10 show ip route

Use the commands to display the configuration of the IP routing table.

**show ip route** [[ *network* [ *mask* [**longer-prefix**] ] | **count** | *protocol* [ *process-id* ] | **weight** ] ]

**show ip route** [ [ **normal** | **ecmp** ] [ *network* [ *mask* ] ]

**Parameter Description**

| Parameter | Description |
|---|---|
| *network* | (Optional) Displays the route information to the network. |
| *mask* | (Optional)Displays the route information to the network of this mask. |
| **longer-prefix** | (optional) Displays the routes that match the specified prefix. |
| count | (Optional)Displays the number of existent routes. (for the ECMP/WCMP route, displays one route) |
| *protocol* | (Optional) Displays the route information of specific protocol. |
| *process-id* | (Optional) Routing protocol process ID. |
| weight | (Optional) Displays the route information of non default weight. |
| normal | Displays normal routes and not equivalent routes or fast reroutes. |
| ecmp | Displays only equivalent routes. |

**Defaults**

**Command Mode** Privileged EXEC mode/ Global configuration mode/Interface configuration mode/ Routing protocol configuration mode/ Route map configuration mode

**Usage Guide** This command can display route information flexibly.
This command shows all routes. To show different attributes of routes, specify normal | ecmp | fast-reroute.

**Examples** The following example displays the configuration of the IP routing table.

```
Ruijie# show ip route

Codes:  C - Connected, L - Local, S - Static
       R - RIP, O - OSPF, B - BGP, I - IS-IS, V - Overflow route
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       SU - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       IA - Inter area, * - candidate default
Gateway of last resort is no set
S    20.0.0.0/8 is directly connected, VLAN 1
S    22.0.0.0/8 [1/0] via 20.0.0.1
O E2 30.0.0.0/8 [110/20] via 192.1.1.1, 00:00:06, VLAN 1
```

```
R    40.0.0.0/8 [120/20] via 192.1.1.2, 00:00:23, VLAN 1
B    50.0.0.0/8 [120/0] via 192.1.1.3, 00:00:41
C    192.1.1.0/24 is directly connected, VLAN 1
C    192.1.1.254/32 is local host.
```

| Field | Description |
| --- | --- |
| O | Source routing protocol, which may be:<br>C: directly connected route<br>S: static route<br>R: RIP route<br>B: BGP route<br>O: OSPF route<br>I: IS-IS route |
| E2 | Route type, which may be:<br>E1: OSPF external route type 1<br>E2: OSPF external route type 2<br>N1: OSPF NSSA external type 1<br>N2: OSPF NSSA external type 2<br>IA: OSPF area internal route<br>SU: IS-IS summary route<br>L1: IS-IS level-1 route<br>L2: IS-IS level-2 route<br>IA: IS-IS area internal route |
| 20.0.0.0/8 | Network address and mask of the destination network |
| [1/0] | Administrative distance/metric |

```
Ruijie# show ip route 30.0.0.0
Routing entry for 30.0.0.0/8
Distance 110, metric 20
Routing Descriptor Blocks:
192.1.1.1, 00:01:11 ago, via VLAN 1, generated by OSPF, extern 2
```

| Field | Description |
| --- | --- |
| Routing Descriptor Blocks | Next hop IP address, source, update time, forwarding interface, source routing protocol and type of route information |

```
Ruijie# show ip route count
--------- route info ----------
the num of active route: 5
```

```
Ruijie# show ip route weight
------------[distance/metric/weight]-----------
S    23.0.0.0/8 [1/0/2] via 192.1.1.20
S    172.0.0.0/16 [1/0/4] via 192.0.0.1
```

```
Ruijie#show ip route normal

Codes:  C - Connected, L - Local, S - Static
       R - RIP, O - OSPF, B - BGP, I - IS-IS, V - Overflow route
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       SU - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       IA - Inter area, * - candidate default
Gateway of last resort is no set
S    20.0.0.0/8 is directly connected, VLAN 1
S    22.0.0.0/8 [1/0] via 20.0.0.1
O E2 30.0.0.0/8 [110/20] via 192.1.1.1, 00:00:06, VLAN 1
R    40.0.0.0/8 [120/20] via 192.1.1.2, 00:00:23, VLAN 1
B    50.0.0.0/8 [120/0] via 192.1.1.3, 00:00:41
C    192.1.1.0/24 is directly connected, VLAN 1
C    192.1.1.254/32 is local host
```

```
Ruijie#show ip route ecmp

Codes:  C - Connected, L - Local, S - Static
       R - RIP, O - OSPF, B - BGP, I - IS-IS, V - Overflow route
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       SU - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       IA - Inter area, * - candidate default
Gateway of last resort is 192.168.1.2 to network 0.0.0.0
S*   0.0.0.0/0 [1/0] via 192.168.1.2
             [1/0] via 192.168.2.2
O IA 192.168.10.0/24 [110/1] via 35.1.10.2, 00:38:26, VLAN 1
                      [110/1] via 35.1.30.2, 00:38:26, VLAN 3
```

```
Ruijie#show ip route fast-reroute
```

```
Codes:  C - Connected, L - Local, S - Static
       R - RIP, O - OSPF, B - BGP, I - IS-IS, V - Overflow route
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       SU - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       IA - Inter area, * - candidate default
Status codes: m - main entry, b - backup entry, a – active entry

Gateway of last resort is 192.168.1.2 to network 0.0.0.0
S*   0.0.0.0/0 [ma] via 192.168.1.2
             [b] via 192.168.2.2
O IA 192.168.10.0/24 [m] via 35.1.10.2, 00:38:26, VLAN 1
                  [ba]  via 35.1.30.2, 00:38:26, VLAN 3
```

```
Ruijie# show ip route fast-reroute 30.0.0.0
Routing entry for 30.0.0.0/8
Distance 110, metric 20
Routing Descriptor Blocks:
[m] 192.1.1.1, 00:01:11 ago, via VLAN 1, generated by OSPF, extern 2
[ba]192.1.1.1, 00:01:11 ago, via VLAN 1, generated by OSPF, extern 2
```

## 1.11 show ip route summary

Use this command to display the statistical information about one routing table.

**show ip route summary**

Use this command to display the statistical information about all routing tables.

**show ip route summary all**

| **Parameter Description** | **Parameter** | **Description** |
|---|---|---|
| | N/A | N/A |

**Defaults** N/A

**Command Mode** Privileged EXEC mode

**Usage guideline** N/A

**Examples**

The following example displays the statistics of the global routing table.

```
Ruijie# show ip route summary
Codes: NORMAL – Normal route ECMP – ECMP route FRR – Fast-Reroute route

 Memory: 2000 bytes
Entries: 22,based on route prefixes
                NORMAL ECMP FRR TOTAL
        Connected 3 0 0 3
        Static 2 1 1 4
        RIP  1 2 1 4
        OSPF 2 1 1 4
        ISIS 1 2 0 3
        BGP  2 1 1 4
        TOTAL 11 7 4 22
```

The following example displays the statistics of all routing tables.

```
Ruijie# show ip route summary all
Codes: NORMAL – Normal route ECMP – ECMP route FRR – Fast-Reroute route

IP routing table count:2
Total
    Memory: 4000 bytes
    Entries: 44,based on route prefixes
                NORMAL ECMP FRR TOTAL
        Connected 6 0 0 6
        Static 4 2 2 8
        RIP  2 4 2 8
        OSPF 4 2 2 8
        ISIS 2 4 0 6
        BGP  4 2 2 8
        TOTAL 22 14 8 44

Global
    Memory: 2000 bytes
    Entries: 22,based on route prefixes
                NORMAL ECMP FRR TOTAL
        Connected 3 0 0 3
        Static 2 1 1 4
        RIP  1 2 1 4
        OSPF 2 1 1 4
        ISIS 1 2 0 3
        BGP  2 1 1 4
        TOTAL 11 7 4 22
```

```
VRF1
 Memory: 2000 bytes
     Entries: 22,based on route prefixes
      Entries: 29,based on route nexthops
NORMAL
ECMP FRR TOTAL
          Connected 3 0 0 3
          Static 2 1 1 4
          RIP  1 2 1 4
          OSPF 2 1 1 4
          ISIS 1 2 0 3
          BGP  2 1 1 4
          TOTAL 11 7 4 22
```

| Field | Description |
|---|---|
| NORMAL | Type of the table entries. Value:<br>NORMAL: common routes (not ECMP or FRR);<br>ECMP: equivalent route;<br>FRR: fast reroute;<br>TOTAL: total |
| Memory | Memory occupied by the table. |
| Entries | Number of entries (based on prefix, not next-hop) |
| Connected | Protocol type. Value:<br>Connected: direct connection;<br>Static: static;<br>RIP: RIP;<br>OSPF: OSPF;<br>ISIS: ISIS;<br>BGP: BGP;<br>TOTAL: total |

## 1.12 show ipv6 route

Use the command to display the configuration of the IPv6 routing table.

**show ipv6 route** [ [ *ipv6-prefix* / *prefix-length* [ **longer-prefixes** ] | *protocol* [ *process-id* ] | **weight** ] ]

**Parameter Description**

| Parameter | Description |
|---|---|
| *ipv6-prefix*/*prefix-length* | (Optional) Specifies a prefix for route's IPv6 address. |
| **longer-prefixes** | (Optional) Displays the route with an IPv6 address prefix mostly matched. |
| *protocol* | ((Optional) Displays the route information of specific protocol. |
| *process-id* | (Optional) Specifies a route process ID. |

| | |
|---|---|
| **weight** | (Optional) Displays the non-default-weight routes only. |

**Defaults**

**Command Mode** Privileged EXEC mode

**Usage Guide** Use this command to display route information.

The following example displays the IPv6 routing table.

**Examples**

```
Ruijie(config)# show ipv6 route

IPv6 routing table -  Default - 7 entries
Codes:  C - Connected, L - Local, S - Static
       R - RIP, O - OSPF, B - BGP, I - IS-IS, V - Overflow route
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       SU - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       IA - Inter area

C     10::/64  via Loopback 1, directly connected
L     10::1/128  via Loopback 1, local host
S     20::/64  [20/0] via 10::4, Loopback 1C
C     FE80::/10 via Null 0, directly connected
C     FE80::/64  via Loopback 1, directly connected
L     FE80::2D0:F8FF:FE22:33AB/128  via Loopback 1, local host
```

| Field | Description |
|---|---|
| E2 | Route type, which may be:<br>E1: OSPF external route type 1<br>E2: OSPF external route type 2<br>N1: OSPF NSSA external type 1<br>N2: OSPF NSSA external type 2<br>IA: OSPF area internal route<br>SU: IS-IS summary route<br>L1: IS-IS level-1 route<br>L2: IS-IS level-2 route<br>IA: IS-IS area internal route |
| 20::/64 | Network address and mask of the destination network |
| [20/0] | Administrative distance/metric |

| Related Commands | Command | Description |
|---|---|---|
| | **ipv6 route** | Configures the IPv6 static route. |

**Platform Description**

## 1.13 show ipv6 route summary

Use this command to display the statistics of the IPv6 routing table of a specified VRF.

**show ipv6 route summary**

Use this command to display statistics of all IPv6 routing 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

**Examples**

The following example displays statistics of IPv6 routing table of the global VRF.

```
Ruijie#show ipv6 route summary
IPv6 routing table name is -  Default(0) global scope - 5 entries
IPv6 routing table default maximum-paths is 32
Local          2
Connected      3
Static         0
PIP            0
OSPF           0
BGP            0
------------------------
Total          5
```

| Field | Description |
|---|---|
| Memory | The memory size occupied by the current routing table. |
| Entries | The entries in the current routing table (based on the entry prefix instead of the next hop entry.) |
| Connected | Describes the protocol type of the entry. The field can be;<br>Connected: Connected route entry. |

| | |
|---|---|
| | Static: Static route entry.<br>RIP: RIP route entry.<br>OSPF: OSPF route entry.<br>ISIS: ISIS route entry.<br>BGP: BGP route entry.<br>TOTAL: Total number of all protocol entries. |
| IPv6 routing table count | The number of the routing tables. |
| Global | The name of the current routing table. The field can be:<br>Global : Global (The default VRF)<br>VRF1: VRF name.<br>TOTAL: All VRF routing table summaries. |

**Related Commands**

| Command | Description |
|---|---|
| N/A | N/A |

**Platform Description**

# 2 FPM Commands

## 2.1 clear ip fpm counters

Use this command to clear counters about the IPv4 packets.

**clear ip fpm counters**

**Parameter Description**

| Parameter | Description |
| --- | --- |
| N/A | N/A |

**Command Mode** Privileged EXEC mode

**Usage Guide** N/A

**Configuration Examples** The following example clears counters about the IPv4 packets.

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

**Platform Description** N/A

## 2.2 clear ip v6fpm counters

Use this command to clear counters about the IPv6 packets.

**clear ip v6fpm counters**

**Parameter Description**

| Parameter | Description |
| --- | --- |
| N/A | N/A |

**Command Mode** Privileged EXEC mode

**Usage Guide** N/A

**Configuration Examples** The following example clears counters about the IPv6 packets.

```
Ruijie# clear ip v6fpm counters
```

**Platform Description** N/A

## 2.3 ip session direct-trans-disable

Use this command to disable the function to transparently transmit packets when the flow table is full.
**ip session direct-trans-disable**

Use the **no** form of this command to restore the default setting.
**no ip session direct-trans-disable**

**Parameter Description**

| Parameter | Description |
|---|---|
| N/A | N/A |

**Defaults** This configuration takes effect only on ACs and APs. With this feature, packets are transparently transmitted instead of establishing any flow on wireless products when the flow table is full, and service processing is not accelerated, thereby ensuring that service flows are not interrupted.

**Command Mode** Global configuration mode

**Usage Guide** N/A

**Configuration Examples** The following example disables the function to transparently transmit packets when the flow table is full.

```
Ruijie(config)# ip session direct-trans-disable
```

**Platform Description** N/A

## 2.4 ip session tcp-loose

Use this command to enable the loose TCP status transition check function.
**ip session tcp-loose**

Use the **no** form of this command to restore the default setting.
**no ip session tcp-loose**

**Parameter Description**

| Parameter | Description |
|---|---|
| N/A | N/A |

**Defaults** By default, the loose TCP status check function is disabled on FW products while enabled on wireless and EG products.

**Command** Global configuration mode

**Mode**

**Usage Guide** N/A

**Configuration Examples** The following example enables the loose TCP status transition check function.

```
Ruijie(config)# ip session tcp-loose
```

**Platform Description** N/A

## 2.5 ip session tcp-state-inspection-enable

Use this command to enable the TCP status tracing function.
**ip session tcp-state-inspection- enable**

Use the **no** form of this command to restore the default setting.
**no ip session tcp-state-inspection- enable**

**Parameter Description**

| Parameter | Description |
| --- | --- |
| N/A | N/A |

**Defaults** The TCP status tracing function is disabled on ACs and APs by default.

**Command Mode** Global configuration mode

**Usage Guide** N/A

**Configuration Examples** The following example enables the TCP status tracing function.

```
Ruijie(config)# ip session tcp-state-inspection-enable
```

**Platform Description** N/A

## 2.6 ip session threshold

Use this command to configure the number of packets that can be received for each flow in a certain status.
**ip session threshold** {**icmp-closed** | **icmp-started** | **rawip-closed** | **tcp-syn-sent | tcp-syn-receive** | **tcp-closed | udp-closed**} { *num* }

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

**no ip session threshold** {**icmp-closed | icmp-started** | **rawip-closed | tcp-syn-sent | tcp-syn-receive** | **tcp-closed | udp-closed**}

**Parameter Description**

| Parameter | Description |
|---|---|
| icmp-closed | Sets the number of packets permitted to pass in each ICMP flow in closed status, which is 10 by default and ranges from 1 to 2,000,000,000. |
| icmp-started | Sets the number of packets permitted to pass in each ICMP flow in started status, which is 300 by default and ranges from 5 to 2,000,000,000. |
| rawip-closed | Sets the number of packets permitted to pass in each RAWIP flow in closed status, which is 10 by default and ranges from 1 to 2,000,000,000. |
| tcp-syn-sent | Sets the number of packets permitted to pass in each TCP flow in syn-send status, which is 10 by default and ranges from 5 to 2,000,000,000. |
| tcp-syn-receive | Sets the number of packets permitted to pass in each TCP flow in syn-receive status, which is 20 by default and ranges from 5 to 2,000,000,000. |
| tcp-closed | Sets the number of packets permitted to pass in each TCP flow in closed status, which is 20 by default and ranges from 5 to 2,000,000,000. |
| udp-closed | Sets the number of packets permitted to pass in each UDP flow in closed status, which is 10 by default and ranges from 1 to 2,000,000,000. |
| *num* | Sets the number of packets permitted to pass. |

**Defaults**

**icmp-closed**: 10;
**icmp-started**: 300;
**rawip-closed**: 10;
**tcp-syn-sent**: 10;
**tcp-syn-receive**: 20;
**tcp-closed**: 20;
**udp-closed**: 10.

**Command Mode**

Global configuration mode

**Usage Guide**

To activate this configuration, run the **ip session** [*dev*] [*slot* ] **track-state-strictly** command.

**Configuration Examples**

The following example configures the number of packets that can be received for each flow in a certain status to 100.

```
Ruijie(config)# ip session threshold tcp-closed 100
```

**Platform Description**

N/A

## 2.7 ip session timeout

Use this command to configure the aging time.

**ip session timeout** {**icmp-closed** | **icmp-connected** | **icmp-started** | **rawip-closed** | **rawip-connected** | **rawip-established** | **rawip-started** | **tcp-close-wait** | **tcp-closed | tcp-established** | **tcp-fin-wait1** | **tcp-fin-wait2 | tcp-syn-receive** | **tcp-syn-sent | tcp-syn-sent2 | tcp-time-wait | udp-closed | udp-started** | **udp-connected** | **udp-established**} { *num* }

Use the **no** form of this command to restore the default setting.
**no ip session timeout** {**icmp-closed** | **icmp-connected** | **icmp-started** | **rawip-closed** | **rawip-connected** | **rawip-established** | **rawip-started** | **tcp-close-wait** | **tcp-closed | tcp-established** | **tcp-fin-wait1** | **tcp-fin-wait2 | tcp-syn-receive** | **tcp-syn-sent | tcp-syn-sent2 | tcp-time-wait | udp-closed | udp-started** | **udp-connected** | **udp-established**}

**Parameter Description**

| Parameter | Description |
|---|---|
| icmp-closed | Sets the aging time of ICMP flows in closed status, which is 10 seconds by default and ranges from 5 to 60. |
| icmp-connected | Sets the aging time of ICMP flows in connected status, which is 10 seconds by default and ranges from 5 to 120. |
| icmp-started | Sets the aging time of ICMP flows in started status, which is 10 seconds by default and ranges from 5 to 120. |
| rawip-closed | Sets the aging time of RAWIP flows in closed status, which is 10 seconds by default and ranges from 5 to 60. |
| rawip-connected | Sets the aging time of RAWIP flows in connected status, which is 300 seconds by default and ranges from 10 to 300. |
| rawip-established | Sets the aging time of RAWIP flows in established status, which is 300 seconds by default and ranges from 10 to 600. |
| rawip-started | Sets the aging time of TCP flows in started status, which is 300 seconds by default and ranges from 10 to 300. |
| tcp-close-wait | Sets the aging time of TCP flows in tcp-close-wait status, which is 60 seconds by default and ranges from 10 to 120. |
| tcp-closed | Sets the aging time of TCP flows in tcp-closed status, which is 10 seconds by default and ranges from 5 to 20. |
| tcp-established | Sets the aging time of TCP flows in tcp-established status, which is 1,800 seconds by default and ranges from 300 to 604,800. |
| tcp-fin-wait1 | Sets the aging time of TCP flows in tcp-fin-wait1 status, which is 60 seconds by default and ranges from 10 to 120. |
| tcp-fin-wait2 | Sets the aging time of TCP flows in tcp-fin-wait2 status, which is 60 seconds by default and ranges from 10 to 120. |
| tcp-syn-receive | Sets the aging time of TCP flows in tcp-syn-receive status, which is 10 seconds by default and ranges from 5 to 30. |
| tcp-syn-sent | Sets the aging time of TCP flows in tcp-syn-sent status, which is 10 seconds by default and ranges from 5 to 30. |
| tcp-syn_sent2 | Sets the aging time of TCP flows in tcp-syn_sent2 status, which is 10 seconds by default and ranges from 5 to 30. |
| tcp-time-wait | Sets the aging time of TCP flows in tcp-time-wait status, which is 10 seconds by |

| | |
|---|---|
| | default and ranges from 5 to 60. |
| udp-closed | Sets the aging time of UDP flows in closed status, which is 10 seconds by default and ranges from 5 to 60. |
| udp-connected | Sets the aging time of UDP flows in connected status, which is 30 seconds by default and ranges from 10 to 300. |
| udp-established | Sets the aging time of UDP flows in established status, which is 600 seconds by default and ranges from 120 to 600. |
| udp-started | Sets the aging time of UDP flows in started status, which is 10 seconds by default and ranges from 10 to 300. |
| *num* | Sets the aging time. |

**Defaults** **icmp-closed**: 10 seconds;
**icmp-connected**: 10 seconds;
**icmp-started**: 10 seconds;
**rawip-closed**: 10 seconds;
**rawip-connected**; 300 seconds;
**rawip-established**: 300 seconds;
**rawip-started**: 300 seconds;
**tcp-close-wait**: 60 seconds;
**tcp-closed**: 10 seconds;
**tcp-established**: 1,800 seconds;
**tcp-fin-wait1**: 60 seconds;
**tcp-fin-wait2**: 60 seconds;
**tcp-syn-receive**: 10 seconds;
**tcp-syn-sent**: 10 seconds;
**tcp-syn_sent2**: 10 seconds;
**tcp-time-wait**: 10 seconds;
**udp-closed**: 10 seconds;
**udp-connected**: 30 seconds;
**udp-established**: 600 seconds;
**udp-started**: 10 seconds

**Command Mode** Global configuration mode

**Usage Guide** N/A

**Configuration Examples** The following example sets the aging time of TCP flows in tcp-established status to 600 seconds.

```
Ruijie(config)# ip session timeout tcp-established 600
```

**Platform Description** N/A

## 2.8 ip session track-state-strictly

Use this command to configure packet threshold check for flows in various states.
**ip session track-state-strictly**

Use the **no** form of this command to restore the default setting.
**no ip session track-state-strictly**

**Parameter Description**

| Parameter | Description |
|---|---|
| N/A | N/A |

**Defaults** This function is disabled by default.

**Command Mode** Global configuration mode

**Usage Guide** N/A

**Configuration Examples** The following example configures packet threshold check for flows.

```
Ruijie(config)# ip session track-state-strictly
```

**Platform Description** N/A

## 2.9 show ip fpm counters

Use this command to displays the counters about the IPv4 packets.
**show ip fpmcounters**

**Parameter Description**

| Parameter | Description |
|---|---|
| N/A | N/A |

**Command Mode** Privileged EXEC mode

**Usage Guide** Use this command to display the counters about the IPv4 packets, including information about packet loss and flows.

**Configuration Examples** The following example displays the counters about the IPv4 packets.

```
Ruijie#sh ip fpm 1 2 counters
Dropped packet counters:
```

```
Count     Reason
0         Non-IPv4 packet
0         Bad IPv4 header length
0         Bad IPv4 total length
0         Fragment pkt
0         change flow state notify FW refuse
0         Bad IPv4 checksum
0         Invalid IPv4 address
0         Invalid TCP flags
0         Invalid TCP sequence
0         Invalid ICMP message type
0         Invalid icmp initial message type
54        Invalid tcp init flags
0         Invalid tcp connection state
0         Connect over config threshold
0         Connect has been terminated
0         Invalid egress fid
0         out of vfw session limit
0         Out of capability
<end>
Rejected or terminated connection counters:
Count     Reason
0         Out of life time
1968      Flow Terminated
0         Rejected by policy
<end>
```

**Field Description**

| Field | Description |
| --- | --- |
| count | Packet counters. |
| Reason | Packet loss reason. |

**Platform Description** N/A

## 2.10 show ip fpm flows

Use this command to display IPv4 packet flow information.

**show ip fpm flows**

**Parameter Description**

| Parameter | Description |
| --- | --- |
| N/A | N/A |

**Command** Privileged EXEC mode

**Mode**

**Usage Guide** N/A

**Configuration Examples** The following example displays IPv4 packet flow information.

```
Ruijie#show ip fpm flows
Pr  SrcAddr                      DstAddr                      SrcPort
DstPort     Vrf         SendBytes  RecvBytes  St    srcif
dstif                 ctrl_flag
```

**Field Description**

| Field | Description |
|---|---|
| Pr | Protocol. |
| SrcAddr | Source address. |
| DstAddr | Destination address. |
| SrcPort | Source Port. |
| DstPort | Destination port. |
| Vrf | The VRF of the destination interface. |
| SendBytes | The length of received packets in Tx. |
| RecvBytes | The length of received packets in Rx. |
| St | The current state of flows. |
| srcif | Source interface. |
| dstif | Destination interface. |
| ctrl_flag | Flows control flag. |

**Platform Description** N/A

## 2.11 show ip fpm flows filter

Use this command to display IPv4 packet flow information except specific IPv4 packet flows.

**show ip fpm flows filter** *protocol saddr smask daddr dmask*

**Parameter Description**

| Parameter | Description |
|---|---|
| *protocol* | IP protocol in the range from 0 to 255. |
| *saddr* | Source IP addresses. |
| *smask* | Source IP mask in the range from 1 to 32. |
| *daddr* | Destination IP addresses. |
| *dmask* | Destination IP mask in the range from 1 to 32. |

**Command Mode** Privileged EXEC mode

**Usage Guide** N/A

**Configuration Examples** The following example displays IPv4 packet flow information except specific IPv4 packet flows.

```
Ruijie#show ip fpm flows filter 1 192.168.1.1 32 192.168.2.1 30
Pr  SrcAddr                      DstAddr                      SrcPort
DstPort     Vrf         SendBytes  RecvBytes  St    srcif
dstif                  ctrl_flag
```

**Field Description**

| Field | Description |
|---|---|
| Pr | Protocol |
| SrcAddr | Source address. |
| DstAddr | Destination address. |
| SrcPort | Source Port. |
| DstPort | Destination port. |
| Vrf | The VRF of the destination interface. |
| SendBytes | The length of received packets in Tx. |
| RecvBytes | The length of received packets in Rx. |
| St | The current state of flows. |
| srcif | Source interface. |
| dstif | Destination interface. |
| ctrl_flag | Flows control flag. |

**Platform Description** N/A

## 2.12 show ip fpm statistics

Use this command to display IPv4 flow statistics.

**show ip fpm statistics**

**Parameter Description**

| Parameter | Description |
|---|---|
| N/A | N/A |

**Command Mode** Privileged EXEC mode

**Usage Guide** N/A

**Configuration Examples** The following example displays IPv4 flow statistics on the EG device.

```
Ruijie#show ip fpm statistics
The capacity of the flow table:150016.
Active flows num:109.
event count:65,
```

```
Fpm attribute is eg.
```

**Field Description**

| Field | Description |
| --- | --- |
| The capacity of the flow table | The number of total flow tables. |
| Active flows num | The number of active flow tables. |
| event count:65, | The counter for current events. |
| Fpm attribute is eg | The flow tables are generated based on EG products. |

**Platform Description** N/A

## 2.13 show ip v6fpm counters

Use this command to displays the counters about the IPv6 packets.

**show ip v6fpm counters**

**Parameter Description**

| Parameter | Description |
| --- | --- |
| N/A | N/A |

**Command Mode** Privileged EXEC mode

**Usage Guide** Use this command to display the counters about the IPv6 packets, including information about packet loss and flows.

**Configuration Examples** The following example displays the counters about the IPv6 packets.

```
Ruijie#sh ip v6fpm 1 2 counters
Droped packet counters:
Count     Reason
0         Non-IPv6 packet
0         Err length
0         Fragment packet
0         Err address
0         Invalid TCP flags
0         Invalid TCP sequence
0         Invalid ICMPV6 message type
0         Invalid ICMPV6 initial message type
0         Invalid tcp init flag
0         Invalid tcp flow state
```

```
0         Invalid pkt fid
0         Conn Terminated
0         Out of vfw session limit
0         Out of capability
<end>
Rejected or terminated connection counters:
Count     Reason
0         Out of life time
2105      Flow Terminated
0         Rejected by policy
<end>
```

**Field Description**

| Field | Description |
| --- | --- |
| count | Packet counters. |
| Reason | Packet loss reason. |

**Platform Description** N/A

## 2.14 show ip v6fpm flows

Use this command to display IPv6 packet flow information.

**show ip v6fpm flows**

**Parameter Description**

| Parameter | Description |
| --- | --- |
| N/A | N/A |

**Command Mode** Privileged EXEC mode

**Usage Guide** N/A

**Configuration Examples** The following example displays IPv6 packet flow information.

```
Ruijie# show ip v6fpm flows
Pr  Saddr                                Daddr
Sport  Dport  Sedby      Recby      Vrf    st    src_if     dst_id
ctrl_flag
```

**Field Description**

| Field | Description |
| --- | --- |
| Pr | Protocol. |
| Saddr | Source address. |
| Daddr | Destination address. |
| Sport | Source Port. |

| | |
|---|---|
| Dport | Destination port. |
| Sedby | The length of received packets in Tx. |
| Recby | The length of received packets in Rx. |
| Vrf | The VRF of the destination interface. |
| st | The current state of flows. |
| sifx | Source interface. |
| difx | Destination interface. |
| ctrl_flag | Flows control flag. |

**Platform Description** N/A

## 2.15 show ip v6fpm flows filter

Use this command to display IPv6 packet flow information except specific IPv6 packet flows.

**show ip v6fpm flows filter** *protocol saddr smask daddr dmask*

**Parameter Description**

| Parameter | Description |
|---|---|
| *protocol* | Slot ID in the range from 0 to 255. |
| *saddr* | Source IPv6 addresses. |
| *smask* | Source IPv6 mask in the range from 1 to 128. |
| *daddr* | Destination IPv6 addresses. |
| *dmask* | Destination IPv6 mask in the range from 1 to 128. |

**Command Mode** Privileged EXEC mode

**Usage Guide** N/A

**Configuration Examples** The following example displays IPv6 packet flow information except specific IPv6 packet flows.

```
Ruijie# show ip v6fpm flows
Pr  Saddr                                   Daddr
Sport  Dport  Sedby      Recby      Vrf    st    src_if     dst_id
ctrl_flag
```

**Field Description**

| Field | Description |
|---|---|
| Pr | Protocol. |
| Saddr | Source address. |
| Daddr | Destination address. |
| Sport | Source Port. |
| Sport | Destination port. |
| Sedby | The length of received packets in Tx. |

| | |
|---|---|
| Recby | The length of received packets in Rx. |
| Vrf | The VRF of the destination interface. |
| st | The current state of flows. |
| sifx | Source interface. |
| difx | Destination interface. |
| ctrl_flag | Flows control flag. |

**Platform Description** N/A

## 2.16 show ip v6fpm statistics

Use this command to display IPv6 flow statistics.

**show ip v6fpm statistics**

**Parameter Description**

| Parameter | Description |
|---|---|
| N/A | N/A |

**Command Mode** Privileged EXEC mode

**Usage Guide** N/A

**Configuration Examples** The following example displays IPv6 flow statistics.

```
Ruijie# show ip v6fpm statistics
The capacity of the flow table:150016.
Active flows num:109.
event count:65,
Fpmv6 state inspection disable.
```

**Field Description**

| Field | Description |
|---|---|
| The capacity of the flow table | The number of total flow tables. |
| Active flows num | The number of active flow tables. |
| event count | The counter for current events. |

**Platform Description** N/A

# Security Configuration Commands

# 1 Web Authentication Commands

## 1.1 accounting

Use this command to set an accounting method for the template.
Use the **no** form of this command to restore the default setting.
**accounting** { *method-list* }
**no accounting**

**Parameter Description**

| Parameter | Description |
|---|---|
| *method-list* | Name of the method list |

**Defaults** N/A

**Command Mode** Template configuration mode

**Usage Guide** The *method-list* parameter in this command should be consistent with network accounting list name configured in AAA.

**Configuration Examples** The following example sets the **mlist1** accounting method for the **eportalv2** template.

```
Ruijie(config.tmplt.eportalv2)# accounting mlist1
```

**Related Commands**

| Command | Description |
|---|---|
| N/A | N/A |

**Platform Description** N/A

## 1.2 authentication

Use this command to set an authentication method for the template.
Use the **no** form of this command to restore the default setting.
**authentication** { *method-list* }
**no authentication**

**Parameter Description**

| Parameter | Description |
|---|---|

| | |
|---|---|
| *method-list* | Name of the method list |

**Defaults** N/A

**Command Mode** Template configuration mode

**Usage Guide** The *method-list* parameter in this command should be consistent with the Web authentication method list configured in AAA.
The first generation authentication does not support the authentication method list configuration.

**Configuration Examples** The following example sets the **mlist1** authentication method for the **eportalv2** template.

```
Ruijie(config.tmplt.eportalv2)#authentication mlist1
```

**Related Commands**

| Command | Description |
|---|---|
| N/A | N/A |

**Platform Description** N/A

## 1.3 bindmode

Use this command to set a binding mode for the template.
Use the **no** form of this command to restore the default setting.
**bindmode** { **ip-mac-mode** | **ip-only-mode** }
**no bindmode**

**Parameter Description**

| Parameter | Description |
|---|---|
| **ip-mac-mode** | IP+MAC mode. The device will write both the IP address information and the MAC address information into the forwarding entry. |
| **ip-only-mode** | IP only mode. The device writes only the IP address information into the forwarding entry. On the L3 network, it is recommended to adopt this mode in case that the MAC address is inaccurate. |

**Defaults** The default is **ip-mac-mode**.

**Command Mode** Template configuration mode

**Usage Guide** N/A

**Configuration Examples** The following example adopts the IP only mode for the **eportalv2** template.

```
Ruijie(config.tmplt.eportalv2)# bindmode ip-only-mode
```

**Related Commands**

| Command | Description |
|---|---|
| N/A | N/A |

**Platform Description** N/A

## 1.4 clear web-auth acl

Use this command to clears all blacklists and whitelists.

**clear web-auth acl** [ **black-ip** | **black-port** | **black-url** | **white-url** ]

**Parameter Description**

| Parameter | Description |
|---|---|
| **white-url** | Clears URLs in all whitelists. |
| **black-url** | Clears URLs in all blacklists. |
| **black-ip** | Clears IPs in all blacklists. |
| **black-port** | Clears ports in all blacklists. |

**Command Mode** Privileged EXEC mode

**Usage Guide** N/A

**Configuration Examples** The following example clears all blacklists and whitelists.

```
Ruijie# clear web-auth acl
```

**Platform Description** N/A

## 1.5 clear web-auth direct host

Use this command to clear all authentication-exempted users.

**clear web-auth direct-host**

**Parameter Description**

| Parameter | Description |
|---|---|
| N/A | N/A |

**Defaults** N/A

**Command Mode** Privileged EXEC mode

**Usage Guide** N/A

**Configuration Examples** The following example clears all authentication-exempted users.

```
Ruijie# clear web-auth direct-host
```

**Related Commands**

| Command | Description |
| --- | --- |
| N/A | N/A |

**Platform Description** N/A

## 1.6 clear web-auth direct-site

Use this command to clear all authentication-exempted network resources.

**clear web-auth direct-site**

**Parameter Description**

| Parameter | Description |
| --- | --- |
| N/A | N/A |

**Defaults** N/A

**Command Mode** Privileged EXEC mode

**Usage Guide** N/A

**Configuration Examples** The following example clears all authentication-exempted network resources.

```
Ruijie# clear web-auth direct-site
```

**Related Commands**

| Command | Description |
| --- | --- |
| N/A | N/A |

**Platform Description** N/A

## 1.7 clear web-auth user

Use this command to force the user to go offline.

**clear web-auth user** { **all** | **ip** *ip-address* } | **mac** *mac-address* **| name** *name-string* | **session-id** *num* }

**Parameter Description**

| Parameter | Description |
|---|---|
| *ip-address* | Specifies the user's IPv4 address. |
| *mac-address* | Specifies the user's MAC address. |
| *name-string* | Specifies the user name. |
| *num* | Specifies the user's AAA session ID. |

**Defaults** N/A

**Command Mode** Privileged EXEC mode

**Usage Guide** N/A

**Configuration Examples** The following example forces all users to go offline.

```
Ruijie(config) clear web-auth user all
```

**Related Commands**

| Command | Description |
|---|---|
| N/A | N/A |

**Platform Description** N/A

## 1.8 escape interval

Use this command to enable the single escape function based on the escape interval.

**escape interval** *seconds* **online-time** *minutes*

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

**no escape interval**

**Parameter Description**

| Parameter | Description |
|---|---|
| *seconds* | Indicates the escape interval in the unit of seconds. The recommended value is 5s. |

| | |
|---|---|
| *minutes* | Indicates the maximum online time for escape users in the unit of minutes. When it is set to **0**, the user can access the Internet without time limit. |

**Defaults** N/A

**Command Mode** Template configuration mode

**Usage Guide** N/A

**Configuration Examples** The following example enables the single escape function based on the escape interval.

```
Ruijie(config.tmplt.wechat)# escape interval 5 online-time 10
```

**Platform Description** N/A

## 1.9 eacape user-try-auth

Use this command to enable the single escape function based on the number of authentication attempts.
**escape user-try-auth** *counts* **online-time** *minutes*

Use the **no** form of this command to disable the single escape function.
**no escape user-try-auth**

**Parameter Description**

| Parameter | Description |
|---|---|
| *counts* | Indicates the number of authentication attempts initiated by the STA. After the set value is reached, the user can access the Internet. The recommended value is 4. |
| *minutes* | Indicates the maximum online time for escape users in the unit of minutes. |

**Defaults** N/A

**Command Mode** Template configuration mode

**Usage Guide** N/A

**Configuration Examples** The following example enables the single escape function based on the number of authentication attempts.

```
Ruijie(config.tmplt.wechat)#escape user-try-auth 4 online-time 15
```

**Platform Description** N/A

## 1.10 fmt

Use this command to set the URL redirection format in the second template configuration mode.
**fmt { cmcc-ext1 | cmcc-ext2 | cmcc-mtx | cmcc-normal | cmcc-ext3 | ct-jc | cucc| ruijie | custom }**
Use this command to set the URL redirection format in the first template configuration mode.
**fmt { ace | ruijie | custom }**

Use this command to set the custom URL redirection format in the first & second template configuration modes.
**fmt custom [ encry { md5 | des | des_ecb | des_ecb3 | none } ] [ user-ip** *userip-str* **] [ user-mac** *usermac-str* **mac-format [dot | line | none] ] [ user-vid** *uservid-str* **]** [ **user-id** *userid-str* ] **[ nas-ip** *nasip-str* **] [ nas-id** *nasid-str* **] [ nas-id2** *nasid2-str* **] [ ac-name** *acname-str* **] [ ap-mac** *apmac-str* **mac-format [dot | line | none] ] [ url** *url-str* **] [ ssid** *ssid-str* **] [ port** *port-str* **] [ ac-serialno** *ac-sno-str* **] [ ap-serialno** *ap-sno-str* **] [ additional** *extern-str* **]**

Use the **no** form of **fmt custom** command to remove the custom URL redirection format.
**no fmt custom [ user-ip ] [ user-mac ] [ user-vid ]** [ **user-id** ] **[ nas-ip ] [ nas-id ] [ nas-id2 ] [ ac-name ] [ ap-mac ] [ url ] [ ssid ] [ port ] [ ac-serialno ] [ ap-serialno ] [ additional ]**

**Parameter Description**

| Parameter | Description |
|---|---|
| **cmcc-ext1** | Extended CMCC format |
| **cmcc-ext2** | Liaoning CMCC format |
| **cmcc-ext3** | Ningbo/Jiaxing format for AC manufacturers |
| **cmcc-mtx** | CMCC format for AC manufacturers |
| **cmcc-normal** | Standard CMCC format |
| **ct-jc** | China Telecom format |
| **cucc** | Shandong China Unicom format |
| **ace** | Supports ACE correlation. |
| **ruijie** | Ruijie format |
| **custom** | Custom format |
| *userip-str* | User IP address string |
| *usermac-str* | User MAC address string |
| *uservid-str* | User VID string |
| *nasip-str* | NAS device IP address string |
| *nasid-str* | NAS device ID string |

| | |
|---|---|
| *nasid2-str* | NAS device ID string (supports 2 NAS ID) |
| *acname-str* | AC name string |
| *apmac-str* | Associated AP MAC address string |
| *url-str* | Original URL string |
| *ssid-str* | SSID string |
| *port-str* | Auth-Port string |
| *sno-str* | SN string |
| *extern-str* | Special strings for specific portal servers |
| *md5* | MD5 encryption |
| *des* | DES encryption |
| *des_ecb* | DES_ECB encryption |
| *des_ecb3* | DES_ECB3 encryption |
| *none* | Not-encrypted |

**Defaults** The default URL redirection format is Ruijie format.

**Command Mode** Template configuration mode

**Usage Guide** Use this command to set the URL redirection format based on the corresponding portal standard.

**Configuration Examples** The following example sets the URL redirection format to extended CMCC format.

```
Ruijie(config.tmplt.eportalv2)#fmt cmcc-ext1
```

**Platform Description** N/A

## 1.11 free-auth

Use this command to exempt Wi-Fi authentication for Wechat App.

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

**free-auth pc**

**no free-auth**

**Parameter Description**

| Parameter | Description |
|---|---|
| N/A | N/A |

**Defaults**

**Command Mode** Template configuration mode

**Usage Guide** This command is only supported for Wechat App on PCs.

**Configuration Examples** The following example exempts Wi-Fi authentication for Wechat App on PCs.

```
Ruijie(config.tmplt.wechat)#free-auth pc
```

**Related Commands**

| Command | Description |
| --- | --- |
| N/A | N/A |

**Platform Description** N/A

## 1.12 gateway-id

Use this command to set the value of **gw_id** in the WiFiDog standard protocol used for the interaction between the devices authenticated via WiFiDog and the server.
**gateway-id** *string*

Use the **no** form of this command to delete the value of **gw_id** from the WiFiDog standard protocol used for the interaction between the devices authenticated via WiFiDog and the server.
**no gateway-id**

**Parameter Description**

| Parameter | Description |
| --- | --- |
| *string* | Indicates the value of **gw_id** in the WiFiDog protocol used by the devices and the server. |

**Defaults** The value of **gw_id** is set to the SN of the local device by default.

**Command Mode** Template configuration mode.

**Default Level** 14

**Usage Guide**

The value of **gw_id** is set to the SN of the local device by default. Manual configuration is not required unless a special interworking requirement is imposed.

**Configuration Examples** 1. The following example sets the value of **gw_id** in the WiFiDog protocol used by the devices and the server to **14144b6fb807**.

```
Ruijie(config.tmplt.wifidog)#gateway-id 14144b6fb807
```

**Verification** Run the **show running-config** command to display the currently configured template parameters.

## 1.13 http redirect adapter ios

Use this command to enable automatic IOS window pop-up.

**http redirect adapter ios**

**no http redirect adapter ios**

**Parameter Description**

| Parameter | Description |
|---|---|
| N/A | N/A |

**Defaults** N/A

**Command Mode** Global configuration mode

**Usage Guide** N/A

**Configuration Examples** The following example enables automatic IOS window pop-up.

```
Ruijie# http redirect adapter ios
```

**Related Commands**

| Command | Description |
|---|---|
| N/A | N/A |

**Platform Description** N/A

## 1.14 http redirect direct-arp

Use this command to set the address range of the authentication-exempted ARP.

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

**http redirect direct-arp** { *ip-address* [ *ip-mask* ] }

**no http redirect direct- arp** { *ip-address* [ *ip-mask* ] }

**Parameter Description**

| Parameter | Description |
|---|---|
| *ip-address* | IPv4 address |
| *ip-mask* | (Optional) IPv4 mask |

**Defaults** No authentication-exempted ARP resource is configured by default.

**Command Mode** Global configuration mode

**Usage Guide** The user cannot learn the ARPs of devices such as the gateway with the ARP CHECK function enabled. Use this command to enable the device to learn the ARP within a specified IP address range without authentication.

**Configuration Examples** The following example sets the IP address 172.16.0.1 as the authentication-exempted ARP resource.

```
Ruijie(config)# http redirect direct-arp 172.16.0.1
```

**Related Commands**

| Command | Description |
|---|---|
| N/A | N/A |

**Platform Description** N/A

## 1.15 http redirect direct-site

Use this command to set the range of authentication-exempted network resources.
Use the **no** form of this command to restore the default setting.
**http redirect direct-site** { *ipv6-address* | *ip-address* [ *ip-mask* ] [ **arp** ] }
**no http redirect direct-site** { *ipv6-address* | *ip-address* [ *ip-mask* ]

**Parameter Description**

| Parameter | Description |
|---|---|
| *ipv6-address* | IPv6 address of the authentication-exempted network resources |
| *ip-address* | IPv4 address of the authentication-exempted network resources |
| *ip-mask* | IPv4 address mask of the authentication-exempted network resources (optional) |
| **arp** | If the ARP Check is enabled on the access device, the keyword arp is needed for ARP binding of the authentication-exempted network resources (optional). It is necessary for IPv4 network resources only. |

**Defaults** No authentication-exempted network resource is set.

**Command Mode** Global configuration mode

**Usage Guide** When Web/802.1x authentication is enabled, all users must pass Web/client authentication to access network resources. This command is used to make certain network resources available to

unauthenticated users. All users can access the authentication-exempted Web sites.
Up to 50 authentication-exempted users are supported.

**Configuration Examples** The following example sets the Web site with IP address 172.16.0.1 as the authentication-exempted resource.

```
Ruijie(config)# http redirect direct-site 172.16.0.1
```

**Related Commands**

| Command | Description |
|---|---|
| **show http redirect** | Displays the HTTP redirection configuration. |

**Platform Description** N/A

## 1.16 http redirect port

Use this command to redirect users' HTTP redirection request to a certain destination port.
Use the **no** form of this command to restore the default setting.
**http redirect port** *port-num*
**no http redirect port** *port-num*

**Parameter Description**

| Parameter | Description |
|---|---|
| *port-num* | Destination port of the HTTP request |

**Defaults** The default is port 80.

**Command Mode** Global configuration mode

**Usage Guide** When you access the network resource, you send HTTP packets. The access device can intercept such HTTP packets to detect your access. If the access device detects that an unauthenticated user is accessing the network resource, it stops the users with an authentication page/client download page.
By default, the access device intercepts users' HTTP packets with port 80 to check whether they are accessing network resources.
This command is used to change the destination port of HTTP packets that are intercepted by the access device.
Up to 10 ports can be configured, including port 80.

**Configuration Examples** The following example redirects users' HTTP requests with port 8080.

```
Ruijie(config)# http redirect port 8080
```

The following example does not redirect users' HTTP requests with port 80.

```
Ruijie(config)# no http redirect port 80
```

**Related Commands**

| Command | Description |
| --- | --- |
| **show http redirect** | Displays the HTTP redirection configuration. |

**Platform Description** N/A

## 1.17 http redirect session-limit

Use this command to set the total number of HTTP sessions that can be originated by an unauthenticated user, or the maximum number of HTTP sessions that can be originated by an unauthenticated user connected to each port.
Use the **no** form of this command to restore the default setting.
**http redirect session-limit** *session-num* [ **port** *port-session-num* ]
**no http redirect session-limit**

**Parameter Description**

| Parameter | Description |
| --- | --- |
| *session-num* | Total number of HTTP sessions that can be originated by an unauthenticated user, in the range from 1 to 255. |
| *port-session-num* | The maximum number of HTTP sessions that can be originated by an unauthenticated user connected to each port, in the range from 1 to 65535. |

**Defaults** Totally 255 HTTP sessions can be originated by an unauthenticated user, and 300 HTTP sessions that can be originated by an unauthenticated user connected to each port.

**Command Mode** Global configuration mode

**Usage Guide** To prevent HTTP attacks caused by unauthenticated users from using up the TCP connections of the access device, the maximum number of HTTP sessions by unauthenticated users must be limited on the access device.
In addition to authentication, other programs may also occupy HTTP sessions. Therefore, it is not recommended that the maximum number of HTTP sessions by unauthenticated users be 1

**Configuration Examples** The following example sets the maximum number of HTTP sessions originated by an unauthenticated user to 4.

```
Ruijie(config)# http redirect session-limit 4
```

**Related**

| Command | Description |
| --- | --- |

| Commands | | |
|---|---|---|
| | **show http redirect** | Displays the HTTP redirection configuration. |

**Platform Description** N/A

## 1.18 http redirect timeout

Use this command to set the timeout for the redirection connection maintenance.
Use the **no** form of this command to restore the default setting.
**http redirect timeout** *seconds*
**no http redirect timeout**

| Parameter Description | Parameter | Description |
|---|---|---|
| | *seconds* | Set the timeout for the redirection connection maintenance, in the range from 1 to 10 in the unit of seconds. |

**Defaults** The default is 3 seconds.

**Command Mode** Global configuration mode

**Usage Guide** This command is used to set the timeout for the redirection connection maintenance. After the three-way handshake succeeds, the redirection connection is maintained until the user sends an HTTP GET/HEAD packet and the system returns an HTTP redirection packet. This timeout is set to prevent users from occupying TCP connections for long without sending any GET/HEAD packets.

**Configuration Examples** The following example sets the timeout for the redirection connection maintenance to 4 seconds.

```
Ruijie(config)# http redirect timeout 4
```

| Related Commands | Command | Description |
|---|---|---|
| | **show http redirect** | Displays the HTTP redirection configuration. |

**Platform Description** N/A

## 1.19 ip

Use this command to set an IP address for the portal server.
Use the **no** form of this command to restore the default setting.

**port** { *ip-address* }
**no port**

**Parameter Description**

| Parameter | Description |
|---|---|
| *ip-address* | The IPv4 address of the portal server |

**Defaults** No IP address is set for the portal server by default.

**Command Mode** Template configuration mode

**Usage Guide** This command takes place of the **http redirect** [*ip-address*] command, which is now hidden as a compatible command.

**Configuration Examples** The following example sets the IP address of the eportalv1 template to 172.16.0.1.

```
Ruijie(config.tmplt.eportalv1)#ip 172.16.0.1
Ruijie(config.tmplt.eportalv1)#
```

**Related Commands**

| Command | Description |
|---|---|
| N/A | N/A |

**Platform Description** N/A

## 1.20 ip portal source-interface

Use this command to specify a communication port for the portal server.
Use the **no** form of this command to restore the default setting.
**ip portal source-interface** *interface-type interface-num*
**no ip portal source-interface**

**Parameter Description**

| Parameter | Description |
|---|---|
| *interface-type* | Port type |
| *interface-num* | Port No. |

**Defaults** No communication interface is specified by default.

**Command Mode** Global configuration mode

**Usage Guide** N/A

**Configuration Examples** The following example specifies an aggregate port as the communication port.

```
Ruijie (config)# ip portal source-interface Aggregateport 1
```

**Platform Description** N/A

## 1.21 iportal nat enable

Use this command to enable NAT function for local Web authentication.

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

**iportal nat enable**

**no iportal nat enable**

**Parameter Description**

| Parameter | Description |
|---|---|
| N/A | N/A |

**Defaults** NAT is disabled by default.

**Command Mode** Global configuration mode

**Usage Guide** N/A

**Configuration Examples** The following example enables NAT function for local Web authentication.

```
Ruijie (config)# iportal nat enable
```

**Platform Description** N/A

## 1.22 iportal retransmit

Use this command to set the retransmission count of HTTP packets.

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

**iportal retransmit** *times*

**no iportal retransmit**

**Parameter Description**

| Parameter | Description |
|---|---|
| *times* | Retransmission count |

**Defaults** The retransmission count of HTTP packets is 3 by default.

**Command Mode** Global configuration mode

**Usage Guide** N/A

**Configuration Examples** The following example sets the retransmission count of HTTP packets to 5.

```
Ruijie (config)# iportal retransmit 5
```

**Platform Description** N/A

## 1.23 iportal service

Use this command to configure a service template.
Use the **no** form of this command to restore the default setting.
**iportal service [ internet** *internet-name***] [ local** *local-name* **]**
**no iportal service [ internet** *internet-name***] [ local** *local-name* **]**

**Parameter Description**

| Parameter | Description |
|---|---|
| *internet-name* | External service name |
| *local-name* | Local service name |

**Defaults** No service template is configured by default.

**Command Mode** Global configuration mode

**Usage Guide** N/A

**Configuration Examples** The following example configures a local service template.

```
Ruijie (config)# iportal service local local-srv
```

**Platform Description** N/A

## 1.24 key

Use this command to set the communication key between the Wechat access device and the

authentication server.

Use the **no** form of this command to clear the communication key.

**key** *key-string*

**no key**

**Parameter Description**

| Parameter | Description |
|---|---|
| *key-string* | Communication key between the Wechat access device and the authentication server |

**Defaults** No key is set by default.

**Command Mode** Template configuration mode

**Usage Guide** To use the Web authentication function, the communication key between the Wechat access device and the authentication server must be set as the same.

**Configuration Examples** The following example sets the communication key between the Wechat access device and the authentication server to ruijie.

```
Ruijie(config.tmplt.wechat)#key ruijie
```

**Related Commands**

| Command | Description |
|---|---|
| N/A | N/A |

**Platform Description** N/A

## 1.25 login-popup

Use this command to configure a pre-login popup advertisement.

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

**login-popup** *url-string*

**no login-popup**

**Parameter Description**

| Parameter | Description |
|---|---|
| *url-string* | Ad URL |

**Defaults** No pre-login popup advertisement is configured by default.

**Command** Template configuration mode

**Mode**

**Usage Guide** The URL of the popup advertisement should begin with “http://” or “https://”.

**Configuration Examples** The following example configures a pre-login popup advertisement.

```
Ruijie(config.tmplt.iportal)#login-popup http://www.ruijie.com.cn
```

**Platform Description** N/A

## 1.26 nas-ip

Use this command to configure the IP address of the Wechat access device.

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

**nas-ip** { *ip-address* }

**no nas-ip**

**Parameter Description**

| Parameter | Description |
|---|---|
| *ip-address* | IPv4 address |

**Defaults** No IPv4 address is configure for the Wechat access device by default.

**Command Mode** Template configuration mode

**Usage Guide**

Make sure the IPv4 address is not pass-through.

**Configuration Examples** The following example configures 192.168.0.1 as the IPv4 address of the Wechat access device.

```
Ruijie(config.tmplt.wechat)#nas-ip 192.168.0.1
```

**Platform Description** N/A

## 1.27 online-popup

Use this command to configure a post-login popup advertisement.

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

**online-popup** *url-string*

**no online-popup**

Parameter

| Parameter | Description |
|---|---|

| Description | | |
|---|---|---|
| | *url-string* | Ad URL |

Defaults: No post-login popup advertisement is configured by default.

Command Mode: Template configuration mode

Usage Guide: The URL of the popup advertisement should begin with “http://” or “https://”.

Configuration Examples: The following example configures a post-login popup advertisement.

```
Ruijie(config.tmplt.iportal)#online-popup http://www.ruijie.com.cn
```

Platform Description: N/A

## 1.28 page-suite

Use this command to configure a resource suite for the login page.
Use the **no** form of this command to restore the default setting.
**page-suite** *filename*
**no page-suite**

| **Parameter Description** | **Parameter** | **Description** |
|---|---|---|
| | *filename* | Resource suite name |

**Defaults**: The installed resource suite is used by default.

**Command Mode**: Template configuration mode

**Usage Guide**: Make sure to download page resource files in the directory of portal/zip under FLASH before.

**Configuration Examples**: The following example configures a page suite for internal Web authentication.

```
Ruijie(config.tmplt.iportal)#page-suite ruijiepage
```

**Platform Description**: N/A

## 1.29 port

Use this command to set a surveillance port for the portal server.
Use the **no** form of this command to restore the default setting.
**port** { *port-num* }
**no port**

**Parameter Description**

| Parameter | Description |
|---|---|
| *port* | The surveillance port of the portal server, which is on only the 2nd generation portal server, |

**Defaults** The default is 50100 based on the UDP protocol.

**Command Mode** Template configuration mode

**Usage Guide** N/A

**Configuration Examples** The following example sets the surveillance port number of the eportalv2 server to 10000.

```
Ruijie(config.tmplt.eportalv2)#port 10000
```

**Related Commands**

| Command | Description |
|---|---|
| N/A | N/A |

**Platform Description** N/A

## 1.30 redirect

Use this command to set the redirect packet protocol.
Use the **no** form of this command to restore the default setting.
**redirect** { *http* | *js* }
**no redirect**

**Parameter Description**

| Parameter | Description |
|---|---|
| *http* | HTTP 302 |
| *js* | HTTP 200 |

**Defaults** The default is HTTP 200.

**Command Mode** Template configuration mode

**Usage Guide** N/A

**Configuration Examples** The following example sets the redirect packet protocol to HTTP 200.

```
Ruijie(config.tmplt.eportalv2)#redirect http
```

**Related Commands**

| Command | Description |
| --- | --- |
| N/A | N/A |

**Platform Description** N/A

## 1.31 service-url

Use this command to configure the URL of the authentication server for Wechat access.

**service-url** *url-string*

**no service-url**

**Parameter Description**

| Parameter | Description |
| --- | --- |
| *url-string* | URL of the authentication server for Wechat access |

**Defaults** No URL of the authentication server for Wechat access is configured by default.

**Command Mode** Template configuration mode

**Usage Guide**

The URL can be configured in the format of either IP address or domain name. It cannot start with http:// or https://.

**Configuration Examples** The following example configures the URL of the authentication server for Wechat access.

```
Ruijie(config.tmplt.wechat)#service-url wmc.ruijie.com.cn
```

**Platform Description** N/A

## 1.32 show web-auth acl

Use this command to display blacklists and whitelists.

**show web-auth acl [ black-ip | black-port | black-url | white-url ]**

**Parameter Description**

| Parameter | Description |
| --- | --- |
| *N/A* | N/A |

**Command Mode** Privileged EXEC mode

**Usage Guide** N/A

**Configuration Examples** The following example displays blacklists and whitelists.

```
Ruijie# show web-auth acl
Black URL List:0
-------------------------------------------------------


Black IP List:0
-------------------------------------------------------


White URL List:0
-------------------------------------------------------
```

**Platform Description** N/A

## 1.33 show http redirect

Use this command to display http redirect settings.

**show http redirect**

**Parameter Description**

| Parameter | Description |
| --- | --- |
| N/A | N/A |

**Command Mode** Privileged EXEC mode

**Usage Guide** N/A

**Configuration Examples** The following example displays http redirect settings.

```
Ruijie# show http redirect
HTTP redirection settings:
  server:       192.168.197.79
  port:         80 443
  homepage:     http://192.168.197.79:8080/eportal/index.jsp
  session-limit: 255
  timeout:      3
Direct sites: 3
  Address        Mask          ARP Binding
  ---------------- ---------------- -----------
  192.168.5.120   255.255.255.255 Off
  192.168.58.112  255.255.255.255 Off
  192.168.197.0   255.255.255.0   Off
Direct arps: 0
  Address        Mask
  ---------------- ----------------
Direct hosts: 0
  Address        Mask          Port          ARP Binding
  ---------------- ---------------- --------------- -------------
```

**Platform Description** N/A

## 1.34 show web-auth control

Use this command to display the authentication configuration.

**show web-auth control**

**Parameter Description**

| Parameter | Description |
|---|---|
| N/A | N/A |

**Defaults** N/A

**Command Mode** Privileged EXEC mode

**Usage Guide** N/A

**Configuration** The following example displays the authentication configuration and statistics information on the

**Examples** interface.

```
Ruijie(config)#show web-auth control
 Port                   Control  Server Name         Online User Count
 ---------------------- -------- ------------------- -----------------
 GigabitEthernet 0/1      On      <not configured>     0
Ruijie(config)#
```

| Field | Description |
|---|---|
| Port | Name of the authentication port. |
| Control | Displays whether the Web authentication is enabled on the port or not. |
| Server Name | The customized server name on the port. **<not configured>** indicates the server name has not been configured. |
| Online User Count | The number of online users on this port. |

**Related Commands**

| Command | Description |
|---|---|
| N/A | N/A |

**Platform Description** N/A

## 1.35 show web-auth direct-arp

Use this command to display the address range of the authentication-exempted ARP.

**show web-auth direct-arp**

**Parameter Description**

| Parameter | Description |
|---|---|
| N/A | N/A |

**Defaults** N/A

**Command Mode** Privileged EXEC mode

**Usage Guide** I N/A

**Configuration Examples** The following example displays the address range of the authentication-exempted ARP.

```
Ruijie(config)#show web-auth direct-arp
Direct arps:
  Address        Mask
  --------------- ---------------
```

```
  1.1.1.1         255.255.255.255
  2.2.2.2         255.255.255.255
Ruijie(config)#
```

| Field | Description |
|---|---|
| Address | IPv4 address. |
| Mask | IPv4 mask. |

**Related Commands**

| Command | Description |
|---|---|
| N/A | N/A |

**Platform Description** N/A

## 1.36 show web-auth direct-host

This command is used to display the Web authentication-exempted users.

**show web-auth direct-host**

**Parameter Description**

| Parameter | Description |
|---|---|
| N/A | N/A |

**Defaults** N/A

**Command Mode** Privileged EXEC mode

**Usage Guide** N/A

**Configuration Examples** The following example displays the Web authentication-exempted users.

```
Ruijie# show web-auth direct-host
Direct hosts:
  Address           Mask             Port        ARP Binding
  ---------------- ----------------- ---------- ------------
  192.168.0.1      255.255.255.255   Fa0/2       On
  192.168.4.11     255.255.255.255   Fa0/10       On
  192.168.5.0      255.255.255.0      Fa0/16       Off
```

| Field | Description |
|---|---|

| | |
|---|---|
| Address | IP address of the user free of authentication |
| Mask | IP address mask of the user free of authentication |
| Port | Access device port that is bound with the user's IP address |
| ARP Binding | Enable/Disable ARP binding |

**Related Commands**

| Command | Description |
|---|---|
| N/A | N/A |

**Platform Description** N/A

## 1.37 show web-auth direct site

Use this command to display the range of the Web authentication-exempted network resources.

**show web-auth direct-site**

**Parameter Description**

| Parameter | Description |
|---|---|
| N/A | N/A |

**Defaults**

**Command Mode** Privileged EXEC mode

**Usage Guide** N/A

**Configuration Examples** The following example displays the range of the Web authentication-exempted network resources without authentication.

```
Ruijie(config)#show web-auth direct-site
Direct sites:
  Address        Mask           ARP Binding
  ---------------  ---------------  -----------
  1.1.1.1        255.255.255.255 Off
  2.2.2.2        255.255.255.255 On
Ruijie(config)#
```

| Field | Description |
|---|---|
| Address | IP address. |

| | |
|---|---|
| Mask | IP mask. |
| ARP Binding | Displays whether the ARP binding function is enabled. |

**Related Commands**

| Command | Description |
|---|---|
| N/A | N/A |

**Platform Description** N/A

## 1.38 show web-auth noise

Use this command to display the anti-noise configuration.

**show web-auth noise**

**Parameter Description**

| Parameter | Description |
|---|---|
| N/A | N/A |

**Defaults** N/A

**Command Mode** Privileged EXEC mode

**Usage Guide** N/A

**Configuration Examples** The following example displays the anti-noise configuration.

```
Ruijie#show web-auth noise
Noise Enable:    On
  Aging Timer:    1min
  Hit  Counts:    3
```

**Related Commands**

| Command | Description |
|---|---|
| N/A | N/A |

**Platform Description** N/A

## 1.39 show web-auth parameter

Use this command to display the HTTP redirect configuration.

**show web-auth parameter**

**Parameter Description**

| Parameter | Description |
|---|---|
| N/A | N/A |

**Defaults** N/A

**Command Mode** Privileged EXEC mode

**Usage Guide** N/A

**Configuration Examples** The following example displays the HTTP redirect configuration

```
Ruijie# show web-auth parameter
  session-limit: 10
  timeout:        5
```

| Field | Description |
|---|---|
| session-limit | Total number of HTTP sessions that are created by an unauthenticated user. |
| timeout | Timeout interval of the redirection connection. |

**Related Commands**

| Command | Description |
|---|---|
| N/A | N/A |

**Platform Description** N/A

## 1.40 show web-auth portal-check

Use this command to display the portal-check configuration.

**show web-auth portal-check**

**Parameter Description**

| Parameter | Description |
|---|---|
| N/A | N/A |

**Defaults** N/A

**Command Mode** Privileged EXEC mode

**Usage Guide** N/A

**Configuration Examples** The following example displays the portal-check configuration.

```
Ruijie#sh web portal-check
Check:        Enable
  Interval:    3s
  Timeout:     5s
  Retransmit:  3
Escape:       Enable
Nokick:       Disable
```

**Platform Description** N/A

## 1.41 show web-auth rdport

Use this command to display the TCP interception port.

**show web-auth rdport**

**Parameter Description**

| Parameter | Description |
|---|---|
| N/A | N/A |

**Defaults** N/A

**Command Mode** Privileged EXEC mode

**Usage Guide** N/A

**Configuration Examples** The following example displays the TCP interception port.

```
Ruijie#show web-auth rdport
Rd-Port:
80 443
Ruijie#
```

**Related Commands**

| Command | Description |
|---|---|

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

**Platform Description** N/A

## 1.42 show web-auth template

Use this command to display the portal server configuration.

**show web-auth template**

**Parameter Description**

| Parameter | Description |
|---|---|
| N/A | N/A |

**Defaults** N/A

**Command Mode** Privileged EXEC mode

**Usage Guide** Use this command to display the portal server configuration.

**Configuration Examples** The following example displays the port server configuration.

```
Ruijie#show web-auth template
Webauth Template Settings:
-------------------------------------------------------------
  Name:      eportalv1
  Url:       http://17.17.1.21:8080/eportal/index.jsp
  Ip:        17.17.1.21
  BindMode:  ip-mac-mode
  Type:      v1
-------------------------------------------------------------
  Name:      eportalv2
  Url:       http://17.17.1.21:8080/eportal/index.jsp
  Ip:        17.17.1.21
  BindMode:  ip-only-mode
  Type:      v2
  Port:      50100
  Acctmlist:
  Authmlist:
Ruijie#
```

| Field | Description |
|---|---|

| | |
|---|---|
| Name | Template name. |
| Url | Server homepage address. |
| Ip | Server IP address. |
| Type | Server type, including the first generation portal server v1, the second generation portal server v2 and the intra portal server intra. |
| Port | The protocol packet communication port of the server, which is on only the second generation portal server. |
| Acctmlist | Accounting method list name, which is on only the second generation portal server and the intra portal server |
| Authmlist | Authentication method list name. which is on only the second generation portal server and the intra portal server |

**Related Commands**

| Command | Description |
|---|---|
| N/A | N/A |

**Platform Description** N/A

## 1.43 show web-auth user

Use this comma to display the online information, including IP address, interface, and online duration, of all users or the specified users.

**show web-auth user** { **all** | **ip** *ip-address* | **mac** *mac-address* | **name** *name-string* | **session-id** *num*| **escape** }

**Parameter Description**

| Parameter | Description |
|---|---|
| *ip-address* | IPv4 address of the user. |
| *mac-address* | MAC address of the user. |
| *name-string* | User name. |
| *num* | AAA session ID. |

**Defaults** N/A

**Command Mode** Privileged EXEC mode

**Usage Guide** N/A

**Configuration Examples** The following example displays the global Web authentication configuration and statistics.

```
Ruijie# show web-auth user all
Current user num :  4, online 2

Address         Online   Time Limit    Time Used    Status  Name
--------------- -------  ------------ -------------- -------- ---------
192.168.0.11    On      0d 01:00:00   0d 00:15:10    Active
192.168.0.13    On      0d 01:00:00   0d 00:00:59    Active   111
192.168.0.25    Off     0d 01:00:00   0d 00:00:59    Create
192.168.0.46    Off     0d 01:00:00   0d 01:00:00    Destroy  222

Ruijie# show web-auth user ip 192.168.0.11
Address      :   192.168.0.11
 Mac          :   00d0.f800.2233
 Port         :   Gi0/2
 Online       :   On
 Time Limit   :   0d 01:00:00
 Time Used    :   0d 00:15:10
 Time Start   :   2009-02-22 20:05:10
 Status       :   Active
```

| Field | Description |
|---|---|
| Address | IP address of the user |
| Mac | MAC address of the user |
| Port | Access device port connected to the user |
| Online | Whether the user is online |
| Time Limit | Available duration of the user. 0 means unlimited. |
| Time Used | Online duration of the user |
| Time Start | Time when the user passes authentication and gets online |
| Status | User status. Active means the user is normally online, Create means the user is created without any settings, Destroy means the user is deleted with its settings not cleared. |

**Related Commands**

| Command | Description |
|---|---|
| N/A | N/A |

**Platform Description** N/A

## 1.44 temporary-permit

Use this command to enable the temporary permit function.
Use the **no** form of this command to disable the function.
**temporary-permit** *seconds*
**no temporary-permit**

**Parameter Description**

| Parameter | Description |
|---|---|
| *seconds* | The duration of temporary permit in the unit of seconds. The recommended value ranges from 30s to 60s. |

**Defaults** N/A

**Command Mode** Template configuration mode

**Usage Guide**

**Configuration Examples** The following example configures the temporary permit.

```
Ruijie(config.tmplt.wechat)# temporary-permit 30
```

**Platform Description** N/A

## 1.45 time-interval

Use this command to set the interval for popup advertisement.
Use the **no** form of this command to restore the default setting.
**time-interval** *{ hour }*
**no time-interval**

**Parameter Description**

| Parameter | Description |
|---|---|
| *hour* | The popup interval in the range from 0 to 24 in the unit of hours |

**Defaults** The default is 1 hour.

**Command Mode** Template configuration mode

**Usage Guide** If the parameter hour is 0, it means no popup interval.

**Configuration Examples** The following example sets the interval for popup advertisement to 2 hours.

```
Ruijie(config.tmplt.iportal)#time-interval 2
```

**Platform Description** N/A

## 1.46 url

Use this command to set the portal server URL.
Use the **no** form of this command to restore the default setting.
**url** *url-string*
**no url**

**Parameter Description**

| Parameter | Description |
|---|---|
| *url-string* | Portal server URL, starting with **http://** or **https://**. The maximum length of this address is 255 bytes. |

**Defaults** No portal server URL is set by default.

**Command Mode** Template configuration mode

**Usage Guide** This command takes place of the **http redirect homepage** [ *url-string* ] command, which is now hidden as a compatible command.,
If no URL is specified, the default URL in the **http://[ ip-address ]** format will be adopted, among which **ip-address** is the IP address of the server.

**Configuration Examples** The following example sets the eportalv1 template URL to **http://www.web-auth.net/login**.

```
Ruijie(config.tmplt.eportalv1)#url http://www.web-auth.net/login
```

**Related Commands**

| Command | Description |
|---|---|
| N/A | N/A |

**Platform Description** N/A

## 1.47 version

Use this command to specify the authentication version for Wechat access.

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

**version {1.0 | 16wifi | 3.0}**

**no version**

**Parameter Description**

| Parameter | Description |
|---|---|
| N/A | N/A |

**Defaults** The default is V1.0 for the 11.1(5)B8 version while V3.0 for the 11.1(5)B9 version.

**Command Mode** Template configuration mode

**Usage Guide** The 16wifi version supports QR code scan in Wechat.

**Configuration Examples** The following example specifies the authentication version for Wechat access.

```
Ruijie(config.tmplt.wechat)#version 16wifi
```

**Platform Description** N/A

## 1.48 webauth

Use this command to enable Web authentication.

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

**webauth**

**no webauth**

**Parameter Description**

| Parameter | Description |
|---|---|
| N/A | N/A |

**Defaults** Web authentication is disabled by default.

**Command Mode** WLANSEC configuration mode

**Usage Guide** N/A

**Configuration Examples** The following example enables Web authentication.

```
Ruijie (config)# webauth
```

**Platform Description** N/A

## 1.49 web-auth accounting jitter-off

Use this command to enable jitter-off accounting function.

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

**web-auth accounting jitter-off**

**no web-auth accounting jitter-off**

**Parameter Description**

| Parameter | Description |
|---|---|
| N/A | N/A |

**Defaults** Jitter-off accounting function is disabled by default.

**Command Mode** Global configuration mode

**Usage Guide** N/A

**Configuration Examples** The following example enables jitter-off accounting function.

```
Ruijie (config)# web-auth accounting jitter-off
```

**Platform Description** N/A

## 1.50 web-auth accounting v2

Use this command to specify an accounting method.

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

**web-auth accounting v2 { default |** *name* **}**

**no web-auth accounting v2 { default |** *name* **}**

**Parameter Description**

| Parameter | Description |
|---|---|
| *name* | The accounting method |

**Defaults** No accounting method is specified by default.

**Command Mode** Global configuration mode/Template configuration mode

**Usage Guide** N/A

**Configuration Examples** The following example specifies an accounting method.

```
Ruijie (config.tmplt.eportalv2)# web-auth accounting v2 default
```

**Platform Description** N/A

## 1.51 web-auth authentication v2

Use this command to specify an authentication method.

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

**web-auth authentication v2 [ default |** *name* **]**

**no web-auth authentication v2 [ default |** *name* **]**

**Parameter Description**

| Parameter | Description |
|---|---|
| *name* | The authentication method |

**Defaults** The default method is the same as AAA.

**Command Mode** Global configuration mode

**Usage Guide** N/A

**Configuration Examples** The following example specifies an authentication method.

```
Ruijie (config.tmplt.eportalv2)# web-auth authentication v2 default
```

**Platform Description** N/A

## 1.52 web-auth acl

Use this command to configure a blacklist or whitelist.

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

**web-auth acl** { **black-ip** *ip*|**black-port** *port* | **black-url** *name* | **white-url** *name* }

**no web-auth acl** { **black-ip** *ip* | **black-port** *port* **| black-url** *name* **| white-url** *name* }

**Parameter Description**

| Parameter | Description |
|---|---|
| **ip** | Blacklist /Whitelist IP address |
| **port** | Blacklist /Whitelist Port number in the range from 1 to 65535 |
| **name** | Blacklist /Whitelist URL |

**Defaults** N/A

**Command Mode** Global configuration mode/WLAN security configuration mode

**Usage Guide**

**Configuration Examples** The following example configures a blacklist and a whitelist.

```
Ruijie (config)# web-auth acl black-ip 192.168.1.2
Ruijie (config)# web-auth acl white-url www.ruijie.com.cn
```

**Platform Description** N/A

## 1.53 web-auth bind-portal

Use this command to bind MAC SMS authentication to the portal server.

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

**web-auth bind-portal** *string* [ **type** { **local-spec** | **group-spec** } ]

**no web-auth bind-portal**

**Parameter Description**

| Parameter | Description |
|---|---|
| *string* | Portal server name |

**Defaults** N/A

**Command Mode** WLAN security configuration mode

**Usage Guide** N/A

**Configuration Examples** The following example binds MAC SMS authentication to the portal server.

```
Ruijie (wlansec)# web-auth bind-portal eportalv2
```

| | |
|---|---|
| **Platform Description** | N/A |

## 1.54 web-auth dhcp-check

Use this command to enable DHCP IP address check.

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

**web-auth dhcp-check**

**no web-auth dhcp-check**

**Parameter Description**

| Parameter | Description |
|---|---|
| N/A | N/A |

**Defaults** DHCP IP address check is disabled by default.

**Command Mode** Global configuration mode

**Usage Guide** Only users whose IP addresses are allocated by DHCP are allowed to take authentication.

**Configuration Examples** The following example enables DHCP IP address check.

```
Ruijie (config)# web-auth dhcp-check
```

| | |
|---|---|
| **Platform Description** | N/A |

## 1.55 web-auth direct-host

Use this command to set the authentication-exempted IP/MAC address range.

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

**web-auth direct-host** { *ipv4-address* [ i*p-mask* ] [ **arp** ] | *ipv6-address* | *mac-address*} [ **port** *interface-name* ]

**no web-auth direct-host** { *ipv4-address* [ i*p-mask* ] | *ipv6-address* | *mac-address*}

**Parameter Description**

| Parameter | Description |
|---|---|
| *ipv4-address* | IPv4 address of authentication-exempted user |
| *Ipv6-address* | IPv6 address of authentication-exempted user |
| *ip-mask* | Mask of the IPv4 address free of authentication (optional). |
| **port** *interface-name* | Binds user's IP address with a port of the access device (optional). |

| | |
|---|---|
| **arp** | If ARP CHECK is enabled on the access device, keyword arp is needed for ARP binding of the IP address used by users free of authentication (optional). It is necessary for IPv4 addresses only. |
| *mac-address* | MAC address of authentication-exempted user |

**Defaults** No user is exempted from authentication. All users must pass the Web authentication to access the restricted network resources.

**Command Mode** Global configuration mode

**Usage Guide** When a user is set to be exempted from authentication, it can access all reachable network resources without Web authentication.
Up to 50 users can be set to be exempted from authentication.

**Configuration Examples** The following example sets the user with the IP address 172.16.0.1 to be exempted from authentication.

```
Ruijie(config)# web-auth direct-host 172.16.0.1
```

The following example sets the user with the MAC address 0000:5e00:0101 to be exempted from authentication.

```
Ruijie(config)# web-auth direct-host 0000:5e00:0101
```

**Related Commands**

| Command | Description |
|---|---|
| **show web-auth direct-host** | Displays the users free of Web authentication. |

**Platform Description** N/A

## 1.56 web-auth dkey-compatible url-parameter

Use this command to configure the DKEY-compatible URL string.
Use the **no** form of this command to restore the default setting.
**web-auth dkey-compatible url-parameter** *string*
**no web-auth dkey-compatible url-parameter**

**Parameter Description**

| Parameter | Description |
|---|---|
| *string* | DKEY-compatible URL string |

**Defaults** The DKEY-compatible URL string is not configured by default.

**Command** Global configuration mode

**Mode**

**Usage Guide** N/A

**Configuration Examples** The following example configures the DKEY-compatible URL string as login.

```
Ruijie(config)# web-auth dkey-compatible url-parameter login
```

**Related Commands**

| Command | Description |
|---|---|
| N/A | N/A |

**Platform Description** N/A

## 1.57 web-auth enable

Use this command to enable the Web authentication function on a port. This command is compatible with the **web-auth port-control** command.
Use the **no** form of this command to restore the default setting.
**web-auth enable** [ **eportalv1 | eportalv2 |** *template-name* ]
**no web-auth enable**

**Parameter Description**

| Parameter | Description |
|---|---|
| **eportalv1** | Applies the first generation authentication template. |
| **eportalv2** | Applies the second generation authentication template. |
| *template-name* | Customized template. |

**Defaults** The Web authentication function is disabled on the port by default.
The **default** template is eportalv1.

**Command Mode** Interface configuration mode

**Usage Guide** To ensure the Web authentication function, the authentication page URL should be configured. Because template applications are integrated into the controlled switch, the template or the server applications of the interface where the Web authentication function is disabled will be automatically cleared. This command is compatible with the original command that used to apply the template or server application in the global configuration mode.

**Configuration Examples** The following example enables the Web authentication function on gigabitEthernet 0/14.

```
Ruijie(config)# interface GigabitEthernet 0/14
Ruijie(config-if-GigabitEthernet 0/14)# web-auth enable
```

**Related Commands**

| Command | Description |
| --- | --- |
| N/A | N/A |

**Platform Description** N/A

## 1.58 web-auth logging enable

Use this command to enable the Web authentication syslog function.
Use the **no** form of this command to restore the default setting.
**web-auth logging enable** { *num* }
**no web-auth logging enable**

**Parameter Description**

| Parameter | Description |
| --- | --- |
| *num* | The syslog printing rate, indicating how many syslog entries can be printed in a second. The value is in the range from 0 to 65535. 0 indicates no limit. |

**Defaults** This function is disabled by default.

**Command Mode** Global configuration mode

**Usage Guide** This command is used to limit the syslog printing rate for only the functional module.

**Configuration Examples** The following example enables the syslog printing with no rate limit.

```
Ruijie(config)# web-auth logging enable 0
```

**Related Commands**

| Command | Description |
| --- | --- |
| N/A | N/A |

**Platform Description** N/A

## 1.59 web-auth noise

Use this command to configure the anti-noise policy.
Use the no form of this command to restore the default setting.

**web-auth noise** [ **aging** *agmin* ] [ **hit** *times* ]
**no web-auth noise**

**Parameter Description**

| Parameter | Description |
|---|---|
| *agmin* | Anti-noise aging time in the range from 1 to 30 in the unit of minutes. The default is 1 minute. |
| *times* | Anti-noise time limit in the range from 3 to 100. The default is 3. IP addresses accessing for the time limit are thought as noise. |

**Defaults** The anti-noise policy is not configured by default.

**Command Mode** Global configuration mode

**Usage Guide** N/A

**Configuration Examples** The following example configures the anti-noise policy.

```
Ruijie (config)# web-auth noise aging 1 hit 3
```

**Platform Description** N/A

## 1.60 web-auth offline-detect

Use this command to configure the online keepalive time for users. Authenticated online users are forced to go offline if their traffic is lower than the specified threshold within a specified interval.
**web-auth offline-detect interval** *interval* **flow** *thredshold*

Use this command to restore the default setting.
**default web-auth offline-detect**

Use this command to disable online detection for users.
**no web-auth ping**

**Parameter Description**

| Parameter | Description |
|---|---|
| *interval* | The offline detection interval. The value ranges from 1 min to 65,535 min. The default value is 15 min. |
| *threshold* | The traffic threshold. The value ranges from 0 bytes to 4,294,967,294 bytes. The default value is 0, indicating that traffic detection is not performed. |

**Defaults** 15min

**Command Mode** WLANSEC configuration mode

**Usage Guide**

For 10.x versions, by default, traffic detection is disabled under WLANSEC but enabled under global configuration. Therefore, after an upgrade to 11.x versions, disable WLANSEC manually.

**Configuration Examples** The following example configures user detection under WLANSEC 1. If users' traffic is lower than 5k Bytes within 5minutes, they are forced to go offline.

```
Ruijie(config)#wlansec 1
Ruijie(config-wlansec)# web-auth offline-detect interval 5 flow 5120
```

**Verification** Run the **show running** command to display corresponding configuration of online detection for users.

**Platform Description** N/A

## 1.61 web-auth ping

Use this command to ping the portal server.

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

**web-auth ping** [ **interval** *minutes* ] [ **retry** *times* ]

**no web-auth ping**

**Parameter Description**

| Parameter | Description |
|---|---|
| *minutes* | Ping interval in the range from 1 to 65,535 in the unit of minute<br>The default is 1 minute. |
| *times* | Ping retries in the range from 0 to 65,535<br>The default is 3. |

**Defaults** This function is disabled by default.

**Command Mode** Global configuration mode

**Usage Guide** N/A

**Configuration Examples** The following example configures ping interval as 5 minutes and retries as 4.

```
Ruijie (config)# web-auth ping interval 5 rerty 4
```

**Platform Description** N/A

## 1.62 web-auth portal

Use this command to map different portal servers with users in different subnets.
Use the **no** form of this command to restore the default setting.
**web-auth portal { eportalv1 | eportalv2 | iportal | wechat | wifidog |** *name* **}**
**no web-auth portal { eportalv1 | eportalv2 | iportal | wechat | wifidog |** *name* **}**

**Parameter Description**

| Parameter | Description |
|---|---|
| *name* | Portal server name |

**Defaults** This function is disabled by default.

**Command Mode** Global configuration mode

**Usage Guide** N/A

**Configuration Examples** The following example maps different portal servers with users in different subnets.

```
Ruijie(config)# web-auth portal eportalv2
```

**Platform Description** N/A

## 1.63 web-auth portal extension

Use this command to enable portal extension to support CMCC portal server.
Use the **no** form of this command to restore the default setting.
**no web-auth portal extension**
**default web-auth portal extension**

**Parameter Description**

| Parameter | Description |
|---|---|
| N/A | N/A |

**Defaults** By default, Ruijie portal server is supported.

**Command Mode** Global configuration mode

**Usage Guide** N/A

**Configuration Examples** The following example disables portal extension.

```
Ruijie (config)# no web-auth portal extension
Ruijie (config)# http redirect url-fmt ext1
```

**Platform Description** N/A

## 1.64 web-auth portal key

Use this command to set the communication key between the access device and the authentication server.
Use the **no** form of this command to clear the communication key between the redirected Web request of a user and the authentication server.
**web-auth portal key** *key-string*
**no web-auth portal key**

**Parameter Description**

| Parameter | Description |
|---|---|
| *key-string* | Communication key between the access device and the authentication server. The maximum length of the key is 255 bytes. |

**Defaults** No key is set by default.

**Command Mode** Global configuration mode

**Usage Guide** To use the Web authentication function, the communication key between the access device and the authentication server must be set.

**Configuration Examples** The following example sets the communication key between the access device and the authentication server to web-auth.

```
Ruijie(config)# web-auth portal key web-auth
```

**Related Commands**

| Command | Description |
|---|---|
| **http redirect** | Sets the IP address of the authentication server. |
| **http redirect homepage** | Sets the address of the authentication homepage. |
| **web-auth port-control** | Enables the Web authentication on the port. |

**Platform Description** N/A

## 1.65 web-auth portal-attribute

Use this command to configure transparent transmission of the 0x05 attribute of the portal protocol.
Use the **no** form of this command to restore the default setting.
**web-auth portal-attribute [5 | textinfo]**
**no web-auth portal-attribute [5 | textinfo]**

**Parameter Description**

| Parameter | Description |
|---|---|
| N/A | N/A |

**Defaults**

**Command Mode** Global configuration mode

**Usage Guide** In general, enable this function on the portal server when a device needs to upload the error flag (ErrID), or enable this function on the portal server (using Huawei portal protocol 2.0) when a device needs to upload prompts (TextInfo) from a third-party authentication device such as the RADIUS server.

**Configuration Examples** Both of the following examples configure transparent transmission of the 0x05 attribute of the portal protocol.

```
Ruijie (config)# web-auth portal-attribute 5
```

```
Ruijie (config)# web-auth portal-attribute textinfo
```

Platform Description N/A

## 1.66 web-auth portal-check

Use this command to enable portal server check.
Use the **no** form of this command to restore the default setting.
**web-auth portal-check** [ **interval** *intsec* ] [ **timeout** *tosec* ] [ **retransmit** *retires* ]
**no web-auth porta-check**

**Parameter Description**

| Parameter | Description |
|---|---|
| *Intsec* | Check interval in the range from 1 to 1,000 in the unit of seconds. The default is 10 seconds. |
| *tosec* | Timeout interval in the range from 1 to 1,000 in the unit of seconds. The default is 5 seconds. |
| *retries* | Retry count in the range from 1 to 100. The default is 3. |

**Defaults** Portal server check is disabled by default.

**Command Mode** Global configuration mode

**Usage Guide** It is recommended to use this command when there are multiple servers.

**Configuration Examples** The following example enables portal server check.

```
Ruijie (config)# web-auth portal-check interval 20 timeout 2 retransmit 2
```

Platform Description N/A

## 1.67 web-auth portal-escape

Use this command to enable portal-escape function.
Use the **no** form of this command to restore the default setting.
**web-auth portal-escape**
**no web-auth portal-escape**

**Parameter Description**

| Parameter | Description |
|---|---|
| N/A | N/A |

**Defaults** This function is disabled by default.

**Command Mode** Global configuration mode

**Usage Guide** Use this command together with **web-auth portal-check** command to sustain key services when the portal server is abnormal.

**Configuration Examples** The following example enables portal-escape function.

```
Ruijie (config)# web-auth portal-escape
```

**Platform Description** N/A

## 1.68 web-auth portal-valid unique-name

Use this command to enable uniqueness check of portal authentication accounts.

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

**web-auth portal-valid unique-name**

**no web-auth portal-vallid unique-name**

**Parameter Description**

| Parameter | Description |
|---|---|
| N/A | N/A |

**Defaults** This function is disabled by default.

**Command Mode** Global configuration mode

**Usage Guide**

Enable this feature when the portal server is needed to send preemption prompts to users.

**Configuration Examples** The following example enables uniqueness check of portal authentication accounts.

```
Ruijie (config)# web-auth portal-valid unique-name
```

**Platform Description** N/A

## 1.69 web-auth sms-flow

Use this command to configure the interval and threshold of flow detection.

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

**web-auth sms-flow [ interval** *interval* **] [threshold** *flows* **]**

**no web-auth sms-flow [ interval** *interval* **] [threshold** *flows* **]**

**Parameter Description**

| Parameter | Description |
|---|---|
| *interval* | Detection interval (minute) |
| *flows* | Traffic threshold (Kb) |

**Defaults** No interval and threshold is configured by default.

**Command Mode** Global configuration mode

**Usage Guide**

**Configuration Examples** The following example configures the interval and threshold of flow detection.

```
Ruijie (config)# web-auth sms-flow interval 5 flows 100
```

**Platform Description** N/A

## 1.70 web-auth sta-leave detection

Use this command to disable STA connectivity detection.
**no web-auth sta-leave detection**

Use this command to restore the default setting.
**default web-auth sta-leave detection**

**Parameter Description**

| Parameter | Description |
|---|---|
| N/A | N/A |

**Defaults** The STA connectivity detection is enabled by default.

**Command Mode** Global configuration mode

**Usage Guide**

**Configuration Examples** The following example disables STA connectivity detection.

```
Ruijie (config)# no web-auth sta-leave detection
```

**Platform Description** N/A

## 1.71 web-auth sta-perception enable

Use this command to enable smart authentication for Wechat access.
Use the **no** form of this command to restore the default setting.

**web-auth sta-perception enable**
**no web-auth sta-perception enable**

| Parameter Description | Parameter | Description |
|---|---|---|
| | N/A | N/A |

**Defaults** This function is disabled by default.

**Command Mode** Global configuration mode or WLAN security configuration mode

**Usage Guide** N/A

**Configuration Examples** The following example enables smart authentication for Wechat access.

```
Ruijie (config)# web-auth sta-perception enable
```

**Platform Description** N/A

## 1.72 web-auth template

Use this command to create the first generation authentication template and enter its configuration mode.
**web-auth template eportalv1**

Use this command to create the customized first generation authentication template and enter its configuration mode.
**web-auth template** { template-name } **v1**

Use this command to create the second generation authentication template and enter its configuration mode.
**web-auth template eportalv2**

Use this command to create the customized second generation authentication template and enter its configuration mode.
**web-auth template** { *template-name* } **v2**

Use this command to create the built-in authentication template and enter its configuration mode.
**web-auth template iportal**

Use this command to create the customized built-in authentication template and enter its configuration mode.

**web-auth template** { template-name } **intra**

Use this command to create the WiFiDog authentication template and enter its configuration mode.
**web-auth template wifidog**

Use this command to create the customized WiFiDog authentication template and enter its configuration mode.
**web-auth template** { template-name } **wifidog**

Use this command to create the Wechat authentication template and enter its configuration mode.
**web-auth template wechat**

Use this command to create the customized Wechat authentication template and enter its configuration mode.
**web-auth template** { template-name } **wechat**

Use this command to remove the template.
**no web-auth template** { *template-name* }

**Parameter Description**

| Parameter | Description |
|---|---|
| **eportalv1** | Applies the first generation authentication template. |
| **eportalv2** | Applies the second generation authentication template. |
| **iportal** | Applies the built-in authentication template. |
| **wechat** | Applies the Wechat authentication template. |
| **wifidog** | Applies the WiFiDog authentication template. |
| *template-name* | Sets the name of the customized authentication template. |

**Defaults** No template is configured by default.

**Command Mode** Global configuration mode

**Usage Guide** You can enter the **eportalv1** template mode to configure the IP address and URL instead of executing the **http redirect** and **http redirect homepage** commands**.** The **http redirect** and **http redirect homepage** commands are compatible on the device, which will be converted to this command.
The original command **portal-server** is compatible on the device, which will be converted to this command.
To ensure the Web authentication function, configure and apply a functional portal server. The **eportalv1** template is applied by default. The IP address, the URL and the communication secret key of the **eportalv1** template should be configured. If no URL format is specified, the default **http://[ ip-address ]** format will be adopted. The IP address of the portal server is the network resource exempted from authentication, so the unauthenticated user can access it. The device limits

the uplink traffic that accesses the IP address to prevent attacks. The upper limit is proportionate to the number of the physical ports.

**Configuration Examples** The following example configures the **eportalv1** template.

```
Ruijie(config)# web-auth template eportalv1
Ruijie(config.tmplt.eportalv1)#
```

**Related Commands**

| Command | Description |
|---|---|
| N/A | N/A |

**Platform Description** N/A

## 1.73 web-auth update-interval

Use this command to set the interval at which the online user information is updated.
Use the **no** form of this command to restore the default setting.
**web-auth update-interval** {*seconds*}
**no web-auth update-interval**

**Parameter Description**

| Parameter | Description |
|---|---|
| *seconds* | Update interval in seconds, in the range from 30 to 3,600 in the unit of seconds. |

**Defaults** The default is 180 seconds.

**Command Mode** Global configuration mode

**Usage Guide** N/A

**Configuration Examples** The following example sets the interval at which the online user information is updated to 60 seconds.

```
Ruijie(config)# web-auth update-interval 60
```

**Related Commands**

| Command | Description |
|---|---|
| N/A | N/A |

**Platform Description** N/A

## 1.74 web-auth valid-ip-acct

Use this command to configure the time during which STAs can attempt to obtain IP addresses. The STAs that fail to obtain IP addresses after the specified time has elapsed are forced offline.
**web-auth valid-ip-acct [ timeout** *seconds* **]**

Use this command to restore the default setting.
**no web-auth valid-ip-acct**

**Parameter Description**

| Parameter | Description |
|---|---|
| *seconds* | Time during which STAs can attempt to obtain IP addresses in the unit of seconds. The default value is 30s. |

**Defaults** By default, smart IP address check is not configured.

**Command Mode** Global configuration mode

**Usage Guide**

The configuration only works to users of smart authentication for WeChat access.

**Configuration Examples** Use this command to configure the time as 1min.

```
Ruijie(config)# web-auth valid-ip-acct timeout 60
```

**Platform Description** N/A

## 1.75 web-auth wechat-check

Use this command to configure detection of the authentication server for WeChat access.
Use the **no** form of this command to restore the default setting.
**web-auth wechat-check interval** *minutes*
**no web-auth wechat-check**

**Parameter Description**

| Parameter | Description |
|---|---|
| *minutes* | Interval for server detection. It is recommended to set it to 30minutes. |

**Defaults** Server detection is not configured by default.

**Command Mode** Global configuration mode

**Usage Guide**

Server detection teams up with collective escape. Run the **web-auth wechat-escape interval** *minutes* **times** *count* command to enable collective escape.

**Configuration Examples** The following example configures the interval for server detection.

```
Ruijie (config)# web-auth wechat-check interval 30
```

**Platform Description** N/A

## 1.76 web-auth wechat-escape

Use this command to enable collective escape of the authentication server for WeChat access.
**web-auth wechat-escape interval** *minutes* **times** *count*
Use the **no** form of this command to disable collective escape.
**no web-auth wechat-check**

Use this command to cancel collective escape and resume single escape. As a trigger, it is not displayed when running the **show running-config** command.
**web-auth wechat-escape recover**

**Parameter Description**

| Parameter | Description |
|---|---|
| *minutes* | Escape interval. By default, it is 60minutes. |
| *count* | Number of escape users. By default, the value is 5. |

**Defaults** Collective escape is disabled by default.

**Command Mode** Global configuration mode

**Usage Guide**

To configure collective escape, ensure that single escape has been enabled first. Run the **escape interval** *seconds* **online-time** *minutes* command to enable single escape.

**Configuration Examples** The following example configures the parameters for collective escape.

```
Ruijie (config)# web-auth wechat-escape interval 30 times 10
```

**Platform Description**

## 1.77 web-auth wechat-template wlan-range portal-ip nas-ip

Use this command to enable the one-click switch configuration via WeChat.
**web-auth wechat-template** *name* **wlan-range** *wlanid-start wlanid-end* **portal-ip** *portal-ip-addr* **nas-ip** *nas-ip-addr* **[ios-adapter | perception]**

Use the **no** form of this command to disable the one-click switch configuration via WeChat.
**no web-auth wechat-template** *name*

**Parameter Description**

| Parameter | Description |
|---|---|
| *name* | Indicates the template name. |
| *wlanid-start* | Indicates the start WLAN ID. |
| *wlanid-end* | Indicats the end WLAN ID. |
| *portal-ip-addr* | Indicates the IP address of the portal server. |
| *nas-ip-addr* | Sets the IP address for a device with WeChat configured to access a service, so that the server sends packets to this IP address for communication. |
| **ios-adapter** | Enables automatic popups. |
| **perception** | Enables the non-perception function. |

**Defaults** N/A

**Command Mode** Global configuration mode

**Default Level** 14

**Usage Guide**

The one-click configuration function can control only one port at a time. To control multiple ports, perform one-click configuration for the required times. The **no** form of this command can delete template information and all the controlled ports, but is not globally valid.

**Configuration Examples** The following example enables the one-click switch configuration.

```
Ruijie(config)# web-auth wechat-template aaa interface tenGigabitEthernet 3/2
portal-ip 172.21.6.78 nas-ip 192.168.197.227
```

**Verification**

## 1.78 web-auth wifidog-template wlan-range portal-ip nas-ip url

Use this command to enable the one-click switch configuration via WiFiDog.
**web-auth wifidog-template** *name* **wlan-range** *wlanid-start wlanid-end* **portal-ip** *portal-ip-addr* **nas-ip** *nas-ip-addr* **url** *url-string* **[perception]**

Use the **no** form of this command to disable the one-click switch configuration via WiFiDog.

**no web-auth wifidog-template** *name*

**Parameter Description**

| Parameter | Description |
|---|---|
| *name* | Indicates the template name. |
| *wlanid-start* | Indicates the start WLAN ID. |
| *wlanid-end* | Indicats the end WLAN ID. |
| *portal-ip-addr* | Indicates the IP address of the portal server. |
| *nas-ip-addr* | Sets the IP address for a device with WiFiDog configured to access a service, so that the server sends packets to this IP address for communication. |
| *url-string* | Indicates the URL for portal server authentication. |
| **perception** | Enables the non-perception function. |

**Defaults** N/A

**Command Mode** Global configuration mode

**Default Level** 14

**Usage Guide**

The one-click configuration function can control only one port at a time. To control multiple ports, perform one-click configuration for the required times. The **no** form of this command can delete template information and all the controlled ports, but is not globally valid.

**Configuration Examples** The following example enables the one-click switch configuration via WiFiDog.

```
Ruijie(config)# web-auth wifidog-template aaa interface tenGigabitEthernet 3/2
portal-ip 172.21.6.78 nas-ip 192.168.197.227 url
http://172.21.6.78/auth/wifidogAuth
```

**Verification** Run the **show running-config** command to display the current configurations.

## 1.79 web-auth wlan-ac-ip

Use this command to configure the ACIP parameter in redirect URL.

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

**web-auth wlan-ac-ip** *ipv4*

**no web-auth wlan-ac-ip**

**Parameter Description**

| Parameter | Description |
|---|---|
| *ipv4* | ACIP parameter |

**Defaults** The ACIP Parameter is not configured by default.

**Command Mode** WLAN security configuration mode

**Usage Guide** N/A

**Configuration Examples** The following example configures the ACIP parameter in redirect URL.

```
Ruijie (wlansec)# web-auth wlan-ac-ip 192.168.1.100
```

**Platform Description** N/A

## 1.80 web-auth winterface

Use this command to configure the winterface parameter in redirect URL.

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

**web-auth winterface** *string*

**no web-auth winterface**

**Parameter Description**

| Parameter | Description |
|---|---|
| *string* | winterface parameter |

**Defaults** The winterface parameter is not configured by default.

**Command Mode** WLAN security configuration mode

**Usage Guide** N/A

**Configuration Examples** The following example configures the winterface parameter in redirect URL.

```
Ruijie (wlansec)# web-auth winterface winterface
```

**Platform Description** N/A

# 2 AAA Commands

## 2.1 aaa accounting commands

Use this command to configure NAS command accounting.
Use the **no** form of this command to restore the default setting.
**aaa accounting commands** *level* **{ default |** *list-name* **} start-stop** *method1* [ *method2*…]
**no aaa accounting commands** *level* { **default |** *list-name* }

**Parameter Description**

| Parameter | Description |
|---|---|
| *level* | The accounting command level, 0-15. The message shall be recorded before which command level is executed is determined. |
| **default** | When this parameter is used, the following defined method list is used as the default method for command accounting. |
| *list-name* | Name of the command accounting method list, which could be any character strings. |
| *method* | It must be one of the keywords listed in the following table. One method list can contain up to four methods. |
| **none** | Does not perform accounting. |
| **group** | Uses the server group for accounting, the TACACS+ server group is supported. |

**Defaults** This function is disabled by default.

**Command Mode** Global configuration mode

**Usage Guide** RGOS enables the accounting command function after enabling the login authentication. After enabling the accounting function, it sends the command information to the security service.
The configured accounting command method must be applied to the terminal line that needs accounting command; otherwise it is ineffective.

**Configuration Examples** The following example enables NAS command accounting.

```
Ruijie(config)# aaa accounting commands 15 default start-stop group tacacs+
```

**Related Commands**

| Command | Description |
|---|---|
| **aaa new-model** | Enables the AAA security service. |
| **aaa authentication** | Defines AAA authentication. |
| **accounting commands** | Applies the accounting commands to the terminal line. |

**Platform Description** N/A

## 2.2 aaa accounting exec

Use this command to enable NAS access accounting.
Use the **no** form of this command to restore the default setting.
**aaa accounting exec** { **default |** *list-name* } **start-stop** *method1* [ *method2...*]
**no aaa accounting exec** { **default** | *list-name* }

**Parameter Description**

| Parameter | Description |
|---|---|
| **default** | When this parameter is used, the following defined method list is used as the default method for Exec accounting. |
| *list-name* | Name of the Exec accounting method list, which could be any character strings |
| *method* | It must be one of the keywords: **none** and **group**. One method list can contain up to four methods. |
| **none** | Does not perform accounting. |
| **group** | Uses the server group for accounting, the RADIUS and TACACS+ server group is supported. |

**Defaults** This function is disabled by default.

**Command Mode** Global configuration mode

**Usage Guide** RGOS enables the exec accounting function after enabling the login authentication.
After enabling the accounting function, it sends the account start information to the security server when the users log in the NAS CLI, and sends the account stop information to the security server when the users log out. If it does not send the account start information to the security server when a user logs in, it does not send the account stop information to the security server when a user logs out, either.
The configured exec accounting method must be applied to the terminal line that needs accounting command; otherwise it is ineffective.

**Configuration Examples** The following example enables NAS access accounting.

```
Ruijie(config)# aaa accounting network start-stop group radius
```

**Related Commands**

| Command | Description |
|---|---|
| **aaa new-model** | Enables the AAA security service. |
| **aaa authentication** | Defines AAA authentication. |
| **accounting commands** | Applies the Exec accounting to the terminal line. |

**Platform Description** N/A

## 2.3 aaa accounting network

Use this command to enable network access accounting.

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

**aaa accounting network { default |** *list-name* **} start-stop** *method1* [ *method2*..]

**no aaa accounting network** { **default** | *list-name* }

**Parameter Description**

| Parameter | Description |
|---|---|
| **default** | When this parameter is used, the following defined method list is used as the default method for Network accounting. |
| *list-name* | Name of the accounting method list |
| **start-stop** | Sends accounting messages at both the start time and the end time of access. Users are allowed to access the network, no matter whether the start accounting message enables the accounting successfully. |
| *method* | A method list includes up to four methods. |
| **none** | Does not perform accounting. |
| **group** | Uses the server group for accounting, the RADIUS and TACACS+ server group is supported. |

**Defaults** This function is disabled by default.

**Command Mode** Global configuration mode

**Usage Guide** RGOS performs accounting of user activities by sending record attributes to the security server. Use the **start-stop** keyword to set the user accounting option.

**Configuration Examples** The following example enables network access accounting.

```
Ruijie(config)# aaa accounting network start-stop group radius
```

**Related Commands**

| Command | Description |
|---|---|
| **aaa new-model** | Enables the AAA security service. |
| **aaa authorization network** | Defines a network authorization method list. |
| **aaa authentication** | Defines AAA authentication. |
| **username** | Defines a local user database. |

**Platform Description** N/A

## 2.4 aaa accounting update

Use this command to enable the accounting update function.
Use the **no** form of this command to restore the default setting.
**aaa accounting update**
**no aaa accounting update**

**Parameter Description** N/A

**Defaults** This function is disabled by default.

**Command Mode** Global configuration mode

**Usage Guide** If the AAA security service is not enabled, the accounting update function cannot be used. This command is used to set the accounting interval if the AAA security service has been enabled.

**Configuration Examples** The following example enables the accounting update function.

```
Ruijie(config)# aaa new-model
Ruijie(config)# aaa accounting update
```

**Related Commands**

| Command | Description |
|---|---|
| **aaa new-model** | Enables the AAA security service. |
| **aaa accounting network** | Defines a network accounting method list. |

**Platform Description** N/A

## 2.5 aaa accounting update periodic

Use this command to set the interval of sending the accounting update message.
Use the **no** form of this command to restore the default setting.
**aaa accounting update periodic** *interval*
**no aaa accounting update periodic**

**Parameter Description**

| Parameter | Description |
|---|---|
| *interval* | Interval of sending the accounting update message, in the unit of minutes. The shortest interval is 1 minute. |

**Defaults** The default is 5 minutes.

**Command** Global configuration mode

**Mode**

**Usage Guide** If the AAA security service is not enabled, the accounting update function cannot be used. This command is used to set the accounting interval if the AAA security service has been enabled.

**Configuration Examples** The following example sets the interval of accounting update to 1 minute.

```
Ruijie(config)# aaa new-model
Ruijie(config)# aaa accounting update
Ruijie(config)# aaa accounting update periodic 1
```

**Related Commands**

| Command | Description |
|---|---|
| **aaa new-model** | Enables the AAA security service. |
| **aaa accounting network** | Defines a network accounting method list. |

**Platform Description** N/A

## 2.6 aaa authentication dot1x

Use this command to enable AAA authentication 802.1x and configure the 802.1x user authentication method list.

Use the **no** form of this command to delete the 802.1x user authentication method list.

**aaa authentication dot1x** { **default** | *list-name* } *method1* [ *method2*...]

**no aaa authentication dot1x** { **default** | *list-name* }

**Parameter Description**

| Parameter | Description |
|---|---|
| **default** | When this parameter is used, the following defined 802.1x user authentication method list is used as the default method for user authentication. |
| *list-name* | Name of the 802.1x user authentication method list, which could be any character string |
| *method* | It must be one of the keywords: **local**, **none** and **group**. One method list can contain up to four methods. |
| **local** | Uses the local user name database for authentication. |
| **none** | Does not perform authentication. |
| **group** | Uses the server group for authentication. At present, the RADIUS server group is supported. |

**Defaults** N/A

**Command Mode** Global configuration mode

**Usage Guide** If the AAA 802.1x security service is enabled on the device, users must use AAA for 802.1x user authentication negotiation. You must use the **aaa authentication dot1x** command to configure a default or optional method list for 802.1x user authentication.
The next method can be used for authentication only when the current method does not work.

**Configuration Examples** The following example defines an AAA authentication method list named **RDS_D1X**. In the authentication method list, first the RADIUS security server is used for authentication. If the RADIUS security server does not respond, the local user database is used for authentication.

```
Ruijie(config)# aaa authentication dot1x rds_d1x group radius local
```

**Related Commands**

| Command | Description |
|---|---|
| **aaa new-model** | Enables the AAA security service. |
| **dot1x authentication** | Associates a specific method list with the 802.1x user. |
| **username** | Defines a local user database. |

**Platform Description** N/A

## 2.7 aaa authentication enable

Use this command to enable AAA Enable authentication and configure the Enable authentication method list.
Use the **no** form of this command to delete the user authentication method list.
**aaa authentication enable default** *method1* [ *method2*...]
**no aaa authentication enable default**

**Parameter Description**

| Parameter | Description |
|---|---|
| **default** | When this parameter is used, the following defined authentication method list is used as the default method for Enable authentication. |
| *method* | It must be one of the keywords: **local, none** and **group**. One method list can contain up to four methods. |
| **local** | Uses the local user name database for authentication. |
| **none** | Does not perform authentication. |
| **group** | Uses the server group for authentication. At present, the RADIUS and TACACS+ server groups are supported. |
| **enable** | Enables AAA Enable authentication. |

**Defaults** N/A

**Command Mode** Global configuration mode

**Usage Guide** If the AAA Enable authentication service is enabled on the device, users must use AAA for Enable

authentication negotiation. You must use the **aaa authentication enable** command to configure a default or optional method list for Enable authentication.
The next method can be used for authentication only when the current method does not work.
The Enable authentication function automatically takes effect after configuring the Enable authentication method list.

**Configuration Examples** The following example defines an AAA Enable authentication method list. In the authentication method list, first the RADIUS security server is used for authentication. If the RADIUS security server does not respond, the local user database is used for authentication.

```
Ruijie(config)# aaa authentication enable default group radius local
```

**Related Commands**

| Command | Description |
|---|---|
| **aaa new-model** | Enables the AAA security service. |
| **enable** | Switchover the user level. |
| **username** | Defines a local user database. |

**Platform Description** N/A

## 2.8 aaa authentication iportal

Use this command to enable AAA Portal Web user authentication.
Use the **no** form of this command to delete the authentication method list.
**aaa authentication iportal** { **default** | *list-name* } *method1* [ *method2...*]
**no aaa authentication iportal** { **default** | *list-name* }

**Parameter Description**

| Parameter | Description |
|---|---|
| **default** | When this parameter is used, the following defined authentication method list is used as the default method for Login authentication. |
| *list-name* | Name of the user authentication method list, which could be any character strings |
| *method* | It must be one of the keywords: **local**, **none**, **subs** and **group**. One method list can contain up to four methods. |
| **local** | Uses the local user name database for authentication. |
| **none** | Does not perform authentication. |
| **group** | Uses the server group for authentication. At present, the RADIUS server group is supported. |
| **subs** | Uses the subs database for authentication. |

**Defaults** N/A

**Command Mode** Global configuration mode

**Usage Guide** If the AAA Portal Web security service is enabled on the device, users must use AAA for Portal Web authentication negotiation. You must use the **aaa authentication iportal** command to configure a default or optional method list for Portal Web authentication.

**Configuration Examples** The following example defines an AAA Portal Web authentication method list named **rds_web**. 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 iportal rds_web group radius local
```

**Related Commands**

| Command | Description |
|---|---|
| **aaa new-model** | Enables the AAA security service. |
| **login authentication** | Applies the Login authentication method to the terminal lines. |
| **username** | Defines a local user database. |

**Platform Description** N/A

## 2.9 aaa authentication login

Use this command to enable AAA Login authentication and configure the Login authentication method list.

Use the **no** form of this command to delete the authentication method list.

**aaa authentication login** { **default** | *list-name* } *method1* [ *method2*..]

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

**Parameter Description**

| Parameter | Description |
|---|---|
| **default** | When this parameter is used, the following defined authentication method list is used as the default method for Login authentication. |
| ***list-name*** | Name of the user authentication method list, which could be any character strings |
| ***method*** | It must be one of the keywords: **local**, **none**, **group** and **subs**. One method list can contain up to four methods. |
| **local** | Uses the local user name database for authentication. |
| **none** | Does not perform authentication. |
| **group** | Uses the server group for authentication. At present, the RADIUS and TACACS+ server groups are supported. |
| **subs** | Uses the subs database for authentication. |

**Defaults** N/A

**Command Mode** Global configuration mode

**Usage Guide** If the AAA Login authentication security service is enabled on the device, users must use AAA for Login authentication negotiation. You must use the **aaa authentication login** command to configure a default or optional method list for Login authentication.
The next method can be used for authentication only when the current method does not work.
You need to apply the configured Login authentication method to the terminal line which needs Login authentication. Otherwise, the configured Login authentication method is invalid.

**Configuration Examples** The following example defines an AAA Login authentication method list named list-1. In the authentication method list, first the RADIUS security server is used for authentication. If the RADIUS security server does not respond, the local user database is used for authentication.

```
Ruijie(config)# aaa authentication login list-1 group radius local
```

**Related Commands**

| Command | Description |
|---|---|
| **aaa new-model** | Enables the AAA security service. |
| **login authentication** | Applies the Login authentication method to the terminal lines. |
| **username** | Defines a local user database. |

**Platform Description** N/A

## 2.10 aaa authentication ppp

Use this command to enable the AAA authentication for PPP user and configure the PPP user authentication method list.
Use the **no** form of this command to delete the authentication method list.
**aaa authentication ppp** { **default** | *list-name* } *method1* [ *method2*...]
**no aaa authentication ppp** { **default** | *list-name* }

**Parameter Description**

| Parameter | Description |
|---|---|
| **default** | When this parameter is used, the following defined authentication method list is used as the default method for PPP user authentication. |
| *list-name* | Name of the user authentication method list, which could be any character strings |
| *method* | It must be one of the keywords: **local**, **none group** and **subs**. One method list can contain up to four methods. |
| **local** | Uses the local user name database for authentication. |
| **none** | Does not perform authentication. |
| **group** | Uses the server group for authentication. At present, the RADIUS server group is supported. |
| **subs** | Uses the subs database for authentication. |

**Defaults** N/A

**Command Mode** Global configuration mode

**Usage Guide** If the AAA PPP security service is enabled on the device, users must use AAA authentication for PPP negotiation. You must use the **aaa authentication ppp** command to configure a default or optional method list for PPP user authentication.
The next method can be used for authentication only when the current method does not work.

**Configuration Examples** The following example defines an AAA authentication method list named rds_ppp for PPP session. In the authentication method list, first the RADIUS security server is used for authentication. If the RADIUS security server does not respond, the local user database is used for authentication.

```
Ruijie(config)# aaa authentication ppp rds_ppp group radius local
```

**Related Commands**

| Command | Description |
|---|---|
| **aaa new-model** | Enables the AAA security service. |
| **ppp authentication** | Associates a specific method list with the PPP user. |
| **username** | Defines a local user database. |

**Platform Description** N/A

## 2.11 aaa authentication sslvpn

Use this command to enable AAA authentication for the SSL VPN user and configure the SSL VPN user authentication method list.
Use the **no** form of this command to delete the authentication method list.
**aaa authentication sslvpn** { **default** | *list-name* } *method1* [ *method2...*]
**no aaa authentication sslvpn** { **default** | *list-name* }

**Parameter Description**

| Parameter | Description |
|---|---|
| **default** | When this parameter is used, the following defined authentication method list is used as the default method for SSL VPN user authentication. |
| *list-name* | Name of SSL VPN user authentication method list, which could be any character strings |
| *method* | It must be one of the keywords: **local**, **none**, **subs** and **group**. One method list can contain up to four methods. |
| **local** | Use the local user name database for authentication. |
| **none** | Does not perform authentication. |
| **group** | Uses the server group for authentication. At present, the RADIUS server group is supported. |

| | |
|---|---|
| **subs** | Uses the subs database for authentication. |

**Defaults** N/A

**Command Mode** Global configuration mode

**Usage Guide** If the SSL VPN security service is enabled on the device, users must use the AAA authentication for SSL VPN negotiation. You must use the **aaa authentication sslvpn** command to configure a default or optional method list for user authentication.
The next method can be used for authentication only when the current method does not work.

**Configuration Examples** The following example defines an AAA authentication method list named **rds_sslvpn** for SSL VPN session. In the authentication method list, the RADIUS security server is first used for authentication. If the RADIUS security server does not respond, the local user database is used for authentication.

```
Ruijie(config)# aaa authentication sslvpn rds_sslvpn group radius local
```

**Related Commands**

| Command | Description |
|---|---|
| N/A | N/A |

**Platform Description** N/A

## 2.12 aaa authentication web-auth

Use this command to enable AAA second-generation Web authentication and configure the second-generation Web authentication method list in global configuration mode.
Use the **no** form of this command to delete the authentication method list.
**aaa authentication web-auth** { **default** | *list-name* } *method1* [ *method2*...]
**no aaa authentication web-auth** { **default** | *list-name* }

**Parameter Description**

| Parameter | Description |
|---|---|
| **default** | When this parameter is used, the following defined authentication method list is used as the default method for the second-generation Web authentication. |
| *list-name* | Name of second-generation Web authentication method list, which could be any character strings |
| *method* | It must be one of the keywords: **local**, **none**, **subs** and **group**. One method list can contain up to four methods. |
| **local** | Uses the local user name database for authentication. |
| **none** | Does not perform authentication. |
| **group** | Uses the server group for authentication. At present, the RADIUS server group is supported. |

| | |
|---|---|
| **subs** | Uses the subs database for authentication. |

**Defaults** N/A

**Command Mode** Global configuration mode

**Usage Guide** If the AAA second-generation Web security service is enabled on the device, users must use AAA for the second-generation Web authentication negotiation. You must use the **aaa authentication web-auth** command to configure a default or optional method list for user authentication.
The next method can be used for authentication only when the current method does not work.

**Configuration Examples** The following example defines an AAA authentication method list named **rds_web**. In the authentication method list, the RADIUS security server is first used for authentication. If the RADIUS security server does not respond, the local user database is used for authentication.

```
Ruijie(config)# aaa authentication web-auth rds_web group radius none
```

**Related Commands**

| Command | Description |
|---|---|
| N/A | N/A |

**Platform Description** N/A

## 2.13 aaa authorization commands

Use this command to authorize the command executed by the user who has logged in the NAS CLI.
Use the **no** form of this command to restore the default setting.
**aaa authorization commands** *level* { **default** | *list-name* } *method1* [ *method2...*]
**no aaa authorization commands** *level* { **default** | *list-name* }

**Parameter Description**

| Parameter | Description |
|---|---|
| *level* | Command level to be authorized in the range from 0 to 15 |
| **default** | When this parameter is used, the following defined method list is used as the default method for command authorization. |
| *list-name* | Name of the user authorization method list, which could be any character strings |
| *method* | It must be one of the keywords: **none** and **group**. One method list can contain up to four methods. |
| **none** | Do not perform authorization. |
| **group** | Uses the server group for authorization. At present, the TACACS+ server group is supported. |

**Defaults** This function is disabled by default.

**Command Mode** Global configuration mode

**Usage Guide** RGOS supports authorization of the commands executed by the users. When the users input and attempt to execute a command, AAA sends this command to the security server. This command is to be executed if the security server allows to. Otherwise, it will prompt command deny.
It is necessary to specify the command level when configuring the command authorization, and this specified command level is the default command level.
The configured command authorization method must be applied to terminal line which requires the command authorization. Otherwise, the configured command authorization method is ineffective.

**Configuration Examples** The following example uses the TACACS+ server to authorize the level 15 command.

```
Ruijie(config)# aaa authorization commands 15 default group tacacs+
```

**Related Commands**

| Command | Description |
|---|---|
| **aaa new-model** | Enables the AAA security service. |
| **authorization commands** | Applies the command authorization for the terminal line. |

**Platform Description** N/A

## 2.14 aaa authorization config-commands

Use this command to authorize the configuration commands (including in the global configuration mode and its sub-mode).
Use the **no** form of this command to restore the default setting.
**aaa authorization config-commands**
**no aaa authorization config-commands**

**Parameter Description**

| Parameter | Description |
|---|---|
| N/A | N/A |

**Defaults** This function is disabled by default.

**Command Mode** Global configuration mode

**Usage Guide** If you only authorize the commands in the non-configuration mode (for example, privileged EXEC mode), you can use the **no** form of this command to disable the authorization function in the configuration mode, and execute the commands in the configuration mode and its sub-mode without command authorization.

**Configuration** The following example enables the configuration command authorization function.

**Examples**

```
Ruijie(config)# aaa authorization config-commands
```

**Related Commands**

| Command | Description |
| --- | --- |
| **aaa new-model** | Enables the AAA security service. |
| **aaa authorization commands** | Defines the AAA command authorization. |

**Platform Description** N/A

## 2.15 aaa authorization console

Use this command to authorize the commands of the users who have logged in the console.
Use the **no** form of this command to restore the default setting.
**aaa authorization console**
**no aaa authorization console**

**Parameter Description**

| Parameter | Description |
| --- | --- |
| N/A | N/A |

**Defaults** This function is disabled by default.

**Command Mode** Global configuration mode

**Usage Guide** RGOS supports to identify the users logged in from the console and from other terminals, configure whether to authorize the users logged in from the console or not. If the command authorization function is disabled on the console, the authorization method list applied to the console line is ineffective.

**Configuration Examples** The following example enables the aaa authorization console function.

```
Ruijie(config)# aaa authorization console
```

**Related Commands**

| Command | Description |
| --- | --- |
| **aaa new-model** | Enables the AAA security service. |
| **aaa authorization commands** | Defines the AAA command authorization. |
| **authorization commands** | Applies the command authorization to the terminal line. |

**Platform Description** N/A

## 2.16 aaa authorization exec

Use this command to authorize the users logged in the NAS CLI and assign the authority level.

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

**aaa authorization exec** { **default** | *list-name* } *method1* [ *method2*...]

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

**Parameter Description**

| Parameter | Description |
|---|---|
| **default** | When this parameter is used, the following defined method list is used as the default method for Exec authorization. |
| *list-name* | Name of the user authorization method list, which could be any character strings |
| *method* | It must be one of the keywords listed in the following table. One method list can contain up to four methods. |
| **local** | Uses the local user name database for authorization. |
| **none** | Does not perform authorization. |
| **group** | Uses the server group for authorization. At present, the RADIUS server group is supported. |

**Defaults** This function is disabled by default.

**Command Mode** Global configuration mode

**Usage Guide** RGOS supports authorization of users logged in the NAS CLI and assignment of CLI authority level (0-15). The **aaa authorization exec** function is effective on condition that Login authentication function has been enabled. It cannot enter the CLI if it fails to enable the **aaa authorization exec**. You must apply the exec authorization method to the terminal line; otherwise the configured method is ineffective.

**Configuration Examples** The following example uses the RADIUS server to authorize Exec.

```
Ruijie(config)# aaa authorization exec default group radius
```

**Related Commands**

| Command | Description |
|---|---|
| **aaa new-model** | Enables the AAA security service. |
| **authorization exec** | Applies the command authorization to the terminal line. |
| **username** | Defines a local user database. |

**Platform Description** N/A

## 2.17 aaa authorization network

Use this command to authorize the service requests (including such protocols as PPP and SLIP) from the users that access the network.

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

**aaa authorization network** { **default** | *list-name* } *method1* [ *method2*...]
**no aaa authorization network** { **default** | *list-name* }

**Parameter Description**

| Parameter | Description |
|---|---|
| **default** | When this parameter is used, the following defined method list is used as the default method for Network authorization. |
| *method* | It must be one of the keywords: none and group. One method list can contain up to four methods. |
| **none** | Does not perform authorization. |
| **group** | Uses the server group for authorization. At present, the RADIUS server group is supported. |

**Defaults** This function is disabled by default.

**Command Mode** Global configuration mode

**Usage Guide** RGOS supports authorization of all the service requests related to the network, such as PPP and SLIP. If authorization is configured, all the authenticated users or interfaces will be authorized automatically.
Three different authorization methods can be specified. Like authorization, the next method can be used for authorization only when the current authorization method does not work. If the current authorization method fails, other subsequent authorization method is not used.
The RADIUS server authorizes authenticated users by returning a series of attributes. Therefore, RADIUS authorization is based on RADIUS authorization. RADIUS authorization is performed only when the user passes the RADIUS authorization.

**Configuration Examples** The following example uses the RADIUS server to authorize network services.

```
Ruijie(config)# aaa authorization network default group radius
```

**Related Commands**

| Command | Description |
|---|---|
| **aaa new-model** | Enables the AAA security service. |
| **aaa accounting** | Defines AAA accounting. |
| **aaa authentication** | Defines AAA authentication. |
| **username** | Defines a local user database. |

**Platform Description** N/A

## 2.18 aaa domain

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

**aaa domain** { **default** | *domain-name* }
**no aaa domain** { **default |** *domain-name* }

**Parameter Description**

| Parameter | Description |
|---|---|
| **default** | Uses this parameter to configure the default domain. |
| *domain-name* | The name of the specified domain |

**Defaults** No domain is configured by default.

**Command Mode** Global configuration mode

**Usage Guide** Use this command to configure the domain-name–based AAA service. The **default** is to configure the default domain. That is the method list used by the network device if the users are without domain information. The *domain-name* is the specified domain name, if the users are with this *domain name*, the method lists associated with this domain are used. At present, the system can configure up to 32 domains.

**Configuration Examples** The following example configures the domain name.

```
Ruijie(config)# aaa domain ruijie.com
Ruijie(config-aaa-domain)#
```

**Related Commands**

| Command | Description |
|---|---|
| **aaa new-model** | Enables the AAA security service. |
| **aaa domain enable** | Enables the domain-name-based AAA service. |
| **show aaa domain** | Displays the domain configuration. |

**Platform Description** N/A

## 2.19 aaa domain enable

Use this command to enable domain-name-based AAA service.
Use the **no** form of this command to restore the default setting.
**aaa domain enable**
**no aaa domain enable**

**Parameter Description**

| Parameter | Description |
|---|---|
| N/A | N/A |

**Defaults** This function is disabled by default.

**Command** Global configuration mode

**Mode**

**Usage Guide** To perform the domain-name-based AAA service configuration, enable this service.

**Configuration Examples** The following example enables the domain-name-based AAA service.

```
Ruijie(config)# aaa domain enable
```

**Related Commands**

| Command | Description |
|---|---|
| **aaa new-model** | Enables the AAA security service. |
| **show aaa doamain** | Displays the domain configuration. |

**Platform Description** N/A

## 2.20 aaa local authentication attempts

Use this command to set login attempt times.

**aaa local authentication attempts** *max-attempts*

**Parameter Description**

| Parameter | Description |
|---|---|
| *max-attempts* | In the range from 1 to 2,147,483,647 |

**Defaults** The default is 3.

**Command Mode** Global configuration mode

**Usage Guide** Use this command to configure login attempt times.

**Configuration Examples** The following example sets login attempt times to 6.

```
Ruijie #configure terminal
Ruijie(config)#aaa local authentication attempts 6
```

**Related Commands**

| Command | Description |
|---|---|
| **show running-config** | Displays the current configuration of the switch. |
| **show aaa lockout** | Displays the lockout configuration parameter of current login. |

**Platform Description** N/A

## 2.21 aaa local authentication lockout-time

Use this command to configure the lockout-time period when the login user has attempted for more

than the limited times.

**aaa local authentication lockout-time** *lockout-time*

| Parameter Description | Parameter | Description |
|---|---|---|
| | *lockout-time* | In the range from 1 to 2,147,483,647 in the unit of minutes |

**Defaults** The default is 15 minutes.

**Command Mode** Global configuration mode

**Usage Guide** Use this command to configure the length of lockout-time when the login user has attempted for more than the limited times.

**Configuration Examples** The following example sets the lockout-time period to 5 minutes.

```
Ruijie#configure terminal
Ruijie(config)#aaa local authentication lockout-time 5
```

| Related Commands | Command | Description |
|---|---|---|
| | **show running-config** | Displays the current configuration of the switch. |
| | **show aaa lockout** | Displays the lockout configuration parameter of current login. |

**Platform Description** N/A

## 2.22 aaa local user allow public account

Use this command to allow the local account (username or subs) to be shared by multiple terminals with Web authentication configured or built-in.

**aaa local user allow public account**

| Parameter Description | Parameter | Description |
|---|---|---|
| | N/A | N/A |

**Defaults** One local account cannot be shared by multiple terminals by default.

**Command Mode** Global configuration mode

**Usage Guide** This configuration is supported by EG series products only. For other products, a local account can be shared by multiple terminals by default.

**Configuration** The following example allows the local account (username or subs) to be shared by multiple terminals

**Examples** with Web authentication configured or built-in.

```
Ruijie#configure terminal
Ruijie(config)#aaa local user allow public account
```

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

**Platform Description** This configuration is supported by EG series products only. For other products, a local account can be shared by multiple terminals by default.

## 2.23 aaa log enable

Use this command to enable the system to print the syslog informing AAA authentication success.
Use the **no** form of this command to restore the default setting.
**aaa log enable**
**no aaa log enable**

| **Parameter Description** | **Parameter** | **Description** |
|---|---|---|
| | N/A | N/A |

**Defaults** This function is disabled by default.

**Command Mode** Global configuration mode

**Usage Guide** Use this command to enable the system to print the syslog informing aaa authentication success.

**Configuration Examples** The following example disables the system to print the syslog informing aaa authentication success.

```
Ruijie(config)# no aaa log enable
```

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

**Platform Description** N/A

## 2.24 aaa log rate-limit

Use this command to set the rate of printing the syslog informing AAA authentication success.
Use the **no** form of this command to restore the default printing rate.
**aaa log rate-limit** *num*
**no aaa log rate-limit**

**Parameter Description**

| Parameter | Description |
| --- | --- |
| *num* | The number of syslog entries printed per second. The range is from 0 to 65,535.<br>0 indicates the printing rate is not limited. |

**Defaults** The default is 5.

**Command Mode** Global configuration mode

**Usage Guide**

Too much printing may flood the screen or even reduce device performance. In this case, use this command to adjust the printing rate.

**Configuration Examples** The following example sets the rate of printing the syslog informing AAA authentication success to 10.

```
Ruijie(config)# aaa log rate-limit 10
```

**Related Commands**

| Command | Description |
| --- | --- |
| N/A | N/A |

**Platform Description** N/A

## 2.25 aaa new-model

Use this command to enable the RGOS AAA security service.

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

**aaa new-model**

**no aaa new-model**

**Parameter Description**

| Parameter | Description |
| --- | --- |
| N/A | N/A |

**Defaults** This function is disabled by default.

**Command Mode** Global configuration mode

**Usage Guide** Use this command to enable AAA. If AAA is not enabled, none of the AAA commands can be configured.

**Configuration Examples** The following example enables the AAA security service.

```
Ruijie(config)# aaa new-model
```

| Related Commands | Command | Description |
|---|---|---|
| | **aaa authentication** | Defines a user authentication method list. |
| | **aaa authorization** | Defines a user authorization method list. |
| | **aaa accounting** | Defines a user accounting method list. |

**Platform Description** N/A

## 2.26 access-limit

Use this command to configure the number of users limit for the domain, which is only valid for the IEEE802.1 users.

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

**access-limit** *num*

**no access-limit**

| Parameter Description | Parameter | Description |
|---|---|---|
| | *num* | The number used for the user limitation is only valid for the IEEE802.1 users. |

**Defaults** By default, no number of users is limited.

**Command Mode** Domain configuration mode

**Usage Guide** This command limits the number of users for the domain.

**Configuration Examples** The following example sets the number of users to 20 for the domain named ruijie.com.

```
Ruijie(config)# aaa domain ruijie.com
Ruijie(config-aaa-domain)# access-limit 2
```

| Related Commands | Command | Description |
|---|---|---|
| | **aaa new-model** | Enables the AAA security service. |
| | **aaa domain enable** | Switchover the user level. |
| | **show aaa domain** | Defines a local user database. |

**Platform Description** N/A

## 2.27 accounting network

Use this command to configure the Network accounting list.

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

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

**no accounting network**

| Parameter Description | Parameter | Description |
|---|---|---|
| | **default** | Uses this parameter to specify the default method list. |
| | *list-name* | The name of the network accounting list |

**Defaults** With no method list specified, if the user sends the request, the device will attempt to specify the default method list for the user.

**Command Mode** Domain configuration mode

**Usage Guide** Use this command to configure the Network accounting method list for the specified domain.

**Configuration Examples** The following example sets the Network accounting method list for the specified domain.

```
Ruijie(config)# aaa domain ruijie.com
Ruijie(config-aaa-domain)# accounting network default
```

| Related Commands | Command | Description |
|---|---|---|
| | **aaa new-model** | Enables the AAA security service. |
| | **aaa domain enable** | Enables the domain-name-based AAA service. |
| | **show aaa domain** | Displays the domain configuration. |

**Platform Description** N/A

## 2.28 authentication dot1x

Use this command to configure the IEEE802.1x authentication list.
Use the **no** form of this command to restore the default setting.
**authentication dot1x** { **default** | *list-name* }
**no authentication dot1x**

| Parameter Description | Parameter | Description |
|---|---|---|
| | **default** | Uses this parameter to specify the default method list |
| | *list-name* | The name of the specified method list |

**Defaults** With no method list specified, if users send the request, the device will attempt to specify the default method list for users.

**Command Mode** Domain configuration mode

**Usage Guide** Specify an IEEE802.1x authentication method list for the domain.

**Configuration Examples** The following example sets an IEEE802.1x authentication method list for the specified domain.

```
Ruijie(config)# aaa domain ruijie.com
Ruijie(config-aaa-domain)# authentication dot1x default
```

**Related Commands**

| Command | Description |
|---|---|
| **aaa new-model** | Enables the AAA security service. |
| **aaa domain enable** | Enables the domain-name-based AAA service. |
| **show aaa domain** | Displays the domain configuration. |

**Platform Description** N/A

## 2.29 authorization network

Use this command to configure the Network authorization list.
Use the **no** form of this command to restore the default setting.
**authorization network** { **default** | *list-name* }
**no authorization network**

**Parameter Description**

| Parameter | Description |
|---|---|
| **default** | Uses this parameter to specify the default method list. |
| *list-name* | The name of the specified method list |

**Defaults** With no method list specified, if users send the request, the device will attempt to specify the default method list for users.

**Command Mode** Domain configuration mode

**Usage Guide**

**Configuration Examples** The following example sets an authorization method list for the specified domain.

```
Ruijie(config)# aaa domain ruijie.com
Ruijie(config-aaa-domain)# authorization network default
```

**Related Commands**

| Command | Description |
|---|---|
| **aaa new-model** | Enables the AAA security service. |
| **aaa domain enable** | Enables the domain-name-based AAA service. |
| **show aaa domain** | Displays the domain configuration. |

**Platform** N/A

**Description**

## 2.30 clear aaa local user lockout

Use this command to clear the lockout user list.

**clear aaa local user lockout** { **all | user-name** *word* }

| **Parameter Description** | **Parameter** | **Description** |
|---|---|---|
| | **all** | Indicates all locked users. |
| | **user-name** *word* | Indicates the ID of the locked User. |

**Defaults** N/A

**Command Mode** Privileged EXEC mode

**Usage Guide** Use this command to clear all the user lists or a specified user list.

**Configuration Examples** The following example clears the lockout user list.

```
Ruijie(config)# clear aaa local user lockout all
```

| **Related Commands** | **Command** | **Description** |
|---|---|---|
| | **show running-config** | Displays the current configuration of the switch. |
| | **show aaa lockout** | Displays the lockout configuration parameter of current login. |

**Platform Description** N/A

## 2.31 show aaa accounting update

Use this command to display the accounting update information.

**show aaa accounting update**

| **Parameter Description** | **Parameter** | **Description** |
|---|---|---|
| | N/A | N/A |

**Defaults** N/A

**Command Mode** Privileged EXEC mode/Global configuration mode/Interface configuration mode

**Usage Guide** Use this command to display the accounting update interval and whether the accounting update is enabled.

**Configuration Examples** The following example displays the accounting update information.

```
Ruijie# show aaa accounting update
```

**Related Commands**

| Command | Description |
|---|---|
| **aaa new-model** | Enables the AAA security service. |
| **aaa domain enable** | Enables the domain-name-based AAA service. |

**Platform Description** N/A

## 2.32 show aaa domain

Use this command to display all current domain information.

**show aaa domain** [ **default** | *domain-name* ]

**Parameter Description**

| Parameter | Description |
|---|---|
| **default** | Displays the default domain. |
| *domain-name* | Displays the specified domain. |

**Defaults** N/A

**Command Mode** Privileged EXEC mode/Global configuration mode/Interface configuration mode

**Usage Guide** If no domain-name is specified, all domain information will be displayed.

**Configuration Examples** The following example displays the domain named domain.com.

```
Ruijie(config)# show aaa domain domain.com
=============Domain domain.com=============
State: Active
Username format: Without-domain
Access limit: No limit
802.1X Access statistic: 0

Selected method list:
 authentication dot1x default
```

**Related Commands**

| Command | Description |
|---|---|
| **aaa new-model** | Enables the AAA security service. |
| **aaa domain enable** | Enables the domain-name-based AAA service. |

**Platform** N/A

**Description**

## 2.33 show aaa lockout

Use this command to display the lockout configuration.

**show aaa lockout**

| **Parameter Description** | **Parameter** | **Description** |
|---|---|---|
| | N/A | N/A |

**Defaults** N/A

**Command Mode** Privileged EXEC mode/Global configuration mode/Interface configuration mode

**Usage Guide** Use this command to display the lockout configuration.

**Configuration Examples** The following example displays the lockout configuration.

```
Ruijie# show aaa lockout
Lock tries:   3
Lock timeout:  15 minutes
```

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

**Platform Description** N/A

## 2.34 show aaa group

Use this command to display all the server groups configured for AAA.

**show aaa group**

| **Parameter Description** | **Parameter** | **Description** |
|---|---|---|
| | N/A | N/A |

**Defaults** N/A

**Command Mode** Privileged EXEC mode/Global configuration mode/Interface configuration mode

**Usage Guide** N/A

**Configuration Examples** The following command displays all the server groups.

```
Ruijie# show aaa group
Type      Reference  Name
---------- ---------- ----------
radius    1         radius
tacacs+   1         tacacs+
radius    1         dot1x_group
radius    1         login_group
radius    1         enable_group
```

| Related Commands | Command | Description |
|---|---|---|
| | **aaa group server** | Configures the AAA server group. |

**Platform Description** N/A

## 2.35 show aaa method-list

Use this command to display all AAA method lists.

**show aaa method-list**

| Parameter Description | Parameter | Description |
|---|---|---|
| | N/A | N/A |

**Defaults** N/A

**Command Mode** Privileged EXEC mode/Global configuration mode/Interface configuration mode

**Usage Guide** Use this command to display all AAA method lists.

**Configuration Examples** The following example displays the AAA method list.

```
Ruijie# show aaa method-list
Authentication method-list
aaa authentication login default group radius
aaa authentication ppp default group radius
aaa authentication dot1x default group radius
aaa authentication dot1x san-f local  group angel group rain none
aaa authentication enable default group radius
Accounting method-list
aaa accounting network default start-stop group radius
Authorization method-list
aaa authorization network default group radius
```

| Related Commands | Command | Description |
|---|---|---|
| | **aaa authentication** | Defines a user authentication method list |
| | **aaa authorization** | Defines a user authorization method list |
| | **aaa accounting** | Defines a user accounting method list |

**Platform Description** N/A

## 2.36 show aaa user

Use this command to display AAA user information.

**show aaa user { all | lockout | by-id** *session-id* **| by-name** *user-name* **}**

| Parameter Description | Parameter | Description |
|---|---|---|
| | **all** | Displays all AAA user information. |
| | **lockout** | Displays the locked AAA user information. |
| | **by-id** *session-id* | Displays the information of the AAA user that with a specified session ID. |
| | **by-name** *user-name* | Displays the information of the AAA user with a specified user name. |

**Defaults** N/A

**Command Mode** Privileged EXEC mode/Global configuration mode/Interface configuration mode

**Usage Guide** Use this command to display AAA user information.

**Configuration Examples** The following example displays AAA user information.

```
Ruijie#show aaa user all
------------------------------
      Id ----- Name
 2345687901     wwxy
------------------------------
Ruijie# show aaa user by-id 2345687901
------------------------------
      Id ----- Name
 2345687901     wwxy
Ruijie# show aaa user by-name wwxy
------------------------------
```

```
      Id ----- Name
 2345687901     wwxy
------------------------------


Ruijie# show aaa user lockout


Name                          Tries     Lock      Timeout(min)
-------------------------------- ---------- ---------- ------------
Ruijie#
```

| Related Commands | Command | Description |
|---|---|---|
| | N/A | N/A |

**Platform Description** N/A

## 2.37 state

Use this command to set whether the configured domain is valid.

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

**state** { **block | active** }

**no state**

| Parameter Description | Parameter | Description |
|---|---|---|
| | **block** | The configured domain is invalid. |
| | **active** | The configured domain is valid. |

**Defaults** The default is active.

**Command Mode** Domain configuration mode

**Usage Guide** Use this command to set whether the specified configured domain is valid.

**Configuration Examples** The following example sets the configured domain to be invalid.

```
Ruijie(config)# aaa domain ruijie.com
Ruijie(config-aaa-domain)# state block
```

| Related Commands | Command | Description |
|---|---|---|
| | **aaa new-model** | Enables the AAA security service. |
| | **aaa domain enable** | Enables the domain-name-based AAA service. |

| | |
|---|---|
| **show aaa domain enable** | Displays the domain configuration. |

**Platform Description** N/A

## 2.38 username-format

Use this command to configure the user name whether to be with the domain information when the NAS interacts with the servers.

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

**username-format** { **without-domain** | **with-domain** }

**no username-format**

**Parameter Description**

| Parameter | Description |
|---|---|
| **without-domain** | Sets the user name without the domain information. |
| **with-domain** | Sets the user name with the domain information. |

**Defaults** The default is without-domain.

**Command Mode** Domain configuration mode

**Usage Guide** Use this command to configure the user name whether to be with the domain information when the NAS interacts with the servers.

**Configuration Examples** The following example sets the user name without the domain information.

```
Ruijie(config)# aaa domain ruijie.com
Ruijie(config-aaa-domain)# username-domain without-domain
```

**Related Commands**

| Command | Description |
|---|---|
| **aaa new-model** | Enables the AAA security service. |
| **aaa domain enable** | Enables the domain-name-based AAA service. |
| **show aaa domain** | Displays the domain configuration. |

**Platform Description** N/A

# 3 RADIUS Commands

## 3.1 aaa group server radius

Use this command to enter AAA server group configuration mode.
Use the **no** form of this command to restore the default setting.
**aaa group server radius** *name*
**no aaa group server radius** *name*

**Parameter Description**

| Parameter | Description |
|---|---|
| *name* | Server group name. Keywords “radius” and “tacacs +” are excluded as they are the default RADIUS and TACACS+ server group names. |

**Defaults** N/A

**Command Mode** Global configuration mode

**Usage Guide** This command is used to configure a RADIUS AAA server group.

**Configuration Examples** The following example configures a RADIUS AAA server group named ss.

```
Ruijie(config)# aaa group server radius ss
Ruijie(config-gs-radius)# end
Ruijie# show aaa group
Type      Reference  Name
---------- ---------- ----------
radius    1         radius
tacacs+   1         tacacs+
radius    1         ss
```

**Related Commands**

| Command | Description |
|---|---|
| N/A | N/A |

**Platform Description** N/A

## 3.2 ip radius source-interface

Use this command to specify the source IP address for the RADIUS packet.

Use the **no** form of this command to delete the source IP address for the RADIUS packet.
**ip radius source-interface** *interface-name*
**no radius source-interface** *interface-name*

**Parameter Description**

| Parameter | Description |
|---|---|
| *interface-name* | Interface that the source IP address of the RADIUS packet belongs to. |

**Defaults** The source IP address of the RADIUS packet is set by the network layer.

**Command mode** Global configuration mode

**Usage Guide** In order to reduce the NAS information to be maintained on the RADIUS server, use this command to set the source IP address of the RADIUS packet. This command uses the first IP address of the specified interface as the source IP address of the RADIUS packet. This command is used in the layer 3 devices.

**Configuration Examples** The following example specifies that the RADIUS packet obtains an IP address from the fastEthernet 0/0 interface and uses it as the source IP address of the RADIUS packet.

```
Ruijie(config)# ip radius source-interface fastEthernet 0/0
```

**Related Commands**

| Command | Description |
|---|---|
| **radius-server host** | Defines the RADIUS server. |
| **ip address** | Configures the IP address of the interface. |

**Platform Description** N/A

## 3.3 ip vrf forwarding

Use this command to select a VRF for the AAA server group.
Use the **no** form of this command to restore the default setting.
**ip vrf forwarding** *vrf_name*
**no ip vrf forwarding**

**Parameter Description**

| Parameter | Description |
|---|---|
| *vrf_name* | VRF name |

**Defaults** N/A

**Command Mode** Server group configuration mode

**Usage Guide** This command is used to select a VRF for the specified server.

**Configuration Examples** The following example selects the VRF named vrf_name for AAA server group ss.

```
Ruijie(config)# aaa group server radius ss
Ruijie(config-gs-radius)# server 192.168.4.12
Ruijie(config-gs-radius)# server 192.168.4.13
Ruijie(config-gs-radius)# ip vrf forwarding vrf_name
Ruijie(config-gs-radius)# end
```

**Related Commands**

| Command | Description |
|---|---|
| N/A | N/A |

**Platform Description** N/A

## 3.4 radius attribute

Use this command to set the private attribute type value.

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

**radius attribute** { *id* **| down-rate-limit | dscp | mac-limit | up-rate-limit** } **vendor-type** *type*

**no radius attribute** { *id* | **down-rate-limit** | **dscp** | **mac-limit | up-rate-limit** } **vendor-type**

**Parameter Description**

| Parameter | Description |
|---|---|
| *id* | Function ID, in the range from 1 to 255 |
| *type* | Private attribute type, in the range from 1 to 255. |

**Defaults** Only the default configuration of private attributes in Ruijie is recognized.

| id | Function | type |
|---|---|---|
| 1 | max down-rate | 1 |
| 2 | 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 |
| 2 | file-name-1 | 12 |
| 13 | file-name-2 | 13 |
| 14 | file-name-3 | 14 |
| 15 | file-name-4 | 15 |
| 16 | max up-rate | 16 |
| 17 | version to server | 17 |
| 18 | flux-max-high32 | 18 |
| 19 | flux-max-low32 | 19 |
| 20 | proxy-avoid | 20 |
| 21 | dailup-avoid | 21 |
| 22 | ip privilege | 22 |
| 23 | login privilege | 42 |

Extended attributes:

| id | Function | type |
|---|---|---|
| 1 | max down-rate | 76 |
| 2 | qos | 77 |
| 3 | user ip | 3 |
| 4 | vlan id | 4 |
| 5 | version to client | 5 |
| 6 | net ip | 6 |
| 7 | user name | 7 |
| 8 | password | 8 |
| 9 | file-directory | 9 |
| 10 | file-count | 10 |
| 11 | file-name-0 | 11 |
| 12 | file-name-1 | 12 |
| 13 | file-name-2 | 13 |
| 14 | file-name-3 | 14 |
| 15 | file-name-4 | 15 |

| | | |
|---|---|---|
| 16 | max up-rate | 75 |
| 17 | version to server | 17 |
| 18 | flux-max-high32 | 18 |
| 19 | flux-max-low32 | 19 |
| 20 | proxy-avoid | 20 |
| 21 | dailup-avoid | 21 |
| 22 | ip privilege | 22 |
| 23 | login privilege | 42 |
| 24 | limit to user number | 50 |

**Command Mode** Global configuration mode

**Usage Guide** This command is used to configure the private attribute type value.

**Configuration Examples** The following example sets the type of max up-rate to 211.

```
Ruijie(config)# radius attribute 16 vendor-type 211
```

**Related Commands**

| Command | Description |
|---|---|
| **radius set qos cos** | Sets the qos value sent by the RADIUS server as the cos value of the interface. |

**Platform Description** N/A

## 3.5 radius vendor-specific extend

Use this command to extend RADIUS not to differentiate the IDs of private vendors.

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

**radius vendor-specific extend**

**no radius vendor-specific extend**

**Parameter Description**

| Parameter | Description |
|---|---|
| N/A | N/A |

**Defaults** Only the private vendor IDs of Ruijie are recognized.

**Command Mode** Global configuration mode

**Usage Guide** This command is used to identify the attributes of all vendor IDs by type.

**Configuration Examples** The following example extends RADIUS so as not to differentiate the IDs of private vendors:

```
Ruijie(config)# radius vendor-specific extend
```

**Related Commands**

| Command | Description |
|---|---|
| **radius attribute** | Configures vendor type. |
| **radius set qos cos** | Sets the QoS value sent by the RADIUS server as the cos value of the interface. |

**Platform Description** N/A

## 3.6 radius vendor-specific attribute support

Use this command to configure whether RADIUS accounting request packets carry the private attribute of a specified vendor.
Use the **no** form of this command to configure that RADIUS accounting request packets do not carry the private attribute of a specified vendor.
**radius vendor-specific attribute support { cisco | huawei | ms}**
**no radius vendor-specific attribute support { cisco | huawei | ms}**

**Parameter Description**

| Parameter | Description |
|---|---|
| **cisco** | Indicates the private attribute of Cisco. |
| **huawei** | Indicates the private attribute of Huawei. |
| **ms** | Indicates the private attribute of Microsoft. |

**Defaults** By default, RADIUS accounting request packets carry the private attribute of a specified vendor.

**Command Mode** Global configuration mode

**Usage Guide** This command is used to configure whether RADIUS accounting request packets carry the private attribute of a specified vendor as required.

**Configuration Examples** 1. The following example configures that RADIUS accounting request packets carry the private attribute of Huawei.

```
Ruijie(config)# radius vendor-specific attribute support huawei
```

2. The following example configures that RADIUS accounting request packets do not carry the private attribute of Huawei.

```
Ruijie(config)# no radius vendor-specific attribute support huawei
```

**Related Commands**

| Command | Description |
|---|---|
| N/A | N/A |

**Platform Description** N/A

## 3.7 radius-server account update retransmit

Use this command to configure accounting update packet retransmission for the second generation Web authentication user.
Use the **no** form of this command to restore the default setting,
**radius-server account update retransmit**
**no radius-server account update retransmit**

**Parameter Description**

| Parameter | Description |
|---|---|
| N/A | N/A |

**Defaults** This function is disabled by default.

**Command Mode** Global configuration mode

**Usage Guide** This command is used to configure accounting update packet retransmission for the second generation Web authentication user exclusively.

**Configuration Examples** The following example configures accounting update packet retransmission for the second generation Web authentication user.

```
Ruijie(config)#radius-server account update retransmit
```

**Related Commands**

| Command | Description |
|---|---|
| N/A | N/A |

**Platform** N/A

**Description**

## 3.8 radius-server attribute 31

Use this command to specify the MAC-based format of RADIUS Calling-Station-ID attribute.
Use the **no** form of this command to restore the default setting.
**radius-server attribute 31 mac format** { **ietf** | **normal** | **unformatted** }
**no radius-server attribute 31 mac format**

**Parameter Description**

| Parameter | Description |
|---|---|
| **ietf** | The standard format specified by the IETF RFC3580. '-'is used as the separator, for example: 00-D0-F8-33-22-AC. |
| **normal** | Normal format representing the MAC address. ;.'is used as the separator. For example: 00d0.f833.22ac. |
| **unformatted** | No format and separator. By default, unformatted is used. For example: 00d0f83322ac. |

**Defaults** The default format is unformatted.

**Command Mode** Global configuration mode

**Usage Guide** Some RADIUS security servers (mainly used to 802.1x authentication) may identify the IETF format only. In this case, the RADIUS Calling-Station-ID attribute shall be set as the IETF format type.

**Configuration Examples** The following example defines the RADIUS Calling-Station-ID attribute as IETF format.

```
Ruijie(config)# radius-server attribute 31 mac format ietf
```

**Related Commands**

| Command | Description |
|---|---|
| **radius-server host** | Defines the RADIUS server. |

**Platform Description** N/A

## 3.9 radius-server attribute class

Use this command to analyze the flow control value of the RADIUS CLASS attributes.
Use the **no** form of this command to restore the default setting.
**radius-server attribute class user-flow-control** { **format-16bytes** | **format-32bytes** }
**no radius-server attribute class user-flow-control**

**Parameter Description**

| Parameter | Description |
|---|---|
| **user-flow-control** | Analyzes flow control value in the CLASS attribute. |
| **format-16bytes** | Sets the format of flow control value to 16 bytes. |
| **format-32bytes** | Sets the format of flow control value to 32 bytes. |

**Defaults** This function is disabled by default.

**Command Mode** Global configuration mode

**Usage Guide** This command is required if the server pushes the flow control value through the CLASS attribute.

**Configuration Examples** The following example analyzes the flow control value of the CLASS attribute and sets the format to 32 bytes.

```
Ruijie(config)#radius-server attribute class user-flow-control
format-32bytes
```

**Related Commands**

| Command | Description |
|---|---|
| N/A | N/A |

**Platform Description** N/A

## 3.10 radius-server dead-criteria

Use this command to configure criteria on a device to determine that the Radius server is unreachable.

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

**radius-server dead-criteria** { **time** *seconds* [ **tries** *number* ] **| tries** *number* }

**no radius-server dead-criteria** { **time** *seconds* [ **tries** *number* ] **| tries** *number* }

**Parameter Description**

| Parameter | Description |
|---|---|
| **time** *seconds* | Configures the timeout value. If the device does not receive a correct response packet from the Radius server within the specified time, the Radius server is considered to be unreachable. The value is in the range from 1 to 120 in the unit of seconds. |
| **tries** *number* | Configures the successive timeout times. When sending a request from the device to the Radius server times out for the specified times, the device considers that the Radius server is unreachable. The value is in the range from 1 to 100 in the unit of seconds. |

**Defaults** The default **time** *seconds* is 60 and **tries** *number* is 10.

**Command Mode** Global configuration mode

**Usage Guide** If a Radius server meets the timeout and timeout times at the same time, it is considered to be unreachable. This command is used to adjust the parameter conditions of timeout and timeout times.

**Configuration Examples** The following example sets the timeout to 120 seconds and timeout times to 20.

```
Ruijie(config)# radius-server dead-criteria time 120 tries 20
```

**Related Commands**

| Command | Description |
|---|---|
| **radius-server host** | Defines the RADIUS security server. |
| **radius-server deadtime** | Defines the duration when a device stops sending any requests to an unreachable Radius server. |
| **radius-server timeout** | Defines the timeout for the packet re-transmission. |

**Platform Description** N/A

## 3.11 radius-server deadtime

Use this command to configure the duration when a device stops sending any requests to an unreachable Radius server.
Use the **no** form of this command to restore the default setting.
**radius-server deadtime** *minutes*
**no radius-server deadtime**

**Parameter Description**

| Parameter | Description |
|---|---|
| *minutes* | Defines the duration in minutes when the device stops sending any requests to the unreachable Radius server. The value is in the range from 1 to 1,440 in the unit of minutes. |

**Defaults** The default value of minutes is 0, that is, the device keeps sending requests to the unreachable Radius server.

**Command Mode** Global configuration mode

**Usage Guide** If active Radius server detection is enabled on the device, the time parameter of this command does not take effect on the Radius server. Otherwise, the Radius server becomes reachable when the duration set by this command is shorter than the unreachable time.

**Configuration Examples** The following example sets the duration when the device stops sending requests to 1 minute.

```
Ruijie(config)# radius-server deadtime 1
```

**Related Commands**

| Command | Description |
|---|---|
| **radius-server host** | Defines the RADIUS security server. |
| **radius-server dead-criteria** | Defines the criteria to determine that a Radius server is unreachable. |

**Platform Description** N/A

## 3.12 radius-server host

Use this command to specify a RADIUS security server host.
Use the **no** form of this command to restore the default setting.
**radius-server host** [ **oob**] { *ipv4-address* | *ipv6-address* } [ **auth-port** *port-number* ] [ **acct-port** *port-number* ] [ **test username** *name* [ **idle-time** *time* ] [ **ignore-auth-port** ] [ **ignore-acct-port** ] ] [ **key** [ **0** | **7** ] *text-string* ]
**no radius-server host** { *ipv4-address* | *ipv6-address* }

**Parameter Description**

| Parameter | Description |
|---|---|
| **oob** | Specifies an MGMT port as the source port for TACACS+ communication. |
| *Ipv4-address* | IPv6 address of the RADIUS security server host. |
| *Ipv6-address* | IPv4 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) Enables the active detection to the RADIUS security server and specify the username used by the active detection. |
| **idle-time** *time* | (Optional) Sets the interval of sending the test packets to the reachable RADIUS security server, which is 60 minutes by default and in the range of 1 to 1440 minutes (namely 24 hours). |

| | |
|---|---|
| **ignore-auth-port** | (Optional) Disables the detection to the authentication port on the RADIUS security server. It is enabled by default. |
| **ignore-acct-port** | (Optional) Disables the detection to the authentication port on the RADIUS security server. It is enabled by default. |
| **key** [ **0** \| **7** ] *text-string* | Configure a shared key for the server. The type of encryption can be specified. 0 is no encryption and 7 is simple encryption. The default is 0. |

**Defaults** No RADIUS host is specified by default.

**Command Mode** Global configuration mode

**Usage Guide** In order to implement the AAA security service using RADIUS, you must define a RADIUS security server. You can define one or more RADIUS security servers using the **radius-server host** command.

**Configuration Examples** The following example defines a RADIUS security server host:

```
Ruijie(config)# radius-server host 192.168.12.1
```

The following example defines a RADIUS security server host in the IPv4 environment, enable the active detection with the detection interval 60 minutes and disable the accounting UDP port detection:

```
Ruijie(config)# radius-server host 192.168.100.1 test username viven idle-time 60 ignore-acct-port
```

The following example defines a RADIUS security server host in the IPv6 environment

```
Ruijie(config)# radius-server host 3000::100
```

**Related Commands**

| Command | Description |
|---|---|
| **aaa authentication** | Defines the AAA authentication method list |
| **radius-server key** | Defines a shared password for the RADIUS security server. |
| **radius-server retransmit** | Defines the number of RADIUS packet retransmissions. |

**Platform Description** N/A

## 3.13 radius-server key

Use this command to define a shared password for the network access server (device) to communicate with the RADIUS security server.

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

**radius-server key** [ **0 | 7** ] *text-string*

**no radius-server key**

**Parameter Description**

| Parameter | Description |
|---|---|
| *text-string* | Text of the shared password |
| **0 \| 7** | Password encryption type.<br>0: no encryption;<br>7: Simply-encrypted. |

**Defaults** No shared password is specified by default.

**Command Mode** Global configuration mode.

**Usage Guide** A shared password is the basis for communications between the device and the RADIUS security server. In order to allow the device to communicate with the RADIUS security server, you must define the same shared password on the device and the RADIUS security server.

**Configuration Examples** The following example defines the shared password **aaa** for the RADIUS security server:

```
Ruijie(config)# radius-server key aaa
```

**Related Commands**

| Command | Description |
|---|---|
| **radius-server host** | Defines the RADIUS security server. |
| **radius-server retransmit** | Defines the number of RADIUS packet retransmissions. |
| **radius-server timeout** | Defines the timeout for the RADIUS packet. |

**Platform Description** N/A

## 3.14 radius-server retransmit

Use this command to configure the number of packet retransmissions before the device considers that the RADIUS security server does not respond.

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

**radius-server retransmit** *retries*

**no radius-server retransmit**

**Parameter Description**

| Parameter | Description |
|---|---|

| | |
|---|---|
| *retries* | Number of retransmissions in the range from 1 to 100 |

**Defaults** The default is 3.

**Command Mode** Global configuration mode.

**Usage Guide** AAA uses the next method to authenticate users only when the current security server for authentication does not respond. When the device retransmits the RADIUS packet for the specified times and the interval between every two retries is timeout, the device considers that the security sever does not respond.

**Configuration Examples** The following example sets the number of retransmissions to 4.

```
Ruijie(config)# radius-server retransmit 4
```

**Related Commands**

| Command | Description |
|---|---|
| **radius-server host** | Defines the RADIUS security server. |
| **radius-server key** | Defines a shared password for the RADIUS server. |
| **radius-server timeout** | Defines the timeout for the RADIUS packet. |

**Platform Description** N/A

## 3.15 radius-server source-port

Use this command to configure the source port to send RADIUS packets.
Use the **no** form of this command to restore the default setting.
**radius-server source-port** *port*
**no radius-server source-port**

**Parameter Description**

| Parameter | Description |
|---|---|
| *port* | The port ID, in the range from 0 to 65535. |

**Defaults** The default is a random number.

**Command Mode** Global configuration mode

**Usage Guide** The source port is random by default. This command is used to specify a source port.

**Configuration Examples** The following example configures source port 10000 to send RADIUS packets.

```
Ruijie(config)# radius-server source-port 10000
```

**Related Commands**

| Command | Description |
|---|---|
| N/A | N/A |

**Platform Description** N/A

## 3.16 radius-server timeout

Use this command to set the time for the device to wait for a response from the security server after retransmitting the RADIUS packet.

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

**radius-server timeout** *seconds*

**no radius-server timeout**

**Parameter Description**

| Parameter | Description |
|---|---|
| *seconds* | Timeout in the range from 1 to 1,000 in the unit of seconds. |

**Defaults** The default is 5 seconds.

**Command Mode** Global configuration mode

**Usage Guide** This command is used to change the timeout of packet retransmission.

**Configuration Examples** The following example sets the timeout to 10 seconds.

```
Ruijie(config)# radius-server timeout  10
```

**Related Commands**

| Command | Description |
|---|---|
| **radius-server host** | Defines the RADIUS security server. |
| **radius-server retransmit** | Defines the number of the RADIUS packet retransmissions. |
| **radius-server key** | Defines a shared password for the RADIUS server. |

**Platform Description** N/A

## 3.17 radius set qos cos

Use this command to set the QoS value sent by the RADIUS server as the CoS value of the interface.
Use the **no** form of this command to restore the default setting.
**radius set qos cos**
**no radius set qos cos**

**Parameter Description**

| Parameter | Description |
|---|---|
| N/A | N/A |

**Defaults** Set the QoS value sent by the RADIUS server as the DSCP value.

**Command Mode** Global configuration mode.

**Usage Guide**

**Configuration Examples** The following example sets the QoS value sent by the RADIUS server as the CoS value of the interface:

```
Ruijie(config)# radius set qos cos
```

**Related Commands**

| Command | Description |
|---|---|
| **radius vendor-specific extend** | Extends RADIUS as not to differentiate the IDs of private vendors. |

**Platform Description** N/A

## 3.18 radius support cui

Use this command to enable RADIUS to support the cui function.
Use the **no** form of this command to restore the default setting.
**radius support cui**
**no radius support cui**

**Parameter Description**

| Parameter | Description |
|---|---|
| N/A | N/A |

**Defaults** This function is disabled by default.

**Command Mode** Global configuration mode

**Usage Guide** This command is used to enable RADIUS to support the cui function.

**Configuration Examples** The following example enables RADIUS to support the cui function.

```
Ruijie(config)# radius support cui
```

**Related Commands**

| Command | Description |
|---|---|
| N/A | N/A |

**Platform Description** N/A

## 3.19 server auth-port acct-port

Use this command to add the server of the AAA server group.
Use the **no** form of this command to restore the default setting.
**server** { *ipv4-addr* | *ipv6-addr*} [ **auth-port** *port1* ] [ **acct-port** *port2* ]
**no server** { *ipv4-addr* | *ipv6-addr*} [ **auth-port** *port1* ] [ **acct-port** *port2* ]

**Parameter Description**

| Parameter | Description |
|---|---|
| *ip-addr* | Server IP address |
| *Ipv6-addr* | Server IPv6 address |
| *port1* | Server authentication port |
| *port2* | Server accounting port |

**Defaults** No server is configured by default.

**Command Mode** Server group configuration mode

**Usage Guide** N/A

**Configuration Examples** The following example adds server 192.168.4.12 to server group ss and sets the accounting port and authentication port to 5 and 6 respectively.

```
Ruijie(config)# aaa group server radius ss
Ruijie(config-gs-radius)# server 192.168.4.12 acct-port 5 auth-port 6
Ruijie(config-gs-radius)# end
Ruijie# show aaa group
Type      Reference  Name
```

```
---------- ---------- ----------
radius     1          radius
tacacs+    1          tacacs+
radius     1          ss
```

**Related Commands**

| Command | Description |
| --- | --- |
| N/A | N/A |

**Platform Description** N/A

## 3.20 show radius acct statistics

Use this command to display RADIUS accounting statistics.

**show radius acct statistics**

**Parameter Description**

| Parameter | Description |
| --- | --- |
| N/A | N/A |

**Defaults** N/A

**Command Mode** Global configuration mode/Privileged EXEC mode/Interface configuration mode

**Usage Guide** N/A

**Configuration Examples** The following example displays RADIUS accounting statistics.

```
Ruijie#show radius acct statistics
Accounting Servers:

Server Index..................................... 1
Server Address................................... 192.168.1.1
Server Port...................................... 1813
Msg Round Trip Time.............................. 0 (msec)
First Requests................................... 1
Retry Requests................................... 1
Accounting Responses............................. 0
Malformed Msgs................................... 0
Bad Authenticator Msgs........................... 0
Pending Requests........
```

**Related Commands**

| Command | Description |
| --- | --- |
| N/A | N/A |

**Platform Description** N/A

## 3.21 show radius auth statistics

Use this command to display RADIUS authentication statistics.

**show radius auth statistics**

**Parameter Description**

| Parameter | Description |
| --- | --- |
| N/A | N/A |

**Defaults** N/A

**Command Mode** Global configuration mode/Privileged EXEC mode/Interface configuration mode

**Usage Guide** N/A

**Configuration Examples** The following example displays RADIUS authentication statistics.

```
Ruijie#show radius auth statistics
Authentication Servers:

Server Index..................................... 1
Server Address................................... 192.168.1.1
Server Port...................................... 1812
Msg Round Trip Time.............................. 0 (msec)
First Requests................................... 0
Retry Requests................................... 0
Accept Responses................................. 0
Reject Responses................................. 0
Challenge Responses.............................. 0
Malformed Msgs................................... 0
Bad Authenticator Msgs........................... 0
Pending Requests................................. 0
Timeout Requests................................. 0
Unknowntype Msgs................................. 0
Other Drops...................................... 0
```

**Related Commands**

| Command | Description |
| --- | --- |
| N/A | N/A |

**Platform Description** N/A

## 3.22 show radius group

Use this command to display RADIUS server group configuration.

**show radius group**

**Parameter Description**

| Parameter | Description |
| --- | --- |
| N/A | N/A |

**Defaults** N/A

**Command Mode** Global configuration mode/Privileged EXEC mode/Interface configuration mode

**Usage Guide** N/A

**Configuration Examples** The following example displays RADIUS server group configuration.

```
Ruijie#show radius group
==========Radius group radius==========
Vrf:not-set
Server:192.168.1.1
  Server key:ruijie
  Authentication port:1812
  Accounting port:1813
  State:Active
```

**Related Commands**

| Command | Description |
| --- | --- |
| N/A | N/A |

**Platform Description** N/A

## 3.23 show radius parameter

Use this command to display global RADIUS server parameters.

**show radius parameter**

**Parameter Description**

| Parameter | Description |
|---|---|
| N/A | N/A |

**Defaults** N/A

**Command Mode** Global configuration mode/Privileged EXEC mode/Interface configuration mode

**Usage Guide** N/A

**Configuration Examples** The following example displays global RADIUS server parameters.

```
Ruijie# show radius parameter
Server Timout:   5 Seconds
Server Deadtime: 0 Minutes
Server Retries:  3
Server Dead Critera:
Time:       10 Seconds
Tries:      10
```

**Related Commands**

| Command | Description |
|---|---|
| N/A | N/A |

**Platform Description** N/A

## 3.24 show radius server

Use this command to display the configuration of the RADIUS server.

**show radius server**

**Parameter Description**

| Parameter | Description |
|---|---|
| N/A | N/A |

**Defaults** N/A

**Command Mode** Global configuration mode, privileged EXEC mode, interface configuration mode

**Usage Guide** N/A

**Configuration Examples** The following example displays the configuration of the RADIUS server.

```
Ruijie# show radius server
Server IP:   192.168.4.12
Accounting  Port:  23
Authen  Port:    77
Test Username:   viven
Test Idle Time:   10 Minutes
Test Ports:       Authen
Server State:    Active
   Current duration 765s, previous duration 0s
Dead: total time 0s, count 0
Statistics:
Authen: request 15, timeouts 1
Author: request 0, timeouts 0
Account: request 0, timeouts 0

Server IP:   192.168.4.13
Accounting Port:  45
Authen  Port:    74
Test Username:   <Not Configured>
Test Idle Time:   60 Minutes
Test Ports:       Authen and Accounting
Server State:    Active
Current duration 765s, previous duration 0s
Dead: total time 0s, count 0
Statistics:
Authen: request 0, timeouts 0
Author: request 0, timeouts 0
Account: request 20, timeouts 0
```

**Related Commands**

| Command | Description |
|---|---|
| **radius-server host** | Defines the RADIUS security server. |
| **radius-server retransmit** | Defines the number of RADIUS packet retransmissions. |
| **radius-server key** | Defines a shared password for the RADIUS server. |
| **radius-server timeout** | Defines the packet transmission timeout. |

**Platform Description** N/A

## 3.25 show radius vendor-specific

Use this command to display the configuration of the private vendors.

**show radius vendor-specific**

**Parameter Description**

| Parameter | Description |
|---|---|
| N/A | N/A |

**Defaults** N/A

**Command Mode** Global configuration mode, privileged EXEC mode, interface configuration mode

**Usage Guide** N/A

**Configuration Examples** The following example displays the configuration of the private vendors.

```
Ruijie#show radius vendor-specific
id    vendor-specific     type-value
----- -------------------- ----------
1     max-down-rate       1
2     port-priority       2
3     user-ip            3
4     vlan-id            4
5     last-supplicant-vers 5
      ion
6     net-ip             6
7     user-name           7
8     password           8
9     file-directory      9
10    file-count         10
11    file-name-0         11
12    file-name-1         12
13    file-name-2         13
14    file-name-3         14
15    file-name-4         15
16    max-up-rate         16
17    current-supplicant-version 17
18    flux-max-high32     18
19    flux-max-low32      19
20    proxy-avoid        20
21    dialup-avoid        21
22    ip-privilege        22
23    login-privilege     42
```

```
26   ipv6-multicast-addre 79
     ss
27   ipv4-multicast-addre 87
     ss
```

**Related Commands**

| Command | Description |
|---|---|
| **radius-server host** | Defines the RADIUS security server. |
| **radius-server retransmit** | Defines the number of RADIUS packet retransmissions. |
| **radius-server key** | Defines a shared password for the RADIUS server. |
| **radius-server timeout** | Defines the packet transmission timeout. |

**Platform Description**

N/A

# 4 802.1X Commands

## 4.1 clear dot1x user all

Use this command to clear all the 802.1X authentication users.

**clear dot1x user all**

| Parameter Description | Parameter | Description |
|---|---|---|
| | N/A | N/A |

**Defaults** N/A

**Command Mode** Privileged EXEC mode

**Usage Guide** Use this command to clear all the 802.1X authentication users.

**Configuration Examples** The following example clears all the 802.1X authentication users.

```
Ruijie#clear dot1x user all
```

| Related Commands | Command | Description |
|---|---|---|
| | N/A | N/A |

**Platform Description** N/A

## 4.2 clear dot1x user id

Use this command to clear 802.1X authentication users according to session IDs.

**clear dot1x user id** *session-id*

| Parameter Description | Parameter | Description |
|---|---|---|
| | *session-id* | Session ID |

**Defaults** N/A

**Command Mode** Privileged EXEC mode

**Usage Guide** Use this command to clear 802.1X authentication users according to session IDs.

**Configuration Examples** The following example clears an 802.1X authentication user whose session ID is 12345678.

```
Ruijie#clear dot1x user id 12345678
```

| Related Commands | Command | Description |
|---|---|---|
| | N/A | N/A |

**Platform Description** N/A

## 4.3 clear dot1x user mac

Use this command to clear 802.1X authentication users according to MAC addresses.

**clear dot1x user mac** *mac-addr*

| Parameter Description | Parameter | Description |
|---|---|---|
| | *mac-addr* | MAC address |

**Defaults** N/A

**Command Mode** Privileged EXEC mode

**Usage Guide** Use this command to clear 802.1X authentication users according to MAC addresses.

**Configuration Examples** The following example clears an 802.1X authentication user whose MAC address is 0012.3456.789A.

```
Ruijie#clear dot1x user mac 0012.3456.789A
```

| Related Commands | Command | Description |
|---|---|---|
| | N/A | N/A |

**Platform Description** N/A

## 4.4 clear dot1x user name

Use this command to clear the 802.1 X authentication users according to the username.

**clear dot1x user name** *name-str*

| Parameter Description | Parameter | Description |
|---|---|---|
| | *name-str* | The username of the 802.1X authentication user |

**Defaults** N/A

**Command Mode** Privileged EXEC mode

**Usage Guide** Use this command to clear the 802.1 X authentication users according to the username.

**Configuration Examples** The following example clears the 802.1X authentication user named 802.1X-user.

```
Ruijie#clear dot1x user name dot1x-user
```

**Related Commands**

| Command | Description |
|---|---|
| N/A | N/A |

**Platform Description** N/A

## 4.5 clear dot1x user ip

Use this command to clear 802.1X authentication users according to IP addresses.

**clear dot1x user ip** *ip-addr*

**Parameter Description**

| Parameter | Description |
|---|---|
| *ip-addr* | IP address |

**Defaults** N/A

**Command Mode** Privileged EXEC mode

**Usage Guide** Use this command to clear 802.1X authentication users according to IP addresses.

**Configuration Examples** The following example clears an 802.1X authentication user whose IP address is 11.1.1.1.

```
Ruijie#clear dot1x user ip 11.1.1.1
```

**Platform Description** N/A

## 4.6 dot1x accounting

Use this command to configure the accounting list.

**dot1x accounting** *list-name*

**Parameter Description**

| Parameter | Description |
|---|---|
| *list-name* | The name of the accounting list |

**Defaults** N/A

| | |
|---|---|
| **Command Mode** | Privileged EXEC mode/WLAN security configuration mode |
| **Usage Guide** | If AAA does not adopts 802.1X accounting as the default accounting method. Use this command to configure the 802.1X accounting method.<br>Configuration in WLAN security configuration mode is prior to that in global configuration mode. |
| **Configuration Examples** | The following example configures the accounting list.<br>`Ruijie(config)# dot1x accounting dot1x-acct` |

**Related Commands**

| Command | Description |
|---|---|
| N/A | N/A |

| | |
|---|---|
| **Platform Description** | N/A |

## 4.7 dot1x acct-update base-on first-time server

Use this command to assign the accounting update interval for the first authentication.
Use the **no** form of this command to restore the default settings.
**dot1x acct-update base-on first-time server**
**no dot1x acct-update base-on first-time server**

**Parameter Description**

| Parameter | Description |
|---|---|
| N/A | N/A |

| | |
|---|---|
| **Defaults** | The assignment is disabled by default. |
| **Command Mode** | Global configuration mode |
| **Usage Guide** | Some portal servers do not support the assignment of accounting update interval during re-authentication. Use this command if such servers demand users to issue accounting update packets according to the interval in the first authentication. |
| **Configuration Examples** | The following example assigns the accounting update interval for the first authentication.<br>`Ruijie(config)# dot1x acct-update base-on first-time server` |
| **Platform Description** | N/A |

## 4.8 dot1x auth-mode

Use this command to specify the 802.1X authentication mode.

**dot1x auth-mode** { **eap** | **chap** | **pap** }

| **Parameter Description** | **Parameter** | **Description** |
|---|---|---|
| | N/A | N/A |

**Defaults** The default is EAP-MD5 authentication mode.

**Command Mode** Global configuration mode

**Usage Guide** The selection of authentication mode depends on the suppliant and portal server.

**Configuration Examples** The following example enables CHAP authentication mode.

```
Ruijie(config)# dot1x auth-mode chap
```

| **Related Commands** | **Command** | **Description** |
|---|---|---|
| | **show dot1x** | Displays the 802.1X information. |

**Platform Description** N/A

## 4.9 dot1x authentication

Use this command to configure the authentication method list.

**dot1x authentication** *list-name*

| **Parameter Description** | **Parameter** | **Description** |
|---|---|---|
| | *list-name* | Authentication method list |

**Defaults** N/A

**Command Mode** Global configuration mode/WLAN security configuration mode

**Usage Guide** If AAA does not adopt the default 802.1X authentication, use this command to configure the 802.1X authentication method.

Configuration in WLAN security configuration mode is prior to that in global configuration mode.

**Configuration Examples** The following example configures the authentication method list

```
Ruijie(config)# dot1x authentication dot1x-authen
```

| Related Commands | Command | Description |
|---|---|---|
| | N/A | N/A |

**Platform Description** N/A

## 4.10 dot1x dbg-filter

Use this command to enable debug information print for a user with a specified MAC address.
Use the **no** form of this command to clear the debug information.
**dot1x dbg-filter** *H.H.H*
**no dot1x dbg-filter** *H.H.H*

| Parameter Description | Parameter | Description |
|---|---|---|
| | *H.H.H* | The MAC address of a user |

**Defaults** Debug information of all authentication users is printed by default.

**Command mode** Global configuration mode

**Usage Guide** Use this command to print the debug information of a specific user If you want to locate the fault on the network where there are multiple users.

**Configuration Examples** The following example prints the debug information of the device with the specified MAC address.

```
Ruijie(config)# dot1x dbg-filter 00d0.f800.0001
```

| Related Commands | Command | Description |
|---|---|---|
| | N/A | N/A |

**Platform Description** N/A

## 4.11 dot1x default-user-limit

Use this command to set the maximum auth-user number on controlled interfaces.
Use the **no** form of this command to restore the default setting.
**dot1x default-user-limit** *num*
**no dot1x default-user-limit**

| Parameter Description | Parameter | Description |
|---|---|---|
| | *num* | The maximum auth-user number allowed by a controlled |

| | |
|---|---|
| | interface, in the range from 1 to 1,000,000 |

**Defaults** By default, there is not a limitation for the auth-user number.

**Command mode** Interface configuration mode

**Usage Guide** This command is used to limit the number of users to be authenticated on a specific port.

**Configuration Examples** The following example sets the maximum auth-user number on a controlled interface.

```
Ruijie(config-if)# dot1x default-user-limit 10
```

**Related Commands**

| Command | Description |
|---|---|
| **show dot1x port-control interface fastEthernet 0/10** | Displays the number of users allowed by a specific 802.1X interface. |
| **show dot1x port-control interface fastEthernet 0/10** | Displays the number of users allowed by a specific 802.1X interface. |

**Platform Description** N/A

## 4.12 dot1x default

Use this command to restore 802.1X configuration to the default setting.

**dot1x default**

**Parameter Description**

| Parameter | Description |
|---|---|
| N/A | N/A |

**Defaults** N/A

**Command Mode** Global configuration mode

**Usage Guide** This command is used to restore 802.1X configuration for quick re-configuration.

**Configuration Examples** The following example restores 802.1X configuration to the default setting.

```
Ruijie(config)# dot1x default
```

**Related Commands**

| Command | Description |
|---|---|
| **show dot1x** | Displays the 802.1X information. |

**Platform Description** N/A

## 4.13 dot1x encryption only

Use this command to enable the 802.1X authentication for only encryption purpose. WEB authentication functions in place of 802.1X for authentication purpose.
Use the **no** form of this command to restore the default setting.
**dot1x encryption only**
**no dot1x encryption only**

**Parameter Description**

| Parameter | Description |
|---|---|
| N/A | N/A |

**Defaults** This function is disabled by default.

**Command Mode** WLAN security configuration mode

**Usage Guide** Use this command to enable the 802.1X authentication for only encryption purpose. WEB authentication functions in place of 802.1X for authentication purpose.

**Configuration Examples** The following example enables the 802.1X authentication for only encryption purpose.

```
Ruijie(config-wlansec)#dot1x encryption only
```

**Related Commands**

| Command | Description |
|---|---|
| N/A | N/A |

**Platform Description** This command is supported only on wireless products.

## 4.14 dot1x event server-invalid action bypass-wlan

Use this command to enable the RADIUS server bypass function and support the bypass WLAN.
Use the **no** form of this command to restore the default setting.
**dot1x event server-invalid action bypass-wlan** *wlan-id*
**no dot1x event server-invalid action bypass-wlan**

**Parameter Description**

| Parameter | Description |
|---|---|
| *wlan-id* | The ID of the bypass WLAN |

**Defaults** This function is disabled by default.

**Command Mode** Global configuration mode

**Usage Guide** Use this command to enable the RADIUS server bypass function and support the bypass WLAN.

**Configuration Examples** The following example enables the RADIUS server bypass function.

```
Ruijie(config)#dot1x event server-invalid action bypass-wlan 10
```

**Related Commands**

| Command | Description |
| --- | --- |
| N/A | N/A |

**Platform Description** This command is supported only on wireless products.

## 4.15 dot1x get-static-ip enable

Use this command to obtain static IP addresses.

**dot1x get-static-ip enable**

Use this command to restore the default setting.

**no dot1x get-static-ip enable**

**Parameter Description**

| Parameter | Description |
| --- | --- |
| N/A | N/A |

**Defaults** This function is disabled by default.

**Command Mode** Global configuration mode

**Usage Guide** Enable this function when wireless terminals use static IP addresses and need to upload the static IP addresses to the server.

Note that the IP addresses are uploaded to the server via accounting packets. In addition, when static IP addresses are used, terminal identification information is not provided.

**Configuration Examples** The following example obtains static IP addresses.

```
Ruijie(config)# dot1x get-static-ip enable
```

**Platform Description**

## 4.16 dot1x logging rate-limit

Use this command to set the logging rate-limit.
**dot1x logging rate-limit** *value*
Use this command to restore the default setting.
**no dot1x logging**

**Parameter Description**

| Parameter | Description |
|---|---|
| *value* | Logging rate<br>0: logging rate is not limited. |

**Defaults** The default is 5 logs per second.

**Command Mode** Global configuration mode

**Usage Guide** The default setting is recommended. Lower the limit in case of much online/offline which raises CPU occupation.

**Configuration Examples** The following example sets the logging rate-limit to 20 logs per second.

```
Ruijie(config)# dot1x logging rate-limit 20
```

**Platform Description** This command is supported only on wireless products.

## 4.17 dot1x mab-username upper

Use this command to enable uppercase letters in MAB user names.
**dot1x mab-username upper**

**Parameter Description**

| Parameter | Description |
|---|---|
| N/A | N/A |

**Defaults** This function is disabled by default.

**Command Mode** Global configuration mode.

**Usage Guide** By default, lowercase letters are used in the user name of MAB. After this function is enabled, uppercase letters are used in new user names of MAB to meet server requirements.

**Configuration** The following example enables uppercase letters in MAB user names.

**Examples**

```
Ruijie(config)# dot1x mab-username upper
```

**Related Commands**

| Command | Description |
| --- | --- |
| N/A | N/A |

**Platform Description** N/A

## 4.18 dot1x mab-username format

Use this command to configure the MAB authentication user name format.
Use the **no** form of this command to restore the default settings.
**dot1x mab-username format [with-dot | with-colon | with-hyphen]**
**no dot1x mab-username format**

**Parameter Description**

| Parameter | Description |
| --- | --- |
| N/A | N/A |

**Defaults** By default, this function is disabled.

**Command Mode** Global configuration mode

**Usage Guide**
**dot1x mab-username format with-dot** is used to configure the MAB authentication user name format xxxx.xxxx.xxxx.
**dot1x mab-username format with-colon** is used to configure the MAB authentication user name format xx:xx:xx:xx:xx:xx.
**dot1x mab-username format with-hyphen** is used to configure the MAB authentication user name format xx-xx-xx-xx-xx-xx.

**Configuration Examples** The following example configures the MAB authentication user name format.

```
Ruijie(config)# dot1x mab-username format with-hyphen
```

**Platform Description** N/A

## 4.19 dot1x max-req

Use this command to set the maximum attempts of authentication requests.
**dot1x max-req** *num*

**Parameter**

| Parameter | Description |
| --- | --- |

| Description | *num* | Maximum attempts |
|---|---|---|

**Defaults** The default is 3.

**Command Mode** Global configuration mode

**Usage Guide** Use the **show dot1x** command to display the 802.1X configuration.

**Configuration Examples** The following example sets the maximum attempts of authentication requests to 2.

```
Ruijie(config)# dot1x max-req 2
```

| Related Commands | Command | Description |
|---|---|---|
| | **show dot1x** | Displays the information about 802.1X. |

**Platform Description** N/A

## 4.20 dot1x multi-account enable

Use this command to enable the user with one single MAC address to perform authentication with multiple accounts.
Use the **no** form of this command to restore the default setting.
**dot1x multi-account enable**
**no dot1x multi-account enable**

| Parameter Description | Parameter | Description |
|---|---|---|
| | N/A | N/A |

**Defaults** This function is disabled by default.

**Command Mode** Global configuration mode

**Usage Guide** Use the command to enable the multiple-account authentication if you want to switch the username in the authentication or re-authentication, especially in the windows domain authentication.

**Configuration Examples** The following example enables the multiple-account authentication.

```
Ruijie(config)# dot1x multi-account enable
```

| Related Commands | Command | Description |
|---|---|---|
| | N/A | N/A |

**Platform Description** N/A

## 4.21 dot1x offline-detect

Use this command to enable traffic detection.
Use the **no** form of this command to disable this function.
**dot1x offline-detect** {[**interval** *val*] | [**flow** *num*]}
**no dot1x offline-detect** {[**interval** *val*] | [**flow** *num*]}

**Parameter Description**

| Parameter | Description |
|---|---|
| *val* | Traffic detection interval in the unit of minutes<br>The default is 15 minutes. |
| *num* | Traffic threshold in the unit of KB<br>The default is 0 KB. |

**Defaults** AC: This function is enabled by default.
AP: This function is disabled by default.

**Command Mode** WLAN security configuration mode

**Usage Guide** (Optional) Use this command to prevent the device from accounting when a STA has been offline. The traffic detection parameters configured in WLAN security configuration mode are prior to those configured in global configuration mode.

**Configuration Examples** The following example enables traffic detection.

```
Ruijie(config)# dot1x offline-detect interval 5 flow 20
```

**Platform Description** This command is supported only on wireless products.

## 4.22 dot1x reauth-max

Use this command to set the maximum re-auth attempts.
Use the **no** form of this command to restore the default setting.
**dot1x reauth-max** *num*

**Parameter Description**

| Parameter | Description |
|---|---|
| *num,* | Maximum re-auth attempts. The range is from 1 to 10. |

**Defaults** The default is 3.

**Command Mode** Global configuration mode

**Usage Guide** Use this command to specify the maximum number of supplicant re-authentications. Use the **show dot1x** command to display 802.1X configuration.

**Configuration Examples** The following example sets the maximum re-auth attempts to 2.

```
Ruijie(config)# dot1x reauth-max 2
```

**Related Commands**

| Command | Description |
|---|---|
| **show dot1x** | Displays the 802.1X information. |

**Platform Description** N/A

## 4.23 dot1x re-authentication

Use this command to enable timed re-authentication function.
Use the **no** form of the command to restore the default setting.
**dot1x re-authentication**
**no dot1x re-authentication**

**Parameter Description**

| Parameter | Description |
|---|---|
| N/A | N/A |

**Defaults** This function is disabled by default.

**Command Mode** Global configuration mode

**Usage Guide** This command will re-authenticate the supplicant periodically after he passes the authentication. Use the **show dot1x** command to display 802.1X configuration. The default setting is recommended.

**Configuration Examples** The following example enables timed re-authentication function.

```
Ruijie(config)# dot1x re-authentication
```

**Related Commands**

| Command | Description |
|---|---|
| **show dot1x** | Displays the 802.1X information. |

**Platform Description** N/A

## 4.24 dot1x timeout re-authperiod

Use this command to set the re-authentication interval when re-authentication is enabled.

**dot1x timeout re-authperiod** *time*

| **Parameter Description** | **Parameter** | **Description** |
|---|---|---|
| | *time* | Authentication interval, in the range from 1 to 65,535 in the unit of seconds. |

**Defaults** The default is 3,600 seconds.

**Command Mode** Global configuration mode

**Usage Guide** Use the **show dot1x** command to display the 802.1X configuration.

**Configuration Examples** The following example sets the re-authentication interval to 2,400 seconds.

```
Ruijie(config)# dot1x timeout re-authperiod 2400
```

| **Related Commands** | **Command** | **Description** |
|---|---|---|
| | **show dot1x** | Displays the information about 802.1X. |

**Platform Description** N/A

## 4.25 dot1x timeout quiet-period

Use this command to set the quiet period after authentication failure.

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

**dot1x timeout quiet-period** *time*

| **Parameter Description** | **Parameter** | **Description** |
|---|---|---|
| | *time* | Sets the quiet period after authentication failure, in the range from 1 to 65,535 in the unit of seconds. |

**Defaults** The default is 10 seconds.

**Command Mode** Global configuration mode

**Usage Guide** When authentication fails, the supplicant must wait for a period of time before re-authentication.

**Configuration** The following example sets the quiet period after authentication failure to 60 seconds.

**Examples**

```
Ruijie(config)# dot1x timeout quiet-period 60
```

**Related Commands**

| Command | Description |
| --- | --- |
| **show dot1x** | Displays the 802.1X information. |

**Platform Description** N/A

## 4.26 dot1x timeout supp-timeout

Use this command to set the authentication timeout between the device and the supplicant.

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

**dot1x timeout supp-timeout** *time*

**Parameter Description**

| Parameter | Description |
| --- | --- |
| *time* | Authentication timeout between the device and the supplicant<br>The range is from 1 to 65,535 seconds. |

**Defaults** The default is 3 seconds.

**Command Mode** Global configuration mode

**Usage Guide** Use the **show dot1x** command to show display 802.1X configuration.

**Configuration Examples** The following example sets the authentication timeout between the device and the supplicant to 10s:

```
Ruijie(config)# dot1x timeout supp-timeout 10
```

**Related Commands**

| Command | Description |
| --- | --- |
| **show dot1x** | Displays the information about 802.1x. |

**Platform Description** N/A

## 4.27 dot1x timeout server-timeout

Use this command to set the server timeout interval.

**dot1x timeout server-timeout** *time*

**Parameter Description**

| Parameter | Description |
| --- | --- |
| *time* | The server timeout interval, in the range from 1 to 65,535 in the unit of seconds |

**Defaults** The default is 5 seconds.

**Command Mode** Global configuration mode

**Usage Guide** By default, the timeout of the 802.1X server is less than that of the Radius server. Use this command to raise the 802.1X timeout so as to exceed the Radius value. For details, see *Configuration Guide*.

**Configuration Examples** The following example set the server timeout interval to 10 seconds.

```
Ruijie(config)# dot1x timeout server-timeout 10
```

**Related Commands**

| Command | Description |
|---|---|
| **show dot1x** | Displays the 802.1X information. |

**Platform Description** N/A

## 4.28 dot1x timeout tx-period

Use this command to set the request/id packet re-transmission interval.

**dot1x timeout tx-period** *time*

**Parameter Description**

| Parameter | Description |
|---|---|
| *time* | The request/id packet re-transmission interval, in range from 1 to 65,535 in the unit of seconds |

**Defaults** The default is 3 seconds.

**Command Mode** Global configuration mode

**Usage Guide** Use the **show dot1x** command to display 802.1X configuration.

**Configuration Examples** The following example sets the request/id packet re-transmission interval to 5 seconds.

```
Ruijie(config)# dot1x timeout tx-period 5
```

**Related Commands**

| Command | Description |
|---|---|
| **show dot1x** | Displays the information about 802.1X. |

**Platform Description** N/A

## 4.29 dot1x user-trap enable

Use this command to enable users to send online/offline traps.

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

**dot1x user-trap enable**

**no dot1x user-trap enable**

| **Parameter Description** | **Parameter** | **Description** |
|---|---|---|
| | N/A | Authentication timeout between the device and the supplicant<br>The range is from 0 to 65,535 seconds. |

**Defaults** This function is disabled by default.

**Command Mode** Global configuration mode

**Usage Guide** Use this command to enable users to send online/offline traps to the SNMP server.

**Configuration Examples** The following example enables STAs to send online/offline traps.

```
Ruijie(config)# dot1x user-trap enable
```

**Platform Description** N/A

## 4.30 dot1x valid-ip-acct enable

Use this command to enable IP address-triggered accounting.

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

**dot1x valid-ip-acct enable**

**no dot1x valid-ip-acct enable**

| **Parameter Description** | **Parameter** | **Description** |
|---|---|---|
| | N/A | N/A |

**Defaults** This function is disabled by default.

**Command Mode** Global configuration mode

**Usage Guide** Use this command to enable accounting only when users obtain valid IP addresses.

**Configuration** The following example enables IP address-triggered accounting.

**Examples**

```
Ruijie(config)#dot1x valid-ip-acct enable
```

**Platform Description** N/A

## 4.31 dot1x valid-ip-acct timeout

Use this command to configure IP address-triggered accounting timeout.
Use the **no** form of this command to restore the default setting.
**dot1x valid-ip-acct timeout** *time*
**no dot1x valid-ip-acct timeout**

**Parameter Description**

| Parameter | Description |
|---|---|
| *time* | IP address-triggered accounting timeout in the unit of minutes |

**Defaults** The default is 5 minutes.

**Command Mode** Global configuration mode

**Usage Guide** The SNMP server will not start accounting until users obtain IP addresses. In this case, use this command to configure the IP address-triggered accounting timeout.

**Configuration Examples** The following example configures IP address-triggered accounting timeout.

```
Ruijie(config)# dot1x valid-ip-acct timeout 10
```

**Platform Description** N/A

## 4.32 dot1x-mab

Use this command to enable MAB function in WLAN.
Use the **no** form of this command to restore the default setting.
**dot1x-mab**
**no dot1x-mab**

**Parameter Description**

| Parameter | Description |
|---|---|
| N/A | N/A |

**Defaults** This function is disabled by default.

**Command Mode** WLAN security configuration mode

**Usage Guide** (Optional) Use this command to enable MAB function for MAC-based security authentication in WLAN.

**Configuration Examples** The following example enables MAB function in WLAN.

```
Ruijie(config-wlansec)# dot1x-mab
```

**Platform Description** This command is supported only on wireless products.

## 4.33 show dot1x

Use this command to display the 802.1X setting.

**show dot1x**

**Parameter Description**

| Parameter | Description |
|---|---|
| N/A | N/A |

**Defaults** N/A

**Command Mode** Privileged EXEC mode/Global configuration mode/Interface configuration mode

**Usage Guide** N/A

**Configuration Examples** The following example displays the 802.1X setting.

```
Ruijie#show dot1x

802.1X basic information:
  802.1X Status ..................... enable
  Authentication Mode ................ eap
  Authorization mode ................. disable
  Total User Number .................. 0 (exclude dynamic user)
  Authenticated User Number ..... 0 (exclude dynamic user)
  Dynamic User Number ................ 0
  Re-authentication .................. disable
  Re-authentication Period ..... 3600 seconds
  Re-authentication max ..... 3 times
  Quiet Period ..... 10 seconds
  Tx Period ..... 30 seconds
  Supplicant Timeout ..... 3 seconds
  Server Timeout ..... 5 seconds
  Maximum Request ..... 3 times
```

```
Client Online Probe .................. disable
Eapol Tag ............................ enable
802.1x redirect ...................... disable
Private supplicant only ............... disable
```

**Related Commands**

| Command | Description |
|---|---|
| **dot1x auth-mode** | Sets the 802.1X authentication mode. |
| **dot1x max-req** | Sets the maximum number of authentication request re-transmissions. |
| **dot1x port-control auto** | Sets the port to participate in authentication. |
| **dot1x reauth-max** | Sets the maximum number of the supplicant re-authentications. |
| **dot1x re-authentication** | Sets the re-authentication attribute. |
| **dot1x timeout quiet-period** | Sets the time the device waits before re-authentication. |
| **dot1x timeout re-authperiod** | Sets the re-authentication period for the supplicant. |
| **dot1x timeout server-timeout** | Sets the authentication timeout between the device and authentication server. |
| **dot1x timeout supp-timeout** | Sets the authentication timeout between the device and the supplicant. |
| **dot1x timeout tx-period** | Sets the re-transmission interval. |

**Platform Description** N/A

## 4.34 show dot1x auth-address-table

Use this command to display 802.1X authentication address table.

**show dot1x auth-address-table** [ **address** *addr* | **interface** *interface* ]

**Parameter Description**

| Parameter | Description |
|---|---|
| *addr* | Physical IP address that can be authenticated |
| *interface* | Interface number |

**Defaults** N/A

**Command Mode** Privileged EXEC mode/Global configuration mode/Interface configuration mode

**Usage Guide** N/A

**Configuration Examples** The following example displays the 802.1X authentication address table.

```
Ruijie #show dot1x auth-address-table
Interface       Address
--------------- -------------------
```

```
Fa0/1          00d0.f800.0c0e
Fa0/2          001a.c800.0102

Ruijie #show dot1x auth-address-table interface fastEthernet 0/1
Interface       Address
--------------- ------------------
Fa0/1          00d0.f800.0c0e

Ruijie #show dot1x auth-address-table address 00d0.f8.00.0c0e
Interface       Address
--------------- ------------------
Fa0/1          00d0.f800.0c0e
```

**Related Commands**

| Command | Description |
|---|---|
| **dot1x auth-mode** | Sets the 802.1x authentication mode. |
| **dot1x max-req** | Sets the maximum number of authentication request re-transmissions. |
| **dot1x port-control auto** | Sets the port to participate in authentication. |
| **dot1x reauth-max** | Sets the maximum number of the supplicant re-authentications. |
| **dot1x re-authentication** | Sets the re-authentication attribute. |
| **dot1x timeout quiet-period** | Sets the time the device waits before re-authentication. |
| **dot1x timeout re-authperiod** | Sets the re-authentication period for the supplicant. |
| **dot1x timeout server-timeout** | Sets the authentication timeout between the device and authentication server. |
| **dot1x timeout supp-timeout** | Sets the authentication timeout between the device and the supplicant. |
| **dot1x timeout tx-period** | Sets the re-transmission interval. |

**Platform Description** N/A

## 4.35 show dot1x auto-req

Use this command to display the auto-request authentication information.

**show dot1x auto-req**

**Parameter Description**

| Parameter | Description |
|---|---|
| N/A | N/A |

**Defaults** N/A

**Command Mode** Privileged EXEC mode/Global configuration mode/Interface configuration mode

**Usage Guide** N/A

**Configuration Examples** The following example displays the auto-request authentication information.

```
Ruijie# show dot1x auto-req
Auto-Req: Enabled
User-Detect : Enabled
Packet-Num  : 0
Req-Interval: 30 Seconds
```

**Related Commands**

| Command | Description |
|---|---|
| **dot1x auth-mode** | Sets the 802.1X authentication mode. |
| **dot1x max-req** | Sets the maximum number of authentication request re-transmissions. |
| **dot1x port-control auto** | Sets the port to participate in authentication. |
| **dot1x reauth-max** | Sets the maximum number of the supplicant re-authentications. |
| **dot1x re-authentication** | Sets the re-authentication attribute. |
| **dot1x timeout quiet-period** | Sets the time the device waits before re-authentication. |
| **dot1x timeout re-authperiod** | Sets the re-authentication period for the supplicant. |
| **dot1x timeout server-timeout** | Sets the authentication timeout between the device and authentication server. |
| **dot1x timeout supp-timeout** | Sets the authentication timeout between the device and the supplicant. |
| **dot1x timeout tx-period** | Sets the re-transmission interval. |

**Platform Description** N/A

## 4.36 show dot1x max-req

Use this command to display the maximum number of request/challenge packet transmission.

**show dot1x max-req**

**Parameter Description**

| Parameter | Description |
|---|---|
| N/A | N/A |

**Defaults** N/A

**Command Mode** Privileged EXEC mode/Global configuration mode/Interface configuration mode

**Usage Guide** N/A

**Configuration Examples** The following example displays the maximum number of request/challenge packet transmission.

```
Ruijie#show dot1x max-req

Max-Req: 3 Times
```

**Related Commands**

| Command | Description |
|---|---|
| **dot1x auth-mode** | Sets the 802.1X authentication mode. |
| **dot1x max-req** | Sets the maximum number of authentication request re-transmissions. |
| **dot1x port-control auto** | Sets the port to participate in authentication. |
| **dot1x reauth-max** | Sets the maximum number of the supplicant re-authentications. |
| **dot1x re-authentication** | Sets the re-authentication attribute. |
| **dot1x timeout quiet-period** | Sets the time the device waits before re-authentication. |
| **dot1x timeout re-authperiod** | Sets the re-authentication period for the supplicant. |
| **dot1x timeout server-timeout** | Sets the authentication timeout between the device and authentication server. |
| **dot1x timeout supp-timeout** | Sets the authentication timeout between the device and the supplicant. |
| **dot1x timeout tx-period** | Sets the re-transmission interval. |

**Platform Description** N/A

## 4.37 show dot1x port-control

Use this command to display the port-control information.

**show dot1x port-control** [ **interface** *interface-type interface-number*]

**Parameter Description**

| Parameter | Description |
|---|---|
| *interface-type* | Interface type |
| *interface-number* | Interface ID |

**Defaults** N/A

**Command Mode** Privileged EXEC mode/Global configuration mode/Interface configuration mode

**Usage Guide** N/A

**Configuration Examples** The following example displays the port-control information.

```
Ruijie#show dot1x port-control
```

```
Interface Mode      Dynamic-User Static-User Max-User  Authened MAB
--------- ---------- ------------ ----------- --------- -------- ---------
Gi0/5    mac-based  0          0          unlimited no      disable
```

**Related Commands**

| Command | Description |
|---|---|
| **dot1x auth-mode** | Sets the 802.1X authentication mode. |
| **dot1x max-req** | Sets the maximum number of authentication request re-transmissions. |
| **dot1x port-control auto** | Sets the port to participate in authentication. |
| **dot1x reauth-max** | Sets the maximum number of the supplicant re-authentications. |
| **dot1x re-authentication** | Sets the re-authentication attribute. |
| **dot1x timeout quiet-period** | Sets the time the device waits before re-authentication. |
| **dot1x timeout re-authperiod** | Sets the re-authentication period for the supplicant. |
| **dot1x timeout server-timeout** | Sets the authentication timeout between the device and authentication server. |
| **dot1x timeout supp-timeout** | Sets the authentication timeout between the device and the supplicant. |
| **dot1x timeout tx-period** | Sets the re-transmission interval. |

**Platform Description** N/A

## 4.38 show dot1x private-supplicant-only

Use this command to display the information about the private supplicant.

**show dot1x private-supplicant-only**

**Parameter Description**

| Parameter | Description |
|---|---|
| N/A | N/A |

**Defaults** N/A

**Command Mode** Privileged EXEC mode/Global configuration mode/Interface configuration mode

**Usage Guide** N/A

**Configuration Examples** The following example displays the information about the private supplicant:

```
Ruijie#show dot1x private-supplicant-only

private-supplicant-only: Disabled
```

**Related Commands**

| Command | Description |
|---|---|
| **dot1x auth-mode** | Sets the 802.1X authentication mode. |
| **dot1x max-req** | Sets the maximum number of authentication request re-transmissions. |
| **dot1x port-control auto** | Sets the port to participate in authentication. |
| **dot1x reauth-max** | Sets the maximum number of the supplicant re-authentications. |
| **dot1x re-authentication** | Sets the re-authentication attribute. |
| **dot1x timeout quiet-period** | Sets the time the device waits before re-authentication. |
| **dot1x timeout re-authperiod** | Sets the re-authentication period for the supplicant. |
| **dot1x timeout server-timeout** | Sets the authentication timeout between the device and authentication server. |
| **dot1x timeout supp-timeout** | Sets the authentication timeout between the device and the supplicant. |
| **dot1x timeout tx-period** | Sets the re-transmission interval. |

**Platform Description** N/A

## 4.39 show dot1x probe-timer

Use this command to display the configuration of online user probe.

**show dot1x probe-timer**

**Parameter Description**

| Parameter | Description |
|---|---|
| N/A | N/A |

**Defaults** N/A

**Command Mode** Privileged EXEC mode/Global configuration mode/Interface configuration mode

**Usage Guide** N/A

**Configuration Examples** The following example displays the configuration of online user probe.

```
Ruijie#show dot1x probe-timer
Hello Interval   : 20
Hello Alive      : 60
```

Field Description

| Command | Description |
|---|---|
| Hello Interval | Sets the probe period. |
| Hello Alive | Sets the probe alive interval. |

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

**Platform Description** N/A

## 4.40 show dot1x re-authentication

Use this command to display re-authentication status.

**show dot1x re-authentication**

| Parameter Description | Parameter | Description |
|---|---|---|
| | N/A | N/A |

**Defaults** N/A

**Command Mode** Privileged EXEC mode/Global configuration mode/Interface configuration mode

**Usage Guide** N/A

**Configuration Examples** The following example displays re-authentication status.

```
Ruijie#show dot1x re-authentication

Reauth-Enabled: Disabled
```

| Command | Description |
|---|---|
| Reauth-Enabled | Whether to enable re-authentication. |

| Related Commands | Command | Description |
|---|---|---|
| | N/A | N/A |

**Platform Description** N/A

## 4.41 show dot1x reauth-max

Use this command to display the maximum re-auth attempts.

**show dot1x reauth-max**

| Parameter Description | Parameter | Description |
|---|---|---|
| | N/A | N/A |

**Defaults** N/A

**Command Mode** Privileged EXEC mode/Global configuration mode/Interface configuration mode

**Usage Guide** N/A

**Configuration Examples** The following example displays the maximum re-authentication attempts.

```
Ruijie#show dot1x reauth-max

Reauth-Max: 3 Times
```

| Command | Description |
|---|---|
| Reauth-Enabled | Sets the maximum re-authentication attempts. |

**Related Commands**

| Command | Description |
|---|---|
| N/A | N/A |

**Platform Description** N/A

## 4.42 show dot1x summary

Use this command to display the 802.1X authentication summary.

**show dot1x summary**

**Parameter Description**

| Parameter | Description |
|---|---|
| N/A | N/A |

**Defaults** N/A

**Command Mode** Privileged EXEC mode/Global configuration mode/Interface configuration mode

**Usage Guide** It is convenient to display the 802.1X authentication summary according to the MAC address or username.

**Configuration Examples** The following example displays the summary of 802.1X authentication.

```
Ruijie#show dot1x summary
ID      User      MAC           Interface VLAN Auth-State     Backend-State
Port-Status User-Type Time
-------- ---------- --------------  ---------  --------------- -------------
----------- --------- ------------------
```

**Related Commands**

| Command | Description |
|---|---|
| **dot1x auth-mode** | Sets the 802.1X authentication mode. |
| **dot1x max-req** | Sets the maximum number of authentication request re-transmissions**.** |
| **dot1x port-control auto** | Sets the port to participate in authentication. |
| **dot1x reauth-max** | Sets the maximum number of the supplicant re-authentications. |
| **dot1x re-authentication** | Sets the re-authentication attribute. |
| **dot1x timeout quiet-period** | Sets the time the device waits before re-authentication. |
| **dot1x timeout re-authperiod** | Sets the re-authentication period for the supplicant. |
| **dot1x timeout server-timeout** | Sets the authentication timeout between the device and authentication server. |
| **dot1x timeout supp-timeout** | Sets the authentication timeout between the device and the supplicant. |
| **dot1x timeout tx-period** | Sets the re-transmission interval. |

**Platform Description** N/A

## 4.43 show dot1x timeout quiet-period

Use this command to display the time for the device to wait before re-authentication quiet period after the authentication failure.

**show dot1x timeout quiet-period**

**Parameter Description**

| Parameter | Description |
|---|---|
| N/A | N/A |

**Defaults** N/A

**Command Mode** Privileged EXEC mode/Global configuration mode/Interface configuration mode

**Usage Guide** Use this command to display the time for the device to wait before re-authentication quiet period after the authentication failure.

**Configuration Examples** The following example shows how to displays the quiet period the time for the device to wait before re-authentication after the authentication failure.

```
Ruijie#show dot1x timeout quiet-period

Quiet-Period: 10 Seconds
```

Parameter Description:

| Parameter | Description |
| --- | --- |
| Quiet-Period | The time for the device to wait before re-authentication after the authentication failure. |

**Related Commands**

| Command | Description |
| --- | --- |
| N/A | N/A |

**Platform Description** N/A

## 4.44 show dot1x timeout re-authperiod

Use this command to display the re-authentication interval.

**show dot1x timeout re-authperiod**

**Parameter Description**

| Parameter | Description |
| --- | --- |
| N/A | N/A |

**Defaults** N/A

**Command Mode** Privileged EXEC mode/Global configuration mode/Interface configuration mode

**Usage Guide** Use this command to display the re-authentication interval.

**Configuration Examples** The following example displays the re-authentication interval.:

```
Ruijie#show dot1x timeout re-authperiod

Reauth-Period: 3600 Seconds
```

Parameter Description:

| Parameter | Description |
| --- | --- |
| Reauth-Period | Re-authentication interval. |

**Related Commands**

| Command | Description |
| --- | --- |
| N/A | N/A |

**Platform Description** N/A

## 4.45 show dot1x timeout server-timeout

Use this command to display the authentication timeout period.

**show dot1x timeout server-timeout**

| Parameter Description | Parameter | Description |
|---|---|---|
| | N/A | N/A |

**Defaults** N/A

**Command Mode** Privileged EXEC mode/Global configuration mode/Interface configuration mode

**Usage Guide** Use this command to display the authentication timeout period.

**Configuration Examples** Use this command to display the authentication timeout period:

```
Ruijie#show dot1x timeout server-timeout

Server-Timeout: 5 Seconds
```

Parameter Description:

| Parameter | Description |
|---|---|
| Server-Period | AuthenticationServer timeout periodinterval. |

| Related Commands | Command | Description |
|---|---|---|
| | N/A | N/A |

**Platform Description** N/A

## 4.46 show dot1x timeout supp-timeout

Use this command to display the request/challenge packets re-transmission interval.

**show dot1x timeout supp-timeout**

| Parameter Description | Parameter | Description |
|---|---|---|
| | N/A | N/A |

**Defaults** N/A

**Command Mode** Privileged EXEC mode/Global configuration mode/Interface configuration mode

**Usage Guide** Use this command to display the request/challenge packets re-transmission interval.

**Configuration Examples** Use this command to display the request/challenge packets re-transmission interval:

```
Ruijie#show dot1x timeout supp-timeout
```

```
Supp-Timeout: 3 Seconds
```

Field Description:

| Field | Description |
|---|---|
| Server-Period | The request/challenge packets re-transmission interval. |

| Related Commands | Command | Description |
|---|---|---|
| | N/A | N/A |

**Platform Description** N/A

## 4.47 show dot1x timeout tx-period

Use this command to display the request/id packets re-transmission interval.

**show dot1x timeout tx-period**

| Parameter Description | Parameter | Description |
|---|---|---|
| | N/A | N/A |

**Defaults** N/A

**Command Mode** Privileged EXEC mode/Global configuration mode/Interface configuration mode

**Usage Guide** Use this command to display the request/id packets re-transmission interval.

**Configuration Examples** Use this command to display the request/ id packets re-transmission interval:

```
Ruijie#show dot1x timeout tx-period


Tx-Period: 30 Seconds
```

Parameter Description:

| Parameter | Description |
|---|---|
| Tx-Period | Request/id packets re-transmission interval. |

| Related Commands | Command | Description |
|---|---|---|
| | N/A | N/A |

**Platform Description** N/A

# 4.48 show dot1x user id

Use this command to display the information about 802.1X authentication users based on user IDs.

**show dot1x user id** *id*

**Parameter Description**

| Parameter | Description |
|---|---|
| *id* | User ID |

**Defaults** N/A

**Command Mode** Privileged EXEC mode/Global configuration mode/Interface configuration mode

**Usage Guide** Use the **show dot1x summary** command to display 802.1X authentication summaries. And use this command to display detailed information of a specific user based on its ID.

**Configuration Examples** The following example displays the information about the 802.1X authentication user according to the user ID.

```
Ruijie#show dot1x user id 16777225

User name: ts-user
User id: 16777225
Type: static
Mac address is 0023.aeaa.4286
Vlan id is 2
Access from port Gi0/5
Time online: 0days 0h 0m17s
User ip address is 192.168.3.21
Max user number on this port is 0
Authorization session time is 1000 seconds
Supplicant is private
Start accounting
Permit proxy user
Permit dial user
IP privilege is 0
 user acl-name ts-user_6_0_0 :
Parameter Description:
```

| Parameter | Description |
|---|---|
| User name | User name |
| User id | User ID |
| Type | User type |
| Mac address | User's MAC address |
| Vlan id | User VLAN ID |

| | |
|---|---|
| Access from port | The port that user accesses from |
| Time online | User online time |
| User ip address | User IP address |
| Max user number on this port | The maximum number of users on the port |
| Authorization session time | The authorized session time |
| Supplicant is private | Whether the terminal is a Ruijie device |
| Start accounting | The accounting is enabled |
| Permit proxy user | The user is allowed to use the proxy. |
| Permit dial user | The user is allowed to dial. |
| IP privilege | The IP privilege level |
| user acl-name | The ACL information |

**Related Commands**

| Command | Description |
|---|---|
| N/A | N/A |

**Platform Description** N/A

## 4.49 show dot1x user mac

Use this command to display the information about 802.1X authentication users based on MAC addresses.

**show dot1x user mac** *mac-addr*

**Parameter Description**

| Parameter | Description |
|---|---|
| *mac-addr* | MAC address |

**Defaults** N/A

**Command Mode** Privileged EXEC mode/Global configuration mode/Interface configuration mode

**Usage Guide** Use the **show dot1x summary** command to display 802.1X authentication summaries. And use this command to display detailed information of a specific user based on its MAC address.

**Configuration Examples** The following example displays the information about the 802.1X authentication user according to the user's MAC address.

```
Ruijie#show dot1x user mac 0023.aeaa.4286

User name: ts-user
User id: 16777225
Type: static
Mac address is 0023.aeaa.4286
```

```
Vlan id is 2
Access from port Gi0/5
Time online: 0days 0h 0m17s
User ip address is 192.168.3.21
Max user number on this port is 0
Authorization session time is 1000 seconds
Supplicant is private
Start accounting
Permit proxy user
Permit dial user
IP privilege is 0
 user acl-name ts-user_6_0_0 :
```

Parameter Description:

| Parameter | Description |
|---|---|
| User name | User name |
| User id | User ID |
| Type | User type |
| Mac address | User's MAC address |
| Vlan id | User VLAN ID |
| Access from port | The port that user access from |
| Time online | User online time |
| User ip address | User IP address |
| Max user number on this port | The maximum number of users on the port |
| Authorization session time | The authorized session time |
| Supplicant is private | Whether the terminal is a Ruijie device |
| Start accounting | The accounting is enabled. |
| Permit proxy user | The user is allowed to use the proxy. |
| Permit dial user | The user is allowed to dial. |
| IP privilege | The IP privilege level |
| user acl-name | The ACL information |

**Related Commands**

| Command | Description |
|---|---|
| N/A | N/A |

**Platform Description** N/A

## 4.50 show dot1x user name

Use this command to display information about 802.1X authentication users based on usernames.

**show dot1x user name** *name*

**Parameter**

| Parameter | Description |
|---|---|

| Description | *name* | User name |
|---|---|---|

**Defaults** N/A

**Command Mode** Privileged EXEC mode/Global configuration mode/Interface configuration mode

**Usage Guide** Use the **show dot1x summary** command to display 802.1X authentication summaries. And use this command to display detailed information of a specific user based on its username.

**Configuration Examples** The following example displays the information about the 802.1X authentication user according to the user name.

```
Ruijie#show dot1x user name ts-user

User name: ts-user
User id: 16777225
Type: static
Mac address is 0023.aeaa.4286
Vlan id is 2
Access from port Gi0/5
Time online: 0days 0h 0m17s
User ip address is 192.168.3.21
Max user number on this port is 0
Authorization session time is 1000 seconds
Supplicant is private
Start accounting
Permit proxy user
Permit dial user
IP privilege is 0
 user acl-name ts-user_6_0_0 :
```

Parameter Description:

| Parameter | Description |
|---|---|
| User name | User name |
| User id | User ID |
| Type | User type |
| Mac address | User's MAC address |
| Vlan id | User VLAN ID |
| Access from port | The port that user access from |
| Time online | User online time |
| User ip address | User IP address |
| Max user number on this port | The maximum number of users on the port |
| Authorization session time | The authorized session time |
| Supplicant is private | Whether the terminal is a Ruijie device. |
| Start accounting | The accounting is enabled. |

| | |
|---|---|
| Permit proxy user | The user is allowed to use the proxy. |
| Permit dial user | The user is allowed to dial. |
| IP privilege | The IP privilege level. |
| user acl-name | The ACL information. |

**Related Commands**

| Command | Description |
|---|---|
| N/A | N/A |

**Platform Description** N/A

# 5 ARP-Check Commands

## 5.1 arp-check

Use this command to enable the ARP check function on the Layer 2 interface.
Use the **no** form of this command to restore the default setting.
**arp-check**
**no arp-check**

**Parameter Description**

| Parameter | Description |
|---|---|
| N/A | N/A |

**Defaults** This function is disabled by default.

**Command mode** Interface configuration mode/WLAN security configuration mode

**Usage Guide** The ARP check function generates the ARP filtering information according to legal user information, implementing the illegal ARP packet filtering on the network.

**Configuration Examples** This following example enables the APR check function on interface GigabitEthernet 0/1.

```
Ruijie# configure terminal
Ruijie(config)# interface GigabitEthernet 0/1
Ruijie(config-if-GigabitEthernet 0/1)# arp-check
Ruijie(config-if-GigabitEthernet 0/1)# end
Ruijie# configure terminal
Ruijie(config)# wlansec 1
Ruijie(config-wlansec)# arp-check
Ruijie(config-wlansec)# end
```

**Related Commands**

| Command | Description |
|---|---|
| **show interface arp-check list** | Displays the ARP check entries. |

**Platform Description** N/A

## 5.2 show interfaces arp-check list

Use this command to display the ARP check entries on the Layer 2 interface.

**show** { **interface** [ *interface-type interface-number* ] | **wlan** [ *wlan-id* ] } **arp-check list**

**Parameter Description**

| Parameter | Description |
|---|---|
| *interface-type* | Wired interface type |
| *interface-number* | Wired interface number |
| *wlan-id* | WLAN ID |

**Command mode** Privileged EXEC mode

**Usage Guide** Use this command to display the ARP check entries.

**Configuration Examples** The following example displays the ARP check entries.

```
Ruijie(config)#show interface arp-check list
INTERFACE                    SENDER MAC      SENDER IP            POLICY SOUR
CE
---------------------- --------------- --------------- --------------------
GigabitEthernet 0/1       00D0.F800.0003   192.168.1.3     address-bind
GigabitEthernet 0/1       00D0.F800.0001   192.168.1.1     port-security
GigabitEthernet 0/4                     192.168.1.3     port-security
GigabitEthernet 0/5       00D0.F800.0003   192.168.1.3     address-bind
GigabitEthernet 0/7       00D0.F800.0006   192.168.1.6     AAA ip-auth-mode
GigabitEthernet 0/8       00D0.F800.0007   192.168.1.7     GSN
Ruijie(config)#show wlan arp-check list
INTERFACE             SENDER MAC     SENDER IP      POLICY SOURCE
---------------------- --------------- --------------- --------------------
WLAN 1                 00D0.F800.0008   192.168.1.8     GSN
```

| Field | Description |
|---|---|
| INTERFACE | Interface name |
| SENDER MAC | Source MAC address |
| SENDER IP | Source IP address |
| POLICY SOURCE | Source of the entry |

**Related Commands**

| Command | Description |
|---|---|
| N/A | N/A |

**Platform Description** N/A

# 6 Anti-ARP Spoofing Commands

## 6.1 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* | Gateway IP address |

**Defaults** The anti-ARP spoofing function is disabled by default.

**Command Mode** WLAN security configuration mode

**Usage Guide** N/A

**Configuration Examples** The following example enables anti-ARP spoofing.

```
Ruijie(config)#wlansec 1
Ruijie(config-wlansec)#anti-arp-spoofing ip 192.168.1.1
```

**Related Commands**

| Command | Description |
|---|---|
| **show anti-arp-spoofing** | Displays the anti-ARP spoofing configuration. |

**Platform Description** N/A

## 6.2 show anti-arp-spoofing

Use this command to display the anti-ARP spoofing configuration on all interfaces.

**show anti-arp-spoofing**

**Parameter Description**

| Parameter | Description |
|---|---|
| N/A | N/A |

**Defaults** N/A

**Command Mode** Global configuration mode

**Usage Guide** This command is used to display the anti-ARP spoofing configuration on all interfaces.

**Configuration Examples** The following example displays the anti-ARP-spoofing configuration on all interfaces.

```
Ruijie#show anti-arp-spoofing
NO    PORT      IP              STATUS
----- ---------- ---------------- ----------
1     Gi0/1     192.168.1.1     active
```

Field Description

| Field | Description |
|---|---|
| NO | Order number |
| PORT | Port number |
| IP | Gateway IP |
| STATUS | Anti-ARP spoofing status |

**Related Commands**

| Command | Description |
|---|---|
| **anti-arp-spoofing ip** | Configures anti-ARP spoofing. |

**Platform Description** N/A

# 7 Global IP-MAC Binding Commands

## 7.1 address-bind

Use this command to configure global IP-MAC address binding. Use the **no** form of this command to restore the default setting.

**address-bind** { *ip-address* | *ipv6-address* } *mac-address*

**no address-bind** { *ip-address* | *ipv6-address* } *mac-address*

**Parameter Description**

| Parameter | Description |
|---|---|
| *ip-address* | IPv4 address to be bound |
| *ipv6-address* | IPv6 address to be bound |
| *mac-address* | MAC address to be bound |

**Defaults** N/A

**Command Mode** Global configuration mode

**Usage Guide** N/A

**Configuration Examples** The following example configures global IP-MAC address binding.

```
Ruijie# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Ruijie(config)# address-bind 192.168.5.1 00d0.f800.0001
```

**Related Commands**

| Command | Description |
|---|---|
| **show address-bind** | Displays the IP address-MAC address binding table. |

**Platform Description** N/A

## 7.2 address-bind install

Use this command to enable a binding policy globally. Use the **no** form of this command to restore the default setting.

**address-bind install**

**no address-bind install**

**Parameter**

| Parameter | Description |
|---|---|

| | | |
|---|---|---|
| **Description** | N/A | N/A |

**Defaults** N/A

**Command Mode** Global configuration mode

**Usage Guide** If you bind an IP address to a MAC address, run this command to make the installation policy take effect.

**Configuration Examples** The following example enables a binding policy.

```
Ruijie# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Ruijie(config)# address-bind 192.168.5.1 00d0.f800.0001
Ruijie(config)# address-bind install
```

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

**Platform Description** N/A

## 7.3 address-bind ipv6-mode

This command is used to set the IPv6 address binding mode. Use the **no** form of this command to restore the default setting.

This command is also used to set the compatible mode.

**address-bind ipv6-mode** { **compatible** | **loose** | **strict** }

**no address-bind ipv6-mode**

| **Parameter Description** | **Parameter** | **Description** |
|---|---|---|
| | **compatible** | Compatible mode |
| | **loose** | Loose mode |
| | **strict** | Strict mode |

**Defaults** The default is strict mode.

**Command Mode** Global configuration mode.

**Usage Guide** N/A

**Configuration** The following example configures the IPv6 address binding mode.

**Examples**

```
Ruijie# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Ruijie(config)# address-bind ipv6-mode compatible
```

**Related Commands**

| Command | Description |
|---|---|
| **show address-bind uplink** | Displays the exceptional port of the address binding. |

**Platform Description** N/A

## 7.4 address-bind uplink

This command is used to configure the exception port. Use the **no** form of this command to restore the default setting.

**address-bind uplink** *interface-id*

**no address-bind uplink** *interface-id*

**Parameter Description**

| Parameter | Description |
|---|---|
| *interface-id* | Switching port or layer 2 aggregate port. |

**Defaults** All ports are non-exception ports by default.

**Command Mode** Global configuration mode.

**Usage Guide** If you have bound an IP address and a MAC address, the switch will discard the packets that have the same source IP address but different source MAC address.

If the port is an exceptional port and is installed (see address-bind install), this binding policy does not take effect.

**Configuration Examples** The following example configures the exception port.

```
Ruijie# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Ruijie(config)# address-bind uplink GigabitEthernet 0/1
```

**Related Commands**

| Command | Description |
|---|---|
| **show address-bind uplink** | Displays the exceptional port of address binding. |

**Platform Description** N/A

## 7.5 show address-bind

Use this command to display global IP address-MAC address binding.

**show address-bind**

**Parameter Description**

| Parameter | Description |
|---|---|
| N/A | N/A |

**Defaults** N/A

**Command Mode** Privileged EXEC mode.

**Usage Guide** N/A

**Configuration Examples** The following example displays global IPv4 address-MAC address binding.

```
Ruijie#show address-bind
Total Bind Addresses in System : 1
IP Address        Binding MAC Addr
---------------    ----------------
192.168.5.1       00d0.f800.0001
```

| Field | Description |
|---|---|
| Total Bind Addresses in System | IPv4 address-MAC address binding count |
| IP Address | Bound IP address |
| Binding MAC Addr | Bound MAC address |

**Related Commands**

| Command | Description |
|---|---|
| **address-bind** | Enables IP address-MAC address binding. |

**Platform Description** N/A

## 7.6 show address-bind uplink

Use this command to display the exception port.

**show address-bind uplink**

**Parameter Description**

| Parameter | Description |
|---|---|
| N/A | N/A |

**Defaults** N/A

**Command** N/A

**mode**

**Usage Guide** N/A

**Configuration Examples** The following example displays the exception port.

```
Ruijie#show address-bind uplink
Port      State
---------- ---------
Gi0/1     Enabled
Default    Disabled
```

| Field | Description |
|---|---|
| Port | Short for exception ports. All ports are non-exception ports by default. |
| State | Indicates whether the port is exception port. State Enabled indicates that it is an exception port while state Disabled indicates that it it not. |

**Related Commands**

| Command | Description |
|---|---|
| **address-bind uplink** | Sets the exception port. |

**Platform Description** N/A

# 8 DHCP Snooping Commands

## 8.1 clear ip dhcp snooping binding

Use this command to delete the dynamic user information from the DHCP Snooping binding database.

**clear ip dhcp snooping binding** [ *ip* ] [ *mac* ] [ **vlan** *vlan-id* ] [ **interface** *interface-id* | **wlan** *wlan-id* ]

**Parameter Description**

| Parameter | Description |
|---|---|
| *mac* | Specifies the user MAC address to be cleared. |
| *vlan-id* | Specifies the ID of the VLAN to be cleared. |
| *ip* | Specifies the IP address to be cleared. |
| *interface-id* | Specifies the ID of the interface to be cleared. |
| *wlan-id* | Specifies the ID of the WLAN to be cleared. |

**Defaults** N/A

**Command Mode** Privileged EXEC mode

**Usage Guide** Use this command to clear the current dynamic user information from the DHCP Snooping binding database.

After this command is used, all the DHCP clients connecting interfaces with IP Source Guard function enabled should request IP addresses again, or they cannot access network.

**Configuration Examples** The following example clears the dynamic database information from the DHCP Snooping binding database.

```
Ruijie# clear ip dhcp snooping binding
Ruijie# show ip dhcp snooping binding
Total number of bindings: 0
MacAddress IpAddress Lease(sec) Type VLAN Interface
---------- ---------- ---------- -------- ---- ---------
```

**Related Commands**

| Command | Description |
|---|---|
| **show ip dhcp snooping binding** | Displays the information of the DHCP Snooping binding database. |

**Platform Description** N/A

## 8.2 ip dhcp snooping

Use this command to enable the DHCP Snooping function globally.
Use the **no** form of this command to restore the default setting.
**ip dhcp snooping**
**no ip dhcp snooping**

**Parameter Description**

| Parameter | Description |
|---|---|
| N/A | N/A |

**Defaults** This function is disabled by default.

**Command Mode** Global configuration mode

**Usage Guide** The **show ip dhcp snooping** command is used to display whether the DHCP Snooping function is enabled.

**Configuration Examples** The following example enables the DHCP Snooping function.

```
Ruijie# configure terminal
Ruijie(config)# ip dhcp snooping
Ruijie(config)# end
```

**Related Commands**

| Command | Description |
|---|---|
| **show ip dhcp snooping** | Displays the configuration information of DHCP Snooping. |
| **ip dhcp snooping vlan** | Configures DHCP Snooping enabled VLAN. |

**Platform Description** N/A

## 8.3 ip dhcp snooping bootp-bind

Use this command to enable DHCP Snooping BOOTP-bind function.
Use the **no** form of this command to restore the default setting.
**ip dhcp snooping bootp-bind**
**no ip dhcp snooping bootp-bind**

**Parameter Description**

| Parameter | Description |
|---|---|
| N/A | N/A |

**Defaults** This function is disabled by default.

**Command Mode** Global configuration mode

**Usage Guide** By default, the DHCP Snooping only forwards BOOTP packets. With this function enabled, it can Snoop BOOTP packets. After the BOOTP client requests an address successfully, the DHCP Snooping adds the BOOTP user to the static binding database.

**Configuration Examples** The following example enables the DHCP Snooping BOOTP-bind function.

```
Ruijie# configure terminal
Ruijie(config)# ip dhcp snooping bootp-bind
Ruijie(config)# end
```

**Related Commands**

| Command | Description |
|---|---|
| **show ip dhcp snooping** | Displays the DHCP Snooping configuration. |

**Platform Description** N/A

## 8.4 ip dhcp snooping check-giaddr

Use this command to enable DHCP Snooping to support the function of processing Relay requests. Use the **no** form of this command to restore the default setting.

**ip dhcp snooping check-giaddr**

**no ip dhcp snooping check-giaddr**

**Parameter Description**

| Parameter | Description |
|---|---|
| N/A | N/A |

**Defaults** This function is disabled by default.

**Command Mode** Global configuration mode

**Usage Guide** After the feature is enabled, services using DHCP Snooping binding entries generated based on Relay requests, such as IP Source Guard/802.1x authentication, cannot be deployed. Otherwise, users fail to access the Internet.

After the feature is enabled, the **ip dhcp snooping verify mac-address** command cannot be used. Otherwise, DHCP Relay requests will be discarded and as a result, users fail to obtain addresses.

**Configuration Examples** The following example enables DHCP Snooping to support the function of processing Relay requests.

```
Ruijie# configure terminal
Ruijie(config)# ip dhcp snooping check-giaddr
Ruijie(config)# end
```

**Related Commands**

| Command | Description |
| --- | --- |
| **show ip dhcp snooping** | Displays the configuration information of the DHCP Snooping. |

**Platform Description** N/A

## 8.5 ip dhcp snooping clear-broadcast-flag

Use this command to enable the function of clearing the broadcast flag bit.
Use the **no** form of this command to restore the default setting.
**ip dhcp snooping clear-broadcast-flag**
**no ip dhcp snooping clear-broadcast-flag**

**Parameter Description**

| Parameter | Description |
| --- | --- |
| N/A | N/A |

**Defaults** This function is disabled by default.

**Command Mode** Global configuration mode

**Usage Guide** After the feature is enabled, DHCP Snooping checks the broadcast flag bit for non-DHCP Relay requests. If the flag bit is 1, it clears the flag bit. When receiving responses, DHCP Snooping sets the flag bit to 1 and set Layer-2 and Layer-3 destination addresses as broadcast addresses.

**Configuration Examples** The following example enables the function of clearing the broadcast flag bit.

```
Ruijie# configure terminal
Ruijie(config)# ip dhcp snooping clear-broadcast-flag
Ruijie(config)# end
```

**Related Commands**

| Command | Description |
| --- | --- |
| N/A | N/A |

**Platform Description** N/A

## 8.6 ip dhcp snooping database write-delay

Use this command to configure the switch to write the dynamic user information of the DHCP Snooping binding database into the flash periodically.
Use the **no** form of this command to restore the default setting.
**ip dhcp snooping database write-delay** *time*
**no ip dhcp snooping database write-delay**

**Parameter Description**

| Parameter | Description |
|---|---|
| *time* | The interval at which the system writes the dynamic user information of the DHCP Snooping database into the flash, in the range from 600 to 86,400 in the unit of seconds |

**Defaults** This function is disabled by default.

**Command Mode** Global configuration mode

**Usage Guide** This function writes user information into flash in case of loss after restart. In that case, users need to obtain IP addresses again for normal communication.

Too fast writing will reduce flash durability.

**Configuration Examples** The following example sets the interval at which the switch writes the user information into the flash to 3,600 seconds.

```
Ruijie# configure terminal
Ruijie(config)# ip dhcp snooping database write-delay 3600
Ruijie(config)# end
```

**Related Commands**

| Command | Description |
|---|---|
| **show ip dhcp snooping** | Displays the configuration information of the DHCP Snooping. |

**Platform** N/A

**Description**

## 8.7 ip dhcp snooping database write-to-flash

Use this command to write the dynamic user information of the DHCP binding database into flash in real time.

**ip dhcp snooping database write-to-flash**

**Parameter Description**

| Parameter | Description |
|---|---|
| N/A | N/A |

**Defaults** N/A

**Command Mode** Global configuration mode

**Usage Guide** This command is used to write the dynamic user information of the DHCP binding database into flash in real time.

**Configuration Examples** The following example writes the dynamic user information of the DHCP binding database into flash.

```
Ruijie# configure terminal
Ruijie(config)# ip dhcp snooping database write-to-flash
Ruijie(config)# end
```

**Related Commands**

| Command | Description |
|---|---|
| N/A | N/A |

**Platform Description** N/A

## 8.8 ip dhcp snooping information option

Use this command to add option82 to the DHCP request message.

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

**ip dhcp snooping information option** [ **standard-format** ]

**no ip dhcp snooping information option** [ **standard-format** ]

**Parameter Description**

| Parameter | Description |
|---|---|
| **standard-format** | The option82 uses the standard format. |

**Defaults** This function is disabled by default,

**Command Mode** Global configuration mode

**Usage Guide** This command adds option82 to the DHCP request messages based on which the DHCP server assigns IP addresses.
By default, this function is in extended mode.

DHCP Relay function adds option82 by default. Therefore, it is unnecessary to enable functions of DHCP Snooping option82 and DHCP Relay at the same time.

**Configuration Examples** The following example adds option82 to the DHCP request message.

```
Ruijie# configure terminal
Ruijie(config)# ip dhcp snooping information option
Ruijie(config)# end
```

**Related Commands**

| Command | Description |
|---|---|
| **show ip dhcp snooping** | Displays the DHCP Snooping configuration. |

**Platform Description** N/A

## 8.9 ip dhcp snooping information option format remote-id

Use this command to set the option82 sub-option remote-id as the customized character string.
Use the **no** form of this command to restore the default setting.
**ip dhcp snooping information option format remote-id** { **string** *ascii-string* **| hostname** }
**no ip dhcp snooping information option format remote-id** { **string** *ascii-string* **| hostname** }

**Parameter Description**

| Parameter | Description |
|---|---|
| **string** *ascii-string* | The content of the option82 remote-id extension format is customized character string. |
| **hostname** | The content of the option82 remote-id extension format hostname |

**Defaults** This function is disabled by default.

**Command Mode** Global configuration mode

**Usage Guide** This command sets the remote-id in the option82 to be added to the DHCP request message as the customized character string. The DHCP server will assign the IP address according to the option82

information.

**Configuration Examples** The following example adds the option82 into the DHCP request packets with the content of remote-id as hostname.

```
Ruijie# configure terminal
Ruijie(config)# ip dhcp snooping information option format remote-id hostname
```

**Related Commands**

| Command | Description |
| --- | --- |
| N/A | N/A |

**Platform Description** N/A

## 8.10 ip dhcp snooping suppression

Use this command to set the port to be the suppression status.
Use the **no** form of this command to restore the default setting.
**ip dhcp snooping suppression**
**no ip dhcp snooping suppression**

**Parameter Description**

| Parameter | Description |
| --- | --- |
| N/A | N/A |

**Defaults** This function is disabled by default.

**Command Mode** Interface configuration mode/WLAN security configuration mode

**Usage Guide** This command denies all DHCP request messages under the port, that is, all the users under the port are prohibited to request IP addresses through DHCP.
This command is only supported on Layer 2 switch interfaces and aggregate ports (APs).

**Configuration Examples** The following example sets **fastethernet** 0/2 and WLAN 1 to be in the suppression status.

```
Ruijie# configure terminal
Ruijie(config)# interface fastEthernet 0/2
Ruijie(config-if)# ip dhcp snooping suppression
Ruijie(config-if)# end
Ruijie# configure terminal
Ruijie(config)# wlansec 1
Ruijie(config-wlansec)# ip dhcp snooping suppression
Ruijie(config-if-wlansec)# end
```

**Related Commands**

| Command | Description |
| --- | --- |
| **show ip dhcp snooping** | Displays the DHCP Snooping configuration. |

**Platform Description** N/A

## 8.11 ip dhcp snooping trust

Use this command to set the trusted ports for DHCP Snooping.
Use the **no** form of this command to restore the default setting.
**ip dhcp snooping trust**
**no ip dhcp snooping trust**

**Parameter Description**

| Parameter | Description |
| --- | --- |
| N/A | N/A |

**Defaults** All ports are untrusted by default.

**Command Mode** Interface configuration mode

**Usage Guide** Use this command to set a port as a trusted port. The DHCP response messages received under the trust port are forwarded normally, but the response messages received under the untrusted port will be discarded. This command is only supported on Layer 2 switch interfaces and aggregate ports (APs).

**Configuration Examples** The following example sets fastEthernet 0/1 as a trusted port:

```
Ruijie# configure terminal
Ruijie(config)# interface fastEthernet 0/1
Ruijie(config-if)# ip dhcp snooping trust
Ruijie(config-if)# end
```

**Related Commands**

| Command | Description |
| --- | --- |
| **show ip dhcp snooping** | Displays the DHCP Snooping configuration. |

**Platform Description** N/A

## 8.12 ip dhcp snooping verify mac-address

Use this command to check whether the source MAC address of the DHCP request message matches against the **client addr** field of the DHCP message.
Use the **no** form of this command to restore the default setting.
**ip dhcp snooping verify mac-address**
**no ip dhcp snooping verify mac-address**

**Parameter Description**

| Parameter | Description |
|---|---|
| N/A | N/A |

**Defaults** This function is disabled by default.

**Command Mode** Global configuration mode

**Usage Guide** Use this command to check the source MAC address of the DHCP request message. If the MAC address in the link-layer header is different from the CHADDR (Client MAC Address), the check fails ,and the packets will be discarded.

**Configuration Examples** The following example enables the check of the source MAC address of the DHCP request message.

```
Ruijie# configure terminal
Ruijie(config)# ip dhcp snooping verify mac-address
Ruijie(config)# end
```

**Related Commands**

| Command | Description |
|---|---|
| **show ip dhcp snooping** | Displays the DHCP Snooping configuration. |

**Platform Description** N/A

## 8.13 ip dhcp snooping vlan

Use this command to enable DHCP Snooping for the specific VLAN.
Use the **no** form of this command to restore the default setting.
**ip dhcp snooping vlan** {*vlan-rng* | { *vlan-min* [ *vlan-max* ] } }
**no ip dhcp snooping vlan** {*vlan-rng* | { *vlan-min* [ *vlan-max* ] } }

**Parameter Description**

| Parameter | Description |
|---|---|
| *vlan-rng* | VLAN range of effective DHCP Snooping |

| | |
|---|---|
| *vlan-min* | Minimum VLAN of effective DHCP Snooping |
| *vlan-max* | Maximum VLAN of effective DHCP Snooping |

**Defaults** By default, once the DHCP Snooping is enabled globally, it takes effect for all VLANs.

**Command Mode** Global configuration mode

**Usage Guide** Use this command to enable DHCP Snooping for specified VLANs globally.

**Configuration Examples** The following example enables the DHCP Snooping function in VLAN 1000.

```
Ruijie# configure terminal
Ruijie(config)# ip dhcp snooping vlan 1000
Ruijie(config)# end
```

**Related Commands**

| Command | Description |
|---|---|
| **ip dhcp snooping** | Enables DHCP Snooping globally. |

**Platform Description** N/A

## 8.14 ip dhcp snooping vlan information option change-vlan-to vlan

Use this command to enable the option82 sub-option circuit-id and change the VLAN in the circuit-id into the specified VLAN.
Use the **no** form of this command to restore the default setting.
**ip dhcp snooping vlan** *vlan-id* **information option change-vlan-to vlan** *vlan-id*
**no ip dhcp snooping vlan** *vlan-id* **information option change-vlan-to vlan** *vlan-id*

**Parameter Description**

| Parameter | Description |
|---|---|
| *vlan-id* | The ID of the VLAN to be replaced |

**Defaults** This function is disabled by default.

**Command Mode** Interface configuration mode

**Usage Guide** With this command configured, the option82 is added to the DHCP request packets, the circuit-id in the option82 information is the specified VLAN and the DHCP server will assign the addresses according to the option82 information.

**Configuration Examples** The following adds the option82 to the DHCP request packets and changes the VLAN 4094 in the option82 sub-option circuit-id to VLAN93:

```
Ruijie# configure terminal
Ruijie(config)# interface fastEthernet 0/1
Ruijie(config-if)# ip dhcp snooping vlan 4094 information option
change-vlan-to vlan 4093
Ruijie(config-if)# end
```

**Related Commands**

| Command | Description |
|---|---|
| N/A | N/A |

**Platform Description** N/A

## 8.15 ip dhcp snooping vlan information option format-type circuit-id string

Use this command to configure the option82 sub-option circuit-id as user-defined (the storage format is ASCII) and to perform the packet forwarding.
Use the **no** form of this command to restore the default setting.
**ip dhcp snooping vlan** *vlan-id* **information option format-type circuit-id string** *ascii-string*
**no ip dhcp snooping vlan** *vlan-id* **information option format-type circuit-id string** *ascii-string*

**Parameter Description**

| Parameter | Description |
|---|---|
| *vlan-id* | The VLAN where the DHCP request packets are |
| *ascii-string* | The user-defined content to fill to the Circuit ID |

**Defaults** This function is disabled by default.

**Command Mode** Interface configuration mode

**Usage Guide** This command is used to add the option82 to the DHCP request packets. The content of the sub-option circuit-id is customized with 3 to 63 bytes, and the DHCP server will assign the addresses according the option82 information.

**Configuration Examples** The following example adds the option82 to the DHCP request packets with the content of the sub-option circuit-id as *port-name*.

```
Ruijie# configure terminal
Ruijie(config)# interface fastEthernet 0/1
Ruijie(config-if)# ip dhcp snooping vlan 4094 information option format-type
```

```
circuit-id string port-name
Ruijie(config-if)# end
```

**Related Commands**

| Command | Description |
|---|---|
| N/A | N/A |

**Platform Description** N/A

## 8.16 ip dhcp snooping vlan max-user

Use this command to set the maximum number of users bound with the VLAN.
Use the **no** form of this command to restore the default setting.
**ip dhcp snooping vlan** *vlan-word* **max-user** *user-number*
**no ip dhcp snooping vlan** *vlan-word* **max-user** *user-number*

**Parameter Description**

| Parameter | Description |
|---|---|
| *vlan-word* | The VLAN range |
| *user-number* | The maximum number of users bound with the VLAN |

**Defaults** This function is disabled by default.

**Command Mode** Interface configuration mode

**Usage Guide** Use this command to set the maximum number of users bound with the VLAN. This function combined with the corresponding topology can prevent illegal DHCP packet attacks.

**Configuration Examples** The following example sets the maximum number of users bound with VLAN 1 to 10 and VLAN 20 to 30 respectively.

```
Ruijie# configure terminal
Ruijie(config)# interface GigabitEthernet 0/1
Ruijie(config-if-GigabitEthernet 0/1)# ip dhcp snooping vlan 1-10,20 max-user
30
Ruijie(config-if-GigabitEthernet 0/1)# end
```

**Related Commands**

| Command | Description |
|---|---|
| N/A | N/A |

**Platform** N/A

**Description**

## 8.17 renew ip dhcp snooping database

Use this command to import the information in current flash to the DHCP Snooping binding database manually as needed.

**renew ip dhcp snooping database**

**Parameter Description**

| Parameter | Description |
|---|---|
| N/A | N/A |

**Defaults** N/A

**Command Mode** Privileged EXEC mode

**Usage Guide** This command is used to import the flash file information to the DHCP Snooping database in real time.

Records out of lease time and repeated will be neglected.

**Configuration Examples** The following example imports the flash file information to the DHCP Snooping database.

```
Ruijie# renew ip dhcp snooping database
```

**Related Commands**

| Command | Description |
|---|---|
| N/A | N/A |

**Platform Description** N/A

## 8.18 show ip dhcp snooping

Use this command to display the DHCP Snooping configuration.

**show ip dhcp snooping**

**Parameter Description**

| Parameter | Description |
|---|---|
| N/A | N/A |

**Defaults** N/A

**Command Mode** Privileged EXEC mode

**Usage Guide** N/A

**Configuration Examples**

```
The following example displays the DHCP Snooping configuration.
Ruijie# show ip dhcp snooping
Switch DHCP snooping status :ENABLE
Verification of hwaddr field status :DISABLE
DHCP snooping database write-delay time: 0 seconds
DHCP snooping option 82 status: ENABLE
DHCP snooping Support Bootp bind status: ENABLE
Interface                                    Trusted           Rate
limit(pps)
------------------------                       ----------------
----------------
GigabitEthernet 0/4                            YES              unlimited
Default                                      No
```

**Related Commands**

| Command | Description |
|---|---|
| **ip dhcp snooping** | Enables the DHCP Snooping globally. |
| **ip dhcp snooping verify mac-address** | Enables the check of source MAC address of DHCP Snooping packets. |
| **ip dhcp snooping write-delay** | Sets the interval of writing user information to FLASH periodically. |
| **ip dhcp snooping information option** | Adds option82 to the DHCP request message. |
| **ip dhcp snooping bootp-bind** | Enables the DHCP Snooping bootp bind function. |
| **ip dhcp snooping trust** | Sets the port as a trust port. |

**Platform Description** N/A

## 8.19 show ip dhcp snooping binding

Use this command to display the information of the DHCP Snooping binding database.

**show ip dhcp snooping binding**

**Parameter Description**

| Parameter | Description |
|---|---|
| N/A | N/A |

**Defaults** N/A

**Command Mode** Privileged EXEC mode

**Usage Guide** This command is used to display all the information of the DHCP Snooping binding database.

**Configuration Examples** 1: The following example displays the information of the DHCP Snooping binding database.

```
Ruijie# show ip dhcp snooping binding
Total number of bindings: 1
NO.   MACADDRESS        IPADDRESS      LEASE(SEC)   TYPE         VLAN
INTERFACE
----- ------------------ --------------- ------------ ------------- -----
--------------------
1     0000.0000.0001     1.1.1.1        78128       DHCP-Snooping 1
GigabitEthernet 0/1
2     0000.0000.0002     2.2.2.2        78111       DHCP-Snooping 1     WLAN 1
```

| Parameter | Description |
|---|---|
| Total number of bindings | The total number of bindings in the DHCP Snooping database. |
| NO. | The record order. |
| MacAddress | The MAC address of the user. |
| IpAddress | The IP address of the user. |
| Lease(sec) | The lease time of the record. |
| Type | The record type. |
| VLAN | The VLAN where the user belongs. |
| INNER-VLAN | The inner VLAN of the user. It is applicable to all QINQ-termination products. |
| VXLAN | The VXLAN where the user belongs. |
| Interface | The user's connection interface. It can be a either a wired access interface or wireless access WLAN. |

**Related Commands**

| Command | Description |
|---|---|
| **ip dhcp snooping binding** | Adds the static user information to the DHCP Snooping database. |
| **clear ip dhcp snooping binding** | Clears the dynamic user information from the DHCP Snooping binding database. |

**Platform** N/A

**Description**

# 9 IP Source Guard Commands

## 9.1 ip source binding

Use this command to add static user information to IP source address binding database.
Use the **no** form of this command to delete static user information from IP source address binding database.
**ip source binding** *mac-address* **vlan** *vlan-id ip-address* { **interface** *interface-id* **| wlan** *wlan-id* **| ip-mac | ip-only** }
**no ip source binding** *mac-address* **vlan** *vlan-id ip-address* { **interface** *interface-id* **| wlan** *wlan-id* **| ip-mac | ip-only** }

**Parameter Description**

| Parameter | Description |
|---|---|
| *mac-address* | Adds user MAC address statically. |
| *vlan-id* | Adds user VLAN ID statically. |
| *ip-address* | Adds user IP address statically. |
| *interface-id* | Adds user interface ID statically. |
| **wlan** *wlan-id* | Add user WLAN ID statically. |
| **ip-mac** | The global binding type is IP+MAC |
| **ip-only** | The global binding type is IP only. |

**Defaults** No static address is added by default.

**Command Mode** Global configuration mode

**Usage Guide** This command allows specific clients to go through IP source guard detection instead of DHCP.
This command is supported on the wired L2 switching port, AP port, sub interface and WLAN.
This command enables global binding for IP source guard so that specific clients will get detected on all interfaces.

A static IPv6 source binding is valid either on wired and WLAN interfaces or in global configuration mode.

A new binding will overwrite the old one sharing the same configuration.

**Configuration Examples** The following example adds the interface Id and WLAN ID of static users.

```
Ruijie# configure terminal
Ruijie(config)# ip source binding 0000.0000.0001 vlan 1 1.1.1.1 interface
GigabitEthernet 0/1
Ruijie(config)# ip source binding 0000.0000.0002 vlan 1 1.1.1.2 wlan 1
```

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

The following example adds static user information based on IP-MAC binding.

```
Ruijie# configure terminal
Ruijie(config)# ip source binding 0000.0000.0001 vlan 1 1.1.1.1 ip-mac
Ruijie(config)# end
```

The following example adds static user information based on IP binding.

```
Ruijie# configure terminal
Ruijie(config)# ip source binding 0000.0000.0001 vlan 1 1.1.1.1 ip-only
Ruijie(config)# end
```

**Related Commands**

| Command | Description |
| --- | --- |
| **show ip source binding** | Displays the binding information of IP source address and database. |

**Platform Description** N/A

## 9.2 ip verify source

Use this command to enable IP Source Guard function on the interface.
Use the **no** form of this command to restore the default setting.
**ip verify source** [ **port-security** ]
**no ip verify source**

**Parameter Description**

| Parameter | Description |
| --- | --- |
| **port-security** | Configures IP Source Guard to do IP+MAC-based detection. |

**Defaults** This function is disabled by default.

**Command Mode** Interface configuration mode/WLAN security configuration mode

**Usage Guide** This command enables IP Source Guard function on the interface to do IP-based or IP+MAC-based detection.
This command is supported on the wired L2 switching port, AP port, sub interface and WLAN.

⚠ IP Source Guard takes effect only on DHCP Snooping untrusted port. In other words, IP Source Guard does not take effect when configuring it on Trust port or the port which is not controlled by DHCP Snooping.

**Configuration Examples**

The following example enables IP-based IP Source Guard function.

```
Ruijie# configure terminal
Ruijie(config)# interface GigabitEthernet 0/1
Ruijie(config-if-GigabitEthernet 0/1)# ip verify source
Ruijie(config-if)# end
Ruijie(config)# wlansec 1
Ruijie(config-wlansec)# ip verify source
Ruijie(config-wlansec)# end
```

The following example enables IP+MAC-based IP Source Guard function.

```
Ruijie# configure terminal
Ruijie(config)# interface GigabitEthernet 0/2
Ruijie(config-if-GigabitEthernet 0/2)# ip verify source port-security
Ruijie(config-if)# end
Ruijie(config)# wlansec 2
Ruijie(config-wlansec)# ip verify source port-security
Ruijie(config-wlansec)# end
```

**Related Commands**

| Command | Description |
|---|---|
| **show ip verify source** | Displays user filtering entry of IP Source Guard. |

**Platform Description**

N/A

## 9.3 ip verify source exclude-vlan

Use this command to exclude a VLAN from the IP source guard configuration on the port.

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

**ip verify source exclude-vlan** *vlan-id*

**no ip verify source exclude-vlan** *vlan-id*

**Parameter Description**

| Parameter | Description |
|---|---|
| *vlan-id* | The ID of VLAN excluded from the IP source guard configuration. |

**Defaults**

This function is disabled by default.

**Command Mode**

Interface configuration mode/WLAN security configuration mode

**Usage Guide**

- This command is used to exclude a VLAN from the IP source guard configuration. IP packets in this VLAN are forwarded without being checked and filtered.
- Once the IP source guard function is disabled, the excluded VLAN is cleared automatically.
- This command is supported on the wired L2 switching port, AP port, sub interface and WLAN.

Only when the IP source guard configuration is enabled on the port can a VLAN be excluded.

**Configuration Examples**

The following example configuration configures the IP source guard configuration for the port and excludes a VLAN.

```
Ruijie# configure terminal
Ruijie(config)# interface GigabitEthernet 0/1
Ruijie(config-if-GigabitEthernet 0/1)# ip verify source
Ruijie(config-if-GigabitEthernet 0/1)# ip verify exclude-vlan 1
Ruijie(config-if)# end
Ruijie(config)# wlansec 1
Ruijie(config-wlansec)# ip verify source
Ruijie(config-wlansec)# ip verify exclude-vlan 1
Ruijie(config-wlansec)# end
```

**Related Commands**

| Command | Description |
|---|---|
| N/A | N/A |

**Platform Description**

N/A

## 9.4 show ip source binding

Use this command to display the binding information of IP source addresses and database.

**show ip source binding** [ *ip-address* ] [ *mac-address* ] [ **dhcp-snooping** ] [ **static** ] [ **vlan** *vlan-id* ] [ **interface** *interface-id* ] [**wlan** *wlan-id*]

**Parameter Description**

| Parameter | Description |
|---|---|
| *ip-address* | Displays user binding information of corresponding IP. |
| *mac-address* | Displays user binding information of corresponding MAC. |
| **dhcp-snooping** | Displays binding information of dynamic user. |
| **static** | Displays binding information of static user. |
| *vlan-id* | Displays user binding information of corresponding VLAN. |

| | |
|---|---|
| *interface-id* | Displays user binding information of corresponding interface. |
| *wlan-id* | Displays user information bound with the corresponding WLAN. |

**Defaults** N/A

**Command Mode** Privileged EXEC mode

**Usage Guide** N/A

**Configuration Examples** The following example displays the binding information of IP source guard addresses and database.

```
Ruijie# show ip source binding static
Ruijie#show ip source binding static
Total number of bindings: 5
NO.    MACADDRESS         IPADDRESS       LEASE(SEC)    TYPE          VLAN  INTERFACE
----- ------------------ --------------- ------------ ------------- -----
--------------------
1      0001.0002.0001     1.2.3.2         Infinite      Static        1     Global
2      0001.0002.0002     1.2.3.3         Infinite      Static        1     GigabitEthernet
0/5
3      0001.0002.0003     1.2.3.4         Infinite      Static        1     Global
4      0001.0002.0004     1.2.3.5         Infinite      Static        1     Global
5      0001.0002.0005     1.2.3.6         Infinite      Static        1     WLAN 1
```

**Related Commands**

| Command | Description |
|---|---|
| **ip source binding** | Sets the binding static user. |

**Platform Description** N/A

## 9.5 show ip verify source

Use this command to display user filtering entry of IP Source Guard.

**show ip verify source** [ **interface** *interface-id* ] [**wlan** *wlan-id*]

**Parameter Description**

| Parameter | Description |
|---|---|
| *interface-id* | Displays user filtering entry of corresponding interface. |
| *wlan-id* | Displays user filtering entry of corresponding WLAN. |

**Defaults** N/A

**Command Mode** Privileged EXEC mode

**Usage Guide** If IP Source Guard is not enabled on the corresponding interface, the printing information will be shown on the terminal as: “IP source guard is not configured on the interface FastEthernet 0/10”
Now, IP Source Guard supports the following filtering modes:
**inactive-restrict-off**: the IP Source Guard is disabled on bound interfaces.
**inactive--not-apply**: the IP Source Guard cannot adds bound entries into filtering entries for system errors.
**active**: the IP Source Guard is active.

**Configuration Examples** The following example displays user filtering entry of IP Source Guard.

```
Ruijie # show ip verify source
Total number of bindings: 7
NO.   INTERFACE          FILTERTYPE  FILTERSTATUS         IPADDRESS
MACADDRESS     VLAN TYPE
----- -------------------- ----------- ---------------------
--------------- --------------- -------- -------------
1     Global             IP+MAC     Inactive-not-apply    192.168.0.127
0001.0002.0003  1 Static
2     GigabitEthernet 0/5  IP-ONLY    Active              1.2.3.4
0001.0002.0004  1 DHCP-Snooping
3     Global             IP-ONLY    Active              1.2.3.7
0001.0002.0007  1 Static
4     Global             IP+MAC     Active              1.2.3.6
0001.0002.0006  1 Static
5     GigabitEthernet 0/1  UNSET      Inactive-restrict-off  1.2.3.9
0001.0002.0009  1 DHCP-Snooping
6     GigabitEthernet 0/5  IP-ONLY    Active              Deny-All
7     WLAN 1             IP-ONLY    Active              Deny-ALL
```

**Related Commands**

| Command | Description |
| --- | --- |
| **ip verify source** | Sets IP Source Guard on the interface. |

**Platform Description** N/A

# 10 DNS Snooping Commands

## 10.1 clear free-url

Use this command to clear authentication-free URLs.

**clear free-url**

**Parameter Description**

| Parameter | Description |
| --- | --- |
| N/A | N/A |

**Command Mode** Privileged mode, global configuration mode

**Usage Guide** Run this command to clear authentication-free URLs.

**Configuration Example** The following example clears authentication-free APP URLs.

```
Ruijie(config)#clear free-url
```

**Platform** N/A

## 10.2 free-url

Use this command to configure authentication-free URL.

**free-url** { **weixin** | **sina** | **iphone** | **url** *url* }

Use the **no** form of this command to clear authentication-free URL.

**no free-url** { **weixin** | **sina** | **iphone** | **url** *url* }

**Parameter Description**

| Parameter | Description |
| --- | --- |
| **weixin** | Indicates Weixin to be free of authentication. |
| **sina** | Indicates Sina APPs to be free of authentication. |
| **iphone** | Indicates specified iphone APP to be free of authentication. |
| *url* | Indicates authentication-free URL. |

**Defaults** By default, this function is disabled.

**Command Mode** Global configuration mode

14

**Usage Guide** You can configured multiple authentication-free URLs.

**Configuration Example** The following example configures authentication-free URL.

```
Ruijie#configure terminal
Ruijie(config)# free-url weixin
Ruijie(config)#exit
```

**Verification** Run the **show free-url** command to check the authentication-free URL information.

**Common Errors** N/A

**Platform** N/A

## 10.3 show free-url

Displays authentication-free URLs.

**show free-url**

**Parameter Description**

| Parameter | Description |
| --- | --- |
| N/A | N/A |

**Command Mode** Privileged mode, global configuration mode

**Usage Guide** Run this command to display authentication-free URLs.

**Configuration Example** The following example displays authentication-free APP URLs.

```
Ruijie(config)#show free-url
Total number of domain name   : 4
Total number of ip address    : 11

====================== free-url domain name table ========================
Host                    type
*.qpic.cn               weixin
*.weixin.qq.com         weixin
weixin.qq.com           weixin
*.baidu.com             url
==========================================================================

======================== free-url ip table ===============================
```

```
Host                    type    Address                 TTL(sec)
*.weixin.qq.com         weixin  61.151.224.41           2118
                                140.207.135.125         2118
                                140.207.54.47           2118
*.qpic.cn               weixin  140.206.160.234         2118
                                183.61.49.180           151
                                101.226.129.204         554
                                14.17.52.136            16
weixin.qq.com           weixin  14.17.42.45             800
*.baidu.com             url     115.239.210.246         19
                                115.239.211.235         2286
                                115.239.210.14          284
============================================================================
```

Parameters:

| Parameter | Description |
|---|---|
| Host | Indicates a domain name. |
| type | Indicates a type. |
| Address | Indicates an IP address. |
| TTL | Indicates time to live. |

**Platform** N/A

# 11 IGMP Snooping Commands

## 11.1 clear ip igmp snooping gda-table

Use this command to clear the Group Destination Address (GDA) table.

**clear ip igmp snooping gda-table**

**Parameter Description**

| Parameter | Description |
|---|---|
| N/A | N/A |

**Defaults** N/A

**Command Mode** Privileged EXEC mode

**Usage Guide** The IGMP Snooping GDA table contains VLAN IDs (VIDs), group addresses, routing interface (static or dynamic) ID, and member interface ID. Among them, the VID and group address identify a forwarding entry; the static routing interfaces will not age and cannot be deleted by using the **clear ip igmp snooping gda-table** command.

**Configuration Examples** The following example clears the Group Destination Address (GDA) table.

```
Ruijie# clear ip igmp snooping gda-table
```

**Platform Description** N/A

## 11.2 ip igmp snooping

Use this command to enable IGMP snooping and enter the IVGL mode.

**ip igmp snooping**

Use the **no** or **default** command to restore the default setting.

**no ip igmp snooping**

**default ip igmp snooping**

**Parameter Description**

| Parameter | Description |
|---|---|
| N/A | N/A |

**Defaults** IGMP Snooping is disabled by default.

**Command Mode** Global configuration mode, AP configuration mode

**Usage Guide** **IVGL (Independent VLAN Group Learning):** In this mode, the multicast flows in different VLANs are independent. A host can only request multicast flows to the router interface in the same VLAN. Upon receiving the multicast flow in any VLAN, the switch forwards the flow to the member port in the same VLAN.

**Configuration Examples** The following example enables IGMP Snooping and enters the IVGL mode.

```
Ruijie(config)# ip igmp snooping ivgl
```

**Platform Description** N/A

## 11.3 ip igmp snooping fast-leave enable

Use this command to enable the fast leave function.
Use the **no** or **default** form of this command to restore the default setting.
**ip igmp snooping fast-leave enable**
**no ip igmp snooping fast-leave enable**
**default ip igmp snooping fast-leave enable**

**Parameter Description**

| Parameter | Description |
|---|---|
| N/A | N/A |

**Defaults** This function is disabled by default.

**Command Mode** Global configuration mode

**Usage Guide** After you execute this command to enable the fast-leave function, the system will remove the corresponding multicast group on the corresponding interface upon the receipt of the IGMP leave message.
Subsequently, when the system receives a specific group query packet, the system does not forward it to the corresponding interface. Leave packets include IGMPv2 leave packets and IGMPv3 report packets of the include type without source addresses. The fast leave function applies to scenarios in which one interface is connected to only one host. This function saves bandwidth and resources.

**Configuration Examples** The following example enables the fast leave function.

```
Ruijie(config)# ip igmp snooping fast-leave
```

**Platform Description** N/A

## 11.4 ip igmp snooping host-aging-time

Use this command to configure the aging time of IGMP dynamic ports.
Use the **no** or **default** form of this command to restore the default setting.
**ip igmp snooping host-aging-time** *seconds*
**no ip igmp snooping host-aging-time**
**default ip igmp snooping host-aging-time**

**Parameter Description**

| Parameter | Description |
|---|---|
| *seconds* | Aging time. The unit is second. The value ranges from 1 to 65,535. |

**Defaults** The default is 260 seconds.

**Command Mode** Global configuration mode, AP configuration mode

**Usage Guide** The aging time of a dynamic port is set by the system when the port receives an IGMP packet from the host for joining a certain IP multicast group.
When such an IGMP packet is received, the system resets the aging timer for the port. The duration of this timer is determined by **host-aging-time**. If the timer expires, the system determines that there is no host in this port for receiving multicast packets. The multicast device removes the port from the IGMP Snooping group. After the **ip igmp snooping host-aging-time** command is executed, the aging time will be determined by **host-aging-time**. This command takes effect only after the system receives the next IGMP packet. This command does not change the current aging time.

In AP configuration mode, run the **igmp snooping host-aging-time** *seconds* command to configure the aging time of IGMP dynamic ports, and run the **no igmp snooping host-aging-time** command to restore the default setting.

**Configuration Examples** The following example sets the aging time to 30 seconds.

```
Ruijie(config)# ip igmp snooping host-aging-time 30
```

**Related Commands**

| Command | Description |
|---|---|
| N/A | N/A |

**Platform Description** N/A

## 11.5 ip igmp snooping ignore-query-timer

Use this command to ignore the query timer.
Use the **no** or **default** form of this command to restore the default setting.
**ip igmp snooping ignore-query-timer**

**no ip igmp snooping ignore-query-timer**
**default ip igmp snooping ignore-query-timer**

**Parameter Description**

| Parameter | Description |
|---|---|
| N/A | N/A |

**Defaults** The query timer is not ignored by default.

**Command Mode** Global configuration mode, AP configuration mode

**Usage Guide** This command is used for instable networks like WLAN, in case that the interface ages due to report packet loss.

In AP configuration mode, run the **igmp snooping ignore-query-timer** command to ignore the query timer and run the **no igmp snooping ignore-query-timer** command to restore the default setting.

**Configuration Examples** The following example ignores the query timer.

```
Ruijie(config)# ip igmp snooping ignore-query-timer
```

**Platform Description** N/A

## 11.6 ip igmp snooping mcast-to-unicast enable

Use this command to enable multicast-to-unicast forwarding.
Use the **no** or **default** form of this command to restore the default setting.
**ip igmp snooping mcast-to-unicast enable**
**no ip igmp snooping mcast-to-unicast enable**
**default ip igmp snooping mcast-to-unicast enable**

**Parameter Description**

| Parameter | Description |
|---|---|
| N/A | N/A |

**Defaults** This function is disabled by default.

**Command Mode** AC: AP configuration mode
Fat AP: Global configuration mode

**Usage Guide** In unicast WLAN, this function is supported only on APs.

- With this function enabled, packets arriving at APs are differentiated in whether to apply this

function.

- In AP configuration mode, run the **igmp snooping mcast-to-unicast enable** command to enable this function and the **no igmp snooping mcast-to-unicast enable** command to disabled it.

This function takes effect only when enabled on users following multicast-to-unicast policies like the packet rate and the group range.

**Configuration Examples** The following example enables multicast-to-unicast forwarding.

```
Ruijie(config-ap)# igmp snooping mcast-to-unicast enable
```

**Platform Description** N/A

## 11.7 ip igmp snooping mcast-to-unicast group-range

Use this command to set the multicast-to-unicast group range.
Use the **no** or **default** form of this command to restore the default setting.
**ip igmp snooping mcast-to-unicast group-range** *ip-addr ip-addr*
**no ip igmp snooping mcast-to-unicast group-range**
**default ip igmp snooping mcast-to-unicast group-range**

**Parameter Description**

| Parameter | Description |
|---|---|
| *ip-addr* | The group range from 224.0.1.0 to 239.255.255.255 |

**Defaults** No multicast-to-unicast group range is set by default.

**Command Mode** AC: AP configuration mode
Fat AP: Global configuration mode

**Usage Guide** In unicast WLAN, this function is supported only on APs.
This function optimizes bandwidth utilization, which only permits the multicast-to-unicast forwarding of groups in need.

In AP configuration mode, run the **igmp snooping mcast-to-unicast group-range** command to enabled this function and the **no igmp snooping mcast-to-unicast group-range** command to restore the default setting.

**Configuration Examples** The following example sets the multicast-to-unicast group range in AP configuration mode.

```
Ruijie(config-ap)# igmp snooping mcast-to-unicast group-range 239.1.1.1.
239.10.1.1.1
```

**Platform Description** N/A

## 11.8 ip igmp snooping mast-to-unicast max-group

Use this command to set the maximum multicast-to-unicast group number.
Use the **no** or **default** form of this command to restore the default setting.
**ip igmp snooping mcast-to-unicast max-group** *number*
**no ip igmp snooping mcast-to-unicast max-group**
**default ip igmp snooping mcast-to-unicast max-group**

**Parameter Description**

| Parameter | Description |
|---|---|
| *number* | The maximum group number from 1 to 64 |

**Defaults** The default is 64.

**Command Mode** AC: AP configuration mode
Fat AP: Global configuration mode

**Usage Guide** In unicast WLAN, this function is supported only on APs.
This function optimizes bandwidth utilization, which only permits the multicast-to-unicast forwarding of groups with the configured number. When the bandwidth is not enough, use this command to reduce the maximum group number. When a multicast group is deleted, this command allows another group to join in the activity.

In AP configuration mode, run the **igmp snooping mcast-to-unicast max-group** command to enable this function and the **no igmp snooping mcast-to-unicast max-group** command to restore the default setting.

**Configuration Examples** The following example sets the maximum multicast-to-unicast group number in AP configuration mode.

```
Ruijie(config-ap)# igmp snooping mcast-to-unicast max-group 10
```

**Platform Description** N/A

## 11.9 ip igmp snooping mrouter learn pim-dvmrp

Use this command to configure a device to listen to the IGMP Query/Dvmrp or PIM Help packets dynamically in order to automatically identify a routing interface
Use the **no** form of this command to disable the dynamic learning.
Use the **default** form of this command to restore the default setting.
**ip igmp snooping mrouter learn pim-dvmrp**
**no ip igmp snooping mrouter learn pim-dvmrp**
**default ip igmp snooping** [ **vlan** *vid* ] **mrouter learn pim-dvmrp**

**Parameter Description**

| Parameter | Description |
|---|---|
| **vlan** *vid* | VLAN ID. By default, the specified version is supported on all VLANs. |

**Defaults** This function is enabled by default.

**Command Mode** Global configuration mode

**Usage Guide** Routing interface is a port through which a multicast device (with IGMP Snooping enabled) is directly connected to a multicast neighbouring device (with multicast routing protocols enabled).
By default, the dynamic routing interface learning function is enabled. You can use the no form of this command to disable this function and clear all routing interfaces learnt dynamically. With dynamic routing interface learning function disabled globally, the function of all vlans will be disabled. Beside, with this function enabled globally, if the function of specified vlan is disabled, the dynamic routing interface learning function of the corresponding vlan is disabled. When the source port check function is enabled, only the multicast flow enters from the routing interface is legal and it is forwarded to the registered interface by the multicast equipment, the multicast flow from the non routing interface is considered to be the illegal and is discarded. With the source port check function enabled, the dynamic routing interface learning function will improve the application flexibility of IGMP snooping.

**Configuration Examples** The following example enables the dynamic routing interface learning function on VLAN 1.

```
Ruijie(config)# no ip igmp snooping mrouter learn pim-dvmrp
Ruijie(config)# ip igmp snooping vlan 1 mrouter learn pim-dvmrp
```

**Platform Description** N/A

## 11.10 ip igmp snooping querier

Use this command to enable the IGMP querier.
Use **no** or **default** form of this command to restore the default setting.
**ip igmp snooping** [ **vlan** *vid* ] **querier**
**no ip igmp snooping** [ **vlan** *vid* ] **querier**
**default ip igmp snooping** [ **vlan** *vid* ] **querier**

**Parameter Description**

| Parameter | Description |
|---|---|
| **vlan** *vid* | VLAN ID. By default, the specified version is supported on all VLANs. |

**Defaults** This function is disabled by default.

**Command** Global configuration mode

**Mode**

**Usage Guide** After globally enabling the IGMP querier, you must enable the IGMP querier function in VLAN to activate this function.
If the IGMP querier function is disabled globally, the IGMP querier will be disabled in all VLANs.

**Configuration Examples** The following example enables the IGMP querier function in VLAN 2.

```
Ruijie(config)# ip igmp snooping querier
Ruijie(config)# ip igmp snooping vlan 2 querier
```

**Platform Description** N/A

## 11.11 ip igmp snooping querier address

Use this command to specify a source IP address for IGMP querier.
Use **no** or **default** form of this command to remove the source IP address configured.
**ip igmp snooping** [ **vlan** *vid* ] **querier address** *a.b.c.d*
**no ip igmp snooping** [ **vlan** *vid* ] **querier address**
**default ip igmp snooping** [ **vlan** *vid* ] **querier address**

**Parameter Description**

| Parameter | Description |
|---|---|
| **vlan** *vid* | VLAN ID. By default, the specified version is supported on all VLANs. |
| *a.b.c.d* | Source IP address of the IGMP querier |

**Defaults** N/A

**Command Mode** Global configuration mode

**Usage Guide** After enabling IGMP querier, you msut configure a source IP address for the IGMP querier to activate this function..
If the IGMP querier source IP has been specified in VLAN, the source IP configured in the relevant VLAN will be used first.

**Configuration Examples** The following example specifies the source IP of the IGMP querier as 1.1.1.1 on the device.

```
Ruijie(config)# ip igmp snooping querier address 1.1.1.1
```

The following example specifies the source IP of the IGMP querier as 1.1.1.1 in VLAN 3.

```
Ruijie(config)# ip igmp snooping vlan 3 querier address 1.1.1.1
```

**Platform Description**

## 11.12 ip igmp snooping querier max-response-time

Use this command to configure the maximum response time of the IGMP querier.
Use **no** or **default** form of this command to restore to the default setting.
**ip igmp snooping** [ **vlan** *vid* ] **querier max-response-time** *seconds*
**no ip igmp snooping [ vlan** *vid* **] querier max-response-time**
**default ip igmp snooping** [ **vlan** *vid* ] **querier max-response-time**

**Parameter Description**

| Parameter | Description |
|---|---|
| *num* | Maximum response time from 1 to 25 in the unit of seconds |
| **vlan** *vid* | VLAN ID. By default, the specified version is supported on all VLANs. |

**Defaults** The default is 10 seconds.

**Command Mode** Global configuration mode

**Usage Guide** Configure this command to specify the maximum response time to query packets.
By default, the maximum response time is 10 seconds. If the maximum response time has been specified in the corresponding VLAN, the value specified in VLAN will be used first.

**Configuration Examples** The following example specifies the maximum response time of the IGMP querier on the device.

```
Ruijie(config)# ip igmp snooping querier max-response-time 15
```

The following example specifies the maximum response time of the IGMP querier in VLAN 3.

```
Ruijie(config)# ip igmp snooping vlan 3 querier max-response-time 15
```

**Platform Description** N/A

## 11.13 ip igmp snooping querier query-interval

Use this command to specify the interval for IGMP querier to send query packets.
Use **no** or **default** form of this command to restore the default setting.
**ip igmp snooping querier query-interval** *seconds*
**no ip igmp snooping querier query-interval**
**default ip igmp snooping** [ **vlan** *vid* ] **querier query-interval**

**Parameter Description**

| Parameter | Description |
|---|---|
| *seconds* | Query interval from 1 to 18,000 in the unit of seconds |
| **vlan** *vid* | VLAN ID. By default, the specified version is supported on all VLANs. |

**Defaults** The default is 60 seconds.

**Command Mode** Global configuration mode

**Usage Guide** If the query interval has been configured in the corresponding VLAN, the value specified in VLAN will be used first.

**Configuration Examples** The following example configures the query interval on the device.

```
Ruijie(config)# ip igmp snooping querier query-interval 100
```

The following example configures the query interval in VLAN 3.

```
Ruijie(config)# ip igmp snooping vlan 3 querier query-interval 100
```

**Platform Description** N/A

## 11.14 ip igmp snooping querier timer expiry

Use this command to specify the expiration timer for non-querier.
Use **no** form of this command to restore the default setting.
**ip igmp snooping** [ **vlan** *vid* ] **querier timer expiry** *seconds*
**ip igmp snooping** [ **vlan** *vid* ] **querier timer expiry** *seconds*
**default ip igmp snooping** [ **vlan** *vid* ] **querier timer expiry**

**Parameter Description**

| Parameter | Description |
|---|---|
| *seconds* | Theexpiration timer from 60 to 300 in the unit of seconds |
| **vlan** *vid* | VLAN ID. By default, the specified version is supported on all VLANs. |

**Defaults** The default is 125 seconds.

**Command Mode** Global configuration mode

**Usage Guide** After globally enabling IGMP querier, if the device is elected as a non-querier, execute this command to change the expiration timer for non-querier.
If expiration timer has been configured in the corresponding VLAN, the value specified in VLAN will be used first.

**Configuration Examples** The following example configures the non-querier expiration timer on the device.

```
Ruijie(config)# ip igmp snooping querier timer expiry 60
```

The following example configures the non-querier expiration timer in VLAN 3.

```
Ruijie(config)# ip igmp snooping vlan 3 querier timer expiry 60
```

**Platform Description** N/A

## 11.15 ip igmp snooping querier version

Use the following commands to specify IGMP Snooping querier version.
**ip igmp snooping** [ **vlan** *vid* ] **querier version 1**
**ip igmp snooping** [ **vlan** *vid* ] **querier version 2**
Use **no** or **default** form of this command to restore to the default setting.
**no ip igmp snooping** [ **vlan** *vid* ] **querier version**
**default ip igmp snooping** [ **vlan** *vid* ] **querier version**

**Parameter Description**

| Parameter | Description |
|---|---|
| **vlan** *vid* | VLAN ID. By default, the specified version is supported on all VLANs. |

**Defaults** The default version is IGMPv2.

**Command Mode** Global configuration mode

**Usage Guide** If an IGMP querier version has been configured in a VLAN, the version specified in the VLAN will be used first.

**Configuration Examples** The following example configures IGMP querier version on the device.

```
Ruijie(config)# ip igmp snooping querier version 1
```

**Platform Description** N/A

## 11.16 ip igmp snooping query-max-response-time

Use this command to specify the time for the switch to wait for the member join message after receiving the **query** message.
Use the **no** or **default** form of this command to restore the default setting.
**ip igmp snooping query-max-response-time** *seconds*
**no ip igmp snooping query-max-resposne-time**
**default ip igmp snooping query-max-response-time**

**Parameter Description**

| Parameter | Description |
|---|---|
| *seconds* | The aging time of the routing inerface that the switch learns dynamically, in the range from 1 to 65.535 |

**Defaults** The default is 10 seconds.

**Command Mode** Global configuration mode, AP configuration mode

**Usage Guide** You can specify the time for the switch to wait for the member join message after receiving the query message. If the switch does not receive the member join message in the specified time, it considers that the member has left and then deletes the member.
This command lets you adjust the waiting time after receiving the query message. This command takes effect only after the switch receives the next member join message. This command does not change the current wait time.

In AP configuration mode, run the **igmp snooping query-max-response-time** *seconds* command to enable this function and the **no igmp snooping query-max-response-time** command to restore the default setting.

**Configuration Examples** The following examples sets the aging time of the routing interface that the switch learns dynamically to 100 seconds.

```
Ruijie(config)# ip igmp snooping query-max-response-time 100
```

**Platform Description** N/A

## 11.17 ip igmp snooping suppression enable

Use this command to enable IGMP snooping suppression.
Use the **no** or **default** form of this command to restore the default setting.
**ip igmp snooping suppression enable**
**no ip igmp snooping suppression enable**
**default ip igmp snooping suppression enable**

**Parameter Description**

| Parameter | Description |
|---|---|
| N/A | N/A |

**Defaults** This function is disabled by default.

**Command Mode** Global configuration mode

**Usage Guide** When this function is enabled, IGMP Snooping only forwards the first report from a specific VLAN or group, and suppresses the following reports to constrain traffic in the networks.
This function is only supported on IGMPv1 and IGMPv2 reports.

**Configuration Examples** The following example enables IGMP snooping suppression on the device.

```
Ruijie(config)# ip igmp snooping suppression enable
```

**Platform Description** N/A

## 11.18 ip igmp snooping vlan

Use this command to enable the IGMP Snooping in the specified VLAN and enter IVGL mode.
Use the **no** form of this command is used to disable the IGMP Snooping.
Use the **default** form of this command to restore the default setting.
**ip igmp snooping vlan** *vid*
**no ip igmp snooping vlan** *vid*
**default ip igmp snooping vlan** *vid*

**Parameter Description**

| Parameter | Description |
|---|---|
| *vid* | VLAN ID in the range from 1 to 4,094 |

**Defaults** IGMP Snooping is disabled by default.

**Command Mode** Global configuration mode

**Usage Guide** Use this command to enable or disable the IGMP snooping on the specified vlan.

The PIM Snooping in the specified VLAN works only when IGMP Snooping is configured. To disable PIM Snooping, you must disable IGMP Snooping in the VLAN first, or disabling will fail and be prompted.

**Configuration Examples** The following example enters IVGL mode and disables the IGMP Snooping in the VLAN 2.

```
Ruijie(config)# ip igmp snooping ivgl
Ruijie(config)# no ip igmp snooping vlan 2
```

**Platform Description** N/A

## 11.19 ip igmp snooping vlan fast-leave enable

Use this command to enable fast-leave function for the specified VLAN.
Use the **no** form of this command to disable this function.
Use the **default** form of this command to restore the default setting.

**ip igmp snooping vlan** *vid* **fast-leave enable**
**no ip igmp snooping vlan** *vid* **fast-leave enable**
**default ip igmp snooping vlan** *vid* **fast-leave enable**

**Parameter Description**

| Parameter | Description |
|---|---|
| *vid* | VLAN ID in the range from 1 to 4,094 |

**Defaults** This function is enabled by default.

**Command Mode** Global configuration mode

**Usage Guide** This command must be used with the **ip igmp snooping fast-leave enable** command.

**Configuration Examples** The following example disables the fast-leave function for VLAN 1.

```
Ruijie(config)# no ip igmp snooping vlan 1 fast-leave enable
```

**Platform Description** N/A

## 11.20 ip igmp snooping vlan mrouter interface

Use this command to configure a static routing interface.
Use the **no** form of this command to delete a static routing interface.
Use the **default** form of this command to restore the default setting.
**ip igmp snooping vlan** *vid* **mrouter interface** *interface-type interface-number*
**no ip igmp snooping vlan** *vid* **mrouter interface** *interface-type interface-number*
**default ip igmp snooping vlan** *vid* **mrouter interface** *interface-type interface-number*

**Parameter Description**

| Parameter | Description |
|---|---|
| *vid* | VLAN ID in the range from 1 to 4,094 |
| *interface-type interface-number* | Interface ID |

**Defaults** No static routing interface is configured by default.

**Command Mode** Global configuration mode

**Usage Guide** A dynamic routing interface is learned dynamically through IGMP Snooping. A static routing interface is configured by using this command and cannot age.
When an interface is configured as a static routing interface, all multicast streams received on this

interface will be forwarded.
When the source port check function is enabled, only the multicast flows from the routing interface are forwarded, and other flows will be discarded.

**Configuration Examples** The following example configures a static routing interface.

```
Ruijie(config)# ip igmp snooping vlan 1 mrout erinterface fastEthernet 0/1
```

**Platform Description** N/A

## 11.21 ip igmp snooping vlan static interface

Use this command to configure a static member interface of a multicast group.
Use the **no** form of this command to delete a static member interface from a multicast group.
Use the **default** form of this command to restore the default setting.
**ip igmp snooping vlan** *vid* **static** *group-address* **interface** *interface-type interface-number*
**no ip igmp snooping vlan** *vid* **static** *group-address* **interface** *interface-type interface-number*
**default ip igmp snooping vlan** *vid* **static** *group-address* **interface** *interface-type interface-number*

**Parameter Description**

| Parameter | Description |
|---|---|
| *vid* | VLAN ID in the range from 1 to 4,094 |
| *ip-addr* | Multicast IP address |
| *interface-id* | Interface ID |

**Defaults** No static member interface of any multicast group is configured by default.

**Command Mode** Global configuration mode

**Usage Guide** The IGMP Snooping GDA table contains VLAN IDs (VIDs), group addresses, routing interface (static or dynamic) ID, and member interface ID. Among them, the VID and group address identify a forwarding entry; the static routing interfaces will not age and cannot be deleted by using the **clear ip igmp snooping gda-table** command.

**Configuration Examples** The following example configures a static member interface for the multicast group 224.1.1.1.

```
Ruijie(config)# ip igmp snooping vlan 1 static 224.1.1.1 interface GigabitEthernet 0/1
```

**Platform Description** N/A

## 11.22 ip multicast wlan

Use this command to enable global multicast mode.
Use the **no** or **default** form of this command to restore the default setting.
**ip multicast wlan**
**no ip multicast wlan**
**default ip multicast wlan**

**Parameter Description**

| Parameter | Description |
|---|---|
| N/A | N/A |

**Defaults** Global multicast mode is disabled by default.

**Command Mode** Global configuration mode

**Usage Guide** This command is only supported on ACs and fat APs. With global multicast mode disabled, ACs or fat APs will discards received multicast packets without disposals.

**Configuration Examples** The following example enables global multicast mode.

```
Ruijie(config)# ip multicast wlan
```

**Platform Description** N/A

## 11.23 show ip igmp snooping

Use this command to display related information of IGMP Snooping.
**show ip igmp snooping** [**gda-table** | **interfaces** *interface-type interface-number* | **mdevice**| **statistics** [**vlan** *vlan-id*] | **querier** [ **detail | vlan** *vid* ] | **user-info** ]

**Parameter Description**

| Parameter | Description |
|---|---|
| **vlan** *vid* | VLAN ID. By defualt, IGMP Snooping information of all VLANs are displayed. |

**Defaults** N/A

**Command Mode** Privileged EXEC mode

**Usage Guide** N/A

**Configuration Examples** The following example displays global IGMP Snooping information.

```
Ruijie#show ip igmp snooping
IGMP Snooping running mode: IVGL
IGMP Snooping L2-entry-limit: 65536
Source port check: Disable
Source ip check: Disable
IGMP Fast-Leave: Disable
IGMP Report suppress: Disable
IGMP Global Querier: Disable
IGMP Preview: Disable
IGMP Tunnel: Disable
IGMP Preview group aging time : 60(Seconds)
Dynamic Mroute Aging Time : 300(Seconds)
Dynamic Host Aging Time : 260(Seconds)
The following example displays VLAN1 IGMP Snooping information.
Ruijie#show ip igmp snooping vlan 1
IGMP Snooping running mode: IVGL
IGMP Snooping L2-entry-limit: 65536
Global IGMPv2 Fast-Leave :Disable
Global multicast router learning mode :Enable
Query Max Response Time: 10 (Seconds)
Dynamic Mroute Aging Time : 300(Seconds)
Dynamic Host Aging Time : 260(Seconds)

vlan 1
-------------
IGMP Snooping state: Enable
Multicast router learning mode: pim-dvmrp
IGMP Fast-Leave: Disable
IGMP VLAN querier: Disable
IGMP VLAN Mode: STATIC
```

**Platform Description** N/A

# 12 ACL Commands

## 12.1 command ID table

For IDs used in the following commands, refer to the command ID table below:

| ID | Meaning |
|---|---|
| ID | Number of access list. Range:<br>Standard IP ACL: 1 to 99, 1300 to 1999<br>Extended IP ACL: 100 to 199,2000 to 2699<br>Extended MAC ACL: 700 to 799<br>Extended expert ACL: 2700 to 2899 |
| name | ACL name |
| sn | ACL SN (products can be set according to the priority) |
| start-sn | Start sequence number |
| inc-sn | Sequence number increment |
| deny | If matched, access is denied. |
| permit | If matched, access is permitted. |
| port | Protocol number. For IPv6, this field can be IPv6, ICMP, TCP, UDP and numbers 0 to 255. For IPv4, it can be one of EIGRP, GRE, IPINIP, IGMP, NOS, OSPF, ICMP, UDP, TCP,AHP, ESP, PCP, PIM and IP, or it can be numbers 0 to 255 that represent the IP protocol. It is described when some important protocols, such as ICMP, TCP and UDP, are listed individually. |
| interface *idx* | Interface index |
| src | Packet source IP address (host address or network address) |
| src-wildcard | Source IP address wildcard. It can be discontinuous, for example, 0.255.0.32. |
| src-ipv6-pfix | Source IPv6 network address or network type |
| dst-ipv6-pfix | Destination IPv6 network address or network type |
| pfix-len | Prefix mask length |
| src-ipv6-addr | Source IPv6 address |
| dst-ipv6-addr | Destination IPv6 address |
| dscp | Differential service code point, and code point value. Range: 0 to 63 |
| flow-label | Flow label in the range 0 to 1048575 |
| dst | Packet destination IP address (host address or network address) |
| dst-wildcard | Destination IP address wildcard. It can be discontinuous, such as 0.255.0.32 |
| fragment | Packet fragment filtering. (Not supported on wireless products) |

| | |
|---|---|
| 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)<br>*port* indicates the port number. Dyadic operation needs two port numbers, while other operators only need one port number |
| src-mac-addr | Physical address of the source host |
| dst-mac-addr | Physical address of the destination host |
| VID vid | VLAN ID |
| VID inner vid | VID of the tag |
| ethernet-type | Ethernet protocol type. 0x value can be entered. |
| match-all *tcpf* | Match all bits of the TCP flag. |
| established | Match the RST or ACK bit of the TCP flag. |
| *text* | Remark text |
| *in* | Filter the incoming packets of the interface |
| *out* | Filter the outgoing packets of the interface |
| {rule mask offset}$^{+}$ | rule: Hexadecimal value field; mask: Hexadecimal mask field<br>offset: Refer to the offset table<br>"+" sign indicates at least one group |
| log | Output the matching syslog when the packet matches the ACL rule. |

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.

## 12.2 access-list

Use this command to create an access list to filter data packets. Use the **no** form of this command to remove the specified access list.

1. Standard IP access list (1 to 99, 1300 to 1999)

**access-list** *id* { **deny** | **permit** } { *source source-wildcard* | **host** *source* | **any | interface** *idx* } [**time-range** *tm-range-name* ] [ **log** ]

2. Extended IP access list (100 to 199, 2000 to 2699)

**access-list** *id* {**deny** | **permit**} **protocol** {*source source-wildcard* | **host** *source* | **any| interface** *idx* } {*destination destination-wildcard* | **host** *destination* | **any**} [**precedence** *precedence*] [**tos** *tos*] [**fragment**] [**range** *lower upper*] [**time-range** *time-range-name*] [ **log** ]

3. Extended MAC access list (700 to 799)

**access-list** *id* {**deny** | **permit**} {**any** | **host** *source-mac-address* } {**any** | **host** *destination-mac-address* } [*ethernet-type*][**cos** [*out*][ **inner** *in*]]

4. Extended expert access list (2700 to 2899)

**access-list** *id* {**deny** | **permit**} [**protocol** | [*ethernet-type*][ **cos** [*out*][ **inner** *in*]]] [**VID** [*out*][**inner** *in*]] {**source** *source-wildcard* | **host** *source* | **any**} {**host** *source-mac-address* | **any**} {**destination** *destination-wildcard* | **host** *destination* | **any**} {**host** *destination-mac-address* | **any**} ][**precedence** *precedence*] [**tos** *tos*] [**fragment**] [**time-range** *time-range-name*]

- When you select the Ethernet-type field or cos field:

**access-list** *id* {**deny** | **permit**} {*ethernet-type*| **cos** [*out*][ **inner** *in*]} [**VID** [*out*][**inner** *in*]] {**source** *source-wildcard* | **host** *source* | **any**} {**host** *source-mac-address* | **any** } {**destination**

*destination-wildcard* | **host** *destination* | **any**} {**host** *destination-mac-address* | **any**} [**time-range** *time-range-name*]

- When you select the protocol field:

**access-list** *id* {deny | permit} **protocol [VID** [*out*][**inne**r *in*]] {**source** *source-wildcard* | host *source* | **any**} {**host** *source-mac-address* | **any** }{destination *destination-wildcard* | **host** *destination* | **any}** **{host** *destination-mac-address* | **any} [precedence** *precedence*] [**tos** *tos*] **[fragment]** [**range** *lower upper*] **[time-range** *time-range-name*]

- Extended expert ACLs of some important protocols:

**Internet Control Message Protocol** (ICMP)
**access-list** *id* {**deny** | **permit**} **icmp** [**VID** [*out*][**inner** *in*]] {**source** *source-wildcard* | **host** *source* | **any**} {**host** *source-mac-address* | **any** } {**destination** *destination-wildcard* | **host** *destination* | **any**} {**host** *destination-mac-address* | **any**} [ *icmp-type* ] [ [ *icmp-type* [*icmp-code* ] ] | [ *icmp-message* ] ] [**precedence** *precedence*] [**tos** *tos*] [**fragment**] [**time-range** *time-range-name*]
**Transmission Control Protocol** (TCP)
**access-list** *id* {**deny** | **permit**} **tcp** [**VID** [*out*][**inner** *in*]]{**source** *source-wildcard* | **host** *Source* | **any**} {**host** *source-mac-address* | **any** } [**operator** port [*port*] ] {**destination** *destination-wildcard* | **host** *destination* | **any**} {**host** *destination-mac-address* | **any**} [**operator port** [*port*] ] [**precedence** *precedence*] [**tos** *tos*] [**fragment**] [**range** *lower upper*] [**time-range** *time-range-name*] [ **match-all** *tcp-flag* | **established** ]
**User Datagram Protocol** (UDP)
**access-list** *id* {**deny** | **permit**} **udp** [ **VID** [*out*][**inner** *in*]] {**source** *source –wildcard* | **host** *source* | **any**} {**host** *source-mac-address* | **any** } [ **operator port** [*port*] ] {**destination** *destination-wildcard* | **host** *destination* | **any**}{**host** *destination-mac-address* | **any**} [**operator port** [*port*] ] [**precedence** *precedence*] [**tos** *tos*] [**fragment**] [**range** *lower upper*] [**time-range** *time-range-name*]

**Parameter Description**

| Parameter | Description |
|---|---|
| id | Access list number. The ranges available are 1 to 99, 100 to 199, 1300 to 1999, 2000 to 2699, 2700 to 2899, and 700 to 799. |
| deny | If not matched, access is denied. |
| permit | If matched, access is permitted. |
| source | Specify the source IP address (host address or network address). |
| source-wildcard | It can be discontinuous, for example, 0.255.0.32. |
| protocol | IP protocol number. It can be one of EIGRP, GRE, IPINIP, IGMP, NOS, OSPF, ICMP, UDP, TCP, and IP. It can also be a number representing the IP protocol between 0 and 255. The important protocols such as ICMP, TCP, and UDP are described separately. |
| destination | Specify the destination IP address (host address or network address). |
| destination-wildcard | Wildcard of the destination IP address. It can be discontinuous, for example, 0.255.0.32. |
| fragment | Packet fragment filtering |
| precedence | Specify the packet priority. |
| precedence | Packet precedence value (0 to 7) |

| | |
|---|---|
| range | Layer4 port number range of the packet. |
| lower | Lower limit of the layer4 port number. |
| upper | Upper limit of the layer4 port number. |
| time-range | Time range of packet filtering |
| time-range-name | Time range name of packet filtering |
| tos | Specify type of service. |
| tos | ToS value (0 to 15) |
| icmp-type | ICMP message type (0 to 255) |
| icmp-code | ICMP message type code (0 to 255) |
| icmp-message | ICMP message type name |
| operator | Operator (lt-smaller, eq-equal, gt-greater, neq-unequal, range-range) |
| port [ port ] | Port number; range needs two port numbers, while other operators only need one port number. |
| host source-mac-address | Source physical address |
| host destination-mac-address | Destination physical address |
| VID vid | Match the specified VID. |
| ethernet-type | Ethernet type |
| match-all | Match all the bits of the TCP flag. |
| tcp-flag | Match the TCP flag. |
| established | Match the RST or ACK bits, not other bits of the TCP flag. |

**Defaults** N/A

**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

To remove ACL rules, run the **no** {**sn** | **permit** | **deny**} command in ACL configuration mode.

**Configuration Examples**

1. Example of the standard IP ACL

The following basic IP ACL allows the packets whose source IP addresses are 192.168.1.64 - 192.168.1.127 to pass:

```
Ruijie (config)#access-list 1 permit 192.168.1.64 0.0.0.63
```

2. Example of the extended IP ACL

The following extended IP ACL allows the DNS messages and ICMP messages to pass:

```
Ruijie(config)#access-list 102 permit tcp any any eq domain log
Ruijie(config)#access-list 102 permit udp any any eq domain log
Ruijie(config)#access-list 102 permit icmp any any echo log
Ruijie(config)#access-list 102 permit icmp any any echo-reply
```

3. Example of the extended MAC ACL

This example shows how to deny the host with the MAC address 00d0f8000c0c to provide service with the protocol type 100 on gigabit Ethernet port 1/1. The configuration procedure is as below:

```
Ruijie(config)#access-list 702 deny host 00d0f8000c0c any aarp
Ruijie(config)# interface gigabitethernet 1/1
Ruijie(config-if)# mac access-group 702 in
```

4. Example of the extended expert ACL

The following example shows how to create and display an extended expert ACL. This expert ACL denies all the TCP packets with the source IP address 192.168.12.3 and the source MAC address 00d0.f800.0044.

```
Ruijie(config)#access-list 2702 deny tcp host 192.168.12.3 mac 00d0.f800.0044
any any
Ruijie(config)# access-list 2702 permit any any any any
Ruijie(config)# show access-lists
expert access-list extended 2702
10 deny tcp  host  192.168.12.3 mac 00d0.f800.0044 any any
10 permit any any any any
```

**Related Commands**

| Command | Description |
|---|---|
| show access-lists | Show all the ACLs. |
| mac access-group | Apply the extended MAC ACL on the interface. |

**Platform Description** N/A

## 12.3 access-list list-remark

Use this command to write a helpful comment (remark) for an access list. Use the **no** form of this command to remove the remark.

**access-list** *id* **list-remark** *text*

**no access-list** *id* **list-remark**

**Parameter Description**

| Parameter | Description |
|---|---|
| *id* | Access list number.<br>Standard IP ACL: 1 to 99, 1300 to 1999.<br>Extended IP ACL: 100 to 199. 2000 to 2699.<br>Extended MAC ACL: 700 to 799.<br>Extended Expert ACL: 2700 to 2899. |
| *text* | Comment that describes the access list. |

**Defaults** The access lists have no remarks by default.

**Command Mode** Global configuration mode

**Usage Guide** You can use this command to write a helpful comment for a specified access list. If the specified access list does not exist, the command will create the access list, then add remarks for the access list.

**Configuration Examples** The following example writes a comment of “this acl is to filter the host 192.168.4.12” for ACL100.

```
Ruijie(config)# ip access-list extended 100
Ruijie(config)# access-list 100 list-remark this acl is to filter the host
192.168.4.12
```

**Related Commands**

| Command | Description |
|---|---|
| show access- lists | Displays all access lists, including the remarks for the access lists. |
| show access-lists *id* | Displays the access list of a specified number, including the remarks for the access list. |
| show access-lists *name* | Displays the access list of a specified name, including the remarks for the access list. |

**Platform**

**Description**

## 12.4 access-list remark

Use this command to write a helpful comment (remark) for an entry in a numbered access list. Use the **no** form of this command to remove the remark.

**access-list** *id* **remark** *text*

**no access-list** *id* **remark** *text*

**Parameter Description**

| Parameter | Description |
|---|---|
| *id* | Access list number.<br>Standard IP ACL: 1 to 99, 1300 to 1999.<br>Extended IP ACL: 100 to 199. 2000 to 2699.<br>Extended MAC ACL: 700 to 799.<br>Extended Expert ACL: 2700 to 2899. |
| *text* | Comment that describes the access list entry. |

**Defaults** The access list entries have no remarks by default.

**Command Mode** Global configuration mode

**Usage Guide** You can use this command to write a helpful comment for an entry in a specified access list. If the specified access list does not exist, the command will create the access list, then add remarks for the access entry.

**Configuration Examples** The following example writes a comment for an entry in ACL102.

```
Ruijie(config)# access-list 102 remark deny-host-10.1.1.1
```

**Related Commands**

| Command | Description |
|---|---|
| show access-lists | Displays all access lists, including the remarks for the access list entries. |
| show access-lists *id* | Displays the access list of a specified number, including the remarks for the access list entry. |
| show access-lists *name* | Displays the access list of a specified name, including the remarks for the access list entry. |

**Platform Description**

## 12.5 deny

One or multiple **deny** conditions are used to determine whether to forward or discard the packet. In ACL configuration mode, you can modify the existent ACL or configure according to the protocol details.

5. Standard IP ACL

[*sn*] **deny** {*source source-wildcard* | **host** *source* | **any| interface** *idx* }[**time-range** *tm-range-name*] [ **log** ]

6. Extended IP ACL

[*sn*] **deny protocol source** *source-wildcard* **destination** *destination-wildcard* [**precedence** *precedence*] [**tos** *tos*] [**fragment**] [**range** *lower upper*] [**time-range** *time-range-name*] [ **log** ]

Extended IP ACLs of some important protocols:

- Internet Control Message Prot (ICMP)

[*sn*] **deny icmp** {**source** *source-wildcard* | **host** *source* | **any**} {**destination** *destination-wildcard* | **host** *destination* | **any**} [*icmp-type*] [[*icmp-type* [*icmp-code*]] | [*icmp-message*]] [**precedence** *precedence*] [**tos** *tos*] [**fragment**] [**time-range** *time-range-name*]

- Transmission Control Protocol (TCP)

[*sn*] deny udp {*source source –wildcard* | **host** *source* | **any**} [ *operator* **port** [*port*]] {*destination destination-wildcard* | **host** *destination* | **any**} [*operator* **port** [*port*]] [**precedence** *precedence*] [**tos** *tos*] [**fragment**] [**range** *lower upper*] [**time-range** *time-range-name*] [ **match-all** *tcp-flag* | **established** ]

- User Datagram Protocol (UDP)

[*sn*] deny udp {*source source –wildcard* | **host** *source* | **any**} [ *operator* **port** [*port*]] {*destination destination-wildcard* | **host** *destination* | **any**} [*operator* **port** [*port*]] [**precedence** *precedence*] [**tos** *tos*] [**fragment**] [**range** *lower upper*] [**time-range** *time-range-name*]

7. Extended MAC ACL

[ *sn* ] **deny** { **any** | **host** *source-mac-address* } { **any** | **host** *destination-mac-address* } [ *ethernet-type* ] [ **cos** [ *out* ] [ **inner** *in* ] ]

8. Extended expert ACL

[*sn*] **deny**[**protocol** | [*ethernet-type*][ **cos** [*out*] [**inner** *in*]]] [[**VID** [*out*][**inner** *in*]]] {*source source-wildcard* | **host** *source* | **any**}{**host** *source-mac-address* | **any** } {*destination destination-wildcard* | **host** *destination* | **any**} {**host** *destination-mac-address* | **any**} [**precedence** *precedence*] [**tos** *tos*][**fragment**] [**range** *lower upper*] [**time-range** *time-range-name*]

- When you select the ethernet-type field or cos field:

[*sn*] **deny** {[*ethernet-type*}[**cos** [*out*] [**inner** *in*]]} [[**VID** [*out*][**inner** *in*]]] {*source source-wildcard* | **host** *source* | **any**} {**host** *source-mac-address* | **any** } {*destination destination-wildcard* | **host** *destination* | **any**} {**host** *destination-mac-address* | **any**} [**time-range** *time-range-name*]

- When you select the protocol field:

[*sn*] **deny protocol** [[**VID** [*out*][**inner** *in*]]] {*source source-wildcard* | **host** *source* | **any**} {**host** *source-mac-address* | **any** } {*destinationdestination-wildcard* | **host** *destination* | **any**} { **host** *destination-mac-address* | **any**} [**precedence** *precedence*] [**tos** *tos*] [**fragment**] [**range** *lower upper*] [**time-range** *time-range-name*]

- Extended expert ACLs of some important protocols

**Internet Control Message Protocol** (ICMP)
[*sn*] **deny icmp** [[**VID** [*out*][**inner** *in*]]] {*source source-wildcard* | **host** *source* | **any**} {**host** *source-mac-address* | **any**} {*destination destination-wildcard* | **host** *destination* | **any**} {**host** *destination-mac-address* | **any**} [*icmp-type*] [[*icmp-type* [*icmp-code* ]] | [*icmp-message*]] [**precedence** *precedence*] [**tos** *tos*] [**fragment**] [**time-range** *time-range-name*]
**Transmission Control Protocol** (TCP)
[*sn*] **deny tcp** [[**VID** [*out*][**inner** *in*]]]{*source source-wildcard* | **host** *Source* | **any**} {**host** *source-mac-address* | **any** } [*operator* **port** [*port*]] {*destination destination-wildcard* | **host** *destination* | **any**} {**host** *destination-mac-address* | **any**} [*operator* **port** [*port*]] [**precedence** *precedence*] [**tos** *tos*] [**fragment**] [**range** *lower upper*] [**time-range** *time-range-name*] [**match-all** *tcp-flag* | **established**]
**User Datagram Protocol** (UDP)
[*sn*] **deny udp** [[**VID** [*out*][**inner** *in*]]]{*source source –wildcard* | **host** *source* | **any**} {**host** *source-mac-address* | **any** } [ *operator* **port** [*port*]] {*destination destination-wildcard* | **host** *destination* | **any**}{**host** *destination-mac-address* | **any**} [*operator* **port** [*port*]] [**precedence** *precedence*] [**tos** *tos*] [**fragment**] [**range** *lower upper*] [**time-range** *time-range-name*]
**Address Resolution Protocol** (ARP)
[*sn*] **deny arp** {**vid** *vlan-id*}[ **host** *source-mac-address* | **any**] [**host** *destination –mac-address* | **any**] {*sender-ip sender-ip–wildcard* | **host** *sender-ip* | **any**} {*sender-mac sender-mac-wildcard* | **host** *sender-mac* | **any**} {*target-ip target-ip–wildcard* | **host** *target-ip* | **any**}

5. Extended IPv6 ACL
[*sn*] **deny protocol**{*source-ipv6-prefix*/*prefix-length* | **any** | **host** *source-ipv6-address* } {*destination-ipv6-prefix / prefix-length* | **any**| *hostdestination-ipv6-address*} [**dscp** *dscp*] [**flow-label** *flow-label*] [**fragment**] [**range** *lower upper*] [**time-range** *time-range-name*]
Extended ipv6 ACLs of some important protocols:
**Internet Control Message Protocol** (ICMP)
[*sn*]**deny icmp** {*source-ipv6-prefix / prefix-length* | *any source-ipv6-address* | **host**} {*destination-ipv6-prefix / prefix-length*| **host** *destination-ipv6-address* | **any**} [*icmp-type*] [[*icmp-type* [*icmp-code*]] | [*icmp-message*]] [**dscp** *dscp*] [**flow-label** *flow-label*] [**fragment**] [**time-range** *time-range-name*]
**Transmission Control Protocol** (TCP)
[*sn*] **deny tcp** {*source-ipv6-prefix / prefix-length* | **host***source-ipv6-address* | **any**}[*operator* **port**[*port*]] {*destination-ipv6-prefix /prefix-length* | **host** *destination-ipv6-address* | **any**} [*operator* **port** [*port*]] [**dscp** *dscp*] [**flow-label** *flow-label*] [**fragment**] [**range** *lower upper*] [**time-range** *time-range-name*] [**match-all** *tcp-flag* | **established**]
**User Datagram Protocol** (UDP)
[sn] **deny udp** {*source-ipv6-prefix/prefix-length* | **host** *source-ipv6-address* | **any**} [*operator* **port** [*port*]] {*destination-ipv6-prefix /prefix-length* | **host** *destination-ipv6-address* | **any**}[*operator* **port** [*port*]] [**dscp** *dscp*] [**flow-label** *flow-label*] [**fragment**] [**range** *lower upper*] [**time-range**

*time-range-name*]

**Parameter Description**

| Parameter | Description |
|---|---|
| *sn* | ACL entry sequence number |
| *source-ipv6-prefix* | Source IPv6 network address or network type |
| *destination-ipv6-prefix* | Destination IPv6 network address or network type |
| *prefix-length* | Prefix mask length |
| *source-ipv6-address* | Source IPv6 address |
| *destination-ipv6-address* | Destination IPv6 address |
| dscp | Differential Service Code Point |
| *dscp* | Code value, within the range of 0 to 63 |
| flow-label | Flow label |
| *flow-label* | Flow label value, within the range of 0 to 1048575. |
| *protocol* | For the IPv6, the field can be ipv6 \| icmp \| tcp \| udp and number in the range 0 to 255 |
| time-range | Time range of the packet filtering |
| *time-range-name* | Time range name of the packet filtering |

**Defaults** No entry

**Command mode** ACL configuration mode.

**Usage Guide** Use this command to configure the filtering entry of ACLs in ACL configuration mode.

**Configuration Examples** The following example shows how to create and display an extended expert ACL. This expert ACL denies all the TCP packets with the source IP address 192.168.4.12 and the source MAC address 001300498272.

```
Ruijie(config)#expert access-list extended 2702
Ruijie(config-exp-nacl)#deny tcp  host
192.168.4.12 host 0013.0049.8272 any any
Ruijie(config-exp-nacl)#permit any any any any
Ruijie(config-exp-nacl)#show access-lists
expert access-list extended 2702
10 deny tcp  host  192.168.4.12 host 0013.0049.8272 any any
20 permit any any any any
Ruijie(config-exp-nacl)#
```

This example shows how to use the extended IP ACL. The purpose is to deny the host with the IP address 192.168.4.12 to provide services through the TCP port 100 and apply the ACL to Interface gigabitethernet 1/1. The configuration procedure is as below:

```
Ruijie(config)# ip access-list extended ip-ext-acl
Ruijie(config-ext-nacl)# deny tcp host 192.168.4.12 eq 100 any
Ruijie(config-ext-nacl)# show access-lists
```

```
ip access-list extended ip-ext-acl
10 deny tcp host 192.168.4.12 eq 100 any
Ruijie(config-ext-nacl)#exit
Ruijie(config)#interface gigabitethernet 1/1
Ruijie(config-if)#ip access-group ip-ext-acl in
Ruijie(config-if)#
```

This example shows how to use the extended MAC ACL. The purpose is to deny the host with the MAC address 0013.0049.8272 to send Ethernet frames of the type 100 and apply the rule to Interface gigabitethernet 1/1. The configuration procedure is as below:

```
Ruijie(config)#mac access-list extended mac1
Ruijie(config-mac-nacl)#deny host 0013.0049.8272 any aarp
Ruijie(config-mac-nacl)# show access-lists
mac access-list extended mac1
10 deny host 0013.0049.8272 any aarp
Ruijie(config-mac-nacl)#exit
Ruijie(config)# interface gigabitethernet 1/1
Ruijie(config-if)# mac access-group mac1 in
```

This example shows how to use the standard IP ACL. The purpose is to deny the host with the IP address 192.168.4.12 and apply the rule to Interface gigabitethernet 1/1. The configuration procedure is as below:

```
Ruijie(config)#ip access-list standard 34
Ruijie(config-ext-nacl)# deny host 192.168.4.12
Ruijie(config-ext-nacl)#show access-lists
ip access-list standard 34
10 deny host 192.168.4.12
Ruijie(config-ext-nacl)#exit
Ruijie(config)# interface gigabitethernet 1/1
Ruijie(config-if)# ip access-group 34 in
```

This example shows how to use the extended IPV6 ACL. The purpose is to deny the host with the IP address 192.168.4.12 and apply the rule to Interface gigabitethernet 1/1. The configuration procedure is as below:

```
Ruijie(config)#ipv6 access-list extended v6-acl
Ruijie(config-ipv6-nacl)#11 deny ipv6 host 192.168.4.12 any
Ruijie(config-ipv6-nacl)#show access-lists
ipv6 access-list extended v6-acl
11 deny ipv6 host 192.168.4.12 any
Ruijie(config-ipv6-nacl)# exit
Ruijie(config)# interface gigabitethernet 1/1
Ruijie(config-if)# ipv6 traffic-filter v6-acl in
```

**Related Commands**

| Command | Description |
|---|---|
| show access-lists | Displays all ACLs. |
| ipv6 traffic-filter | Applies the extended IPv6 ACL on the |

| | |
|---|---|
| | interface. |
| ip access-group | Applies the IP ACL on the interface. |
| mac access-group | Applies the extended MAC ACL on the interface. |
| ip access-list | Defines an IP ACL. |
| mac access-list | Defines an extended MAC ACL. |
| expert access-list | Defines an extended expert ACL. |
| ipv6 access-list | Defines an extended IPv6 ACL. |
| permit | Permits the access. |

**Platform Description** N/A

## 12.6 expert access-group

Use this command to apply the specified expert access list on the specified interface to control the input and output data streams. Use the **no** form of the command to remove the application.

**expert access-group** { *id* | *name* } { **in** | **out** }

**no expert access-group** { *id* | *name* } { **in** | **out** }

**Parameter Description**

| Parameter | Description |
|---|---|
| *id* | Expert access list number: 2700 to 2899 |
| *name* | Name of the expert access list |
| in | Specifies filtering on inbound packets. |
| out | Specifies filtering on outbound packets. |

**Defaults** No expert access list is applied.

**Command mode** Interface configuration mode.

**Usage Guide** N/A

**Configuration Examples** The following example applies the expert ACL named **accept_00d0f8xxxxxx_only** to Gigabit interface 0/1:

```
Ruijie(config)# interface GigaEthernet 0/1
Ruijie(config-if-GigabitEthernet 0/1)# expert access-group accept_00d0f8xxxxxx_only in
```

**Related Commands**

| Command | Description |
|---|---|
| **show access-group** | Displays the ACL configuration. |

**Platform Description** N/A

## 12.7 expert access-list extended

Use this command to create an extended expert access list. Use the **no** form of the command to remove the ACL.

**expert access-list extended** {*id* | *name*}

**no expert access-list extended** {*id* | *name*}

**Parameter Description**

| Parameter | Description |
|---|---|
| *id* | Extended expert access list number: 2700 to 2899 |
| *name* | Name of the extended expert access list |

**Defaults** N/A

**Command mode** Global configuration mode.

**Usage Guide** Use the **show access-lists** command to display the ACL configurations**.**

**Configuration Examples** Create an extended expert ACL named exp-acl:

```
Ruijie(config)# expert access-list extended exp-acl
Ruijie(config-exp-nacl)#  show  access-lists  expert  access-list  extended
exp-acl
Ruijie(config-exp-nacl)#
```

Create an extended expert ACL numbered 2704:

```
Ruijie(config)# expert access-list extended 2704
Ruijie(config-exp-nacl)# show access-lists  access-list extended 2704
Ruijie(config-exp-nacl)#
```

**Related Commands**

| Command | Description |
|---|---|
| **show access-lists** | Displays the extended expert ACLs |

**Platform Description** N/A

## 12.8 expert access-list resequence

Use this command to resequence an expert access list. Use the no form of this command to restore the default order of access entries.

**expert access-list resequence** { *id* | *name* } *start-sn inc-sn*

**no expert access-list resequence** { *id* | *name* }

**Parameter Description**

| Parameter | Description |
|---|---|
| *Id* | Expert access list number: 2700 to 2899. |
| *name* | Name of the expert access list |
| *start-sn* | Start sequence number. Range: 1 to 2147483647 |
| *inc-sn* | Increment of the sequence number. Range: 1 to 2147483647 |

**Defaults**

*start-sn*: 10

*inc-sn*: 10

**Command mode**

Global configuration mode

**Usage Guide**

Use this command to change the order of the access entries.

**Configuration Examples**

The following example resequences entries of expert access list “exp-acl”:

Before the configuration:

```
Ruijie# show access-lists
expert access-list extended exp-acl
 10 permit ip any any any any
 20 deny ip any any any any
```

After the configuration:

```
Ruijie# config
Ruijie(config)# expert access-list resequence exp-acl 21 43
Ruijie(config)# exit
Ruijie# show access-lists
expert access-list extended exp-acl
 21 permit ip any any any any
 64 deny ip any any any any
```

**Related Commands**

| Command | Description |
|---|---|
| show access-lists | Displays all access lists.. |

**Platform**

N/A

**Description**

## 12.9 ip access-group

Use this command to apply a specific access list globally or to an interface or VXLAN. Use the **no** form of this command to remove the access list from the interface.

**ip access-group** {*id* | *name*} {**in** | **out**}

**no ip access-group** { *id* | *name*} {**in** | **out**}

**Parameter Description**

| Parameter | Description |
|---|---|
| *id* | IP access list or extended IP access list number:<br>1 to 199, 1300 to 2699 |
| *name* | Name of the IP ACL |
| **in** | Filters the incoming packets of the interface. |
| **out** | Filters the outgoing packets of the interface. |

**Defaults** No access list is applied by default.

**Command mode** interface configuration mode.

**Usage Guide** Use this command to control access to a specified interface, VXLAN or globally.

**Configuration Examples** The following example applies the ACL 120 on interface fastEthernet0/0 to filter the incoming packets:

```
Ruijie(config)# interface fastEthernet 0/0
Ruijie(config-if)# ip access-group 120 in
```

**Related Commands**

| Command | Description |
|---|---|
| **access-list** | Defines an ACL. |
| **show access-lists** | Displays all ACLs. |

**Platform Description** N/A

## 12.10 ip access-list

Use this command to create a standard IP access list or extended IP access list. Use the **no** form of the command to remove the access list.

**ip access-list** {**extended** | **standard**} {*id* | *name*}

**no ip access-list** {**extended** | **standard**} {*id* | *name*}

**Parameter Description**

| Parameter | Description |
|---|---|
| *id* | Access list number:<br>Standard: 1 to 99, 1300 to 1999;<br>Extended: 100 to 199, 2000 to 2699. |
| *name* | Name of the access list |

**Defaults** N/A

**Command mode** Global configuration mode

**Usage Guide** Configure a standard access list if you need to filter on source address only. If you want to filter on anything other than source address, you need to create an extended access list.
Refer to **deny** or **permit** in the two modes. Use the **show access-lists** command to display the ACL configurations**.**

**Configuration Examples** The following example creates a standard access list named std-acl.

```
Ruijie(config)# ip access-list standard std-acl
Ruijie(config-std-nacl)# show access-lists
ip access-list standard std-acl
Ruijie(config-std-nacl)#
```

The following example creates an extended ACL numbered 123:

```
Ruijie(config)# ip access-list extended 123
Ruijie(config-ext-nacl)# show access-lists
ip access-list extended 123
```

**Related Commands**

| Command | Description |
|---|---|
| show access-lists | Displays all ACLs. |

**Platform Description** N/A

## 12.11 ip access-list resequence

Use this command to resequence a standard or extended IP access list. Use the **no** form of this command to restore the default order of access entries.
**ip access-list resequence** { *id* | *name* } *start-sn inc-sn*
**no ip access-list resequence** { *id* | *name* }

**Parameter Description**

| Parameter | Description |
|---|---|
| *id* | IP access list number:<br>Standard IP access list: 1 to 99, 1300 to 1999;<br>Extended IP access list: 100 to 199, 2000 to 2699. |
| *name* | Name of the standard or extended IP access list |
| *start-sn* | Start sequence number. Range: 1 to 2147483647 |
| *inc-sn* | Increment of the sequence number. Range: 1 to 2147483647 |

**Defaults** *start-sn*: 10
*inc-sn*: 10

**Command mode** Global configuration mode

**Usage Guide** Use this command to change the order of the access entries.

**Configuration Examples** The following example resequences entries of ACL1:
Before the configuration:

```
Ruijie# show access-lists
ip access-list standard 1
10 permit host 192.168.4.12
20 deny any any
```

After the configuration:

```
Ruijie# config
Ruijie(config)# ip access-list resequence 1 21 43
Ruijie(config)# exit
Ruijie# show access-lists
ip access-list standard 1
21 permit host 192.168.4.12
64 deny any any
```

**Related Commands**

| Command | Description |
|---|---|
| show access-lists | Displays all access lists.. |

**Platform Description** N/A

## 12.12 ipv6 access-list

Use this command to create an IPv6 access list and to place the device in IPv6 access list

configuration mode. Use the **no** form of this command to remove the access list.

**ipv6 access-list** *name*

**no ipv6 access-list** *name*

**Parameter Description**

| Parameter | Description |
|---|---|
| *name* | Name of the IPv6 access list. |

**Defaults** N/A

**Command mode** Global configuration mode

**Usage Guide** To filter the IPv6 packets through the access list, you need to define an IPv6 access list by using the **ipv6 access-list** command.

**Configuration Examples** The following example creates an IPv6 access list named v6-acl:

```
Ruijie(config)# ipv6 access-list v6-acl
Ruijie(config-ipv6-nacl)# show access-lists
ipv6 access-list extended v6-acl
Ruijie(config-ipv6-nacl)#
```

**Related Commands**

| Command | Description |
|---|---|
| show access-lists | Displays all access lists. |

**Platform Description** N/A

## 12.13 ipv6 access-list resequence

Use this command to resequence an IPv6 access list. Use the **no** form of this command to restore the default order of access entries.

**ipv6 access-list resequence** *name start-sn inc-sn*

**no ipv6 access-list resequence** *name*

**Parameter Description**

| Parameter | Description |
|---|---|
| *name* | Name of the IPv6 access list |
| *start-sn* | Start sequence number. Range: 1 to 2147483647 |
| *inc-sn* | Increment of the sequence number. Range: 1 to 2147483647 |

**Defaults** *start-sn*: 10

*inc-sn*: 10

**Command mode** Global configuration mode

**Usage Guide** Use this command to change the order of the access entries.

**Configuration Examples** The following example resequences entries of IPv6 access list “v6-acl”:

Before the configuration:

```
Ruijie# show access-lists
ipv6 access-list v6-acl
 10 permit ipv6 any any
 20 deny ipv6 any any
```

After the configuration:

```
Ruijie# config
Ruijie(config)# ipv6 access-list resequence v6-acl 21 43
Ruijie(config)# exit
Ruijie# show access-lists
ipv6 access-list v6-acl
 21 permit ipv6 any any
 64 deny ipv6 any any
```

**Related Commands**

| Command | Description |
|---|---|
| show access-lists | Displays all access lists.. |

**Platform Description** N/A

## 12.14 ipv6 traffic-filter

Use this command to apply an IPV6 access list on the specified interface/VXLAN. Use the **no** form of the command to remove the IPv6 access list from the interface/VXLAN.

**ipv6 traffic-filter** *name* { **in** | **out** }

**no ipv6 traffic-filter** *name* { **in** | **out** }

**Parameter Description**

| Parameter | Description |
|---|---|
| *name* | Name of IPv6 access list |
| **in** | Specifies filtering on inbound packets |
| **out** | Specifies filtering on outbound packets |

**Defaults** N/A

**Command mode** Interface configuration mode.

**Usage Guide** Use this command to apply the IPv6 access list to a specified interface/VXLAN to filter the inbound or outbound packets.

**Configuration Examples** The following example applies the IPv6 access list named **v6-acl** to interface GigabitEthernet 0/1:

```
Ruijie(config)# interface GigaEthernet 0/1
Ruijie(config-if-GigabitEthernet 0/1)# ipv6 traffic-filter v6-acl in
```

**Related Commands**

| Command | Description |
|---|---|
| show access-group | Displays ACL configurations on the interface. |

**Platform Description** N/A

## 12.15 list-remark

Use this command to write a helpful comment (remark) for an access list. Use the **no** form of this command to remove the remark.

**list-remark** *text*

**no list-remark**

**Parameter Description**

| Parameter | Description |
|---|---|
| *text* | Comment that describes the access list. |

**Defaults** The access lists have no remarks by default.

**Command mode** ACL configuration mode

**Usage Guide** You can use this command to write a helpful comment for a specified access list.

**Configuration Examples** The following example writes a comment of “this acl is to filter the host 192.168.4.12” for ACL102.

```
Ruijie(config)# ip access-list extended 102
Ruijie(config-ext-nacl)# list-remark this acl is to filter the host
192.168.4.12
Ruijie(config-ext-nacl)# show access-lists
ip access-list extended 102
deny ip host 192.168.4.12 any
```

```
1000 hits
this acl is to filter the host 192.168.4.12
Ruijie(config-ext-nacl)#
```

**Related Commands**

| Command | Description |
|---|---|
| show access-lists | Displays all access lists. |
| ip access-list | Defines an IPv4 access list. |
| access-list list remark | Adds a helpful comment for an access list in global configuration mode. |
| | |

**Platform Description** N/A

## 12.16 mac access-group

Use this command to apply the specified MAC access list on the specified interface. Use the **no** form of the command to remove the access list from the interface.

**mac access-group** { *id* | *name* } { **in** | **out** }

**no mac access-group** { *id* | *name* } { **in** | **out** }

**Parameter Description**

| Parameter | Description |
|---|---|
| *id* | MAC access list number. The range is from 700 to 799. |
| *name* | Name of the MAC access list |
| in | Specifies filtering on the inbound packets. |
| out | Specifies filtering on the outbound packets. |

**Defaults** No MAC access list is applied by default.

**Command mode** interface configuration mode.

**Usage Guide** Use this command to apply the access list to filter the inbound or outbound packets based on the MAC address.

**Configuration Examples** The following example applies the MAC access-list **accept_00d0f8xxxxxx_only** to interface GigabitEthernet 1/1:

```
Ruijie(config)# interface GigaEthernet 1/1
Ruijie(config-if-GigabitEthernet 1/1)# mac access-group
accept_00d0f8xxxxxx_only in
```

**Related**

| Command | Description |
|---|---|

**Commands**

| | |
|---|---|
| **show access-group** | Displays the ACL configuration on the interface. |

**Platform Description** N/A

## 12.17 mac access-list extended

Use this command to create an extended MAC access list. Use the **no** form of the command to remove the MAC access list.

**mac access-list extended** { *id* | *name* }

**no mac access-list extended** { *id* | *name* }

**Parameter Description**

| Parameter | Description |
|---|---|
| *id* | Extended MAC access list number. The range is from 700 to 799. |
| *name* | Name of the extended MAC access list |

**Defaults** N/A

**Command mode** Global configuration mode.

**Usage Guide** To filter the packets based on the MAC address, you need to define a MAC access list by using the **mac access-list extended** command.

**Configuration Examples** The following command creates an extended MAC access list named mac-acl:

```
Ruijie(config)# mac access-list extended mac-acl
Ruijie(config-mac-nacl)# show access-lists mac access-list extended mac-acl
```

The following command creates an extended MAC access list numbered 704:

```
Ruijie(config)# mac access-list extended 704
Ruijie(config-mac-nacl)# show access-lists mac access-list extended 704
```

**Related Commands**

| Command | Description |
|---|---|
| show access-lists | Displays all access lists. |

**Platform Description** N/A

## 12.18 mac access-list resequence

Use this command to resequence an extended MAC access list. Use the **no** form of this command to restore the default order of access entries.

**mac access-list resequence** { *id* | *name* } *start-sn inc-sn*

**no mac access-list resequence** { *id* | *name* }

**Parameter Description**

| Parameter | Description |
|---|---|
| *id* | Extended MAC access list number: 700 to 799. |
| *name* | Name of the extended MAC access list |
| *start-sn* | Start sequence number. Range: 1 to 2147483647 |
| *inc-sn* | Increment of the sequence number. Range: 1 to 2147483647 |

**Defaults**

*start-sn*: 10

*inc-sn*: 10

**Command mode**

Global configuration mode

**Usage Guide**

Use this command to change the order of the access entries.

**Configuration Examples**

The following example resequences entries of extended MAC access list “mac-acl”:

Before the configuration:

```
Ruijie# show access-lists
mac access-list extended mac-acl
 10 permit any any etype-any
 20 deny any any etype-any
```

After the configuration:

```
Ruijie# config
Ruijie(config)# mac access-list resequence exp-acl 21 43
Ruijie(config)# exit
Ruijie# show access-lists
mac access-list extended mac-acl
 21 permit any any etype-any
 64 deny any any etype-any
```

**Related Commands**

| Command | Description |
|---|---|
| show access-lists | Displays all access lists.. |

**Platform**

N/A

**Description**

## 12.19 permit

One or multiple **permit** conditions are used to determine whether to forward or discard the packet. In ACL configuration mode, you can modify the existent ACL or configure according to the protocol details.

9. Standard IP ACL

[ *sn* ] **permit** {*source source-wildcard* | **host** *source* | **any | interface** *idx* } [ **time-range** *tm-range-name*] [ **log** ]

10. Extended IP ACL

[ *sn* ] **permit protocol** *source source-wildcard destination destination-wildcard* [ **precedence** *precedence* ] [ **tos** *tos* ] [ **fragment** ] [ **range** *lower upper* ] [ **time-range** *time-range-name* ] [ **log** ]

Extended IP ACLs of some important protocols:

Internet Control Message Protocol (ICMP)

[ *sn* ] **permit icmp** {*source source-wildcard* | **host** *source* | **any** } { *destination destination-wildcard* | **host** *destination* | **any** } [ *icmp-type* ] [ [ *icmp-type* [*icmp-code* ] ] | [ *icmp-message* ] ] [ **precedence** *precedence* ] [ **tos** *tos* ] [ **fragment** ] [ **time-range** *time-range-name* ]

Transmission Control Protocol (TCP)

[ *sn* ] **permit tcp** { *source source-wildcard* | **host** *source* | **any** } [ *operator* **port** [ *port* ] ] { *destination destination-wildcard* | **host** *destination* | **any** } [ *operator* **port** [ *port* ] ] [ **precedence** *precedence* ] [ **tos** *tos* ] [ **fragment** ] [ **range** *lower upper* ] [ **time-range** *time-range-name* ] [ **match-all** *tcp-flag* | **established** ]

User Datagram Protocol (UDP)

[*sn*] **permit udp** {*source source -wildcard*|**host** *source* |**any**} [ *operator* **port** [*port*]] {*destination destination-wildcard* |**host** *destination* | **any**} [**operator port** [*port*]] [**precedence** *precedence*] [**tos** *tos*] [**fragment**] [**range** *lower upper*] [**time-range** *time-range-name*]

11. Extended MAC ACL

[*sn*] **permit** { **any** | **host** *source-mac-address* { **any** | **host** *destination-mac-address* } [ *ethernet-type* ] [ **cos** [ *out* ] [ **inner** *in* ] ]

12. Extended expert ACL

[*sn*] **permit** [**protocol** | [*ethernet-type*][ **cos** [*out*] [**inner** *in*]]] [**VID** [*out*]*[***inner** *in]*] {*source source-wildcard* | **host** *source* | **any**} {**host** *source*-mac-*address* | **any** } {*destination destination-wildcard* | **host** *destination* | **any**} {**host** *destination-mac-address* | **any**} [**precedence** *precedence*] [**tos** *tos*][**fragment**] [**range** *lower upper*] [**time-range** *time-range-name*]

When you select the Ethernet-type field or cos field:

[*sn*] **permit** {*ethernet-type*| **cos** [*out*] [**inner** *in*]} [**VID** [*out*][**inner** *in*]] {*source source-wildcard* | **host** *source* | **any**} {**host** *source-mac-address* | **any** } {*destination destination-wildcard* | **host** *destination* | **any**} {**host** *destination-mac-address* | **any**} [**time-range** *time-range-name*]

When you select the protocol field:

[*sn*] **permit protocol** [**VID** [*out]*[**inner** *in*]] {*source source-wildcard* | **host** *Source* | **any**} {**host**

*source-mac-address* | **any** } {*destination destination-wildcard* | **host** *destination* | **any**} {**host** *destination-mac-address* | **any**} [**precedence** *precedence*] [**tos** *tos*] [**fragment**] [**range** *lower upper*] [**time-range** *time-range-name*]

Extended expert ACLs of some important protocols:

Internet Control Message Protocol (ICMP)

[*sn*] **permit icmp** [**VID** [*out*][**inner** *in*]] {*source source-wildcard* | **host** *source* | **any**} {**host** *source-mac-address* | **any** } {*destination destination-wildcard* | **host** *destination* | **any**} {**host** *destination-mac-address* | **any**}[ *icmp-type* ] [[*icmp-type* [*icmp-code* ]] | [ *icmp-message* ]] [**precedence** *precedence*] [**tos** *tos*] [**fragment**] [**time-range** *time-range-name*]

Transmission Control Protocol (TCP)

[*sn*] **permit tcp** [**VID** [*out*][**inner** *in*]]{*source source-wildcard* | **host** *Source* | **any**} {**host** *source-mac-address* | **any** } [*operator* **port** [*port*]] {*destination destination-wildcard* | **host** *destination* | **any**} {**host** *destination-mac-address* | **any**} [*operator* **port** [*port*]] [**precedence** *precedence*] [**tos** *tos*] [**fragment**] [**range** *lower upper*] [**time-range** *time-range-name*] [**match-all** *tcp-flag* | **established**]

User Datagram Protocol (UDP)

[*sn*] **permit udp** [**VID** [*out*][**inner** *in*]]{*source source –wildcard* | **host** *source* | **any**} {**host** *source-mac-address* | **any** } [ *operator* **port** [*port*]] {*destination destination-wildcard* | **host** *destination* | **any**} {**host** *destination-mac-address* | **any**} [*operator* **port** [*port*]] [**precedence** *precedence*] [**tos** *tos*] [**fragment**] [**range** *lower upper*] [**time-range** *time-range-name*]

Address Resolution Protocol (ARP)

[*sn*] **permit arp** {**vid** *vlan-id***}** [**host** *source-mac-address* | **any**] [**host** *destination –mac-address* | **any**] {*sender-ip sender-ip–wildcard* | **host** *sender-ip* | **any**} {*sender-mac sender-mac-wildcard* | **host** *sender-mac* | **any**} {*target-ip target-ip–wildcard* | **host** *target-ip* | **any**}

13. Extended IPv6 ACL

[*sn*] **permit protocol** {*source-ipv6-prefix / prefix-length* | **any** | **host** *source-ipv6-address*} {*destination-ipv6-prefix / prefix-length* | **any**| *hostdestination-ipv6-address*} [**dscp** *dscp*] [**flow-label** *flow-label*] [**fragment**] [**range** *lower upper*] [**time-range** *time-range-name*]

Extended IPv6 ACLs of some important protocols:

Internet Control Message Protocol (ICMP)

[*sn*] **permit icmp** {*source-ipv6-prefix / prefix-length* | **any** *source-ipv6-address* | **host**} {*destination-ipv6-prefix / prefix-length*| **host** *destination-ipv6-address* | **any**} [*icmp-type*] [[*icmp-type* [*icmp-code*]] | [*icmp-message*]] [**dscp** *dscp*] [**flow-label** *flow-label*][**fragment**] [**time-range** *time-range-name*]

Transmission Control Protocol (TCP)

[*sn*] **permit tcp** {*source-ipv6-prefix / prefix-length* | **host** *source-ipv6-address* | **any**} [*operator* **port** [*port*] ] {*destination-ipv6-prefix / prefix-length* | **host** *destination-ipv6-address* | **any**} [*operator* **port** [*port*]] [**dscp** *dscp*] [**flow-label** *flow-label*] [**fragment**] [**range** *lower upper*] [**time-range** *time-range-name*] [**match-all** *tcp-flag* | **established**]

User Datagram Protocol (UDP)

[*sn*] **permit udp** {*source-ipv6-prefix / prefix-length* | **host** *source-ipv6-address* | **any**} [*operator* **port** [*port*] ] {*destination-ipv6-prefix / prefix-length* | **host** *destination-ipv6-address* | **any**} [*operator* **port** [*port*]] [**dscp** *dscp*] [**flow-label** *flow-label*] [**fragment**] [**range** *lower upper*] [**time-range** *time-range-name*]

**Parameter Description**

| Parameter | Description |
| --- | --- |
| N/A | N/A |

**Defaults** N/A

**Command mode** ACL configuration mode.

**Usage Guide** Use this command to configure the **permit** conditions for the ACL in ACL configuration mode.

**Configuration Examples** The following example shows how to create and display an Expert Extended ACL. This expert ACL permits all the TCP packets with the source IP address 192.168.4.12 and the source MAC address 001300498272.

```
Ruijie(config)#expert access-list extended exp-acl
Ruijie(config-exp-nacl)#permit tcp  host  192.168.4.12 host 0013.0049.8272
any any
Ruijie(config-exp-nacl)#deny any any any any
Ruijie(config-exp-nacl)#show access-lists
expert access-list extended exp-acl
10 permit tcp  host  192.168.4.12 host 0013.0049.8272 any any
20 deny any any any any
Ruijie(config-exp-nacl)#
```

This example shows how to use the extended IP ACL. The purpose is to permit the host with the IP address 192.168.4.12 to provide services through the TCP port 100 and apply the ACL to interface gigabitethernet 1/1. The configuration procedure is as below:

```
Ruijie(config)# ip access-list extended 102
Ruijie(config-ext-nacl)# permit tcp host 192.168.4.12 eq 100 any
Ruijie(config-ext-nacl)# show access-lists
ip access-list extended 102
10 permit tcp host 192.168.4.12 eq 100 any
Ruijie(config-ext-nacl)#exit
Ruijie(config)#interface gigabitethernet 1/1
Ruijie(config-if)#ip access-group 102 in
Ruijie(config-if)#
```

This example shows how to use the extended MAC ACL. The purpose is to permit the host with the MAC address 0013.0049.8272 to send Ethernet frames through the type 100 and apply the ACL to interface gigabitethernet 1/1. The configuration procedure is as below:

```
Ruijie(config)#mac access-list extended 702
Ruijie(config-mac-nacl)#permit host 0013.0049.8272 any aarp
Ruijie(config-mac-nacl)#show access-lists
mac access-list extended 702
10 permit host 0013.0049.8272 any aarp 702
```

```
Ruijie(config-mac-nacl)#exit
Ruijie(config)#interface gigabitethernet 1/1
Ruijie(config-if)#mac access-group 702 in
```

This example shows how to use the standard IP ACL. The purpose is to permit the host with the IP address 192.168.4.12 and apply the ACL to interface gigabitethernet 1/1. The configuration procedure is as below:

```
Ruijie(config)#ip access-list standard std-acl
Ruijie(config-std-nacl)#permit host 192.168.4.12
Ruijie(config-std-nacl)#show access-lists
ip access-list standard std-acl
  10 permit host 192.168.4.12
Ruijie(config-std-nacl)#exit
Ruijie(config)# interface gigabitethernet 1/1
Ruijie(config-if)# ip access-group std-acl in
```

This example shows how to use the extended IPV6 ACL. The purpose is to permit the host with the IP address 192.168.4.12 and apply the ACL to interface gigabitethernet 1/1. The configuration procedure is as below:

```
Ruijie(config)#ipv6 access-list extended v6-acl
Ruijie(config-ipv6-nacl)#11 permit ipv6 host ::192.168.4.12 any
Ruijie(config-ipv6-nacl)# show access-lists
ipv6 access-list extended v6-acl
11 permit ipv6 host ::192.168.4.12 any
Ruijie(config-ipv6-nacl)# exit
Ruijie(config)#interface gigabitethernet 1/1
Ruijie(config-if)#ipv6 traffic-filter v6-acl in
```

**Related Commands**

| Command | Description |
|---|---|
| show access-lists | Displays all access lists. |
| ipv6 traffic-filter | Applies the extended IPv6 access list to the interface. |
| ip access-group | Applies the IP access list to the interface. |
| mac access-group | Applies the extended MAC access list to the interface. |
| ip access-list | Defines an IP access list. |
| mac access-list | Defines an extended MAC access list. |
| expert access-list | Define an extended expert access list. |
| ipv6 access-list | Defines an extended IPv6 access list. |
| deny | Defines the **deny** access entry. |

**Platform Description** N/A

## 12.20 remark

Use this command to write a helpful comment (remark) for an entry in the access list. Use the **no** form of this command to remove the remark.

**remark** *text*

**no remark**

**Parameter Description**

| Parameter | Description |
|---|---|
| *text* | Comment that describes the access entry. |

**Defaults** The access entries have no remarks.

**Command mode** ACL configuration mode.

**Usage Guide** Use this command to write a helpful comment for an access entry.
Up to 100 characters are allowed in the remark.
Two identical access entry remarks in one access list is not allowed.
Removing an access entry may delete the remark for it as well.

**Configuration Examples** The following example writes remarks for the entry in extended IP access list 102.

```
Ruijie(config)# ip access-list extended 102
Ruijie(config-ext-nacl)# remark first_remark
Ruijie(config-ext-nacl)# permit tcp 1.1.1.1 0.0.0.0 2.2.2.2 0.0.0.0
Ruijie(config-ext-nacl)# remark second_remark
Ruijie(config-ext-nacl)# permit tcp 3.3.3.3 0.0.0.0 4.4.4.4 0.0.0.0
Ruijie(config-ext-nacl)# end
Ruijie#
```

**Related Commands**

| Command | Description |
|---|---|
| show access-lists | Displays all access lists. |
| ip access-list | Defines an IP access list. |

**Platform Description** N/A

## 12.21 security access-group

Use this command to configure an interface secure channel. Use the **no** form of this command to remove the channel.

**security access-group** { *id* | *name* }

**no security access-group**

**Parameter Description**

| Parameter | Description |
|---|---|
| *id* | Access list number. |
| *name* | Name of the access list. |

**Defaults** N/A

**Command mode** Interface configuration mode

**Usage Guide** If a device is configured authentications such as 802.1x or Web authentication, the user cannot access the external network before passing the authentication. You can use this command to configure a secure channel for the users on the specified interface to access the external network without authentication.

**Configuration Examples** The following example configures a secure channel on interface GigaEthernet 1/1:

```
Ruijie(config)# interface GigaEthernet 1/1
Ruijie(config-if-GigabitEthernet 1/1)# security access-group 1
```

**Related Commands**

| Command | Description |
|---|---|
| show secu-acl | Displays the secure channel configuration. |

**Platform Description** N/A

## 12.22 security global access-group

Use this command to configure the global secure channel.

**security global access-group** { *id* | *name* }

**no security global access-group**

**Parameter Description**

| Parameter | Description |
|---|---|
| *id* | Access list number. |
| *name* | Name of the access list. |

**Defaults** -

**Command mode** Global configuration mode

**Usage Guide** If a device is configured authentications such as 802.1x or Web authentication, the user cannot access the external network before passing the authentication. You can use this command to configure a global secure channel for some users to access the external network without authentication.

**Configuration Examples**

```
The following example configures a global secure channel.
Ruijie(config)#security global access-group 1
```

**Related Commands**

| Command | Description |
|---|---|
| show secu-acl | Displays the secure channel configuration.. |

**Platform Description** N/A

## 12.23 security uplink enable

Use this command to configure an exceptional interface of the global secure channel.
**security uplink enable**
**no security uplink enable**

**Parameter Description**

| Parameter | Description |
|---|---|
| N/A | N/A |

**Defaults** The global secure channel takes effect on all interfaces by default.

**Command mode** Interface configuration mode.

**Usage Guide** The global secure channel takes effect on all interfaces by default. To disable the secure channel function on some interfaces, you can used this command to configure the interface as exceptional.

**Configuration Examples** The following example configures interface GigaEthernet 1/1 as an exceptional interface of the secure channel.

```
Ruijie(config)# interface GigaEthernet 1/1
Ruijie(config-if-GigabitEthernet 1/1)# security uplink enable
```

**Related Commands**

| Command | Description |
|---|---|
| show secu-acl | Displays the secure channel configuration. |

**Platform Description** N/A

## 12.24 show access-group

Use this command to display the access list applied to the interface.

**show access-group** [ **interface** *interface-name* ]

**Parameter Description**

| Parameter | Description |
|---|---|
| *interface* | Interface name |

**Defaults** -

**Command mode** Privileged EXEC mode

**Usage Guide** Use this command to display the access list configuration on the specified interface. If no interface is specified, access list configuration on all interfaces is displayed.

**Configuration Examples** The following example displays the interfaces where the ACL is applied.

```
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.
ip access-group 33 in
Applied On vxlan 1
```

The following example displays whether ACL is applied on the interface GigabitEthernet 0/3 and which direction data streams flow to.

```
Ruijie# show access-group interface GigabitEthernet 0/3
ip access-list extended 101
Applied On interface GigabitEthernet 0/3 in.
```

**Related Commands**

| Command | Description |
|---|---|
| ip access-group | Applies the IP access list to the interface. |
| mac access-group | Applies the MAC access list to the interface. |

| | |
|---|---|
| expert access-group | Applies the expert access list to the interface. |
| ipv6 traffic-filter | Applies the IPv6 access list to the interface. |

**Platform Description** N/A

## 12.25 show access-lists

Use this command to display all access lists or the specified access list.

**show access-lists** [ *id* | *name* ] [ **summary** ]

**Parameter Description**

| Parameter | Description |
|---|---|
| *id* | Access list number |
| *name* | Name of the IP access list |
| summary | Access list summary |

**Defaults** N/A

**Command mode** Global configuration mode

**Usage Guide** Use this command to display the specified access list. If no access list number or name is specified, all the access lists are displayed.

**Configuration Examples** The following example displays configuration of the ACL named “n_acl”.

```
Ruijie# show access-lists n_acl
ip access-list standard n_acl
Ruijie# show access-lists 102
ip access-list extended 102
```

The following example displays configuration of all ACLs.

```
Ruijie# show access-lists
ip access-list standard n_acl
ip access-list extended 101
permit icmp host 192.168.1.1 any log (1080 matches)
  permit tcp host 1.1.1.1 any established
  deny ip any any (80021 matches)
mac access-list extended mac-acl
expert access-list extended exp-acl
ipv6 access-list extended v6-acl
petmit ipv6 ::192.168.4.12 any (100 matches)
deny any any (9 matches)
```

**Related Commands**

| Command | Description |
|---|---|
| ip access-list | Defines an IP access list. |
| mac access-list | Defines an extended MAC access list. |
| expert access-list | Defines an extended expert access list. |
| ipv6 access-list | Defines an extended IPv6 access list. |

**Platform Description** N/A

## 12.26 show expert access-group

Use this command to display the expert access list applied to the interface.

**show expert access-group** [ **interface** *interface-name* ] ]

**Parameter Description**

| Parameter | Description |
|---|---|
| *Interface-name* | Interface name |

**Defaults** -

**Command mode** Privileged EXEC mode

**Usage Guide** Use this command to display the expert access list configured on the interface. If no interface is specified, the expert access lists on all interfaces are displayed.

**Configuration Examples**

```
Ruijie# show expert access-group interface gigabitethernet 0/2
expert access-group ee in
Applied On interface GigabitEthernet 0/2.
```

**Related Commands**

| Command | Description |
|---|---|
| expert access-list | Defines an extended expert access list. |

**Platform Description** N/A

## 12.27 show ip access-group

Use this command to display the standard and extended IP access lists on the interface.

**show ip access-group** [ **interface** *interface-name* ]

**Parameter Description**

| Parameter | Description |
| --- | --- |
| *Interface-name* | Interface name |

**Defaults** N/A

**Command mode** Privileged EXEC mode

**Usage Guide** Use this command to display the standard and extended IP access lists configured on the interface. If no interface is specified, the standard and extended IP access lists on all interfaces are displayed.

**Configuration Examples** The following example displays whether the standard or extended IP access list is applied on the interface GigabitEthernet 0/1 and which direction data streams flow to.

```
Ruijie# show ip access-group interface gigabitethernet 0/1
ip access-group aaa in
Applied On interface GigabitEthernet 0/1.
```

**Related Commands**

| Command | Description |
| --- | --- |
| ip access-list | Defines an IP access list. |

**Platform Description** N/A

## 12.28 show ipv6 traffic-filter

Use this command to display the IPv6 access list on the interface.

**show ipv6 traffic-filter** [ **interface** *interface-name* ]

**Parameter Description**

| Parameter | Description |
| --- | --- |
| *Interface-name* | Interface name |

**Defaults** -

**Command mode** Privileged EXEC mode

**Usage Guide** Use this command to display the IPv6 access list configured on the interface. If no interface is specified, the IPv6 access lists on all interfaces are displayed.

**Configuration Examples** The following example displays whether IPv6 ACL is applied on the interface GigabitEthernet 0/1 and which direction data streams flow to.

```
Ruijie# show ipv6 traffic-filter interface gigabitethernet 0/4
ipv6 access-group v6 in
Applied On interface GigabitEthernet 0/4.
```

**Related Commands**

| Command | Description |
|---|---|
| ipv6 access-list | Defines an IPv6 access list. |

**Platform Description** N/A

## 12.29 show mac access-group

Use this command to display the MAC access list on the interface.

**show mac access-group** [ **interface** *interface-name* ]

**Parameter Description**

| Parameter | Description |
|---|---|
| *Interface-name* | Interface name |

**Defaults** N/A

**Command mode** Privileged EXEC mode

**Usage Guide** Use this command to display the MAC access list configured on the interface. If no interface is specified, the MAC access lists on all interfaces are displayed.

**Configuration Examples** The following example displays the MAC access list is applied on the interface and which direction data streams flow to.

```
Ruijie# show mac access-group interface gigabitethernet 0/3
mac access-group mm in
Applied On interface GigabitEthernet 0/3.
```

**Related Commands**

| Command | Description |
|---|---|
| mac access-list | Defines a MAC access list. |

**Platform Description** N/A

## 12.30 svi router-acls enable

Use this command to enable the SVI filter only for the Layer3 packets. Use the **no** form of this command to disable this function.

**svi router-acls enable**

**no svi router-acls enable**

**Parameter Description**

| Parameter | Description |
|---|---|
| N/A | N/A. |

**Defaults** The SVI filter takes effect for both Layer2 and Layer3 packets by default.

**Command mode** Global configuration mode

**Usage Guide** Use this command to make the SVI filter take effect only for the Layer3 packets,

**Configuration Examples** The following example enables the SVI filter only for the Layer3 packets.

```
Ruijie(config)#svi router-acls enable
```

**Related Commands**

| Command | Description |
|---|---|
| N/A | N/A |

**Platform Description** N/A

# 13 SCC Commands

## 13.1 Identifier Description

The following is a list of command identifiers used in commands for reference:

| Identifier | Description |
|---|---|
| vlanlist | Authentication-exemption VLAN list |
| interval | Authenticated-user online-status detection interval |
| thredshold | The traffic threshold of authenticated-user online-status detection |

## 13.2 downstream average-rate burst-rate

Use this command to configure the downstream traffic average and burst threshold.
**downstream average-rate** *avg-threshold* **burst-rate** *burst-threshold*

Use this command to remove the downstream traffic average and burst threshold.
**no downstream**

**Parameter Description**

| Parameter | Description |
|---|---|
| avg-threshold | Indicates the traffic average. |
| burst-threshold | Indicates the traffic burst threshold. |

**Defaults** N/A

**Command Mode** Speed-limit strategy configuration mode

**Default Level** 14

**Usage Guide** The burst thresholds of downstream parameters must not be smaller than the average.

**Configuration Examples** The following example configures the downstream traffic average and burst threshold.

```
Ruijie(config)# rate-policy user-rate
Ruijie (config-rate-policy)#downstream average-rate 10 burst-rate 10
```

**Verification** Use the **show running** command to display the speed-limit downstream policy rule.

**Prompt** N/A

**Messages**

**Common Errors** N/A

**Platforms**

## 13.3 filter-policy

Use this command to enter filtering policy configuration mode.
**filter-policy** *filter-name*

Use this command to configure in filtering policy configuration mode.
**filter-acl** { *acl-name* | *acl-id* }

**Parameter Description**

| Parameter | Description |
|---|---|
| filter-name | Indicates the name of a filtering policy. |
| acl-name | Indicates the name of the security ACL associated with the filtering policy. |
| acl-id | Indicates the ID of the security ACL associated with the filtering policy. |

**Defaults** N/A

**Command Mode** Global configuration mode

**Default Level** 14

**Usage Guide** One filtering policy can be deployed in different service strategies.

**Configuration Examples** The following example configures a filtering policies.

```
Ruijie(config)# ip access-list extended user_2000
Ruijie(config)# filter-policy user-filter
Ruijie(config-filter-policy)#filter-acl user_2000
```

**Verification** Use the **show running** command to display the filtering configuration policy.

**Prompt Messages** N/A

**Common Errors** N/A

**Platforms**

## 13.4 filter-policy apply

Use this command to configure the filtering policy to be used.
**filter-policy** *filter-name* **apply**

Use this command to enable the specified filtering policy.
**no filter-policy**

**Parameter Description**

| Parameter | Description |
|---|---|
| filter-name | Indicates the name of the filtering policy to be used. |

**Defaults**

**Command Mode** User policy configuration mode

**Default Level** 14

**Usage Guide** The name of the filtering policy to be used should be configured first.

**Configuration Examples** The following example configures a user policy and specifies the filtering policy name.

```
Ruijie(config)# ip access-list extended user_2000
Ruijie(config)# filter-policy user-filter
Ruijie(config-filter-policy)#filter-acl user_2000
Ruijie (config)# service-policy user-policy
Ruijie (config-service-policy)# filter-policy user-filter apply
```

**Verification** Use the **show running** command to display the filtering policy to be used.

**Prompt Messages** N/A

**Common Errors** N/A

**Platforms**

## 13.5 filter-acl

Use this command to configure the security ACL associated with the filtering policy.

**filter-acl** { *acl-name* | *acl-id* }

Use this command to remove the security ACL associated with the filtering policy.
**no filter-acl**

**Parameter Description**

| Parameter | Description |
|---|---|
| acl-name | Indicates the name of the security ACL associated with the filtering policy. |
| acl-id | Indicates the ID of the security ACL associated with the filtering policy. |

**Defaults** N/A

**Command Mode** Filtering policy configuration mode

**Default Level** 14

**Usage Guide** One filtering policy can be deployed in different service strategies.

**Configuration Examples** The following example configures a filtering policy.

```
Ruijie(config)# ip access-list extended user_2000
Ruijie(config)# filter-policy user-filter
Ruijie(config-filter-policy)#filter-acl user_2000
```

**Verification** Use the **show running** command to display the security ACL associated with the filtering policy.

**Prompt Messages** N/A

**Common Errors** N/A

**Platforms**

## 13.6 offline-detect interval threshold

Use this command to configure user online-status detection, so that a user is disconnected when its traffic is lower than a specified threshold or is zero in a specified interval.
**offline-detect interval** *interval* **threshold** *thredshold*

Use this command to restore the default user online-status detection configuration.
**default offline-detect**

Use this command to disable user online-status detection.
**no offline-detect**

**Parameter Description**

| Parameter | Description |
|---|---|
| *interval* | Indicates the interval of traffic detection (in minutes). The range is from 1 to 65,535 in minutes on a non-switch device or from 6 to 65,535 in minutes on a switch. |
| *threshold* | Indicates the traffic threshold (in bytes). The range is from 0 to 4,294,967,294 in bytes. The value of 0 indicates that the user is disconnected when no traffic of the user is detected. |

**Defaults** By default, the detection interval is 8 hours and the traffic threshold is 0.

**Command Mode** Global configuration mode

**Default Level** 14

**Usage Guide** You can use this command to configure user online-status detection to enable the device to disconnect the authenticated user whose traffic is lower than a specified value and end accounting process.

**Configuration Examples** The following example directly disconnects a user for the user's traffic is lower than 5 Kbytes within 5 minutes.

```
Ruijie(config)#offline-detect interval 5 threshold 5120
```

**Verification** Use the **show running** command to display the configuration of online-status detection for authenticated users.

**Prompt Messages** N/A

**Common Errors** N/A

**Platforms** N/A

## 13.7 rate-policy

Use this command to enter speed-limit policy configuration mode.
**show direct-vlan**

Use this command to configure the upstream traffic average and burst threshold.
**{downstream | upstream } average-rate** *avg-threshold* **burst-rate** *burst-threshold*

**Parameter Description**

| Parameter | Description |
| --- | --- |
| rate-name | Indicates the name of a speed-limit policy. |
| avg-threshold | Indicates the traffic average. |
| burst-threshold | Indicates the traffic burst threshold. |

**Command Mode** Global configuration mode

**Level** 14

**Usage Guide** One speed-limit policy can be deployed in different service strategies.

**Configuration Examples** The following example configures the upstream traffic average and burst threshold.

```
Ruijie(config)# rate-policy user-rate
Ruijie (config-rate-policy)#upstream average-rate 10 burst-rate 10
Ruijie (config-rate-policy)#downstream average-rate 10 burst-rate 10
```

**Verification** Run the **show running** command to display the speed limit policy.

**Prompt Messages** N/A

**Platforms**

## 13.8 rate-policy apply

Use this command to configure the speed-limit policy to be used.
**rate-policy** *rate-name* **apply**

Use this command to apply the specified speed-limit policy.
**no rate-policy**

**Parameter Description**

| Parameter | Description |
| --- | --- |
| rate-name | Indicates the name of the speed-limit policy to be used. |

**Command Mode** User policy configuration mode

**Level** 14

**Usage Guide** The name of the speed-limit policy to be used should be configured first.

**Configuration Examples** The following example configures the speed-limit policy to be used and specifies the policy name.

```
Ruijie(config)# rate-policy user-rate
Ruijie (config-rate-policy)#upstream average-rate 10 burst-rate 10
Ruijie (config-rate-policy)#downstream average-rate 10 burst-rate 10
Ruijie (config)# service-policy user-policy
Ruijie (config-service-policy)# rate-policy user-rate apply
```

**Verification** Run the **show running** command to display the speed-limit policy rule.

**Prompt Messages** N/A

**Platforms**

## 13.9 service-policy

Use this command to enter user policy configuration mode.
**service-policy** *service-name*

Use this command to apply the specified speed-limit policy.
**rate-policy** *rate-name* **apply**

**Parameter Description**

| Parameter | Description |
|---|---|
| service-name | Indicates the name of the user policy. |
| rate-name | Indicates the name of the speed-limit policy to be used. |

**Command Mode** Global configuration mode

**Level** 14

**Usage Guide** The name of the speed-limit policy to be used should be configured first.

**Configuration Examples** The following example configures the speed-limit policy to be used and specifies the policy name.

```
Ruijie(config)# rate-policy user-rate
Ruijie (config-rate-policy)#upstream average-rate 10 burst-rate 10
Ruijie (config-rate-policy)#downstream average-rate 10 burst-rate 10
Ruijie (config)# service-policy user-policy
Ruijie (config-service-policy)# rate-policy user-rate apply
```

**Verification** Run the **show running** command to display the user policy configuration.

**Prompt Messages** N/A

**Platforms**

## 13.10 upstream average-rate burst-rate

Use this command to configure the upstream traffic average and burst threshold.
**upstream average-rate** *avg-threshold* **burst-rate** *burst-threshold*

Use this command to remove the upstream traffic average and burst threshold.
**no upstream**

**Parameter Description**

| Parameter | Description |
|---|---|
| avg-threshold | Indicates the traffic average. |
| burst-threshold | Indicates the traffic burst threshold. |

**Defaults** N/A

**Command Mode** Speed-limit strategy configuration mode

**Default Level** 14

**Usage Guide** The burst thresholds of upstream parameters must not be smaller than the average.

**Configuration Examples** The following example configures the upstream traffic average and burst threshold.

```
Ruijie(config)# rate-policy user-rate
Ruijie (config-rate-policy)#upstream average-rate 10 burst-rate 10
```

**Verification** Use the **show running** command to display the speed-limit upstream policy rule.

**Prompt Messages** N/A

**Common Errors** N/A

**Platforms**

# 14 SSH Commands

## 14.1 crypto key generate

Use this command to generate a public key to the SSH server.

**crypto key generate** { **rsa | dsa** }

**Parameter Description**

| Parameter | Description |
|---|---|
| **rsa** | Generates an RSA key. |
| **dsa** | Generates a DSA key. |

**Defaults** By default, the SSH server does not generate a public key.

**Command Mode** Global configuration mode

**Usage Guide** When you need to enable the SSH SERVER service, use this command to generate a public key on the SSH server and enable the SSH SERVER service by command **enable service ssh-server** at the same time. SSH 1 uses the RSA key; SSH 2 uses the RSA or DSA key. Therefore, if a RSA key has been generated, both SSH1 and SSH2 can use it. If only a DSA key is generated, only SSH2 can use it.

- Only DSA/RSA authentication is available for one connection. Also, the key algorithm may differ in different client. Thus, it is recommended to generate both RSA and DSA keys so as to ensure connection with the portal server.
- RSA has a minimum modulus of 512 bits and a maximum modulus of 2,048 bits; DSA has a minimum modulus of 360 bits and a maximum modulus of 2,048 bits. For some clients like SCP clients, a 768-bit or more key is required. Thus, it is recommended to generate the key of 768 bits or more.
- A key can be deleted by using the **no crypto key generate** command. The **no crypto key zeroize** command is not available.

**Configuration Examples** The following example generates an RSA key to the SSH server.

```
Ruijie# configure terminal
Ruijie(con fig)# crypto key generate rsa
```

**Related Commands**

| Command | Description |
|---|---|
| **show ip ssh** | Displays the current status of the SSH server. |
| **crypto key zeroize** { **rsa** \| **dsa** } | Deletes DSA and RSA keys and disables the SSH server function. |

**Platform Description** N/A

## 14.2 crypto key zeroize

Use this command to delete a public key to the SSH server.

**crypto key zeroize** { **rsa | dsa** }

**Parameter Description**

| Parameter | Description |
|---|---|
| **rsa** | Deletes the RSA key. |
| **dsa** | Deletes the DSA key. |

**Defaults** N/A

**Command Mode** Global configuration mode

**Usage Guide** This command deletes the public key to the SSH server. After the key is deleted, the SSH server state becomes DISABLE. If you want to disable the SSH server, run the **no enable service ssh-server** command.

**Configuration Examples** The following example deletes a RSA key to the SSH server.

```
Ruijie# configure terminal
Ruijie(config)# crypto key zeroize rsa
```

**Related Commands**

| Command | Description |
|---|---|
| **show ip ssh** | Displays the current status of the SSH server. |
| **crypto key generate** { **rsa | dsa** } | Generates DSA and RSA keys. |

**Platform Description** N/A

## 14.3 disconnect ssh

Use this command to disconnect the established SSH connection.

**disconnect ssh** [ **vty** ] *session-id*

**Parameter Description**

| Parameter | Description |
|---|---|
| **vty** | Established VTY connection |
| *session-id* | ID of the established SSH connection, in the range from 0 to 35 |

**Defaults** N/A

**Command Mode** Privileged EXEC mode

**Usage Guide** You can disconnect a SSH connection by entering the ID of the SSH connection or disconnect a SSH connection by entering the specified VTY connection ID. Only connections of the SSH type can be disconnected.

**Configuration Examples** The following example disconnects the established SSH connection by specifying the SSH session ID.

```
Ruijie# disconnect ssh 1
```

The following example disconnects the established SSH connection by specifying the VTY session ID.

```
Ruijie# disconnect ssh vty 1
```

**Related Commands**

| Command | Description |
|---|---|
| **show ssh** | Displays the information about the established SSH connection. |
| **clear line vty** *line_number* | Disconnects the current VTY connection. |

**Platform Description** N/A

## 14.4 ip scp server enable

Use this command to enable the SCP server function on a network device.
Use the **no** form of this command to restore the default setting.
**ip scp server enable**
**no ip scp server enable**

**Parameter Description**

| Parameter | Description |
|---|---|
| N/A | N/A |

**Defaults** This function is disabled by default.

**Command Mode** Global configuration mode

**Usage Guide** Secure Copy (SCP) enables an authenticated user to transfer files to/from a remote device in an encrypted way, with high security and guarantee.

**Configuration Examples** The following example enables the SCP server function.

```
Ruijie# configure terminal
Ruijie(config)# ip scp server enable
```

| Related Commands | Command | Description |
|---|---|---|
| | **show ip ssh** | Displays the current status of the SSH server. |

**Platform Description** N/A

## 14.5 ip ssh authentication-retries

Use this command to set the authentication retry times of the SSH server.

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

**ip ssh authentication-retries** *retry times*

**no ip ssh authentication-retries**

| Parameter Description | Parameter | Description |
|---|---|---|
| | *retry times* | Authentication retry times, ranging from 0 to 5 |

**Defaults** The default is 3.

**Command Mode** Global configuration mode

**Usage Guide** User authentication is considered failed if authentication is not successful when the configured authentication retry times on the SSH server is exceeded. Use the **show ip ssh** command to display the configuration of the SSH server

**Configuration Examples** The following example sets the authentication retry times to 2.

```
Ruijie# configure terminal
Ruijie(config)# ip ssh authentication-retries 2
```

| Related Commands | Command | Description |
|---|---|---|
| | **show ip ssh** | Displays the current status of the SSH server. |

**Platform Description** N/A

## 14.6 ip ssh cipher-mode

Use this command to set the SSH server encryption mode.

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

**ip ssh cipher-mode** { **cbc** | **ctr** | **others** }

**no ip ssh cipher-mode**

| Parameter Description | Parameter | Description |
|---|---|---|
| | **cbc** | Encryption mode: CBC (Cipher Block Chaining) |

| | |
|---|---|
| | Encryption algorithm: DES-CBC, 3DES-CBC, AES-128-CBC, AES-192-CBC, AES-256-CBC, Blow fish-CBC |
| **ctr** | Encryption mode: CTR (Counter)<br>Encryption algorithm: AES128-CTR, AES192-CTR, AES256-CTR |
| **others** | Encryption mode: Others<br>Encryption algorithm: RC4 |

**Defaults** All encryption modes are supported by default.

**Command Mode** Global configuration mode

**Usage Guide** This command is used to set the SSH server encryption mode.
For Ruijie Networks, the SSHv1 server supports DES-CBC, 3DES-CBC, and Blowfish-CBC; the SSHv2 server supports AES128-CTR, AES192-CTR, AES256-CTR, DES-CBC, 3DES-CBC, AES-128-CBC, AES-192-CBC, AES-256-CBC, Blowfish-CBC, and RC4. All these algorithms can be grouped into CBC, CTR and Other as shown above.
With the advancement of cryptography study, CBC and Others encryption modes are proved to easily decipher. It is recommended to enable the CTR mode to raise assurance for organizations and enterprises demanding high security.

**Configuration Examples** The following example enables CTR encryption mode.

```
Ruijie# configure terminal
Ruijie(config)# ip ssh cipher-mode ctr
```

**Platform Description** N/A

## 14.7 ip ssh hmac-algorithm

Use this command to set the algorithm for message authentication.
Use the **no** form of this command to restore the default setting.
**ip ssh hmac-algorithm** { **md5** | **md5-96** | **sha1** | **sha1-96** }
**no ip ssh hmac-algorithm**

**Parameter Description**

| Parameter | Description |
|---|---|
| **md5** | MD5 algorithm |
| **md5-96** | MD5-96 algorithm |
| **sha1** | SHA1 algorithm |
| **sha1-96** | SHA1-96 algorithm |

**Defaults** SSHv1: all the algorithms are not supported.
SSHv2: all the algorithms are supported.

**Command Mode** Global configuration mode

**Usage Guide** Ruijie SSHv1 servers do not support algorithms for message authentication.
For Ruijie Networks, the SSHv1 server does not support message authentication algorithms; the SSHv2 server supports MD5, MD5-96, SHA1, and SHA1-96 algorithms. Set the algorithm on your demand.

**Configuration Examples** The following example sets the algorithm for message authentication to SHA1.

```
Ruijie# configure terminal
Ruijie(config)# ip ssh hmac-algorithm sha1
```

**Platform Description** N/A

## 14.8 ip ssh peer

Use this command to associate the public key file and the user name on the client. During client login authentication, you can specify a public key file based on the user name.
Use the **no** form of this command to restore the default setting.
**ip ssh peer** *username* **public-key** { **rsa** | **dsa** } *filename*
**no ip ssh peer** *username* **public-key** { **rsa** | **dsa** } *filename*

**Parameter Description**

| Parameter | Description |
|---|---|
| *username* | User name |
| *filename* | Name of a public key file |
| **rsa** | The public key is a RSA key |
| **dsa** | The public key is a DSA key |

**Defaults** N/A

**Command Mode** Global configuration mode

**Usage Guide** N/A

**Configuration Examples** The following example sets RSA and DSA key files associated with user **test**.

```
Ruijie# configure terminal
Ruijie(config)# ip ssh peer test public-key rsa flash:rsa.pub
Ruijie(config)# ip ssh peer test public-key dsa flash:dsa.pub
```

**Related Commands**

| Command | Description |
|---|---|
| **show ip ssh** | Displays the current status of the SSH server. |

**Platform Description** N/A

## 14.9 ip ssh time-out

Use this command to set the authentication timeout for the SSH server.
Use the **no** form of this command to restore the default setting.
**ip ssh time-out** *time*
**no ip ssh time-out**

**Parameter Description**

| Parameter | Description |
|---|---|
| *time* | Authentication timeout, in the range from 1 to 120 in the unit of seconds |

**Defaults** The default is 120 seconds.

**Command Mode** Global configuration mode

**Usage Guide** The authentication is considered timeout and failed if the authentication is not successful within 120 seconds starting from receiving a connection request. Use the **show ip ssh** command to display the configuration of the SSH server.

**Configuration Examples** The following example sets the timeout value to 100 seconds.

```
Ruijie# configure terminal
Ruijie(config)# ip ssh time-out 100
```

**Related Commands**

| Command | Description |
|---|---|
| **show ip ssh** | Displays the current status of the SSH server. |

**Platform Description** N/A

## 14.10 ip ssh version

Use this command to set the version of the SSH server.
Use the **no** form of this command to restore the default setting.
**ip ssh version** { **1** | **2** }
**no ip ssh version**

**Parameter Description**

| Parameter | Description |
|---|---|
| **1** | Supports the SSH1 client connection request. |
| **2** | Supports the SSH2 client connection request. |

**Defaults** SSH1 and SSH2 are compatible by default.

**Command Mode** Global configuration mode

**Usage Guide** This command is used to configure the SSH connection protocol version supported by SSH server. By default, the SSH server supports SSH1 and SSH2. If Version 1 or 2 is set, only the SSH client of this version can connect to the SSH server. Use the **show ip ssh** command to display the current status of SSH server.

**Configuration Examples** The following example sets the version of the SSH server.

```
Ruijie# configure terminal
Ruijie(config)# ip ssh version 2
```

**Related Commands**

| Command | Description |
|---|---|
| **show ip ssh** | Displays the current status of the SSH server. |

**Platform Description** N/A

## 14.11 show crypto key mypubkey

Use this command to display the information about the public key part of the public key to the SSH server.

**show crypto key mypubkey** { **rsa | dsa** }

**Parameter Description**

| Parameter | Description |
|---|---|
| **rsa** | Displays the RSA key. |
| **dsa** | Displays the DSA key. |

**Defaults** N/A

**Command Mode** Privileged EXEC mode/Global configuration mode

**Usage Guide** This command is used to show the information about the public key part of the generated public key on the SSH server, including key generation time, key name, contents in the public key part, etc.

**Configuration Examples** The following example displays the information about the public key part of the public key to the SSH server.

```
Ruijie(config)#show crypto key mypubkey rsa
% Key pair was generated at: 7:1:25 UTC Jan 16 2013
```

```
 Key name: RSA1 private
 Usage: SSH Purpose Key
 Key is not exportable.
 Key Data:
       AAAAAwEA AQAAAEEA 2m6H/J+2 xOMLW5MR 8tOmpW1I XU1QItVN mLdR+G7O
Q10kz+4/
       /IgYR0ge 1sZNg32u dFEifZ6D zfLySPqC MTWLfw==

% Key pair was generated at: 7:1:25 UTC Jan 16 2013
 Key name: RSA private
 Usage: SSH Purpose Key
 Key is not exportable.
 Key Data:
       AAAAAwEA AQAAAEEA 0E5w2H0k v744uTIR yZBd/7AM 8pLItnW3 XH3LhEEi
BbZGZvn3
       LEYYfQ9s pgYL0ZQf S0s/GY0X gJOMsc6z i8OAkQ==
```

| Related Commands | Command | Description |
|---|---|---|
| | **crypto key generate** { **rsa** \| **dsa** } | Generates DSA and RSA keys. |

**Platform Description** N/A

## 14.12 show ip ssh

Use this command to display the information of the SSH server.

**show ip ssh**

| Parameter Description | Parameter | Description |
|---|---|---|
| | N/A | N/A |

**Defaults** N/A

**Command Mode** Privileged EXEC mode/Global configuration mode

**Usage Guide** This command is used to display the information of the SSH server, including version, enablement state, authentication timeout, and authentication retry times.

Note: If no key is generated for the SSH server, the SSH version is still unavailable even if this SSH version has been configured.

**Configuration Examples** The following example displays the information of the SSH server.

```
SSH and SCP disabled:
Ruijie(config)#show ip ssh
```

```
SSH Disable - version 1.99
please generate rsa and dsa key to enable SSH
Authentication timeout: 120 secs
Authentication retries: 3
SSH SCP Server: disabled

SSH and SCP enabled:
Ruijie(config)#show ip ssh
SSH Enable - version 1.99
Authentication timeout: 120 secs
Authentication retries: 3
SSH SCP Server: enabled
```

**Related Commands**

| Command | Description |
|---|---|
| **ip ssh version** {**1** \| **2**} | Configures the version for the SSH server. |
| **ip ssh time-out time** | Sets the authentication timeout for the SSH server. |
| **ip ssh authentication-retries** | Sets the authentication retry times for the SSH server. |

**Platform Description** N/A

## 14.13 show ssh

Use this command to display the information about the established SSH connection.

**show ssh**

**Parameter Description**

| Parameter | Description |
|---|---|
| N/A | N/A |

**Defaults** N/A

**Command Mode** Privileged EXEC mode/Global configuration mode

**Usage Guide** This command is used to display the information about the established SSH connection, including VTY number of connection, SSH version, encryption algorithm, message authentication algorithm, connection status, and user name.

**Configuration Examples** The following example displays the information about the established SSH connection:

```
Ruijie#show ssh
Connection Version Encryption      Hmac        Compress   State
Username
        0    1.5 blowfish                  zlib      Session started test
```

```
        1     2.0 aes256-cbc      hmac-sha1    zlib      Session started test
```

Field Description

| Field | Description |
|---|---|
| Connection | VTY number |
| Version | SSH version |
| Encryption | Encryption algorithm |
| Hmac | Message authentication algorithm |
| Compress | Compress algorithm |
| State | Connection state |
| Username | Username |

**Related Commands**

| Command | Description |
|---|---|
| N/A | N/A |

**Platform Description** N/A

# System Configuration Commands

# 1 Command Line Interface Commands

## 1.1 alias

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

**alias** *mode command-alias original-command*

**no alias** *mode command-alias*

**default 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 user or privileged EXEC mode have default alias.

**Command Mode** Global configuration mode.

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

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

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

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

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

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

```
......
```

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

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

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

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

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

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

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

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

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

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

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

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

**Configuration Examples**

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

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

**Platform Description**

N/A

## 1.2 privilege

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

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

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

**Parameter Description**

| Parameter | Description |
|---|---|
| *mode* | CLI mode of the command to which the execution rights are attributed. |
| **all** | Command alias |
| **level** *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** The following example sets the password of CLI level 1 as **test** and attribute the **reload** rights to reset the device:

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

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

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

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

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

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

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

**Related Commands**

| Command | Description |
|---|---|
| **enable secret** | Sets the CLI-level password. |

**Platform Description** N/A.

## 1.3 show aliases

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

**show aliases** [ *mode* ]

**Parameter Description**

| Parameter | Description |
|---|---|
| *mode* | Mode of the command represented by the alias. |

**Defaults** N/A.

**Command Mode** Privileged EXEC mode.

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

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

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

**Related Commands**

| Command | Description |
|---|---|
| **alias** | Sets a command alias. |

**Platform Description** N/A.

# 2 Basic Configuration Management Commands

## 2.1 <1-99>

Use this command to restore the suspended Telnet Client session.

**<1-99>**

**Parameter Description**

| Parameter | Description |
|---|---|
| N/A | N/A |

**Defaults** N/A

**Command Mode** User EXEC mode

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

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

```
Ruijie# 1
```

**Related Commands**

| Command | Description |
|---|---|
| N/A | N/A |

**Platform Description** N/A

## 2.2 banner exec

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

**banner exec** *c message c*

**no banner exec**

**Parameter Description**

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

| | |
|---|---|
| *message* | Contents of the message. |

**Defaults** N/A

**Command Mode** Global configuration mode

**Usage Guide** This command is used to configure the welcome message. The system discards all the characters next to the terminating symbol.
When you are logging in to the device, the MOTD message is displayed at first, and then the banner login message. After you have logged in, the EXEC message or the incoming message is displayed. If it's a reverse Telnet session, the incoming message is displayed. Otherwise, the EXEC message is displayed.
The messages are for all lines. If you want to disable display the EXEC message on a specific line, configure the **no exec-banner** command on the line.

**Configuration Examples** The following example configures a welcome message.

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

**Related Commands**

| Command | Description |
|---|---|
| N/A | N/A |

**Platform Description** N/A

## 2.3 banner incoming

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

**Parameter Description**

| Parameter | Description |
|---|---|
| *c* | Separator of the message. Delimiters are not allowed in the message. |
| *message* | Contents of the message. |

**Defaults** N/A

**Command Mode** Global configuration mode

**Usage Guide** This command is used to configure a prompt message. The system discards all the characters next to the terminating symbol.
When you are logging in to the device, the MOTD message is displayed at first, and then the banner login message. After you have logged in, the welcome message or the prompt message is displayed. If it's a reverse Telnet session, the prompt message is displayed. Otherwise, the welcome message is displayed.

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

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

**Related Commands**

| Command | Description |
|---|---|
| N/A | N/A |

**Platform Description** N/A

## 2.4 banner login

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

**Parameter Description**

| Parameter | Description |
|---|---|
| *c* | Separator of the message contained in the login banner. Delimiters are not allowed in the MOTD. |
| *message* | Contents of the login banner |

**Defaults** N/A

**Command Mode** Global configuration mode

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

**Configuration Examples** The following example configures a login banner.

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

**Related Commands**

| Command | Description |
|---|---|
| N/A | N/A |

**Platform Description** N/A

## 2.5 banner motd

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

**banner** [ **motd** ] *c message c*

**no banner** [ **motd** ]

**Parameter Description**

| Parameter | Description |
|---|---|
| *c* | Separator of the MOTD. Delimiters are not allowed in the MOTD. |
| *message* | Contents of an MOTD |

**Defaults** N/A

**Command Mode** Global configuration mode

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

**Configuration Examples** The following example configures the MOTD.

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

**Related Commands**

| Command | Description |
|---|---|
| N/A | N/A |

**Platform Description** N/A

## 2.6 banner prompt-timeout

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

**banner prompt-timeout** *c message c*

**no banner prompt-timeout**

**Parameter Description**

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

| | |
|---|---|
| | message. |
| *message* | Contents of the message. |

**Defaults** N/A

**Command Mode** Global configuration mode

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

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

```
Ruijie(config)# banner exec $ authentication timeout $
```

**Related Commands**

| Command | Description |
|---|---|
| N/A | N/A |

**Platform Description** N/A

## 2.7 banner slip-ppp

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

**Parameter Description**

| Parameter | Description |
|---|---|
| *c* | Separator of the message. Delimiters are not allowed in the message. |
| *message* | Contents of the message. |

**Defaults** N/A

**Command Mode** Global configuration mode

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

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

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

**Related Commands**

| Command | Description |
| --- | --- |
| N/A | N/A |

**Platform Description** N/A

## 2.8 configure

Use this command to enter global configuration mode.

**configure** [ **terminal** ]

**Parameter Description**

| Parameter | Description |
| --- | --- |
| N/A | N/A |

**Defaults** N/A

**Command Mode** Privileged EXEC mode

**Usage Guide** N/A

**Configuration Examples** The following example enters global configuration mode.

```
Ruijie# configure
Ruijie(config)#
```

**Related Commands**

| Command | Description |
| --- | --- |
| N/A | N/A |

**Platform Description** N/A

## 2.9 disable

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

**disable** [ *privilege-level* ]

**Parameter Description**

| Parameter | Description |
| --- | --- |
| privilege-level | Privilege level |

**Defaults** N/A

**Command Mode** User EXEC mode

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

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

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

```
Ruijie# disable 10
```

**Related Commands**

| Command | Description |
| --- | --- |
| **enable** | Moves from user EXEC mode enter to privileged EXEC mode or reaches a higher level of authority. |

**Platform Description** N/A

## 2.10 disconnect

Use this command to disconnect the Telnet Client session.

**disconnect** *session-id*

**Parameter Description**

| Parameter | Description |
| --- | --- |
| *session-id* | Telnet Client session ID. |

**Defaults** N/A

**Command Mode** User EXEC mode

**Usage Guide** This command is used to disconnect the Telnet Client session by setting the session ID.

**Configuration** The following example disconnects the Telnet Client session by setting the session ID.

**Examples**

```
Ruijie# disconnect 1
```

**Related Commands**

| Command | Description |
| --- | --- |
| N/A | N/A |

**Platform Description** N/A

## 2.11 enable

Use this command to enter privileged EXEC mode.

**enable** [ *privilege-level* ]

**Parameter Description**

| Parameter | Description |
| --- | --- |
| *privilege-level* | Privilege level |

**Defaults** N/A

**Command Mode** User EXEC mode

**Usage Guide** N/A

**Configuration Examples** The following example lowers the privilege level to 14.

```
Ruijie> enable 14

Password:
```

**Related Commands**

| Command | Description |
| --- | --- |
| N/A | N/A |

**Platform Description** N/A

## 2.12 enable password

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

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

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

**Parameter Description**

| Parameter | Description |
| --- | --- |
| *password* | Password for the user to enter the EXEC configuration layer |
| **level** | User's level. |
| **0** | “”“” ‘The password is in plain text. |
| **7** *encrypted-password* | The password is encrypted. |

**Defaults** N/A

**Command Mode** Global configuration mode

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

A valid password is defined as follows:

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

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

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

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

**Related Commands**

| Command | Description |
| --- | --- |
| **enable secret** | Sets the security password |

**Platform Description** N/A

**enable secret** Sets the security password

## 2.13 enable secret

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

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

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

**Parameter Description**

| Parameter | Description |
|---|---|
| **level** | User's level. |
| **0** | The password is in plain text. |
| **5** *encrypted-password* | The password is encrypted. |
| *password* | Password for the user to enter the privileged EXEC configuration. |

**Defaults** N/A

**Command Mode** Global configuration mode

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

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

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

**Related Commands**

| Command | Description |
|---|---|
| **enable password** | Sets passwords for different privilege levels. |

**Platform Description** N/A

## 2.14 enable service

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

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

**Parameter Description**

| Parameter | Description |
|---|---|
| **ssh-server** | Enables SSH Server. IPv4 and IPv6 services are enabled at the same time. |
| **telnet-server** | Enables Telnet Server. IPv4 and IPv6 services are enabled at the |

| | |
|---|---|
| | same time. |
| **web-server** [ **http \| https \| all** ] | Enables HTTP Server. IPv4 and IPv6 services are enabled at the same time. |
| **snmp-agent** | Enables SNMP Agent. IPv4 and IPv6 services are enabled at the same time. |

**Defaults** telnet-server, snmp-agent and web-server are enabled and ssh-server is disabled by default.

**Command Mode** Global configuration mode

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

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

**Configuration Examples** The following example enables the SSH Server.

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

**Related Commands**

| Command | Description |
|---|---|
| **show service** | Displays the service status in the current system. |

**Platform Description** N/A

## 2.15 exec-banner

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

**exec-banner**

**no exec-banner**

**Parameter Description**

| Parameter | Description |
|---|---|
| N/A | N/A |

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

**Command** LINE configuration mode

**Mode**

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

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

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

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

**Related Commands**

| Command | Description |
|---|---|
| N/A | N/A |

**Platform Description** N/A

## 2.16 exec-timeout

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

**exec-timeout** *minutes* [ ***seconds*** ]

**no exec-timeout**

**Parameter Description**

| Parameter | Description |
|---|---|
| *minutes* | Timeout in minutes. |
| **seconds** | (Optional) Timeout in minutes |

**Defaults** The default is 10 minutes.

**Command Mode** Line configuration mode

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

**Configuration Examples** The following example sets the connection timeout to 5’30’’.

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

**Related Commands**

| Command | Description |
| --- | --- |
| N/A | N/A |

**Platform Description** N/A

## 2.17 help

Use this command to display the help information.

**help**

**Parameter Description**

| Parameter | Description |
| --- | --- |
| N/A | N/A |

**Defaults**

**Command Mode** Any mode

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

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

```
Ruijie#help
Help may be requested at any point in a command by entering
a question mark '?'.  If nothing matches, the help list will
be empty and you must backup until entering a '?' shows the
available options.
Two styles of help are provided:
1. Full help is available when you are ready to enter a
   command argument (e.g. 'show ?') and describes each possible
   argument.
2. Partial help is provided when an abbreviated argument is entered
   and you want to know what arguments match the input
   (e.g. 'show pr?'.)
```

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

```
Ruijie(config-if-GigabitEthernet 0/0)#?
Interface configuration commands:
  arp            ARP interface subcommands
  bandwidth       Set bandwidth informational parameter
  carrier-delay    Specify delay for interface transitions
  dampening       Enable event dampening
```

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

The following example displays the parameters of a specified command.

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

```
host    A single source host
```

**Related Commands**

| Command | Description |
| --- | --- |
| N/A | N/A |

**Platform Description** N/A

## 2.18 hostname

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

**hostname** *name*

**Parameter Description**

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

**Defaults** The default is Ruijie.

**Command Mode** Global configuration mode

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

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

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

**Related Commands**

| Command | Description |
| --- | --- |
| N/A | N/A |

**Platform Description** N/A

## 2.19 ip telnet source-interface

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

**ip telnet source-interface** *interface-name*

**Parameter Description**

| Parameter | Description |
| --- | --- |
| *interface-name* | Configures the IP address of the interface as the source address for Telnet connection. |

**Defaults** N/A

**Command Mode** Global configuration mode

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

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

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

**Related Commands**

| Command | Description |
| --- | --- |
| **telnet** | Logs in a Telnet server. |

**Platform Description** N/A

## 2.20 lock

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

**lock**

**Parameter Description**

| Parameter | Description |
| --- | --- |
| N/A | N/A |

**Defaults** N/A

**Command Mode** User EXEC mode

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

- Enter the **lock** command, and the system will prompt you for a password:
- Enter the password, which can be any character string. The system will prompt you to confirm

the password, clear the screen, and display the "Locked" information.

- To access the terminal, enter the preset temporary password.
- To lock the terminal, run the **lockable** command in line configuration mode and enable terminal locking in the corresponding line.

**Configuration Examples** The following example locks a terminal interface.

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

**Related Commands**

| Command | Description |
|---|---|
| **lockable** | Supports terminal locking in the line. |

**Platform Description** N/A

## 2.21 lockable

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

**lockable**

**no lockable**

**Parameter Description**

| Parameter | Description |
|---|---|
| N/A | N/A |

**Defaults** This function is disabled by default.

**Command Mode** Line configuration mode

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

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

```
Ruijie(config)# line console 0
Ruijie(config-line)# lockable
```

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

**Related Commands**

| Command | Description |
|---|---|
| **lock** | Locks the terminal. |

**Platform Description** N/A

## 2.22 login

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

**login**

**no login**

**Parameter Description**

| Parameter | Description |
|---|---|
| N/A | N/A |

**Defaults** The login function is disabled for console and enabled for VTY terminal by default.

**Command Mode** Line configuration mode

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

**Configuration Examples** The following example sets a login password authentication on VTY..

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

**Related Commands**

| Command | Description |
|---|---|
| **password** | Configures the line login password |

**Platform** N/A

**Description**

## 2.23 login authentication

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

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

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

**Parameter Description**

| Parameter | Description |
|---|---|
| **default** | Name of the default authentication method list |
| *list-name* | Name of the method list |

**Defaults** The default authentication method is used when AAA is enabled,

**Command Mode** Line configuration mode

**Usage Guide**

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

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

**Related Commands**

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

**Platform Description** N/A

## 2.24 login local

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

**login local**

**no login local**

**Parameter Description**

| Parameter | Description |
| --- | --- |
| N/A | N/A |

**Defaults** N/A

**Command Mode** Line configuration mode

**Usage Guide** If the AAA security server is inactive, this command is used for local user login authentication. The user is allowed to use the **username** command.

**Configuration Examples** The following example sets local user authentication on VTY.

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

**Related Commands**

| Command | Description |
| --- | --- |
| **username** | Configures local user information. |

**Platform Description** N/A

## 2.25 motd-banner

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

**motd-banner**

**no motd-banner**

**Parameter Description**

| Parameter | Description |
| --- | --- |
| N/A | N/A |

**Defaults** The MOTD message is displayed on all lines by default.

**Command Mode** Line configuration mode

**Usage Guide** After you configure the **banner exec** and the **banner motd** commands, the EXEC and the MOTD messages are displayed on all lines by default. If you want to disable display of the EXEC and the

MOTD messages on a specific line, configure the **no** form of this command on the line.

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

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

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

**Related Commands**

| Command | Description |
|---|---|
| N/A | N/A |

**Platform Description** N/A

## 2.26 password

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

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

**no password**

**Parameter Description**

| Parameter | Description |
|---|---|
| *password* | Password for remote line login |
| **0** | The password is in plain text. |
| **7** *encrypted-password* | The password is encrypted. |

**Defaults** N/A

**Command Mode** Line configuration mode

**Usage Guide**

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

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

**Related Commands**

| Command | Description |
|---|---|
| **login** | Moves from user EXEC mode to privileged |

| | |
|---|---|
| | EXEC mode or enables a higher level of authority. |

**Platform Description** N/A

## 2.27 prompt

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

**prompt string**

**no prompt**

**Parameter Description**

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

**Defaults** N/A

**Command Mode** Global configuration mode

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

**Configuration Examples** The following example sets the prompt string to rgnos.

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

**Related Commands**

| Command | Description |
|---|---|
| N/A | N/A |

**Platform Description** N/A

## 2.28 secret

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

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

**no secret**

**Parameter Description**

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

**Defaults** N/A

**Command mode** Line configuration mode

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

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

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

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

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

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

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

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

**Related Commands**

| Command | Description |
|---|---|
| **login** | Sets simple password authentication on the interface as the login authentication mode |

**Platform Description** N/A

## 2.29 session-timeout

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

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

**no session-timeout**

**Parameter Description**

| Parameter | Description |
|---|---|
| *minutes* | Timeout in minutes. |
| **output** | Regards data output as the input to determine whether the session expires. |

**Defaults** The default timeout is 0.

**Command Mode** LINE configuration mode

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

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

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

**Related Commands**

| Command | Description |
|---|---|
| N/A | N/A |

**Platform Description** N/A

## 2.30 show line

Use this command to display the configuration of a line.

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

**Parameter Description**

| Parameter | Description |
|---|---|
| **console** | Display s the configuration of a console line. |
| **vty** | Display s the configuration of a vty line. |
| *line-num* | Number of the line. |

**Defaults** N/A

**Command Mode** Privileged EXEC mode

**Usage Guide**

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

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

**Related Commands**

| Command | Description |
|---|---|
| N/A | N/A |

**Platform Description** N/A

## 2.31 show reload

Use this command to display the system restart settings.

**show reload**

**Parameter Description**

| Parameter | Description |
|---|---|
| N/A | N/A |

**Defaults** N/A

**Command Mode** Privileged EXEC mode

**Usage Guide**

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

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

**Related Commands**

| Command | Description |
|---|---|
| N/A | N/A |

**Platform Description** N/A

## 2.32 show running-config

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

**show running-config** [ **interface** *interface* ]

**Parameter Description**

| Parameter | Description |
|---|---|
| N/A | N/A |

**Defaults** N/A

**Command Mode** Privileged EXEC mode

**Usage Guide** N/A

**Configuration Examples** N/A

**Related Commands**

| Command | Description |
|---|---|
| N/A | N/A |

**Platform Description** N/A

## 2.33 show service

Use this command to display the service status.

**show service**

**Parameter Description**

| Parameter | Description |
| --- | --- |
| N/A | N/A |

**Defaults** N/A

**Command Mode** Privileged EXEC mode

**Usage Guide** N/A

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

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

**Related Commands**

| Command | Description |
| --- | --- |
| N/A | N/A |

**Platform Description** N/A

## 2.34 show sessions

Use this command to display the Telnet Client session information.

**show sessions**

**Parameter Description**

| Parameter | Description |
| --- | --- |
| N/A | N/A |

**Defaults** N/A

**Command Mode** User EXEC mode

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

**Configuration Examples** The following example displays the Telnet Client session information.

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

**Related Commands**

| Command | Description |
| --- | --- |
| N/A | N/A |

**Platform Description** N/A

## 2.35 show startup-config

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

**show startup-config**

**Parameter Description**

| Parameter | Description |
| --- | --- |
| N/A | N/A |

**Defaults** N/A

**Command Mode** Privileged EXEC mode

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

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

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

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

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

**Configuration Examples** N/A

**Related Commands**

| Command | Description |
| --- | --- |
| **boot config** | Sets the name of the boot configuration file. |

| | |
|---|---|
| **Platform Description** | N/A |

## 2.36 show this

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

**show this**

| **Parameter Description** | **Parameter** | **Description** |
|---|---|---|
| | N/A | N/A |

| | |
|---|---|
| **Defaults** | N/A |
| **Command Mode** | All modes. |
| **Usage Guide** | The configuration in the following range modes cannot be displayed. If the **show this** command is run, the outcome is NULL.<br>1. Use the **line** *first-line last-line* command to configure lines in a continuous group and enter LINE configuration mode.<br>2. Use the **vlan range** command to configure VLANs and enter vlan range configuration mode.<br>3. Use the interface range command to configure interfaces and enter interface range configuration mode. |

**Configuration Examples**

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

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

| | |
|---|---|
| **Platform Description** | N/A |

## 2.37 speed

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

**speed** *speed*

**no speed**

**Parameter Description**

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

**Defaults** The default is 9600.

**Command Mode** Line configuration mode

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

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

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

**Related Commands**

| Command | Description |
|---|---|
| N/A | N/A |

**Platform Description** N/A

## 2.38 telnet

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

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

**Parameter Description**

| Parameter | Description |
|---|---|
| *host* | The IP address of the host or host name you want to log in. |
| *port* | Selects the TCP port number for login, 23 by default. |
| */source* | Specifies the source IP address or source interface used by the Telnet client. |
| **ip** A.B.C.D | Specifies the source IPv4 address used by the Telnet client. |

| | |
|---|---|
| **ipv6** X:X:X:X::X | Specifies the source IPv6 address used by the Telnet client. |
| **interface** *interface-name* | Specifies the source interface used by the Telnet client. |

**Defaults** N/A

**Command Mode** User EXEC mode

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

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

**Configuration Examples** The following example sets telnet to IPv4 address 192.168.1.11. The port number is the default, and the source interface is Gi 0/1.

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

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

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

**Related Commands**

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

**Platform Description** N/A

## 2.39 username

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

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

**no username** *name*

**Parameter Description**

| Parameter | Description |
|---|---|
| *name* | Username |
| **login mode** | Sets the login mode. |
| **console** | Sets the login mode to console. |

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

**Defaults** N/A

**Command Mode** Global configuration mode

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

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

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

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

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

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

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

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

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

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

**Related Commands**

| Command | Description |
|---|---|
| **login local** | Enables local authentication |

**Platform Description** N/A

## 2.40 username import

Use this command to import user information from the file.

**username import** *filename*

**Parameter Description**

| Parameter | Description |
| --- | --- |
| *filename* | The file name. |

**Defaults** N/A

**Command Mode** Privileged EXEC mode

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

**Configuration Examples** The following example imports user information from the file.

```
Ruijie# username import user.csv
```

**Related Commands**

| Command | Description |
| --- | --- |
| N/A | N/A |

**Platform Description** N/A

## 2.41 username export

Use this command to export user information to the file.

**username export** *filename*

**Parameter Description**

| Parameter | Description |
| --- | --- |
| *filename* | The file name. |

**Defaults** N/A

**Command Mode** Privileged EXEC mode

**Usage Guide** This command is used to export user information to the file.

**Configuration** The following example exports user information to the file.

**Examples**

```
Ruijie# username export user.csv
```

**Related Commands**

| Command | Description |
| --- | --- |
| N/A | N/A |

**Platform Description** N/A

## 2.42 write

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

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

**Parameter Description**

| Parameter | Description |
| --- | --- |
| **memory** | Writes the system configuration (running-config) into NVRAM, which is equivalent to **copy running-config startup-config**. |
| **terminal** | Displays the system configuration, which is equivalent to **show running-config**. |

**Defaults** N/A

**Command Mode** Privileged EXEC mode

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

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

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

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

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

**Related Commands**

| Command | Description |
| --- | --- |
| N/A | N/A |

| | |
|---|---|
| **Platform Description** | N/A |

# 3 LINE Commands

## 3.1 access-class

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

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

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

**Parameter Description**

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

**Defaults** N/A

**Command Mode** Line configuration mode

**Usage Guide** N/A

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

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

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

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

**Related Commands**

| Command | Description |
|---|---|
| **show running** | Displays status information |

**Platform Description** N/A

## 3.2 accounting commands

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

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

**no accounting commands** *level*

**Parameter Description**

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

**Defaults** This function is disabled by default.

**Command Mode** Line configuration mode

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

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

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

**Related Commands**

| Command | Description |
|---|---|
| N/A | N/A |

**Platform Description** N/A

## 3.3 accounting exec

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

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

**no accounting commands** *level*

**Parameter**

| Parameter | Description |
|---|---|

**Description**

| | |
|---|---|
| **default** | Default authorization list name. |
| *list-name* | Optional list name. |

**Defaults** This function is disabled by default.

**Command Mode** Line configuration mode

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

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

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

**Related Commands**

| Command | Description |
|---|---|
| N/A | N/A |

**Platform Description** N/A

## 3.4 authorization commands

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

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

**no authorization commands** *level*

**Parameter Description**

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

**Defaults** This function is disabled by default.

**Command Mode** Line configuration mode

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

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

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

**Related Commands**

| Command | Description |
|---|---|
| N/A | N/A |

**Platform Description** N/A

## 3.5 authorization exec

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

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

**no authorization exec**

**Parameter Description**

| Parameter | Description |
|---|---|
| **default** | Default authorization list name, |
| *list-name* | Optional list name. |

**Defaults** This function is disabled by default,

**Command Mode** Line configuration mode

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

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

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

**Related**

| Command | Description |
|---|---|

**Commands**

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

**Platform Description** N/A

## 3.6 clear line

Use this command to clear connection status of the line.

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

**Parameter Description**

| Parameter | Description |
|---|---|
| **console** | Clears connection status of the console line. |
| **vty** | Clears connection status of the virtual terminal line. |
| *line-num* | Specifies the line to be cleared. |

**Defaults** N/A

**Command Mode** Privileged EXEC mode

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

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

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

**Related Commands**

| Command | Description |
|---|---|
| N/A | N/A |

**Platform Description** N/A

## 3.7 disconnect-character

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

**disconnect-character** *ascii-value*

**no disconnect-character**

**Parameter Description**

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

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

**Command Mode** Line configuration mode

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

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

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

**Related Commands**

| Command | Description |
| --- | --- |
| N/A | N/A |

**Platform Description** N/A

## 3.8 escape-character

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

**escape-character** *escape-value*

**no escape-character**

**Parameter Description**

| Parameter | Description |
| --- | --- |
| *escape-value* | Sets the ASCII value corresponding to the escape character for the line, in the range from 0 to 255. |

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

**Command Mode** Line configuration mode

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

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

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

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

**Related Commands**

| Command | Description |
| --- | --- |
| N/A | N/A |

**Platform Description** N/A

## 3.9 exec

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

**exec**

**no exec**

**Parameter Description**

| Parameter | Description |
| --- | --- |
| N/A | N/A |

**Defaults** This function is enabled by default.

**Command Mode** Line configuration mode

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

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

```
Ruijie(config)# line vty 1
Ruijie(config-line)# no exec
Ruijie# show users
Line           User        Host(s)            Idle      Location
---------------- ------------ -------------------- ----------
------------------
*  0 con 0      ---         idle              00:00:00   ---
   1 vty 0      ---         idle              00:01:03   20.1.1.2
    3 vty 2       ---          idle                 00:00:13   20.1.1.2
```

**Related**

| Command | Description |
| --- | --- |

**Commands**

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

**Platform Description** N/A

## 3.10 history

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

**history** [ **size** *size* ]

**no history**

**no history size**

**Parameter Description**

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

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

**Command Mode** Line configuration mode

**Usage Guide** N/A

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

```
Ruijie(config)# line vty 0 5
Ruijie(config-line)# history size 20
```

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

```
Ruijie(config)# line vty 0 5
Ruijie(config-line)# no history
```

**Related Commands**

| Command | Description |
|---|---|
| N/A | N/A |

**Platform Description** N/A

## 3.11 ipv6 access-class

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

command to restore the default setting.

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

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

**Parameter Description**

| Parameter | Description |
|---|---|
| *access-list-name* | Specifies the ACL name. |
| **in** | Filters the incoming connections. |
| **out** | Filters the outgoing connections. |

**Defaults** N/A

**Command Mode** Line configuration mode

**Usage Guide** N/A

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

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

**Related Commands**

| Command | Description |
|---|---|
| **show running** | Displays status information |

**Platform Description** N/A

## 3.12 length

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

**length** *screen-length*

**no length**

**Parameter Description**

| Parameter | Description |
|---|---|
| *screen-length* | Sets the screen length, in the range from 0 to 512. |

**Defaults** The default is 24.

**Command Mode** Line configuration mode

**Usage Guide** N/A

**Configuration Examples** The following example sets the screen length to 10.

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

**Related Commands**

| Command | Description |
| --- | --- |
| N/A | N/A |

**Platform Description** N/A

## 3.13 line

Use this command to enter the specified LINE mode.

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

**Parameter Description**

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

**Defaults** N/A

**Command Mode** Global configuration mode

**Usage Guide**

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

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

**Related Commands**

| Command | Description |
| --- | --- |
| N/A | N/A |

**Platform Description** N/A

## 3.14 line vty

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

**line vty** *line-number*

**no line vty** *line-number*

**Parameter Description**

| Parameter | Description |
|---|---|
| *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**

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

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

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

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

**Related Commands**

| Command | Description |
|---|---|
| N/A | N/A |

**Platform Description** N/A

## 3.15 location

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

**location** *location*

**no location**

**Parameter Description**

| Parameter | Description |
|---|---|
| *location* | Line location description |

**Defaults** N/A

**Command Mode** Line configuration mode

**Usage Guide** N/A

**Configuration Examples** The following example describes the line location as Swtich's Line VTY 0.

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

**Related Commands**

| Command | Description |
|---|---|
| N/A | N/A |

**Platform Description** N/A

## 3.16 monitor

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

**monitor**

**no monitor**

**Parameter Description**

| Parameter | Description |
|---|---|
| N/A | N/A |

**Defaults** N/A

**Command Mode** Line configuration mode

**Usage Guide** N/A

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

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

**Related Commands**

| Command | Description |
|---|---|
| N/A | N/A |

**Platform Description** N/A

## 3.17 privilege level

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

**privilege level** *level*

**no privilege level**

**Parameter Description**

| Parameter | Description |
|---|---|
| *level* | Privilege level, in the range from 0 to 15. |

**Defaults** The default is 1.

**Command Mode** Line configuration mode

**Usage Guide** N/A

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

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

**Related Commands**

| Command | Description |
|---|---|
| N/A | N/A |

**Platform Description** N/A

## 3.18 refuse-message

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

**refuse-message** [ *c message c* ]

**no refuse-message**

**Parameter Description**

| Parameter | Description |
|---|---|
| *c* | Delimiter of the login refusal message, which is not allowed within the message. |

| | |
|---|---|
| *message* | Login refusal message. |

**Defaults** N/A

**Command Mode** Line configuration mode

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

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

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

**Related Commands**

| Command | Description |
|---|---|
| N/A | N/A |

**Platform Description** N/A

## 3.19 show history

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

**show history**

**Parameter Description**

| Parameter | Description |
|---|---|
| N/A | N/A |

**Defaults** N/A

**Command Mode** Privileged EXEC mode

**Usage Guide** N/A

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

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

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

**Related Commands**

| Command | Description |
| --- | --- |
| N/A | N/A |

**Platform Description** N/A

## 3.20 show line

Use this command to display line configuration.

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

**Parameter Description**

| Parameter | Description |
| --- | --- |
| **console** | Displays configuration for the console line. |
| **vty** | Displays configuration for the virtual terminal line. |
| *line-num* | Displays the line. |

**Defaults** N/A

**Command Mode** Privileged EXEC mode

**Usage Guide** N/A

**Configuration Examples** The following example displays configuration for the console port.

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

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

**Related Commands**

| Command | Description |
|---|---|
| N/A | N/A |

**Platform Description** N/A

## 3.21 show privilege

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

**show privilege**

**Parameter Description**

| Parameter | Description |
|---|---|
| N/A | N/A |

**Defaults** N/A

**Command Mode** Privileged EXEC mode

**Usage Guide** N/A

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

**Examples**

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

**Related Commands**

| Command | Description |
| --- | --- |
| N/A | N/A |

**Platform Description** N/A

## 3.22 show users

Use this command to display the login user information.

**show users** [ **all** ]

**Parameter Description**

| Parameter | Description |
| --- | --- |
| **all** | Displays line user information, including users logging into the line and users not logging into the line. |

**Defaults** N/A

**Command Mode** Privileged EXEC mode

**Usage Guide** N/A

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

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

The following example displays all line user information,

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

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

| Related Commands | Command | Description |
|---|---|---|
| | N/A | N/A |

**Platform Description** N/A

## 3.23 speed

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

**speed** *baudrate*

**no speed**

| Parameter Description | Parameter | Description |
|---|---|---|
| | *baudrate* | Sets the baud rate, in the range from 9600 to 115200. |

**Defaults** The default is 9600.

**Command Mode** LINE configuration mode

**Usage Guide** N/A

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

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

| Related Commands | Command | Description |
|---|---|---|
| | N/A | N/A |

**Platform Description** N/A

## 3.24 terminal escape-character

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

**terminal escape-character** *escape-value*
**terminal no escape-character**

**Parameter Description**

| Parameter | Description |
|---|---|
| *escape-value* | Sets the ASCII value corresponding to the escape character for the current terminal, in the range from 0 to 255. |

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

**Command Mode** Privileged EXEC mode

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

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

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

**Related Commands**

| Command | Description |
|---|---|
| N/A | N/A |

**Platform Description** N/A

## 3.25 terminal history

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

**Parameter Description**

| Parameter | Description |
|---|---|
| **size** *size* | Sets the number of commands, in the range from 0 to 256. |

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

**Command Mode** Privileged EXEC mode

**Usage Guide** N/A

**Configuration Examples** The following example sets the number of commands in the command history to 20 for the current terminal.

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

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

```
Ruijie# terminal no history
```

**Related Commands**

| Command | Description |
| --- | --- |
| N/A | N/A |

**Platform Description** N/A

## 3.26 terminal length

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

**terminal length** *screen-length*

**terminal no length**

**Parameter Description**

| Parameter | Description |
| --- | --- |
| *screen-length* | Sets the screen length, in the range from 0 to 512. |

**Defaults** The default is 24.

**Command Mode** Privileged EXEC mode

**Usage Guide** N/A

**Configuration Examples** The following example sets the screen length for the current terminal to 10.

```
Ruijie# terminal length 10
```

**Related Commands**

| Command | Description |
| --- | --- |
| N/A | N/A |

**Platform Description** N/A

## 3.27 terminal location

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

**terminal location** *location*

**terminal no location**

**Parameter Description**

| Parameter | Description |
|---|---|
| *location* | Configures location description of the current device. |

**Defaults** N/A

**Command Mode** Privileged EXEC mode

**Usage Guide** N/A

**Configuration Examples** The following example configures location description of the current device as “Swtich’s Line Vty 0”.

```
Ruijie# terminal location Swtich’s Line Vty 0
```

**Related Commands**

| Command | Description |
|---|---|
| N/A | N/A |

**Platform Description** N/A

## 3.28 terminal speed

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

**terminal speed** *baudrate*

**terminal no speed**

**Parameter Description**

| Parameter | Description |
|---|---|
| *baudrate* | Sets the baud rate, in the range from 9600 to 115200. |

**Defaults** The default is 9600.

**Command Mode** Privileged EXEC mode

**Usage Guide** N/A

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

```
Ruijie# terminal speed 115200
```

**Related Commands**

| Command | Description |
| --- | --- |
| N/A | N/A |

**Platform Description** N/A

## 3.29 terminal width

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

**terminal width** *screen-width*

**terminal no width**

**Parameter Description**

| Parameter | Description |
| --- | --- |
| *screen-width* | Sets the screen width for the terminal, in the range from 0 to 256. |

**Defaults** The default is 79.

**Command Mode** Privileged EXEC mode

**Usage Guide** N/A

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

```
Ruijie# terminal width 10
```

**Related Commands**

| Command | Description |
| --- | --- |
| N/A | N/A |

**Platform Description** N/A

## 3.30 timeout login

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

command to restore the default setting.

**timeout login response** *seconds*

**no timeout login response**

**Parameter Description**

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

**Defaults** The default is 30.

**Command Mode** Line configuration mode

**Usage Guide** N/A

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

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

**Related Commands**

| Command | Description |
|---|---|
| N/A | N/A |

**Platform Description** N/A

## 3.31 transport input

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

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

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

**Parameter Description**

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

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

**Command Mode** Line configuration mode

**Usage Guide** N/A

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

```
Ruijie(config)# line vty 0 5
Ruijie(config-line)transport input ssh
```

**Related Commands**

| Command | Description |
| --- | --- |
| **show running** | Displays status information |

**Platform Description** N/A

## 3.32 vacant-message

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

**vacant-message** [ *c message c* ]

**no vacant-message**

**Parameter Description**

| Parameter | Description |
| --- | --- |
| *c* | Delimiter of the logout message, which is not allowed within the message. |
| *message* | Logout message. |

**Defaults** N/A

**Command Mode** Line configuration mode

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

**Configuration Examples** The following example sets the logout message to “Logout from the ruijie device”.

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

**Related**

| Command | Description |
| --- | --- |

**Commands**

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

**Platform Description** N/A

## 3.33 width

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

**width** *screen-width*

**no width**

**Parameter Description**

| Parameter | Description |
|---|---|
| *screen-width* | Sets the screen width for the line, in the range from 0 to 256, |

**Defaults** The default is 79.

**Command Mode** Line configuration mode

**Usage Guide** N/A

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

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

**Related Commands**

| Command | Description |
|---|---|
| N/A | N/A |

**Platform Description** N/A

# 4 File System Commands

## 4.1 cd

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

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

**Parameter Description**

| Parameter | Description |
|---|---|
| *filesystem:* | The URL of filesystem, followed by a colon (:). The filesystem includes **flash:**,**tmp:**. |
| *directory* | The path name. A file name starts with "/" is an absolute path. Otherwise, it is a relative path. |

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

**Command Mode** Privileged EXEC mode.

**Usage Guide**

**Configuration Examples** The following example enters the sata hardware.

```
Ruijie#pwd
flash:/
Ruijie#cd sata:
Ruijie#pwd
sata:/
```

**Related Commands**

| Command | Description |
|---|---|
| **pwd** | Displays the present word directory. |

**Platform Description** N/A.

## 4.2 copy

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

***copy*** *source-url destination-url*

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

The following table lists the URL:

| Prefix | Description |
|---|---|
| **running-config** | Running configuration file. |
| **startup-config** | startup configuration file. |
| **flash:** | local FLASH file system. |
| **tftp:** | The URL of TFTP network server, in the format as follows: **tftp**:[[//location]/directory]**/filename** |

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

```
 Ruijie#copy tftp://192.168.64.2/netconfig flash:/netconfig

Do you want to overwrite [/data/netconfig]? [Y/N]:y

Press Ctrl+C to quit

!

Copy success.
```

**Related Commands**

| Command | Description |
|---|---|
| **delete** | Deletes the file. |
| **rename** | Renames the file. |
| **dir** | Displays the file list of the specified directory. |

**Platform Description** N/A

## 4.3 delete

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

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

**Parameter Description**

| Parameter | Description |
|---|---|
| *filesystem:* | The URL of file system, followed by a colon (:). The file system includes **flash: tmp:**. |

| | |
|---|---|
| *file-url* | The file name containing the path. A file name starts with “/” is an absolute path. Otherwise, it is a relative path. |

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

**Command Mode** Privileged EXEC mode.

**Usage Guide**

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

```
Ruijie#pwd
flash:/
Ruijie#dir
Directory of flash:/
1   -rw-       336   Jan 03 2012 18:53:42  fstab
2   -rw-      4096   Jan 03 2012 12:32:09  rc.d
3   -rw-   10485760   Jan 03 2012 18:13:37  rpmdb
3 files, 0 directories
10,490,192 bytes total (13,192,656 bytes free)
Ruijie#delete flash:/fstab
Do you want to delete [flash:/fstab]? [Y/N]:y
Delete success.
Ruijie#dir
Directory of flash:/
1   -rw-      4096   Jan 03 2012 12:32:09  rc.d
2   -rw-   10485760   Jan 03 2012 18:13:37  rpmdb
2 files, 0 directories
```

10,489,856 bytes total (13,192,992 bytes free)

**Related Commands**

| Command | Description |
|---|---|
| **copy** | Copies the file. |
| **dir** | Displays the file list of the specified directory. |

**Platform Description** N/A

## 4.4 dir

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

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

**Parameter**

| Parameter | Description |
|---|---|

**Description**

| | |
|---|---|
| *filesystem* | The URL of file system, followed by a colon (:). The file system includes **flash:**, **tmp:**. |
| *directory* | The path name. A file name starts with "/" is an absolute path. Otherwise, it is a relative path. |

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

**Command Mode** Privileged EXEC mode.

**Usage Guide**

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

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

| Field | Description |
|---|---|
| 1, 2, 3… | Index number |
| -rw- | Permissions on a file include:<br>● d: directory<br>● r: read<br>● w: write<br>● x: executable |
| 10485760 | File size |
| rpmdb | File name |
| files | File number |
| directories | Directory number |
| total | Total size |
| free | Available space |

**Related Commands**

| Command | Description |
|---|---|
| **pwd** | Displays the present directory. |
| **cd** | Sets the present directory of the file system. |

**Platform Description** N/A.

## 4.5 erase

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

**erase** *filesystem*

| **Parameter Description** | **Parameter** | **Description** |
|---|---|---|
| | *filesystem*: | Name of the file system, followed by a colon (:). |

**Defaults** N/A

**Command Mode** Privileged EXEC mode

**Usage Guide** N/A

**Configuration Examples** The following example erases the USB filesystem.

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

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

**Platform Description** N/A

## 4.6 mkdir

Use this command to create a directory.

**mkdir** [ *filesystem*: ] *directory*

| **Parameter Description** | **Parameter** | **Description** |
|---|---|---|
| | *filesystem:* | The URL of file system, followed by a colon (:). The file system includes **flash:**, **tmp:**. |
| | *directory* | The path name. A file name starts with "/" is an absolute path. Otherwise, it is a relative path. |

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

**Command Mode** Privileged EXEC mode.

**Usage Guide**

**Configuration Examples** The following example creates a directory named newdir:

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

**Related Commands**

| Command | Description |
|---|---|
| **rmdir** | Deletes the directory. |
| **pwd** | Displays the present directory. |

**Platform Description** N/A

## 4.7 more

Use this command to display the content of a file.

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

**Parameter Description**

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

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

**Command Mode** Privileged EXEC mode

**Usage Guide** N/A

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

```
Ruijie#more flash:/netconfig
#
# The network configuration file. This file is currently only used in
# conjunction with the TI-RPC code in the libtirpc library.
#
# Entries consist of:
#
#      <network_id> <semantics> <flags> <protofamily> <protoname> \
#            <device> <nametoaddr_libs>
#
# The <device> and <nametoaddr_libs> fields are always empty in this
# implementation.
#
udp       tpi_clts     v    inet    udp    -      -
tcp       tpi_cots_ord  v    inet    tcp    -      -
udp6      tpi_clts     v    inet6   udp    -      -
tcp6      tpi_cots_ord  v    inet6   tcp    -      -
rawip     tpi_raw      -    inet    -      -      -
local     tpi_cots_ord  -    loopback  -      -      -
```

**Related Commands**

| Command | Description |
|---|---|
| N/A | N/A |

**Platform Description** N/A

## 4.8 pwd

Use this command to display the working path.

**pwd**

**Parameter Description**

| Parameter | Description |
|---|---|
| N/A. | N/A. |

**Defaults** N/A.

**Usage Guide**

**Configuration Examples** The following example displays the process of switching the working directory from flash: to sata:.

```
Ruijie#pwd
flash:/
Ruijie#cd sata:/
Ruijie#pwd
sata:/
```

**Related Commands**

| Command | Description |
|---|---|
| **cd** | Changes the file system in the present directory. |

**Platform Description** N/A.

## 4.9 rename

Use this command to move or rename the specified file.

***rename*** *src-url dst-url*

**Parameter Description**

| Parameter | Description |
|---|---|
| *src-url* | The source file URL to move. |
| *dst-url* | The URL of the destination file or directory. |

**Defaults** N/A.

**Command Mode** Privileged EXEC mode.

**Usage Guide** N/A

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

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

```
2   -rw-      4096   Jan 03 2012 12:32:09  rc.d
3   -rw-   10485760   Jan 03 2012 18:13:37  rpmdb
3 files, 0 directories
10,490,192 bytes total (13,192,656 bytes free)
```

**Related Commands**

| Command | Description |
|---|---|
| **delete** | Deletes the file. |
| **copy** | Copies the file. |

**Platform Description** N/A

## 4.10 rmdir

Use this command to delete an empty directory.

**rmdir** [ *filesystem*: ] *directory*

**Parameter Description**

| Parameter | Description |
|---|---|
| *filesystem*: | The URL of file system, followed by a colon (:). The file system includes **flash:**, **tmp:**. |
| *directory* | The path name. A file name starts with "/" is an absolute path. Otherwise, it is a relative path. |

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

**Command Mode** Privileged EXEC mode.

**Usage Guide**

**Configuration Examples** The following example deletes the null test directories.

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

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

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

**Platform Description** N/A.

## 4.11 show file systems

Use this command to display the file system information.

**show file systems**

| Parameter Description | Parameter | Description |
|---|---|---|
| | N/A. | N/A. |

**Defaults** N/A.

**Command Mode** N/A

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

**Configuration Examples** The following example displays the file system information:

```
Ruijie#show file systems
  Size(KB)      Free(KB)    Type   Flags  Prefixes
       NA           NA      ram    rw  tmp:
       NA           NA   network    rw  tftp:
     8192         2416     disk    rw  flash:
167772160    147772160     disk    rw  sata0:
  1048576       548576     disk    rw  usb0:
   262144       152144     disk    rw  sd0:
```

| Field | Description |
|---|---|
| Size(KB) | File system space, in the unit of KB. |
| Free(KB) | Available file system space, in the unit of KB. |
| Type | File system type |
| Flags | Permissions on the file system include: |

| | |
|---|---|
| | • ro: read-only<br>• wo: write-only<br>• rw: read and write |
| Prefixes | File system prefix |

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

**Platform Description** N/A.

## 4.12 show mount

Use this command to display the mounted information.

**show mount**

| Parameter Description | Parameter | Description |
|---|---|---|
| | N/A | N/A |

**Defaults** N/A

**Command Mode** N/A

**Usage Guide** N/A

**Configuration Examples** The following example displays the mounted information.

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

| Field | Description |
|---|---|

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

**Related Commands**

| Command | Description |
|---|---|
| N/A | N/A |

**Platform Description** N/A

## 4.13 tree

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

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

**Parameter Description**

| Parameter | Description |
|---|---|
| *filesystem*: | The URL of file system, followed by a colon (:). The file system includes **flash:**,**tmp:**. |
| *directory* | The path name. A file name starts with “/” is an absolute path. Otherwise, it is a relative path. |

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

**Command Mode** Privileged EXEC mode

**Usage Guide** N/A

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

```
Ruijie#tree flash:/echo
+-- client_module
+-- client_userspace
+-- echo_cli.c
+-- echo_client.c
+-- echo_client.h
+-- echo_client.o
+-- echo_cli.o
+-- echo_flag.h
+-- echo.h
+-- echo.ko
```

```
+-- echo_server.h
+-- exec_set_echo.h
+-- exec_show_echo.h
+-- Makefile
+-- module
¦   +-- echo.ko
¦   +-- echo.mod.c
¦   +-- echo.mod.o
¦   +-- echo_module.c
¦   +-- echo_module.o
¦   +-- echo.o
¦   +-- echo_server.c
¦   +-- echo_server.o
¦   +-- echo_sysfs.c
¦   +-- echo_sysfs.h
¦   +-- echo_sysfs.o
¦   +-- Makefile
¦   +-- modules.order
¦   +-- Module.symvers
¦   +-- msg_fd.c
¦   +-- msg_fd.o
+-- readme
+-- server_module
+-- server_userspace
+-- sys_rgos.ko
+-- user_space
   +-- echo_server.c
   +-- echo_server.o
   +-- Makefile
   +-- msg_fd.c
   +-- msg_fd.o 10,490,132 bytes total (13,192,656 bytes free)
```

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

**Platform Description** N/A

## 4.14 verify

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

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

| **Parameter** | **Parameter** | **Description** |
|---|---|---|

**Description**

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

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

**Command Mode** Privileged EXEC mode.

**Usage Guide** N/A

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

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

The following example

**Related Commands**

| Command | Description |
|---|---|
| N/A | N/A |

**Platform Description** N/A

## 4.15 show disk

Use this command to display USB/Flash information.

**show disk** [ **usb** | **flash** ]

**Parameter Description**

| Parameter | Description |
|---|---|
| **flash** | Displays FLASH information. |
| **usb** | Displays USB information. |

**Defaults** N/A

**Command Mode** Privileged EXEC mode

**Usage Guide** N/A

**Configuration** The following example displays USB information.

**Examples**

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

The following example displays FLASH information.

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

**Related Commands**

| Command | Description |
|---|---|
| N/A | N/A |

**Platform Description** N/A

# 5 SNMP Commands

## 5.1 clear snmp locked-ip

Use this command to clear the source IP addresses which are locked after continuous SNMP authentication failures.

**clear snmp locked-ip** [ **ipv4** *ipv4-address* | **ipv6** *ipv6-address* ]

**Parameter Description**

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

**Defaults** N/A

**Command mode** Privileged EXEC mode.

**Usage Guide** Use this command to clear the source IP addresses which are locked after continuous SNMP authentication failures. You can clear the whole source IP address table or a specific source IP address.

After the source IP addresses locked are cleared, the SNMP packets with these source IP addresses could be authenticated again.

**Configuration Examples** The following example clears the whole source IP address table locked after continuous SNMP authentication failures.

```
Ruijie#clear snmp locked-ip
```

**Related Commands**

| Command | Description |
|---|---|
| N/A | N/A |

**Platform Description** N/A

## 5.2 no snmp-server

Use this command to disable the SNMP agent function.

**no snmp-server**

**Parameter Description**

| Parameter | Description |
| --- | --- |
| N/A | N/A |

**Defaults** SNMP agent is enabled by default.

**Command mode** Global configuration mode.

**Usage Guide** This command disables the SNMP agent services of all versions supported on the device.

**Configuration Examples** The following example disables the SNMP agent.

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

**Related Commands**

| Command | Description |
| --- | --- |
| N/A | N/A |

**Platform Description** N/A

## 5.3 show snmp

Use this command to display the SNMP configuration.

**show snmp** [ **mib** | **user** | **view** | **group** | **host | locked-ip | process-mib-time** ]

**Parameter Description**

| Parameter | Description |
| --- | --- |
| **mib** | Displays the SNMP MIBs supported. |
| **user** | Displays the SNMP user information. |
| **view** | Displays the SNMP view information. |
| **group** | Displays the SNMP user group information. |
| **host** | Displays the explicit host configuration. |
| **locked-ip** | Displays the source IP addresses locked after continuous SNMP authentication failures. |
| **process-mib-time** | Displays the MIB node requiring the longest processing time. |

**Defaults** N/A

**Command mode** Privileged EXEC mode.

**Usage Guide** N/A

**Configuration Examples** The example below displays the SNMP configuration:

```
Ruijie# show snmp
Chassis: 60FF60
0 SNMP packets input
       0 Bad SNMP version errors
       0 Unknown community name
       0 Illegal operation for community name supplied
       0 Encoding errors
       0 Number of requested variables
       0 Number of altered variables
       0 Get-request PDUs
       0 Get-next PDUs
       0 Set-request PDUs
0 SNMP packets output
       0 Too big errors (Maximum packet size 1472)
       0 No such name errors
       0 Bad values errors
       0 General errors
       0 Response PDUs
       0 Trap PDUs
SNMP global trap: disabled
SNMP logging: disabled
SNMP agent: enabled
```

**Related Commands**

| Command | Description |
| --- | --- |
| **snmp-server chassis-id** | Specifies the SNMP system sequence number. |

**Platform Description** N/A

## 5.4 snmp trap link-status

Use this command to enable the interface to send link traps. Use the **no** form of this command to disable the interface to send link traps.

**snmp trap link-status**

**no snmp trap link-status**

**Parameter Description**

| Parameter | Description |
| --- | --- |
| N/A | N/A |

**Defaults** Sending link traps on the interface is enabled by default. If the interface link status changes, SNMP

link traps will be sent.

**Command mode** Interface configuration mode

**Usage Guide** This command can be configured on the Ethernet interface, aggregate ports and SVI interfaces.

**Configuration Examples** The following example disables the interface to send link traps.

```
Ruijie(config)# interface gigabitEthernet 1/1
Ruijie(config-if-GigabitEthernet 1/1)# no snmp trap link-status
```

The following example enables the interface to send link traps.

```
Ruijie(config)# interface gigabitEthernet 1/1
Ruijie(config-if-GigabitEthernet 1/1)# snmp trap link-status
```

**Related Commands**

| Command | Description |
|---|---|
| N/A | N/A |

**Platform Description** N/A

## 5.5 snmp-server authentication attempt

Use this command to configure the maximum number of continuous SNMP authentication failures, and specified the action policy for the authentication failure. Use the **no** form of this command to remove the limit of continuous SNMP authentication failures and the related action policies.

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

**no snmp-server authentication attempt** *times* **exceed** { **lock** | **lock-time** *minutes* | **unlock** }

**Parameter Description**

| Parameter | Description |
|---|---|
| *times* | The maximum number of continuous SNMP authentication failures. The range is from 1 to 10. |
| **exceed** | Indicates the action policy in the case that the maximum number of continuous SNMP authentication failures is exceeded. |
| **lock** | Indicates that the source IP address is permanently locked to be authenticated and can be unlocked only by the administrator's manual configuration. |
| **lock-time** *minutes* | Indicates that the source IP address is locked for a period of time. The *minutes* indicates the lock time, ranging from 1 to 65,535. The unit is minute. |
| **unlock** | Indicates that no action policy is configured for the authentication failed user, that is, the SNMP authentication for this user is allowed. |

**Defaults** SNMP attack prevention is disabled by default.

**Command mode** Global configuration mode

**Usage Guide** The IP address of the SNMP authentication failed user is added to the blacklist. When the maximum number of continuous SNMP authentication failures is exceeded, the system will perform the related authentication limit actions according the configured policy.:

1. For the permanently locked IP addresses: The source IP addresses can be authenticated only after the administrator unlock them manually.
2. For the IP addresses locked for a period time: The source IP addresses can be authenticated only after the lock time expires or the administrator unlock them manually.
3. For the unlocked IP addresses: The source IP address can pass the authentication as long as the correct community (for SNMPv1 and SNMPv2) or username (for SNMPv3) is used.

**Configuration Examples** The following example configures the maximum number of continuous SNMP authentication failures to 4, and sets the IP address lock time to 30 seconds.

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

**Related Commands**

| Command | Description |
|---|---|
| N/A | N/A |

**Platform Description** N/A

## 5.6 snmp-server cache enable

Use this command to enable MIB cache globally. Use the **no** form of this command to disable MIB cache.

**snmp-server cache enable**

**no snmp-server cache enable**

**Parameter Description**

| Parameter | Description |
|---|---|
| N/A | N/A |

**Defaults** MIB cache is disabled by default.

**Command mode** Global configuration mode

**Usage Guide** N/A

**Configuration Examples** The following example enables MIB cache globally.

```
Ruijie(config)# snmp-server cache enable
```

**Related Commands**

| Command | Description |
| --- | --- |
| N/A | N/A |

**Platform Description** N/A

## 5.7 snmp-server cache oid

Use this command to enable MIB cache for a specified node and configure the update interval for the MIB cache. Use the **no** form of this command to restore the default setting.

**snmp-server cache oid** *oid-string* [ **update-timer** *seconds* ]

**no snmp-server cache oid** *oid-string* [ **update-timer** ]

**Parameter Description**

| Parameter | Description |
| --- | --- |
| *oid-string* | Specifies a MIB node (OID name) |
| *seconds* | Configures the update interval for the MIB cache in seconds, in the range from 60 to 3600. |

**Defaults** MIB cache for a specified node is disabled by default.

The update interval for a specified node is consistent with the global update interval by default.

**Command mode** Global configuration mode

**Usage Guide** N/A

**Configuration Examples** The following example enables MIB cache for a specified node.

```
Ruijie(config)# snmp-server cache oid 1.3.6.1.4.1.4881.1.1.10.2.56.2.1.1.1
```

The following example sets the update interval for the MIB cache to 600 seconds.

```
Ruijie(config)# snmp-server cache oid 1.3.6.1.4.1.4881.1.1.10.2.56.2.1.1.1
    update-timer 600
```

**Related Commands**

| Command | Description |
| --- | --- |
| N/A | N/A |

**Platform** N/A

**Description**

## 5.8 snmp-server cache update-timer

Use this command to configure the update interval for the MIB cache globally. Use the **no** form of this command to restore the default setting.

**snmp-server cache update-timer** *seconds*

**no snmp-server cache update-timer**

**Parameter Description**

| Parameter | Description |
|---|---|
| *seconds* | Configures the update interval for the MIB cache in seconds, in the range from 60 to 3600. |

**Defaults** The default update interval is 300s.

**Command mode** Global configuration mode

**Usage Guide** N/A

**Configuration Examples** The following example sets the update interval for the MIB cache to 600s globally:

```
Ruijie(config)# snmp-server cache update-timer 600
```

**Related Commands**

| Command | Description |
|---|---|
| N/A | N/A |

**Platform Description** N/A

## 5.9 snmp-server chassis-id

Use this command to specify the SNMP chassis ID. Use the **no** form of this command to restore the default chassis ID.

**snmp-server chassis-id** *text*

**no snmp-server chassis-id**

**Parameter Description**

| Parameter | Description |
|---|---|
| *text* | SNMP chassis ID: numerals or characters. |

**Defaults** The default is 60FF60.

**Command mode** Global configuration mode.

**Usage Guide** The SNMP chassis ID is generally the serial number of the device to facilitate identification. The SNMP chassis ID can be displayed through the **show snmp** command.

**Configuration Examples** The following example specifies the SNMP chassis ID as 123456:

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

**Related Commands**

| Command | Description |
|---|---|
| **show snmp** | Displays the SNMP configuration. |

**Platform Description** N/A

## 5.10 snmp-server community

Use this command to specify the SNMP community access string. Use the **no** form of this command to remove the SNMP community access string.

**snmp-server community** [ 0 | 7 ] *string* [ **view** *view-name* ] [ [ **ro** | **rw** ] [ **host** *ipaddr* ] [ **ipv6** *ipv6-aclname* ] [ *aclnum* ] [ *aclname* ]

**no snmp-server community** [ 0 | 7 ] *string*

**Parameter Description**

| Parameter | Description |
|---|---|
| 0 | Indicates that the community string is in plaintext. |
| 7 | Indicates that the community string is in ciphertext. |
| *string* | Community string, which is the communication password between the NMS and the SNMP agent |
| *view-name* | View name |
| **ro** | Indicates that the NMS can only read the variables of the MIB. |
| **rw** | Indicates that the NMS can read and write the variables of the MIB. |
| *aclnum* | Access list number (1 to 199), which specifies the IPV4 addresses that are permitted to access the MIB. |
| *aclname* | Access list name, which specifies the IPV4 addresses that are permitted to access the MIB. |
| *ipv6-aclname* | IPv6 access list name, which specifies the IPv6 addresses that are permitted to access the MIB. |
| *ipaddr* | Specifies the IP address of the NMS to access the MIB. |

**Defaults** All communities are read only by default.

**Command mode** Global configuration mode.

**Usage Guide** This command is an essential command to enable the SNMP agent function, such as specifying the community attribute and IP addresses of NMS to access the MIB.
To disable the SNMP agent function, use the **no snmp-server** command.

**Configuration Examples** The following example defines a SNMP community access string named public, which can be read-only.

```
Ruijie(config)# snmp-server community public ro
```

**Related Commands**

| Command | Description |
| --- | --- |
| **access-list** | Defines an access list. |

**Platform Description** N/A

## 5.11 snmp-server contact

Use this command to specify the system contact string. Use the **no** form of this command to remove the system contact string.
**snmp-server contact** *text*
**no snmp-server contact**

**Parameter Description**

| Parameter | Description |
| --- | --- |
| *text* | Defines a system contact string. |

**Defaults** No system contact string is set by default.

**Command mode** Global configuration mode.

**Usage Guide** N/A

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

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

**Related Commands**

| Command | Description |
| --- | --- |
| **show snmp-server** | Displays the SNMP configuration. |
| **no snmp-server** | Disables the SNMP agent function. |

**Platform Description** N/A

## 5.12 snmp-server enable traps

Use this command to enable the SNMP agent to send the SNMP trap massage to NMS. Use the **no** form of this command to disable the SNMP agent to send the SNMP trap massage to NMS.

**snmp-server enable traps** [ *notification-type* ]

**no snmp-server enable traps**

**Parameter Description**

| Parameter | Description |
|---|---|
| *notification-type* | Specifies the type of trap messages.<br>snmp: SNMP trap message<br>bridge: Bridge trap message.<br>mac-notification: MAC trap message.<br>ospf: OSPF trap message.<br>urpf: uRPF trap message.<br>vrrp: VRRP trap message.<br>web-auth: Web authentication trap message. |

**Defaults** Sending trap message to the NMS is disabled by default.

**Command mode** Global configuration mode.

**Usage Guide** This command must be used together with the **snmp-server host** command to send the trap message. Specifying no trap type indicates all trap messages are sent.

**Configuration Examples** The following example enables the SNMP agent to send the SNMP trap message.

```
Ruijie(config)# snmp-server enable traps snmp
Ruijie(config)# snmp-server host 192.168.12.219 public snmp
```

**Related Commands**

| Command | Description |
|---|---|
| **snmp-server host** | Specifies the SNMP host to send the SNMP trap message. |

**Platform Description** N/A

## 5.13 snmp-server flow-control

Use this command to configure the SNMP flow control. Use the **no** form of this command to restore the default setting.

**snmp-server flow-control pps** [ *count* ]

**no snmp-server flow-control pps**

**Parameter Description**

| Parameter | Description |
|---|---|
| *count* | Indicates the number of SNMP requests processed per second, ranging from 50 to 65,535. |

**Defaults** The default count is 150.

**Command mode** Global configuration mode.

**Usage Guide** N/A

**Configuration Examples** The following example configures the number of SNMP requests processed per second to 200.

```
Ruijie(config)# snmp-server flow-control pps 200
```

**Related Commands**

| Command | Description |
|---|---|
| N/A | N/A |

**Platform Description** N/A

## 5.14 snmp-server group

Use this command to configure a new SNMP group**.** Use the **no** form of this command to remove a specified SNMP group.

**snmp-server group** *groupname* { **v1** | **v2c** | **v3** { **auth** | **noauth** | **priv** } } [ **read** *readview* ] [ **write** *writeview* ] [ **access** { [ **ipv6** *ipv6_aclname* | *aclnum* | *aclname* } ]

**no snmp-server group** *groupname* {**v1** | **v2c** | **v3** { **auth** | **noauth** | **priv** } }

**Parameter Description**

| Parameter | Description |
|---|---|
| **v1** \| **v2c** \| **v3** | Specifies the SNMP version |
| **auth** | Specifies authentication of a packet without encrypting it. This applies to SNMPv3 only. |
| **noauth** | Specifies no authentication a packet. This applies to SNMPv3 only. |

| | |
|---|---|
| **priv** | Specifies authentication of a packet with encryption. This applies to SNMPv3 only. |
| *readview* | Specifies a read-only view for the SNMP group. This view enables you to view only the contents of the agent. |
| *writeview* | Specifies a write view for the SNMP group. This view enables you to enter data and configure the contents of the agent. |
| *aclnum* | Access list number, which specifies the IPV4 addresses that are permitted to access the MIB. |
| *aclname* | Name of the access list, which specifies the IPV4 addresses that are permitted to access the MIB. |
| *ipv6_aclname* | Name of the IPv6 access list, which specifies the IPv6 addresses that are permitted to access the MIB. |

**Defaults** No SNMP groups are configured by default.

**Command mode** Global configuration mode.

**Usage Guide** N/A

**Configuration Examples** The following example configures a new SNMP group.

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

**Related Commands**

| Command | Description |
|---|---|
| **show snmp group** | Displays the SNMP group configuration. |

**Platform Description** N/A

## 5.15 snmp-server host

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

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

**no snmp-server host** { *host-addr* | **ipv6** *ipv6-addr* } [ **traps | informs** ] [ **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) |

| | |
|---|---|
| **trap \| informs** | Enables the host to send the SNMP notification as traps or informs. |
| **version** | SNMP version: V1, V2C or V3 |
| **auth** \| **noauth** \| **priv** | Security level of SNMPv3 users |
| *community-string* | Community string or username (SNMPv3 version) |
| *port-num* | Port of the SNMP host |
| *notification-type* | The type of the SNMP trap message, such as **snmp**.<br>If no type of the SNMP trap message is specified, all types of the SNMP trap message will be included. |

**Defaults** No SNMP host is specified by default.

**Command mode** Global configuration mode.

**Usage Guide** This command must be used together with the **snmp-server enable traps** command to send the SNMP trap messages to NMS.
Multiple SNMP hosts can be configured to receive the SNMP trap messages. One host can use different combinations of the types of the SNMP trap message, but the last configuration for the same host will overwrite the previous configurations. In other words, to send different SNMP trap messages to the same host, different combination of SNMP trap messages can be configured.

**Configuration Examples** The following example specifies an SNMP host to receive the SNMP event trap:

```
Ruijie(config)# snmp-server host 192.168.12.219 public snmp
```

**Related Commands**

| Command | Description |
|---|---|
| **snmp-server enable traps** | Enables the SNMP agent to send the SNMP trap message. |

**Platform Description** N/A

## 5.16 snmp-server inform

Use this command to configure the resend times for inform requests and the inform request timeout**.**
Use the **no** form of this command to restore the default settings.
**snmp-server inform** [ **retries** *retry-time* | **timeout** *time* ]
**no snmp-server inform**

**Parameter Description**

| Parameter | Description |
|---|---|
| *retry-num* | Specifies the resend times for inform requests, ranging from 0 to 255. |
| *time* | Specifies the inform request timeout, ranging from 0 to 21,474,836. |

**Defaults** The default *retry-num* is 3, and the default **timeout** *time* is 15 seconds.

**Command mode** Global configuration mode.

**Usage Guide** N/A

**Configuration Examples** The following example configures the resend times of inform requests to 5.

```
Ruijie(config)# snmp-server inform retries 5
```

The following example configures the inform request timeout to 20 seconds.

```
Ruijie(config)# snmp-server inform timeout 20
```

**Related Commands**

| Command | Description |
| --- | --- |
| N/A | N/A |

**Platform Description** N/A

## 5.17 snmp-server location

Use this command to set the system location string. Use the **no** form of this command to remove the system location string.

**snmp-server location** *text*

**no snmp-server location**

**Parameter Description**

| Parameter | Description |
| --- | --- |
| *text* | String that describes the system location information. |

**Defaults** No system location string is set by default.

**Command mode** Global configuration mode.

**Usage Guide** N/A

**Configuration Examples** The following example sets the system location information:

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

**Related**

| Command | Description |
| --- | --- |

**Commands**

| | |
|---|---|
| **snmp-server contact** | Sets the system contact information. |

**Platform Description** N/A

## 5.18 snmp-server net-id

Use this command to configure the network element coding information of the device. Use the **no** form of this command to remove the network element coding information.

**snmp-server net-id** *text*

**no snmp-server net-id**

**Parameter Description**

| Parameter | Description |
|---|---|
| *text* | Configures the network element coding information of the device. The text length ranges from 1 to 255. The text is case-sensitive, and may contain spaces. |

**Defaults** No network element coding information is configured by default.

**Command mode** Global configuration mode.

**Usage Guide** N/A

**Configuration Examples** The following example configures the network element coding text to FZ_CDMA_MSC1.

```
Ruijie(config)# snmp-server net-id FZ_CDMA_MSC1
```

**Related Commands**

| Command | Description |
|---|---|
| N/A | N/A |

**Platform Description** N/A

## 5.19 snmp-server packetsize

Use this command to specify the largest size of the SNMP packet. Use the **no** form of this command to restore the default value.

**snmp-server packetsize** *byte-count*

**no snmp-server packetsize**

**Parameter Description**

| Parameter | Description |
| --- | --- |
| *byte-count* | Packet size. The range is from 484 to 17,876 bytes |

**Defaults** The default is 1,472 bytes.

**Command mode** Global configuration mode.

**Usage Guide** The following example specifies the largest size of SNMP packet as 1,492 bytes:

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

**Configuration Examples** N/A

**Related Commands**

| Command | Description |
| --- | --- |
| **snmp-server queue-length** | Specifies the length of the message queue for each SNMP trap host. |

**Platform Description** N/A

## 5.20 snmp-server queue-length

Use this command to specify the length of the message queue for each SNMP trap host. Use the **no** form of this command to restore the default value.

**snmp-server queue-length** *length*

**no snmp-server queue-length**

**Parameter Description**

| Parameter | Description |
| --- | --- |
| *length* | Queue length. The range is from 1 to 1000. |

**Defaults** The default is 100.

**Command mode** Global configuration mode.

**Usage Guide** Use this command to adjust the length of message queue for each SNMP trap host for the purposes of controlling the speed of sending the SNMP trap messages. The max speed is four messages per second.

**Configuration** The following example specifies the length of message queue as 4.

**Examples**

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

**Related Commands**

| Command | Description |
| --- | --- |
| **snmp-server packetsize** | Specifies the largest size of the SNMP packet. |

**Platform Description** N/A

## 5.21 snmp-server system-shutdown

Use this command to enable the SNMP message reload function. Use the **no** form of this command to disable the SNMP message reload function.

**snmp-server system-shutdown**

**no snmp-server system-shutdown**

**Parameter Description**

| Parameter | Description |
| --- | --- |
| N/A | N/A |

**Defaults** The SNMP message reload function is disabled by default.

**Command mode** Global configuration mode.

**Usage Guide** Use this command to enable the SNMP message reload function which may enable the system to send the device reload traps to the NMS before the device is reloaded or rebooted.

**Configuration Examples** The following example enables the SNMP message reload function:

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

**Related Commands**

| Command | Description |
| --- | --- |
| N/A | N/A |

**Platform Description** N/A

## 5.22 snmp-server trap-format private

Use this command to configure the SNMP traps with private fields. Use the **no** form of this command to restore the default trap format.

**snmp-server trap-format private**

**no snmp-server trap-format private**

**Parameter Description**

| Parameter | Description |
| --- | --- |
| N/A | N/A |

**Defaults** The private field is not carried in the SNMP trap by default.

**Command mode** Global configuration mode.

**Usage Guide** Use this command to configure the SNMP trap format with the private field. Currently, the supported data in the private field is alarm occurrence time. For the specific data type and range of each field, refer to RUIJIE-TRAP-FORMAT-MIB.mib file.
This command does not work if the traps are sent with SNMPv1.

**Configuration Examples** The following example configures the SNMP trap format with the private field.

```
Ruijie(config)# snmp-server trap-format private
```

**Related Commands**

| Command | Description |
| --- | --- |
| N/A | N/A |

**Platform Description** N/A

## 5.23 snmp-server trap-source

Use this command to specify the source interface of the SNMP trap message. Use the **no** form of this command to restore the default value.
**snmp-server trap-source** *interface*
**no snmp-server trap-source**

**Parameter Description**

| Parameter | Description |
| --- | --- |
| *interface* | Specifies the source interface of the SNMP trap messages. |

**Defaults** By default, the IP address of the interface from which the SNMP packet is sent is just the source address.

**Command mode** Global configuration mode.

**Usage Guide** For easy management and identification, you can use this command to fix a local IP address as the SNMP source address.

**Configuration Examples** The following example specifies the IP address of Ethernet interface 0/1 as the source address of the SNMP trap message:

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

**Related Commands**

| Command | Description |
|---|---|
| **snmp-server enable traps** | Enables t the SNMP agent to send the SNMP trap massage to NMS. |
| **snmp-server host** | Specifies the NMS host to send the SNMP trap message. |

**Platform Description** N/A

## 5.24 snmp-server trap-timeout

Use this command to define the retransmission timeout time of the SNMP trap message. Use the **no** form of this command to restore the default value.

**snmp-server trap-timeout** *seconds*

**no snmp-server trap-timeout**

**Parameter Description**

| Parameter | Description |
|---|---|
| *seconds* | Timeout ( in seconds) of retransmit the SNMP trap message. The range is from 1 to 1,000. |

**Defaults** The default is 30 seconds.

**Command mode** Global configuration mode.

**Usage Guide** N/A

**Configuration Examples** The following example specifies the timeout period as 60 seconds.

```
Ruijie(config)# snmp-server trap-timeout 60
```

**Related Commands**

| Command | Description |
|---|---|
| **snmp-server queue-length** | Specifies the length of message queue for the SNMP trap host. |

| | |
|---|---|
| **snmp-server host** | Specifies the NMS host to send the SNMP trap message. |
| **snmp-server trap-source** | Specifies the source address of the SNMP trap message. |

**Platform Description** N/A

## 5.25 snmp-server udp-port

Use this command to specify a port to receive SNMP packets**.** Use the **no** form of this command to restore the default setting.

**snmp-server udp port** *port-number*

**no snmp-server udp port**

**Parameter Description**

| Parameter | Description |
|---|---|
| *port-number* | Specifies a port to receive the SNMP packets. |

**Defaults** The default is 161.

**Command mode** Global configuration mode.

**Usage Guide** N/A

**Configuration Examples** The following example specifies port 15000 to receive the SNMP packets.

```
Ruijie(config)# snmp-server udp-port 15000
```

**Related Commands**

| Command | Description |
|---|---|
| N/A | N/A |

**Platform Description** N/A

## 5.26 snmp-server user

Use this command to configure a new user to an SNMP group**.** Use the **no** form of this command to remove a user from an SNMP group.

**snmp-server user** *username groupname* { **v1** | **v2c** | **v3** [ **encrypted** ] [ **auth** { **md5** | **sha** } *auth-password* ] [ **priv des56** *priv-password* ] } [ **access** { [ **ipv6** *ipv6_aclname* ] [ *aclnum* | *aclname* } ] ]

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

**Parameter Description**

| Parameter | Description |
|---|---|
| *username* | Name of the user on the host that connects to the agent. |
| *groupname* | Name of the group to which the user belongs. |
| **v1 \| v2c \| v3** | Specifies the SNMP version. But only SNMPv3 supports the following security parameters. |
| **encrypted** | Specifies whether the password appears in cipher text.<br>In cipher text format, you need to enter continuous hexadecimal numeric characters. Note that the authentication password of MD5 has a length of 16 bytes, while that of SHA has a length of 20 bytes. Two characters make a byte. The encrypted key can be used only by the local SNMP engine on the switch. |
| **auth** | Specifies which authentication level should be used. |
| *auth-password* | Password string (no more than 32 characters) used by the authentication protocol. The system will change the password to the corresponding authentication key. |
| **priv** | Encryption mode. des56 refers to 56-bit DES encryption protocol.<br>*priv-password*: password string (no more than 32 characters) used for encryption. The system will change the password to the corresponding encryption key. |
| *priv-password* | Password for encryption (no more than 32 characters). |
| **md5** | Enables the MD5 authentication protocol. While the **sha** enables the SHA authentication protocol. |
| *aclnumber* | Access list number, which specifies the IPV4 addresses that are permitted to access the MIB. |
| *aclname* | Name of the access list, which specifies the IPV4 addresses that are permitted to access the MIB. |
| *ipv6_aclname* | Name of the IPv6 access list, which specifies the IPv6 addresses that are permitted to access the MIB. |

**Defaults** No user is configured by default.

**Command mode** Global configuration mode.

**Usage Guide** N/A

**Configuration Examples** The following example configures an SNMPv3 user with MD5 authentication and DES encryption:

```
Ruijie(config)# snmp-server user user-2 mib2user v3 auth md5 authpassstr priv des56 despassstr
```

**Related Commands**

| Command | Description |
| --- | --- |
| **show snmp user** | Displays the SNMP user configuration. |

**Platform Description** N/A

## 5.27 snmp-server view

Use this command to configure an SNMP view**.** Use the **no** form of this command to remove an SNMP view.

**snmp-server view** *view-name oid-tree* { **include** | **exclude** }

**no snmp-server view** *view-name* [ *oid-tree* ]

**Parameter Description**

| Parameter | Description |
| --- | --- |
| *view-name* | View name |
| *oid-tree* | Specifies the MIB object to associate with the view. |
| **include** | Includes the sub trees of the MIB object in the view. |
| **exclude** | Excludes the sub trees of the MIB object from the view. |

**Defaults** By default, a view is set to access all MIB objects.

**Command mode** Global configuration mode.

**Usage Guide** N/A

**Configuration Examples** The following example sets a view that includes all MIB-2 sub-trees (oid is 1.3.6.1).

```
Ruijie(config)# snmp-server view mib2 1.3.6.1 include
```

**Related Commands**

| Command | Description |
| --- | --- |
| **show snmp view** | Displays the SNMP view configuration. |

**Platform** N/A

**Description**

# 6 HTTP Service Commands

## 6.1 enable service web-server

Use this command to enable the HTTP service function.

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

**enable service web-server** [ **http** | **https** | **all** ]

**no enable service web-server** [ **http** | **https** ]

**default enable service web-server** [ **http** | **https** ]

**Parameter Description**

| Parameter | Description |
|---|---|
| **http** | Enables the HTTP service. |
| **https** | Enables the HTTPS service. |
| **all** | Enables both the HTTP service and the HTTPS service. |

**Defaults** By default, the HTTP service function is disabled.

**Command mode** Global configuration mode.

**Usage Guide** If run a command ends with the keyword **all** or without keyword, it indicates enabling both the HTTP service and the HTTPS service; if run a command ends with keyword **http**, it indicates enabling the HTTP service; if run a command ends with keyword **https**, it indicates enabling the HTTPS service. Use the command **no enable service web-server** to disable the corresponding HTTP service.

**Configuration Examples** The following example enables both the HTTP service and the HTTPS service:

```
Ruijie#configure terminal
Ruijie(config)#enable service web-server
```

**Related Commands**

| Command | Description |
|---|---|
| N/A | N/A |

**Platform Description** N/A

## 6.2 http port

Use this command to configure the HTTP port number.

Use the **no** form of this command to restore the default HTTP port number.

**http port** *port-number*
**no http port**

**Parameter Description**

| Parameter | Description |
| --- | --- |
| *port-number* | Configures the HTTP port number. The value includes 80, 1025 to 65,535. |

**Defaults** The default HTTP port number is 80.

**Command mode** Global configuration mode.

**Usage Guide** Use this command to configure the HTTP port number.

**Configuration Examples** The following example configures the HTTP port number as 8080:.

```
Ruijie(config)#http port 8080
```

**Related Commands**

| Command | Description |
| --- | --- |
| N/A | N/A |

**Platform Description** N/A

## 6.3 http secure-port

Use this command to configure the HTTPS port number.
Use the **no** form of this command to restore the default HTTPS port number.
**http secure-port** *port-number*
**no http secure-port**

**Parameter Description**

| Parameter | Description |
| --- | --- |
| *port-number* | Configures the HTTPS port number. The value includes 443, 1025 to 65,535. |

**Defaults** The default HTTP port number is 443.

**Command mode** Global configuration mode.

**Usage Guide** Use this command to configure the HTTPS port number.

**Configuration Examples** The following example configures the HTTPS port number as 4443:

```
Ruijie#configure terminalRuijie(config)#http secure-port 4443
```

**Related Commands**

| Command | Description |
|---|---|
| **enable service web-server** | Enables the HTTP service. |
| **show web-server status** | Displays the configuration and status of the Web service. |

**Platform Description** N/A

## 6.4 show web-server status

Use this command to display the configuration and status of the Web service.

**show web-server status**

**Parameter Description**

| Parameter | Description |
|---|---|
| N/A | N/A |

**Defaults** N/A

**Command mode** Privileged EXEC mode

**Usage Guide** N/A

**Configuration Examples** The following example displays the configuration and status of the Web service:

```
Ruijie#show web-server status
http server status : enabled
http server port : 80
https server status: enabled
https server port: 443
```

**Related Commands**

| Command | Description |
|---|---|
| **enable service web-server** | Enables the HTTP service. |
| **http port** | Configures the HTTP port number. |
| **http secure-port** | Configures the HTTPS port number. |

**Platform Description** N/A

## 6.5 upgrade web

Use this command to upgrade the Web package in local file system.

**upgrade web** *uri*

**Parameter Description**

| Parameter | Description |
|---|---|
| *uri* | The storage path of the Web package. |

**Defaults** N/A

**Command mode** Privileged EXEC mode

**Usage Guide** Please use the **copy** command to copy the Web package into the file system before you use this command to upgrade the Web package.

**Configuration Examples** The following example copies a Web package into the file system and upgrades the package.

```
Ruijie#copy tftp://192.168.23.24/web.upd flash:/web.upd
Ruijie#upgrade web flash:/web.upd
```

**Related Commands**

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

**Platform Description** N/A

## 6.6 upgrade web download

Use this command to download the Web package from the TFTP server and upgrade the package automatically.

**upgrade web download tftp:** *path*

**Parameter Description**

| Parameter | Description |
|---|---|
| **tftp:** *path* | *path* indicates the storage path of the Web package on the TFTP server.<br>**tftp** indicates the system downloads the Web package from the TFTP server through the physical port and upgrades the Web package automatically. |

**Defaults** N/A

**Command mode** Privileged EXEC mode.

**Usage Guide** N/A

**Configuration Examples** The following example downloads a Web package form the TFTP server and upgrade the package automatically.

```
Ruijie#upgrade web download tftp://192.168.23.24/web.upd
```

**Related Commands**

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

**Platform Description** N/A

## 6.7 webmaster level

Use this command to configure the username and password for Web login authentication. Use the **no** form of this command to restore the default setting.

**webmaster level** *privilege-level* **username** *name* **password** { *password* | [ **0 | 7** ] *encrypted-password* }

**no webmaster level** *privilege-level* [ **username** name ]

**Parameter Description**

| Parameter | Description |
|---|---|
| *privilege-level* | Configures the user privilege-level. |
| *name* | Username. |
| *password* | Password. |
| **0** \| **7** | Password type; 0 indicates plaintext, 7 indicates ciphertext. |
| *encrypted-password* | Password text. |

**Defaults** By default, two users are configured.

1. User1 is configured with privilege level 0, username of admin and plaintext password of admin.
2. User2 is configured with privilege level 2, username of guest and plaintext password of guest.

**Command mode** Global configuration mode.

**Usage Guide** When HTTP is enabled, users can log in to the Web interface only after being authenticated. Use this command to configure the username and password for Web login authentication.

Use the **no webmaster level** *privilege-level* command to delete all the usernames and passwords with a specified *privilege-level.*

Use the **no webmaster level** *privilege-level* **username** *name* command to delete the specified username and password.

Usernames and passwords come with three permission levels, each of which includes at most 10 usernames and passwords.

**Configuration Examples**

The following example configures the username and password for Web login authentication,

```
Ruijie#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Ruijie(config)#webmaster level 0 username ruijie password admin
```

**Related Commands**

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

**Platform Description**

N/A

# 7 Syslog Commands

## 7. 1 clear logging

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

**clear logging**

**Parameter Description**

| Parameter | Description |
|---|---|
| N/A | N/A |

**Defaults** N/A

**Command Mode** Privileged EXEC mode

**Usage Guide** This command clears the log packets from the memory buffer. You cannot clear the statistics of the log packets.

**Configuration Examples** The following example clears the log packets from the memory buffer.

```
Ruijie# clear logging
```

**Related Commands**

| Command | Function |
|---|---|
| **logging on** | Turns on the log switch. |
| **show logging** | Displays the logs in the buffer. |
| **logging buffered** | Records the logs in the memory buffer. |

**Platform Description** N/A

## 7.2 logging

Use this command to send the log message to the specified syslog server.

**logging** { *ip-address* | **ipv6** *ipv6-address* } [ **udp-prot** *port* ]

Use this command to delete the specified syslog server.

**no logging** { *ip-address* ] | **ipv6** *ipv6-address* }

Use this command to restore the default port 514.

**no logging** { *ip-address*] | **ipv6** *ipv6-address* } **udp-prot**

**Parameter Description**

| Parameter | Description |
|---|---|

| | |
|---|---|
| *ip-address* | **Sets** the IP address of the host receiving log messages. |
| *ipv6-address* | Sets the IPv6 address of the host receiving log messages. |
| **udp-port** *port* | Sets the port number of the host receiving log messages. The default is 514. |

**Defaults** No log message is sent to syslog server by default.

**Command Mode** Global configuration mode

**Usage Guide** This command is used to configure a syslog server to receive log messages from the device. You can configure up to five syslog servers, log messages are sent to all configured syslog servers simultaneously,

**Configuration Examples** The following example configures a syslog server with IP address 202.101.11.1.

```
Ruijie(config)# logging 202.101.11.1
```

The following example configures a syslog server with IP address 10.1.1.100 and port number 8099.

```
Ruijie(config)# logging 202.101.11.1 udp-port 8099
```

The following example configures a syslog server with IPv6 address AAAA:BBBB::FFFF.

```
Ruijie(config)# logging ipv6 AAAA:BBBB::FFFF
```

**Related Commands**

| Command | Description |
|---|---|
| N/A | N/A |

**Platform Description** N/A

## 7.3 logging buffered

Use this command to set the memory buffer parameters (log severity, buffer size) for logs at global configuration layer. Use the **no** form of the command to disable recording logs in the memory buffer. Use the **default** form of this command to restore the default setting.

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

**no logging buffered**

**default logging buffered**

**Parameter Description**

| Parameter | Description |
|---|---|
| *buffer-size* | The value ranges from 4 K to 128 K Bytes. |
| *level* | Severity of logs, from 0 to 7. The name of the severity or the numeral can be used. |

**Defaults** The buffer size is 4 K Bytes

The log severity is 7.

**Command Mode** Global configuration mode

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

The logs in the memory buffer are temporary, and will be cleared in case of device restart or the execution of the **clear logging** command in privileged user mode. To trace a problem, it is required to record logs in flash or send them to Syslog Server.

The log information is classified into the following 8 levels (Table 1):

**Table-1**

| Keyword | Level | Description |
|---|---|---|
| Emergencies | 0 | Emergency case, system cannot run normally |
| Alerts | 1 | Problems that need immediate remedy |
| Critical | 2 | Critical conditions |
| Errors | 3 | Error message |
| warnings | 4 | Alarm information |
| Notifications | 5 | Information that is normal but needs attention |
| informational | 6 | Descriptive information |
| Debugging | 7 | Debugging messages |

Lower value indicates higher level. That is, level 0 indicates the information of the highest level. When the level of log information to be displayed on devices is specified, the log information at or below the set level will be allowed to be displayed.

After running the system for a long time, modifying the log buffer size especially in condition of large buffer may fails due to the insufficent availble continuous memory. The failure message will be shown. It is recommended to modify the log buffer size as soon as the system starts.

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

```
Ruijie(config)# logging buffered 10000 6
```

**Related Commands**

| Command | Description |
|---|---|
| **logging on** | Turns on the log switch. |
| **show logging** | Displays the logs in the buffer. |
| **clear logging** | Clears the logs in the log buffer. |

**Platform Description** N/A

## 7.4 logging console

Use this command to set the severity of logs that are allowed to be displayed on the console in global configuration mode. Use the **no** form of this command to prohibit printing log messages on the console.

**logging console** [ *level* ]

**no logging console**

**Parameter Description**

| Parameter | Description |
|---|---|
| *level* | Severity of log messages, 0 to 7. The name of the severity or the numeral can be used. For the details of log severity, see table 1. |

**Defaults** The default is debugging (7).

**Command Mode** Global configuration mode

**Usage Guide** When a log severity is set, the log messages at or below that severity will be displayed on the console.
The **show logging** command displays the related setting parameters and statistics of the log.

**Configuration Examples** The following example sets the severity of log that is allowed to be displayed on the console as 6:

```
Ruijie(config)# logging console informational
```

**Related Commands**

| Command | Description |
|---|---|
| **logging on** | Turns on the log switch. |
| **show logging** | Displays the logs and related log configuration parameters in the buffer. |

**Platform Description** N/A

## 7.5 logging count

Use this command to enable the log statistics function in global configuration mode. Use the **no** form of this command to restore the default setting.

**logging count**

**no logging count**

**Parameter Description**

| Parameter | Description |
|---|---|
| N/A | N/A |

**Defaults** The log statistics function is disabled by default.

**Command Mode** Global configuration mode

**Usage Guide** This command enables the log statistics function. The statistics begins when the function is enabled. If you run the **no logging count** command, the statistics function is disabled and the statistics data is deleted.

**Configuration Examples** The following example enables the log statistics function:

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

**Related Commands**

| Command | Description |
|---|---|
| **show logging count** | Displays log information about modules of the system. |
| **show logging** | Displays basic configuration of log modules and log information in the buffer. |

**Platform Description** N/A

## 7.6 logging delay-send file

Use this command to set the name of the log file saved locally for delay sending. Use the no form of this command to restore the default setting.

**logging delay-send file flash**:*filename*

**no logging delay-send file**

**Parameter Description**

| Parameter | Description |
|---|---|
| **flash**:filename | Sets the name of the log file saved locally for delay sending. |

**Defaults** The default name format is as follows: file size_device IP address_index.txt. If you want to change the file name, the file sent to the remote server should be named as follows: prefix_ file size_device IP address_index.txt; the file saved locally should be named as follows: prefix_index.txt. The default prefix is syslog_ftp_server.

**Command Mode** Global configuration mode

**Usage Guide** The file name cannot contain special symbols including . \/ : * ” < > and |.
For example, the file name is log_server, file index 5, file size 1000B and device IP address 10.2.3.5. The log file sent to the remote server is named log_server_1000_10.2.3.5_5.txt and the log file saved locally is named log_server_5.txt.
If the device has an IPv6 address, the colon (:) in the IPv6 address is replaced by the hyphen (-).
For example, the is log_server, file index 6, file size 1000B and device IPv6 address 2001::1. The log file sent to the remote server is named log_server_1000_2001-1_6.txt and the log file saved locally is named log_server_6.txt.

**Configuration Examples** The following example sets the name of the log file saved locally to log_server.

```
Ruijie(config)# logging delay-send file flash:log_server
```

**Related Commands**

| Command | Description |
| --- | --- |
| N/A | N/A |

**Platform Description** N/A

## 7.7 logging delay-send interval

Use this command to set the interval at which log sending is delayed. Use the no form of this command to restore the default setting.

**logging delay-send interval** seconds

**no logging delay-send interval**

**Parameter Description**

| Parameter | Description |
| --- | --- |
| seconds | Sets the interval at which log sending is delayed, in the range from 600 to 65535 seconds. |

**Defaults** The default is 3600.

**Command Mode** Global configuration mode

**Usage Guide** N/A

**Configuration Examples** The following example sets the the interval at which log sending is delayed to 600 seconds.

```
Ruijie(config)# logging delay-send interval 600
```

**Related Commands**

| Command | Description |
| --- | --- |

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

**Platform Description** N/A

## 7.8 logging delay-send server

Use this command to configure the serve address and log sending mode. Use the no form of this command to restore the default setting.

**logging delay-send server** { *ip-address* | **ipv6** *ipv6-address* } **mode** { **ftp user** *username* **password** [ **0** | **7** ] *password* | **tftp** }

**no logging delay-send server** { *ip-address* | **ipv6** *ipv6-address* }

**Parameter Description**

| Parameter | Description |
|---|---|
| *ip-address* | Specifies the IP address of the server. |
| **ipv6** *ipv6-address* | Specifies the IPv6 address of the server. |
| *username* | Sets the FTP server username. |
| *password* | Sets the FTP server password. |
| **0** | (Optional) The password is displayed in plaintext. |
| **7** | The password are encrypted. |

**Defaults** This function is disabled by default,

**Command Mode** Global configuration mode

**Usage Guide** This command is used to specify an FTP/TFTP server to receive logs. You can configure five FTP/TFTP servers. Logs are sent to all configured servers simultaneously.

**Configuration Examples** The following example specifies an FTP server whose IP address is 192.168.23.12, username admin and password admin,

```
Ruijie(config)# logging delay-send server 192.168.23.12 mode ftp user admin password admin
```

The following example specifies a TFTP server whose IPv6 address is 2000::1.

```
Ruijie(config)# logging delay-send server ipv6 2000::1 mode tftp
```

**Related Commands**

| Command | Description |
|---|---|
| N/A | N/A |

**Platform Description** N/A

## 7.9 logging delay-send terminal

Use this command to enable delay in sending logs to console and remote terminal. Use the no form of this command to restore the default setting.

**logging delay-send terminal**

**no logging delay-send terminal**

**Parameter Description**

| Parameter | Description |
|---|---|
| N/A | N/A |

**Defaults** This function is disabled by default.

**Command Mode** Global configuration mode

**Usage Guide** N/A

**Configuration Examples** The following example enables delay in sending logs to console and remote terminal.

```
Ruijie(config)# logging delay-send terminal
```

**Related Commands**

| Command | Description |
|---|---|
| N/A | N/A |

**Platform Description** N/A

## 7.10 logging facility

Use this command to configure the device value of the log information in global configuration mode. Use the **no** form of the command to restore the default setting.

**logging facility** *facility-type*

**no logging facility**

**Parameter Description**

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

**Defaults** The default is 23 if the RFC5424 format is enabled (Local7, local use).
The default is 16 if the RFC5424 format is disabled (Local0, local use).

**Command** Global configuration mode

**Mode**

**Usage Guide** The following table (Table-2) is the possible device values of Syslog:

| Numerical Code | Facility |
|---|---|
| 0 (kern) | Kernel messages |
| 1 (user) | User-level messages |
| 2 (mail) | Mail system |
| 3 (daemon) | System daemons |
| 4 (auth1) | security/authorization messages |
| 5 (syslog) | Messages generated internally by syslogd |
| 6 (lpr) | Line printer subsystem |
| 7 (news) | USENET news |
| 8 (uucp) | Unix-to-Unix copy system |
| 9 (clock1) | Clock daemon |
| 10 (auth2) | security/authorization messages |
| 11 (ftp) | FTP daemon |
| 12 (ntp) | NTP subsystem |
| 13 (logaudit) | log audit |
| 14 (logalert) | log alert |
| 15 (clock2) | clock daemon |
| 16 (local0) | Local use |
| 17 (local1) | Local use |
| 18 (local2) | Local use |
| 19 (local3) | Local use |
| 20 (local4) | Local use |
| 21 (local5) | Local use |
| 22 (local6) | Local use |
| 23 (local7) | Local use |

The default device value of RGOS is 23 (local 7).

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

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

**Related Commands**

| Command | Description |
|---|---|
| **logging console** | Sets the severity of logs that are allowed to be displayed on the console. |

**Platform** N/A

**Description**

## 7.11 logging file

Use this command to save log messages in the log file, which can be saved in hardware disk, expanded FLASH. Use the no form of this command to restore the default setting,

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

**no logging file**

**Parameter Description**

| Parameter | Description |
|---|---|
| **flash** | Saves the log file in expanded FLASH. |
| **usb0** | Saves the log file in USB0. This parameter is supported by the device with one USB connector and the USB extension device. |
| *filename* | Sets the file name. The file type is omitted, which is fixed as txt. |
| *max-file-size* | Sets the maximum file size, in the range from 128K to 6M bytes, The default is 128K, |
| *level* | Sets the level of the log message saved in the log file, which can be either the level name or the level number. The default is 6. See Usage Guide for details. |

**Defaults** Log messages are not saved in expanded FLASH by default.

**Command Mode** Global configuration mode

**Usage Guide** You can save log messages in expanded FLASH if you don't want to transmit log messages on the network or there is no syslog server,

The log file cannot be configured with the suffix, which is fixed as txt.

If there is no expanded FLASH, the **logging file flash** command is hidden automatically and cannot be configured.

| Keyword | Level | Description |
|---|---|---|
| Emergencies | 0 | Emergency case. The system fails to run. |
| Alerts | 1 | Problem that call for immediate solution. |
| Critical | 2 | Critical message. |
| Errors | 3 | Error message. |
| warnings | 4 | Alarm message. |
| Notifications | 5 | message that is normal but calls for attention. |

| | | |
|---|---|---|
| informational | 6 | Descriptive message. |
| Debugging | 7 | Debugging message |

**Configuration Examples** The following example saves the log message in expanded FLASH and sets file name, file size and log level to syslog.txt, 128K and 6 respectively.

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

**Related Commands**

| Command | Description |
|---|---|
| N/A | N/A |

**Platform Description** N/A

## 7.12 logging flash flush

Use this command to write log messages in the system buffer into the flash file immediately.

**logging flash flush**

**Parameter Description**

| Parameter | Description |
|---|---|
| N/A | N/A |

**Defaults** N/A

**Command Mode** Global configuration mode

**Usage Guide** In general, the log messages are cached in the log buffer. Only when the buffer is full or the timer expires are log messages written into the flash file. This command is used to write log messages in the system buffer into the flash file immediately.

The **logging flash flush** command takes effect only once for each configuration. The log messages cached in the buffer are written into the flash file immediately after configuration.

**Configuration Examples** The following example writes log messages in the system buffer into the flash file immediately.

```
Ruijie(config)# logging flash flush
```

**Related Commands**

| Command | Description |
|---|---|
| N/A | N/A |

**Platform** N/A

**Description**

## 7.13 logging flash interval

Use this command to set the interval to write log messages into the flash file, Use the no form of this command to restore the default setting.

**logging flash interval** *seconds*

**no logging flash interval**

**Parameter Description**

| Parameter | Description |
|---|---|
| **interval** *seconds* | The interval to write log messages into the flash file, in the range from 1 to 57840 in the unit of seconds. |

**Defaults** The default is 3600.

**Command Mode** Global configuration mode

**Usage Guide** This command is used to set the interval to write log messages into the flash file. The timer starts after configuration, If you want to restore the interval to 3600 seconds, use the no logging flash interval command.

To avoid writing log messages into the flash file too frequently, it is not recommended to set a short interval.

**Configuration Examples** The following example sets the interval to write log messages into the flash file to 300 seconds.

```
Ruijie(config)# logging flash interval 300
```

**Related Commands**

| Command | Description |
|---|---|
| N/A | N/A |

**Platform Description** N/A

## 7.14 logging filter direction

Use this command to filter the log messages destined to a certain direction. Use the no form of this command to restore the default setting.

**logging filter direction** { **all** | **buffer** | **file** | **server** | **terminal** }

**no logging filter direction** { **all** | **buffer** | **file** | **server** | **terminal** }

**Parameter Description**

| Parameter | Description |
| --- | --- |
| **all** | Log messages destined to all directions are filtered, including console, VTY terminal, log buffer, log file and log server. |
| **buffer** | Log messages destined to the log buffer are filtered, including log messages displayed by running the show logging command. |
| **file** | Log messages destined to the log file are filtered. |
| **server** | Log messages destined to the log server are filtered. |
| **terminal** | Log messages destined to the console and the VTY terminal (including Telnet and SSH). |

**Defaults** Log messages destined to all directions are filtered by default.

**Command Mode** Global configuration mode

**Usage Guide** In general, log messages destined to all directions are filtered, including console, VTY terminal, log buffer, log file and log server. If you want to filter log messages destined to a certain direction, the terminal for instance, configure the terminal parameter.

**Configuration Examples** The following example filters log messages destined to the terminal (including the console and the VTY terminal).

```
Ruijie(config)# logging filter direction terminal
```

**Related Commands**

| Command | Description |
| --- | --- |
| N/A | N/A |

**Platform Description** N/A

## 7.15 logging filter type

Use this command to configure the filter type of log messages. Use the no form of this command to restore the default setting.

**logging filter type** { **contains-only** | **filter-only** }

**no logging filter type**

**Parameter Description**

| Parameter | Description |
| --- | --- |
| **contains-only** | The log message containing the key word of the filter rule is printed. |
| **filter-only** | The log message containing the key word of the filter rule is filtered. |

**Defaults** The default filter type is filter-only.

**Command Mode** Global configuration mode

**Usage Guide** When too many log messages are printed, the terminal screen keeps being refreshed. If you are not concerned with these log messages, use the “filter-only” filter type to filter the log messages,
If you are concerned with certain log messages, use the “contains-only” filter type to print log messages containing the key word of the filter rule, so as to monitor whether certain events happen.

In real operation, the contains-only and the fitler-only filter types cannot be configured at the same time.

If you configure the filter direction and the filter type without configuring the filter rule, the log messages are not filtered.

**Configuration Examples** The following example sets the filter type to contains-only.

```
Ruijie(config)# logging filter type contains-only
```

**Related Commands**

| Command | Description |
| --- | --- |
| N/A | N/A |

**Platform Description** N/A

## 7.16 logging filter rule

Use this command to configure the filter rule of the log message,
**logging filter rule** { **exact-match module** *module-name* **mnemonic** *mnemonic-name* **level** *level* | **single-match** [ **level** *level* | **mnemonic** *mnemonic-name* | **module** *module-name* ] }
Use this command to delete the “exact-match” filter rule.
**no logging filter rule exact-match** [ **module** *module-name* **mnemonic** *mnemonic-name* **level** *level* ]
Use this command to delete the “single-match” filter rule.
**no logging filter rule single-match** [ **level** *level* | **mnemonic** *mnemonic-name* | **module** *module-name* ]

**Parameter Description**

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

| | |
|---|---|
| **level** *level* | Log level, |

**Defaults** No filter rule is configured by default,

**Command Mode** Global configuration mode

**Usage Guide** If you want to filter a specific log message, use the “exact-match” filter rule and fill in all three parameters, namely, module name, mnemonic name and log level.
If you want to filter a specific kind of log messages, use the “single-match” filter rule and fill in one of three parameters, namely, module name, mnemonic name and log level.
When configured with the same module name, mnemonic name or log level, the “single-match” filter rule has a higher priority than the “exact-match” filter rule,

**Configuration Examples** The following example configures the “exact-match” filter rule with parameters of module name LOGIN, log level 5 and mnemonic name LOGOUT.

```
Ruijie(config)# logging filter rule exact-match module LOGIN mnemonic LOGOUT
level 5
```

The following example configures the “single-match” filter rule with the parameter of module name SYS.

```
Ruijie(config)# logging filter rule single-match module SYS
```

**Related Commands**

| Command | Description |
|---|---|
| N/A | N/A |

**Platform Description** N/A

## 7.17 logging life-time

Use this command to configure the preservation duration of logs in expanded FLASH. Use the no form of this command to restore the default setting.
**logging life-time level** *level days*
**no logging life-time level** *level*

**Parameter Description**

| Parameter | Description |
|---|---|
| *level* | Sets the log level, which can be either the level name or the level number. |
| *days* | Sets the preservation duration of logs. |

**Defaults** No preservation duration is set by default.

**Command Mode** Global configuration mode

**Usage Guide** Due to difference in expanded FLASH size and log level, logs with different levels can be configured with different preservation durations.

Once log preservation based on time is enabled, log preservation based on file size is disabled automatically. The log files are stored under the syslog/ directory of the expanded FLASH,

**Configuration Examples** The following example sets the preservation duration of logs whose level is 6 to 10 days.

```
Ruijie(config)# logging life-time level 6 10
```

**Related Commands**

| Command | Description |
|---|---|
| N/A | N/A |

**Platform Description** N/A

## 7.18 logging monitor

Use this command to set the severity of logs that are allowed to be displayed on the VTY window (telnet window, SSH window, etc.) in global configuration mode. Use the **no** form of this command to disable this function.

**logging monitor** [ *level* ]

**no logging monitor**

**Parameter Description**

| Parameter | Description |
|---|---|
| *level* | Severity of the log message. The name of the severity or the numeral can be used. For the details of log severity, see Table-1. |

**Defaults** The default is debugging (7).

**Command Mode** Global configuration mode

**Usage Guide** To print log information on the VTY window, run the **terminal monitor** command in privileged EXEC mode. The level of logs to be displayed is defined by **logging monitor**.
The log level defined with "Logging monitor" is for all VTY windows.

**Configuration Examples** The following example sets the severity of log that is allowed to be printed on the VTY window as 6:

```
Ruijie(config)# logging monitor informational
```

**Related Commands**

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

**Platform Description** N/A

## 7.19 logging on

Use this command globally to allow logs to be displayed on different devices. Use the **no** form of this command to disable this fucntion.

**logging on**

**no logging on**

**Parameter Description**

| Parameter | Description |
| --- | --- |
| N/A | N/A |

**Defaults** Logs are allowed to be displayed on different devices.

**Command Mode** Global configuration mode

**Usage Guide** Log information can not only be shown in the Console window and VTY window, but also be recorded in different devices such as the memory buffer, the expanded FLASH and the Syslog Server. This command is the total log switch. If this switch is turned off, no log will be displayed or recorded unless the severity level is greater than 1.

**Configuration Examples** The following example disables the log switch on the device.

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

**Related Commands**

| Command | Description |
| --- | --- |
| **logging buffered** | Records the logs to a memory buffer. |
| **logging server** | Sends logs to the Syslog server. |
| **logging file flash:** | Records logs on the expanded FLASH. |
| **logging console** | Allows the log level to be displayed on the console. |
| **logging monitor** | Allows the log level to be displayed on the VTY window (such as telnet window) . |
| **logging trap** | Sets the log level to be sent to the Syslog server. |

**Platform Description** N/A

## 7.20 logging policy

Use this command to configure the severity ranking policy. Use the no form of this command to remove one policy, Use the no logging policy command to remove all policies.

**logging policy module** *module-name* [ **not-lesser-than** ] *level* **direction** { **all** | **server** | **file** | **console** | **monitor** | **buffer** }

**no logging policy module** *module-name* [ **not-lesser-than** ] *level* **direction** { **all** | **server** | **file** | **console** | **monitor** | **buffer** }

**no logging policy**

**Parameter Description**

| Parameter | Description |
|---|---|
| *module-name* | The name of the module applying the ranking policy. |
| **not-lesser-than** | If this parameter is specified, only when the log's level is not lower than the configured level can the log be sent. Otherwise, the log is filtered.<br>If this parameter is not specified, only when the log's level is not higher than the configured level can the log be sent. Otherwise, the log is filtered. |
| *level* | Severity level |
| **all** | Applies the ranking policy in all directions. |
| **server** | Applies the ranking policy to the direction toward the server. |
| **file** | Applies the ranking policy to the direction toward the log file. |
| **console** | Applies the ranking policy to the direction toward the console. |
| **monitor** | Applies the ranking policy to the direction toward the remote server. |
| **buffer** | Applies the ranking policy to the direction toward the buffer. |

**Defaults** This function is disabled by default.

**Command Mode** Global configuration mode

**Usage Guide** This command is used to send logs to different destinations based on module and severity.

**Configuration Examples** The following example sends logs of the SYS module leveled above 5 to the console and sends logs of the SYS module leveled below 3 to the buffer.

```
Ruijie(config)# logging policy module SYS not-lesser-than 5 direction console
Ruijie(config)# logging policy module SYS 3 direction buffer
```

**Related**

| Command | Description |
|---|---|

| Commands | | |
|---|---|---|
| | N/A | N/A |

**Platform Description** N/A

## 7.21 logging rate-limit

Use this command to enable log rate limit function to limit the output logs in a second in the global configuration mode. Use the **no** form of this command to disable this function.

**logging rate-limit** { *number* | **all** *number* | **console** { *number* | **all** *number* } } [ **except** *severity* ]

**no logging rate-limit**

**Parameter Description**

| Parameter | Description |
|---|---|
| *number* | The number of logs that can be processed in a second in the range from 1 to 10000. |
| **all** | Sets rate limit to all the logs with severity level 0 to 7. |
| **console** | Sets the amount of logs that can be shown in the console in a second. |
| **except** | By default, the severity level is error (3). The rate of the log whose severity level is less than or equal to error (3) is not controlled. |
| *severity* | Log severity level in the range from 0 to 7. The lower the level is, the higher the severity is. |

**Defaults** The log rate limit function is disabled by default.

**Command Mode** Global configuration mode

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

**Configuration Examples** The following example sets the number of the logs (including debug) that can be processed in a second as 10. However, the logs with warning or higher severity level are not controlled:

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

**Related Commands**

| Command | Description |
|---|---|
| **show logging count** | Displays log information about modules of the system. |
| **show logging** | Displays basic configuration of log modules and log information in the buffer. |

**Platform Description** N/A

## 7.22 logging server

Use this command to send the logs to the specified Syslog Sever in global configuration mode. Use the **no** form of this command to remove the setting. Use the **default** form of this command to restore the default setting.

**logging server** { *ip-address* | **ipv6** *ipv6-address* } [ **udp-prot** *port* ]

**no logging server**{ *ip-address* | **ipv6** *ipv6-address* }

**no logging server** { *ip-address* | **ipv6** *ipv6-address* } **udp-prot**

**Parameter Description**

| Parameter | Description |
|---|---|
| *ip-address* | IP address of the host that receives log information. |
| *ipv6-address* | Specifies IPv6 address for the host receiving the logs. |
| **udp-port** *port* | Specifies the port number for the specified host (The default port number is 514). |

**Defaults** No log is sent to any syslog server by default.

**Command Mode** Global configuration mode

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

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

```
Ruijie(config)# logging server 202.101.11.1
```

The following example specifies a syslog server with IP address 10.1.1.100 and port 8099.

```
Ruijie(config)# logging server 202.101.11.1 udp-port 8099
```

The following example specifies an ipv6 address as AAAA:BBBB:FFFF:

```
Ruijie(config)# logging server ipv6 AAAA:BBBB:FFFF
```

**Related Commands**

| Command | Description |
|---|---|
| **logging on** | Turns on the log switch. |
| **show logging** | Displays log messages and related log configuration parameters in the buffer. |
| **logging trap** | Sets the level of logs allowed to be sent to Syslog server. |

**Platform Description** N/A

## 7.23 logging source interface

Use this command to configure the source interface of logs in global configuration mode. Use the **no** form of this command to restore the default setting.

**logging source** [ **interface** ] *interface-type interface-number*

**no logging source** [ **interface** ]

**Parameter Description**

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

**Defaults** No source interface is configured by default.

**Command Mode** Global configuration mode

**Usage Guide** By default, the source address of the log messages sent to the syslog server is the address of the sending interface. For easy tracing and management, this command can be used to fix the source address of all log messages as an interface address, so that the administrator can identify which device is sending the message through the unique addresses. If the source interface is not configured on the device, or no IP address is configured for the source interface, the source address of the log messages is the address of the sending interface.

**Configuration Examples** The following example specifies loopback 0 as the source address of the syslog messages:

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

**Related Commands**

| Command | Description |
|---|---|
| **logging server** | Sends logs to the Syslog server. |

**Platform Description** N/A

## 7.24 logging source ip | ipv6

Use this command to configure the source IP address of logs in global configuration mode. Use the **no** form of this command to restore the default setting.

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

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

**Parameter Description**

| Parameter | Description |
|---|---|
| *ip-address* | Specifies the source IPV4 address sending the logs to IPV4 log server. |

| | |
|---|---|
| *ipv6-address* | Specifies the source IPV6 address sending the logs to IPV6 log server. |

**Defaults** No source address is configured by default.

**Command Mode** Global configuration mode

**Usage Guide** By default, the source address of the log messages sent to the syslog server is the address of the sending interface. For easy tracing and management, this command can be used to fix the source address of all log messages as an address, so that the administrator can identify which device is sending the message through the unique addresses. If this IP address is not configured on the device, the source address of the log messages is the address of the sending interface.

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

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

**Related Commands**

| Command | Description |
|---|---|
| **logging server** | Sends the logs to the Syslog server. |

**Platform Description** N/A

## 7.25 logging statistic enable

Use this command to enable logging periodically. Use no form of this command to restore the default setting.

**logging statistic enable**

**no logging statistic enable**

**Parameter Description**

| Parameter | Description |
|---|---|
| N/A | N/A |

**Defaults** This function is disabled by default.

**Command Mode** Global configuration mode

**Usage Guide** This command is used to send performance statistics at a certain interval for the server to monitor the system performance.

**Configuration Examples** The following example enables logging periodically.

```
Ruijie(config)# logging statistic enable
```

**Related Commands**

| Command | Description |
| --- | --- |
| N/A | N/A |

**Platform Description** N/A

## 7.26 logging statistic interval

Use this command to configure the interval at which logs are sent. Use the no form of this command to restore the default setting.

**logging statistic mnemonic** *mnemonic* **interval** *minutes*

**no logging statistic mnemonic** *mnemonic*

**Parameter Description**

| Parameter | Description |
| --- | --- |
| *mnemonic* | Sets the mnemonics to identify the object. |
| *minutes* | Sets the interval at which logs are sent, in the unit of minutes. |

**Defaults** The default is 15.

**Command Mode** Global configuration mode

**Usage Guide** The available settings include 0, 15, 30, 60 and 120. 0 indicates this function is disabled.

**Configuration Examples** The following example set the interval at which logs are sent to 30 minutes.

```
Ruijie(config)# logging statistic mnemonic TUNNEL_STAT interval 30
```

**Related Commands**

| Command | Description |
| --- | --- |
| N/A | N/A |

**Platform Description** N/A

## 7.27 logging statistic terminal

Use this command to enable logs to be sent to the console and the remote terminal periodically. Use the no form of this command to restore the default setting.

**logging statistic terminal**

**no logging statistic terminal**

**Parameter Description**

| Parameter | Description |
|---|---|
| N/A | N/A |

**Defaults** This function is disabled by default.

**Command Mode** Global configuration mode

**Usage Guide** N/A

**Configuration Examples** The following example enable logs to be sent to the console and the remote terminal.

```
Ruijie(config)# logging statistic terminal
```

**Related Commands**

| Command | Description |
|---|---|
| N/A | N/A |

**Platform Description** N/A

## 7.28 logging synchronous

Use this command to enable synchronization function between user input and log output in line configuration mode to prevent interruption when the user is keying in characters. Use the **no** form of this command to restore the default setting.

**logging synchronous**

**no logging synchronous**

**Parameter Description**

| Parameter | Description |
|---|---|
| N/A | N/A |

**Defaults** The synchronization function between user input and log output is disabled by default.

**Command Mode** Line configuration mode

**Usage Guide** This command enables synchronization function between user input and log output, preventing the user from interrupting when keying in the characters.

**Configuration Examples**

```
Ruijie(config)#line console 0
Ruijie(config-line)#logging synchronous
```

Print UP-DOWN logs on the port when keying in the command, the input command will be output again:

```
Ruijie# configure terminal
Oct  9 23:40:55 %LINK-5-CHANGED: Interface GigabitEthernet 0/1, changed state to down
Oct  9 23:40:55 %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet 0/1, changed state to DOWN
Ruijie# configure terminal//----the input command by the user is output again rather than being intererupted.
```

**Related Commands**

| Command | Description |
|---|---|
| **show running-config** | Displays the configuration. |

**Platform Description** N/A

## 7.29 logging trap

Use this command to set the severity of logs that are allowed to be sent to the syslog server in global configuration mode. Use the **no** form of this command to prohibit sending log messages to the Syslog server.

**logging trap** [*level*]

**no logging trap**

**Parameter Description**

| Parameter | Description |
|---|---|
| *level* | Severity of the log message. The name of the severity or the numeral can be used. For the details of log severity, see Table 1. |

**Defaults** The default is informational(6)

**Command Mode** Global configuration mode

**Usage Guide** To send logs to the Syslog Server, run the **logging** command in global configuration mode to configure the **Syslog Server**. Then, run the **logging trap** command to specify the severity level of logs to be sent.
The **show logging** command displays the configured related parameters and statistics of the log.

**Configuration** The following example enables logs at severity 6 to be sent to the Syslog Server with the address of

**Examples** 202.101.11.22:

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

**Related Commands**

| Command | Description |
|---|---|
| **logging on** | Turns on the log switch. |
| **logging** | Sends logs to the Syslog server. |
| **show logging** | Displays the log messages and related log configuration parameters in the buffer. |

**Platform Description** N/A

## 7.30 logging userinfo

Use this command to enable the logging function to record user log/exit. Use the no form of this command to restore the default setting.

**logging userinfo**

**no logging userinfo**

**Parameter Description**

| Parameter | Description |
|---|---|
| N/A | N/A |

**Defaults** No log message is printed recording user log/exit by default.

**Command Mode** Global configuration mode

**Usage Guide** This command is used to print the log message to remind the administrator of user login. The log message is in the format as follows:

```
Mar 22 14:05:45 %LOGIN-5-LOGIN_SUCCESS: User login from vty0 (192.168.23.68) OK.
```

**Configuration Examples** The following example enables the logging function to record user log/exit.

```
Ruijie(config)# logging user-info
```

**Related Commands**

| Command | Description |
|---|---|
| N/A | N/A |

**Platform Description** N/A

## 7.31 logging userinfo command-log

Use this command to enable the logging function to record user operation. Use the no form of this command to restore the default setting.

**logging userinfo command-log**

**no logging userinfo command-log**

**Parameter Description**

| Parameter | Description |
|---|---|
| N/A | N/A |

**Defaults** No log message is printed recording user operation by default.

**Command Mode** Global configuration mode

**Usage Guide** This command is used to print the log message to remind the administrator of configuration change. The log message is in the format as follows:

```
Mar 22 14:10:40 %CLI-5-EXEC_CMD: Configured from vty0 (192.168.23.68)
command-log: logging server 192.168.23.68.
```

**Configuration Examples** The following example enables the logging function to record user operation.

```
Ruijie(config)# logging user-info command-log
```

**Related Commands**

| Command | Description |
|---|---|
| N/A | N/A |

**Platform Description** N/A

## 7.32 service log-format rfc5424

Use this command to enable the RFC5424 format. Use the no form of this command to restore the default setting.

**service log-format rfc5424**

**no service log-format rfc5424**

**Parameter Description**

| Parameter | Description |
|---|---|
| N/A | N/A |

**Defaults** The RFC3164 format is used by default.

**Command Mode** Global configuration mode

**Usage Guide** After the RFC5424 format is enabled, the service sequence-numbers, service sysname, **service timestamps**, **service private-syslog** and **service standard-syslog** commands become invalid and hidden.
After switching back to the RFC3164 format, the **logging delay-send, logging policy** and **logging statistic** commands become invalid and hidden.
After switching the log format, the results of running the **show logging** and **show logging config** commands change,

**Configuration Examples** The following example enables the RFC5424 format.

```
Ruijie(config)# service log-format rfc5424
```

**Related Commands**

| Command | Description |
| --- | --- |
| N/A | N/A |

**Platform Description** N/A

## 7.33 service private-syslog

Use this command to set the syslog format to the private syslog format. Use the no form of this command to restore the default setting.
**service private-syslog**
**no service private-syslog**

**Parameter Description**

| Parameter | Description |
| --- | --- |
| N/A | N/A |

**Defaults** The syslog is displayed in the default format.

**Command Mode** Global configuration mode

**Usage Guide** By default, the syslog is displayed in the format as follows:
*timestamp: %facility-severity-mnemonic: description
Here is an example:

```
*May 31 23:25:21: %SYS-5-CONFIG_I: Configured from console by console
```

With this function enabled, the syslog is displayed in the format as follows:
timestamp facility-severity-mnemonic: description

Here is an example:

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

The difference between the private syslog format and the default syslog format lies in the following marks:

The private syslog does not have "*" before the timestamp, ":" after the timestamp and "%" before the identifying string.

**Configuration Examples** The following example sets the private syslog format.

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

**Related Commands**

| Command | Description |
|---|---|
| N/A | N/A |

**Platform Description** N/A

## 7.34 service sequence-numbers

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

**service sequence-numbers**

**no service sequence-numbers**

**Parameter Description**

| Parameter | Description |
|---|---|
| N/A | N/A |

**Defaults** No serial number is contained in the logs by default.

**Command Mode** Global configuration mode

**Usage Guide** In addition to the timestamp, you can add serial numbers to the logs, numbering from 1. Then, it is clearly known whether the logs are lost or not and their sequence.

**Configuration Examples** The following example adds serial numbers to the logs.

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

**Related Commands**

| Command | Description |
|---|---|
| **logging on** | Turns on the log switch. |
| **service timestamps** | Attaches timestamps to the logs. |

**Platform Description** N/A

## 7.35 service standard-syslog

Use this command to set the syslog format to the standard syslog format defined in RFC3164. Use the no form of this command to restore the default setting.

**service standard-syslog**

**no service standard-syslog**

**Parameter Description**

| Parameter | Description |
|---|---|
| N/A | N/A |

**Defaults** The syslog is displayed in the default format.

**Command Mode** Global configuration mode

**Usage Guide** By default, the syslog is displayed in the format as follows:

*timestamp: %facility-severity-mnemonic: description

Here is an example:

```
*May 31 23:25:21: %SYS-5-CONFIG_I: Configured from console by console
```

With this function enabled, the syslog is displayed in the format as follows:

timestamp %facility-severity-mnemonic: description

Here is an example:

```
May 31 23:31:28 %SYS-5-CONFIG_I: Configured from console by console
```

The difference between the standard syslog format and the default syslog format lies in the following marks:

The standard syslog does not have “*” before the timestamp and “:” after the timestamp.

**Configuration Examples** The following example sets the standard syslog format.

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

**Related Commands**

| Command | Description |
|---|---|
| N/A | N/A |

**Platform Description** N/A

## 7.36 service sysname

Use this command to attach system name to logs in global configuration mode. Use the **no** form of this command to restore the default setting.

**service sysname**

**no service sysname**

**Parameter Description**

| Parameter | Description |
|---|---|
| N/A | N/A |

**Defaults** No system name is attached to logs by default.

**Command Mode** Global configuration mode

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

**Configuration Examples** The following example adds a system name in the log information:

```
Mar 22 15:28:02 %SYS-5-CONFIG: Configured from console by console
Ruijie #config terminal
Enter configuration commands, one per line. End with CNTL/Z.
Ruijie (config)#service sysname
Ruijie (config)#end
Ruijie #
```

Mar 22 15:35:57 S3250 %SYS-5-CONFIG: Configured from console by console

**Related Commands**

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

**Platform Description** N/A

## 7.37 service timestamps

Use this command to attach timestamp into logs in global configuration mode. Use the **no** form of this command to remove the timestamp from the logs. Use the **default** form of this command to restore the default setting.

**service timestamps** [ *message-type* [ **uptime | datetime** [ **msec** | **year** ] ] ]

**no service timestamps** [ *message-type* ]

**default service timestamps** [ *message-type* ]

**Parameter Description**

| Parameter | Description |
| --- | --- |
| *message-type* | The log type, including **Log** and **Debug**. The **log** type indicates the log information with severity levels of 0 to 6. The **debug** type indicates that with severity level 7. |
| **uptime** | Device start time in the format of *Day*Hour*Minute*Second, for example, 07:00:10:41. |
| **datetime** | Current time of the device in the format of Month*Date*Hour*Minute*Second, for example, Jul 27 16:53:07. |
| **msec** | Current time of the device in the format of Month*Date*Hour*Minute*Second*milisecond, for example, Jul 27 16:53:07.299 |
| **year** | Current time of the device in the format of Year*Month*Date*Hour*Minute*Second, for example, 2007 Jul 27 16:53:07 |

**Defaults** The time stamp in the log information is the current time of the device. If the device has no RTC, the time stamp is automatically set to the device start time.

**Command Mode** Global configuration mode

**Usage Guide** When the **uptime** option is used, the time format is the running period from the last start of the device to the present time, in seconds. When the **datetime** option is used, the time format is the date of the current device, in the format of YY-MM-DD, HH:MM:SS.

**Configuration Examples** The following example enables the timestamp for **log** and **debug** information, in format of Datetime, supporting millisecond display.

```
Ruijie(config)# service timestamps debug datetime msec
Ruijie(config)# service timestamps log datetime msec
Ruijie(config)# end
Ruijie(config)# Oct 8 23:04:58.301 %SYS-5-CONFIG I: configured from console
by console
```

**Related Commands**

| Command | Description |
| --- | --- |
| **logging on** | Turns on the log switch. |
| **service sequence-numbers** | Enables serial numbers of logs. |

**Platform Description** N/A

# 7. 38 show logging

Use this command to display configured parameters and statistics of logs and log messages in the memory buffer at privileged user layer. The log messages are sorted by the timestamp from before to now.

**show logging**

**Parameter Description**

| Parameter | Description |
|---|---|
| N/A | N/A |

**Defaults** N/A

**Command Mode** Privileged EXEC mode

**Usage Guide** N/A

**Configuration Examples** The following command displays the result of the **show logging** command with RFC5424 format disabled.

```
Ruijie# show logging
Syslog logging: enabled
  Console logging: level debugging, 15495 messages logged
  Monitor logging: level debugging, 0 messages logged
  Buffer logging: level debugging, 15496 messages logged
  Standard format: false
  Timestamp debug messages: datetime
  Timestamp log messages: datetime
  Sequence-number log messages: enable
  Sysname log messages: enable
  Count log messages: enable
  Trap logging: level informational, 15242 message lines logged,0 fail
    logging to  202.101.11.22
    logging to  192.168.200.112
Log Buffer (Total 131072 Bytes): have written 1336,
015487: *Sep 19 02:46:13: Ruijie %LINK-3-UPDOWN: Interface FastEthernet 0/24,
changed state to up.
015488: *Sep 19 02:46:13: Ruijie %LINEPROTO-5-UPDOWN: Line protocol on
Interface FastEthernet 0/24, changed state to up.
015489: *Sep 19 02:46:26: Ruijie %LINK-3-UPDOWN: Interface FastEthernet 0/24,
changed state to down.
015490: *Sep 19 02:46:26: Ruijie %LINEPROTON/A5N/AUPDOWN: Line protocol on
Interface FastEthernet 0/24, changed state to down.
```

```
015491: *Sep 19 02:46:28: Ruijie %LINKN/A3N/AUPDOWN: Interface FastEthernet
0/24, changed state to up.
015492: *Sep 19 02:46:28: Ruijie %LINEPROTO-5-UPDOWN: Line protocol on
Interface FastEthernet 0/24, changed state to up.
```

Log information description:

| Field | Description |
|---|---|
| Syslog logging | Logging flag: enabled or disabled |
| Console logging | Level of the logs printed on the console, and statistics |
| Monitor logging | Level of the logs printed on the VTY window, and statistics |
| Buffer logging | Level of the logs recorded in the memory buffer, and statistics. |
| Standard format | Standard log format. |
| Timestamp debug messages | Timestamp format of the Debug messages |
| Timestamp log messages | Timestamp format of the Log messages |
| Sequence-number log messages | Serial number switch |
| Sequence log messages | Attaches system names to the logs. |
| Count log messages | Log statistics function |
| Trap logging | Level of the logs sent to the syslog server, and statistics |
| Log Buffer | Log files recorded in the memory buffer |

The following example displays the result of the **show logging** command with RFC5424 format enabled.

```
Ruijie# show logging
Syslog logging: enabled
  Console logging: level debugging, 4740 messages logged
  Monitor logging: level debugging, 0 messages logged
  Buffer logging: level debugging, 4745 messages logged
  Statistic log messages: disable
  Statistic log messages to terminal: disable
  Delay-send file name:syslog_ftp_server, Current write index:3, Current send
index:3, Cycle:10 seconds
   Count log messages: enable
  Trap logging: level informational, 2641 message lines logged,4155 fail
    logging to  192.168.23.89
    logging to  2000::1
  Delay-send logging: 2641 message lines logged
```

```
   logging to  192.168.23.89  by tftp
Log Buffer (Total 4096 Bytes): have written 4096, Overwritten 3292
<135>1 2013-07-24T12:19:33.130290Z ruijie - 7 - - Please config the IP address
for capwap.
<132>1 2013-07-24T12:20:02.80313Z ruijie CAPWAP 4 NO_IP_ADDR - No ip address
for capwap.
<135>1 2013-07-24T12:20:02.80343Z ruijie - 7 - - Please config the IP address
for capwap.
<132>1 2013-07-24T12:20:32.250265Z ruijie CAPWAP 4 NO_IP_ADDR - No ip address
for capwap.
<134>1 2013-07-24T12:29:33.410123Z ruijie SYS 6 SHELL_LOGIN [USER@4881
name="" type="" from="console"] user login success.
<134>1 2013-07-24T12:29:34.343763Z ruijie SYS 6 SHELL_CMD
[USER@4881 name=""][CMD@4881 task="rl_con" cmd="enable"]
```

| Field | Description |
|---|---|
| Syslog logging | Logging flag: enabled or disabled |
| Console logging | Level of the logs printed on the console, and statistics |
| Monitor logging | Level of the logs printed on the VTY window, and statistics |
| Buffer logging | Level of the logs recorded in the memory buffer, and statistics. |
| Count log messages | Log statistics function |
| Statistic log messages | Enables/disables log sending periodically |
| Statistic log messages to terminal | Enables/ disables log sending to console and remote terminal |
| Delay-send file name | Local filename of log delay-sending cache, index of write file and delay interval |
| Trap logging | Level of the logs sent to the syslog server and statistics |
| Delay-send logging | The server address, log sending mode and statistics |
| Log Buffer | Log files recorded in the memory buffer |

**Related Commands**

| Command | Function |
|---|---|
| **logging on** | Turns on the log switch. |
| **clear logging** | Clears the log messages in the buffer. |

**Platform Description** N/A

## 7.39 show logging config

Use this command to display log configuration and statistics.

**show logging config**

**Parameter Description**

| Parameter | Description |
|---|---|
| N/A | N/A |

**Defaults** N/A

**Command Mode** Privileged EXEC mode

**Usage Guide** N/A

**Configuration Examples** The following example displays the outcome of running the **show logging config** command with RFC5424 disabled.

```
Ruijie# show logging config
Syslog logging: enabled
  Console logging: level debugging, 15495 messages logged
  Monitor logging: level debugging, 0 messages logged
  Buffer logging: level debugging, 15496 messages logged
  Standard format: false
  Timestamp debug messages: datetime
  Timestamp log messages: datetime
  Sequence-number log messages: enable
  Sysname log messages: enable
  Count log messages: enable
  Trap logging: level informational, 15242 message lines logged,0 fail
    logging to  202.101.11.22
    logging to  192.168.200.112
```

| Field | Description |
|---|---|
| Syslog logging | Whether the logging function is enabled or disabled. |
| Console logging | The level and statistics of the log message printed on the console. |
| Monitor logging | The level and statistics of the log message printed on the VTY window. |
| Buffer logging | The level and statistics of the log message recorded in the memory buffer. |
| Standard format | Standard log format. |
| Timestamp debug messages | Timestamp format of debugging message. |
| Timestamp log messages | Timestamp format of log message. |
| Sequence-number log messages | Whether the sequence number function is enabled or disabled. |
| Sysname log messages | Adds the system name to the log message. |
| Count log messages | Log-counting function |
| Trap logging | The level and statistics of the log message sent to the syslog server. |

The following example displays the outcome of running the **show logging config** command with RFC5424 enabled.

```
Ruijie# show logging
Syslog logging: enabled
  Console logging: level debugging, 4740 messages logged
  Monitor logging: level debugging, 0 messages logged
  Buffer logging: level debugging, 4745 messages logged
  Statistic log messages: disable
  Statistic log messages to terminal: disable
  Delay-send file name:syslog_ftp_server, Current write index:3, Current send
index:3, Cycle:10 seconds
   Count log messages: enable
  Trap logging: level informational, 2641 message lines logged,4155 fail
    logging to  192.168.23.89
    logging to  2000::1
  Delay-send logging: 2641 message lines logged
     logging to  192.168.23.89  by tftp
```

| Field | Description |
|---|---|
| Syslog logging | Logging flag: enabled or disabled |
| Console logging | Level of the logs printed on the console, and statistics |
| Monitor logging | Level of the logs printed on the VTY window, and statistics |
| Buffer logging | Level of the logs recorded in the memory buffer, and statistics. |
| Count log messages | Log statistics function |
| Statistic log messages | Enables/disables log sending periodically |
| Statistic log messages to terminal | Enables/ disables log sending to output console and remove terminal |
| Delay-send file name | Local filename of log delay-sending cache, index of write file and delay interval |
| Trap logging | Level of the logs sent to the syslog server and statistics |
| Delay-send logging | The server address, log sending way and statistics |

**Related Commands**

| Command | Description |
|---|---|
| N/A | N/A |

**Platform Description** N/A

## 7.40 show logging count

Use this command to display the statistics about occurrence times, and the last occurrence time of each module log in the system in privileged mode.

**show logging count**

**Parameter Description**

| Parameter | Description |
|---|---|
| N/A | N/A |

**Defaults** N/A

**Command Mode** Privileged EXEC mode

**Usage Guide** To use the log packet statistics function, run the **logging count** command in global configuration mode. The **show logging count** command can show the information of a specific log, occurrence times, and the last occurrence time.
You can use the **show logging** command to check whether the log statistics function is enabled.

**Configuration Examples** The following example displays the result of the **show logging count** command:

```
Ruijie# show logging count
Module Name   Message Name Sev Occur     Last Time
SYS          CONFIG_I        5   1        Jul 6 10:29:57
SYS TOTAL                        1
```

**Related Commands**

| Command | Function |
|---|---|
| **logging count** | Enables the log statistics function. |
| **show logging** | Displays basic configuration of log modules and log information in the buffer. |
| **clear logging** | Clears the logs in the buffer. |

**Platform Description** N/A

## 7.41 show logging reverse

Use this command to display configured parameters and statistics of logs and log messages in the memory buffer at privileged user layer. The log messages are sorted by the timestamp from now to before.

**show logging reverse**

**Parameter Description**

| Parameter | Description |
|---|---|
| N/A | N/A |

**Defaults** N/A

**Command Mode** Privileged EXEC mode

**Usage Guide**

**Configuration Examples** The following command displays the result of the **show logging reverse** command with RFC5424 format disabled.

```
Ruijie# show logging reverse
Syslog logging: enabled
  Console logging: level debugging, 15495 messages logged
  Monitor logging: level debugging, 0 messages logged
  Buffer logging: level debugging, 15496 messages logged
  Standard format: false
  Timestamp debug messages: datetime
  Timestamp log messages: datetime
  Sequence-number log messages: enable
  Sysname log messages: enable
  Count log messages: enable
  Trap logging: level informational, 15242 message lines logged,0 fail
    logging to  202.101.11.22
    logging to  192.168.200.112
Log Buffer (Total 131072 Bytes): have written 1336,
015492: *Sep 19 02:46:28: Ruijie %LINEPROTO-5-UPDOWN: Line protocol on
Interface FastEthernet 0/24, changed state to up.
015491: *Sep 19 02:46:28: Ruijie %LINK-3-UPDOWN: Interface FastEthernet 0/24,
changed state to up.
015490: *Sep 19 02:46:26: Ruijie %LINEPROTO-5-UPDOWN: Line protocol on
Interface FastEthernet 0/24, changed state to down.
015489: *Sep 19 02:46:26: Ruijie %LINK-3-UPDOWN: Interface FastEthernet 0/24,
changed state to down.
015488: *Sep 19 02:46:13: Ruijie %LINEPROTO-5-UPDOWN: Line protocol on
Interface FastEthernet 0/24, changed state to up.
015487: *Sep 19 02:46:13: Ruijie %LINK-3-UPDOWN: Interface FastEthernet 0/24,
changed state to up.
```

| Field | Description |
|---|---|
| Syslog logging | Logging flag: enabled or disabled |
| Console logging | Level of the logs printed on the console, and statistics |
| Monitor logging | Level of the logs printed on the VTY window, and statistics |
| Buffer logging | Level of the logs recorded in the memory buffer, and statistics. |

| | |
|---|---|
| Standard format | Standard log format. |
| Timestamp debug messages | Timestamp format of the Debug messages |
| Timestamp log messages | Timestamp format of the Log messages |
| Sequence-number log messages | Serial number switch |
| Sequence log messages | Attaches system names to the logs. |
| Count log messages | Log statistics function |
| Trap logging | Level of the logs sent to the syslog server, and statistics |
| Log Buffer | Log files recorded in the memory buffer |

The following example displays the result of the **show logging reverse** command with RFC5424 format enabled.

```
Ruijie# show logging reverse
Syslog logging: enabled
  Console logging: level debugging, 4740 messages logged
  Monitor logging: level debugging, 0 messages logged
  Buffer logging: level debugging, 4745 messages logged
  Statistic log messages: disable
  Statistic log messages to terminal: disable
  Delay-send file name:syslog_ftp_server, Current write index:3, Current send
index:3, Cycle:10 seconds
   Count log messages: enable
  Trap logging: level informational, 2641 message lines logged,4155 fail
    logging to  192.168.23.89
    logging to  2000::1
  Delay-send logging: 2641 message lines logged
    logging to  192.168.23.89  by tftp
Log Buffer (Total 4096 Bytes): have written 4096, Overwritten 3292
<134>1 2013-07-24T12:29:34.343763Z ruijie SYS 6 SHELL_CMD [USER@4881
name=""][CMD@4881 task="rl_con" cmd="enable"]
<134>1 2013-07-24T12:29:33.410123Z ruijie SYS 6 SHELL_LOGIN [USER@4881 name=""
type="" from="console"] user login success.
<132>1 2013-07-24T12:20:32.250265Z ruijie CAPWAP 4 NO_IP_ADDR - No ip address
for capwap.
<135>1 2013-07-24T12:20:02.80343Z ruijie - 7 - - Please config the IP address
for capwap.
<132>1 2013-07-24T12:20:02.80313Z ruijie CAPWAP 4 NO_IP_ADDR - No ip address
for capwap.
<135>1 2013-07-24T12:19:33.130290Z ruijie - 7 - - Please config the
IP address for capwap.
```

| Field | Description |
|---|---|

| | |
|---|---|
| Syslog logging | Logging flag: enabled or disabled |
| Console logging | Level of the logs printed on the console, and statistics |
| Monitor logging | Level of the logs printed on the VTY window, and statistics |
| Buffer logging | Level of the logs recorded in the memory buffer, and statistics. |
| Count log messages | Log statistics function |
| Statistic log messages | Enables/disables log sending periodically |
| Statistic log messages to terminal | Enables/ disables log sending to console and remote terminal |
| Delay-send file name | Local filename of log delay-sending cache, index of write file and delay interval |
| Trap logging | Level of the logs sent to the syslog server and statistics |
| Delay-send logging | The server address, log sending mode and statistics |
| Log Buffer | Log files recorded in the memory buffer |

**Related Commands**

| Command | Description |
|---|---|
| N/A | N/A |

**Platform Description** N/A

## 7.42 terminal monitor

Use this command to show logs on the current VTY window. Use the **no** form of this command to restore the default setting.

**terminal monitor**

**terminal no monitor**

**Parameter Description**

| Parameter | Description |
|---|---|
| N/A | N/A |

**Defaults** Log information is not allowed to be displayed on the VTY window by default.

**Command Mode** Privileged EXEC mode

**Usage Guide** This command only sets the temporary attributes of the current VTY. As the temporary attribute, it is not stored permanently. At the end of the VTY terminal session, the system will use the default setting, and the temporary setting is invalid. This command can be also executed on the console, but it does not take effect.

**Configuration Examples** The following example allows log information to be printed on the current VTY window:

```
Ruijie# terminal monitor
```

**Related Commands**

| Command | Description |
| --- | --- |
| N/A | N/A |

**Platform Description** N/A

**Command History**

| Version | Description |
| --- | --- |
| N/A | N/A |

# 8 RLOG Commands

## 8.1 rlog server

Use this command to configure the RLOG server.

Use the **no** form of this command to remove the configuration.

**rlog server** *ip-address* [ **vrf** *vrf-name*] [ **port** *port-num* ]

**no rlog server** *ip-address*

**Parameter Description**

| Parameter | Description |
|---|---|
| *ip-address* | IP address of the RLOG server |
| *port-num* | Port number of the RLOG server |
| **vrf** *vrf-name* | VRF name |

**Defaults** N/A

**Command Mode** Global configuration mode

**Usage Guide** Configuring the RLOG server is the precondition for RLOG export.

(Mandatory) Make sure the **vrf** parameter is accurate in case of overwritinginformation.

**Configuration Examples** The following example configures the RLOG server and port on AP.

```
Ruijie(config)# rlog server 10.10.10.10 port 20000
```

**Platform Description**

## 8.2 rlog type

Use this command to set the RLOG type.

Use the **no** form of this command to remove the configuration.

**rlog type** *n* **server** *server-ip* **priority** *prio*

**no rlog type** *n* **server** *server-ip*

**Parameter Description**

| Parameter | Description |
|---|---|
| *n* | RLOG type |
| *server-ip* | IP address of the RLOG server |

| | |
|---|---|
| *prio* | RLOG priority: 0-7. The lower the value is, the higher the priority is. |

**Defaults** N/A

**Command Mode** Global configuration mode

**Usage Guide** (Mandatory) Each log should be configured with this function.

**Configuration Examples** The following example sets the RLOG types on AP.

```
Ruijie(config)# rlog type 16 server 10.10.10.10 priority 1
```

**Platform Description** N/A

## 8.3 rlog export-rate

Use this command to set the RLOG export rate.

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

**rlog export-rate** *val*

**no rlog export-rate**

**Parameter Description**

| Parameter | Description |
|---|---|
| *val* | RLOG export rate in the range from 10 to 100000 (log number per second) |

**Defaults** The default rate is 1000.

**Command Mode** Global configuration mode

**Usage Guide** The RLOG export rate is determined by device and server performance as well as log outputs.

Too low rate causes log loss. Too high rate raises CPU consumption.

**Configuration Examples** The following example sets the RLOG export rate to 10000.

```
rlog export-rate 10000
```

**Platform Description** N/A

## 8.4 rlog set

Use this command to enable RLOG-combination export.

Use the **no** form of this command to remove the configuration.

**rlog set log-com**

**no rlog set log-com**

**Parameter Description**

| Parameter | Description |
| --- | --- |
| N/A | N/A |

**Defaults** N/A

**Command Mode** Global configuration mode

**Usage Guide** Use this command to improve RLOG export efficiency, which also relies on server performance.

If the server does not support this function, this command may cause problems such as packet loss or analysis failure.

**Configuration Examples** N/A

**Platform Description** N/A

## 8.5 rlog dev-ip

Use this command to set the IP address of the RLOG device.

Use the **no** form of this command to remove the configuration.

**rlog dev-ip** *ip*

**no rlog dev-ip**

**Parameter Description**

| Parameter | Description |
| --- | --- |
| *ip* | IP address of the RLOG device |

**Defaults** N/A

**Command Mode** Global configuration mode

**Usage Guide** (Optional) Specific types of logs require the IP address of RLOG device.

If the IP address is not configured, errors may occur when the RLOG server analyzes logs.

**Configuration Examples** The following example sets the IP address of the RLOG device to 10.10.10.2.

```
Ruijie(config)# rlog dev-ip 10.10.10.2
```

**Platform Description** N/A

## 8.6 rlog filter

Use this command to configure the RLOG filtering.

Use the **no** form of this command to remove the configuration.

**rlog filter** *aclid*

**no rlog filter**

**Parameter Description**

| Parameter | Description |
|---|---|
| *aclid* | ACL ID, in the range from 2000 to 2699. |

**Defaults** N/A

**Command Mode** configuration mode

**Usage Guide** This command applies to both remote flow logs and local logs. Use this command when logs are excessive or partial logs are selected.

The ACL should be configured at first.

**Configuration Examples** The following example enables the RLOG filtering.

```
Ruijie(config)# access-list 2000 permit udp any any
Ruijie(config)# rlog filter 2000
```

**Platform Description** N/A

## 8.7 show rlog

Use this command to display the RLOG configuration.

**show rlog**

**Parameter Description**

| Parameter | Description |
|---|---|
| *N/A* | N/A |

**Command Mode** Privileged EXEC mode

**Usage Guide** Use this command to display RLOG configuration including the device IP address, log-export rate and count, and log-combination function.

**Configuration Examples** The following example displays the RLOG configuration.

```
Ruijie#show rlog
rlog server is enable
 port 20000  server 192.168.1.100
 port 20000  server 10.10.10.10
rlog dev-ip 0.0.0.0
rlog export-rate 1000 rlog queue remain 10000
send log count : 0 error count : 0 errorno : 0
recv buf: 0 poll buf err: 0 push buf: 0 local buf: 0
recv err cnt: 0 depatch err cnt: 0

enable log combination: 0
```

Field Description

| Field | Description |
|---|---|
| rlog server is enable | The RLOG server is configured as listed. |
| rlog dev-ip | Device IP address |
| rlog export-rate | RLOG-export rate |
| rlog queue remain | RLOG buffer queue remain |
| send log count | Log-export count |
| error count | Error count |
| errorno | No. of the last export error |
| recv buf | Log receiving count |
| poll buf err | Buffer space error |
| local buf | Local buffer |
| recv err cnt | MSG receiving error count |
| depatch err cnt | The source server of messages received cannot be identified. |
| enable log combination | Log-combination function |

**Platform Description** N/A

## 8.8 show rlog-type

Use this command to display the RLOG type.

**show rlog-type**

**Parameter**

| Parameter | Description |
|---|---|

| Description | | |
|---|---|---|
| | N/A | N/A |

**Command Mode** Privileged EXEC mode

**Usage Guide** N/A

**Configuration Examples** The following example displays the RLOG type.

```
Ruijie#show rlog-type
RLOG_TYPE_FLOW              16
RLOG_TYPE_CPU_MEM           17
RLOG_TYPE_DISC              18
RLOG_TYPE_DEV_LOG           19
RLOG_TYPE_URL_AUDIT         20
RLOG_TYPE_SESSION           21
RLOG_TYPE_IP_APP            22
RLOG_TYPE_IP                23
RLOG_TYPE_CHANNEL           24
RLOG_TYPE_INTERFACE         25
RLOG_TYPE_IP_OFFLINE        26
RLOG_TYPE_MAIL_AUDIT        27
RLOG_TYPE_TELNET_AUDIT      28
RLOG_TYPE_WEB_SEARCH_AUDIT   29
RLOG_TYPE_WEB_BBS_AUDIT     30
RLOG_TYPE_IM_AUDIT          31
RLOG_TYPE_FTP_AUDIT         32
RLOG_TYPE_WEB_AUDIT         33
RLOG_TYPE_APP_AUDIT         34
RLOG_TYPE_FLOOD             35
RLOG_TYPE_FLOOD_CEASEm      36
RLOG_TYPE_SCAN              37
RLOG_TYPE_SCAN_CEASE        38
RLOG_TYPE_ATTACK_FRAG       39
```

**Platform Description** N/A

## 8.9 show rlog-status

Use this command to display the RLOG server details.

**show rlog-status** { [ **server** *ip* ] | [ **client** ] | [ **log** ] }

| Parameter | Parameter | Description |
|---|---|---|

| Description | | |
|---|---|---|
| | *ip* | Specifies a RLOG server. |

**Command Mode** Privileged EXEC mode

**Usage Guide** N/A

**Configuration Examples** The following example displays the RLOG server status.

```
Ruijie#show rlog-status
============================================================
server:192.168.1.100     port:20000
type                       prio
============================================================
server:10.10.10.10     port:20000
type                       prio
RLOG_TYPE_FLOW      16       1
```

The following example displays the RLOG module count.

```
Ruijie#show rlog-status client
rlog client count: 0
```

Field Description

| Field | Description |
|---|---|
| rlog client count | RLOG module count |

The following example displays the RLOG log count.

```
Ruijie#show rlog-status log
local rlog message:

remote rlog message:
[16]RLOG_TYPE_FLOW             : 0
[17]RLOG_TYPE_CPU_MEM          : 0
[18]RLOG_TYPE_DISC             : 0
[19]RLOG_TYPE_DEV_LOG          : 0
[20]RLOG_TYPE_URL_AUDIT        : 0
[21]RLOG_TYPE_SESSION          : 0
[22]RLOG_TYPE_IP_APP           : 0
[23]RLOG_TYPE_IP               : 0
[24]RLOG_TYPE_CHANNEL          : 0
[25]RLOG_TYPE_INTERFACE        : 0
[26]RLOG_TYPE_IP_OFFLINE       : 0
[27]RLOG_TYPE_MAIL_AUDIT       : 0
[28]RLOG_TYPE_TELNET_AUDIT     : 0
[29]RLOG_TYPE_WEB_SEARCH_AUDIT   : 0
```

```
[30]RLOG_TYPE_WEB_BBS_AUDIT      : 0
[31]RLOG_TYPE_IM_AUDIT          : 0
[32]RLOG_TYPE_FTP_AUDIT         : 0
[33]RLOG_TYPE_WEB_AUDIT         : 0
[34]RLOG_TYPE_APP_AUDIT         : 0
[35]RLOG_TYPE_FLOOD             : 0
[36]RLOG_TYPE_FLOOD_CEASEm       : 0
[37]RLOG_TYPE_SCAN              : 0
[38]RLOG_TYPE_SCAN_CEASE        : 0
[39]RLOG_TYPE_ATTACK_FRAG       : 0
```

Field Description

| Field | Description |
|---|---|
| local rlog message | The number of local RLOG messages |
| remote rlog message | The number of remote RLOG messages distinguished by RLOG types |

**Platform Description** N/A

# 9 CWMP Commands

## 9.1 acs password

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

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

**no acs password**

**Parameter Description**

| Parameter | Description |
|---|---|
| *password* | Configures the ACS user password to be authenticated for the CPE to connect to the ACS. |
| *encryption-type* | Specifies the encryption type, which can be set to 0 (indicating that no encryption is used) or 7 (indicating that simple encryption is used). |
| *encrypted-password* | Specifies the password in encrypted form. |

**Defaults**

encryption-type: 0

encrypted-password: N/A

**Command Mode**

CWMP configuration mode

**Usage Guide**

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

- The command contains English letters in upper or lower case and numeric characters.
- Blanks are allowed at the beginning of the password but will be ignored. Intermediate and ending blanks, however, are regarded as a part of the password.

**Configuration Examples**

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

```
Ruijie#config terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Ruijie(config)#cwmp
Ruijie(config-cwmp)#acs password 123
Ruijie(config-cwmp)#
```

**Related Commands**

| Command | Description |
|---|---|

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

**Platform Description** N/A

## 9.2 acs url

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

**Parameter Description**

| Parameter | Description |
|---|---|
| *url* | Specifies the URL of the ACS. |

**Defaults** N/A

**Command Mode** CWMP configuration mode

**Usage Guide** Use this command to configure the URL of the ACS to which the CPE will connect. If no ACS URL is manually specified but a dynamic ACS URL is obtained through DHCP, the CPE initiates a connection to the ACS using the dynamically obtained ACS URL. The URL of the ACS should meet the following format requirements:

- The URL of the ACS is formatted as http://host[:port]/path or https://host[:port]/path.
- The URL of the ACS consists of at most 256 characters.

**Configuration Examples** The following example specifies the URL of the ACS to http://10.10.10.1:8080/acs.

```
Ruijie#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Ruijie(config)#cwmp
Ruijie(config-cwmp)#acs url http://10.10.10.1:8080/acs
Ruijie(config-cwmp)#
```

The following example specifies the URL of the ACS to http://www.test.com/service/tr069servlet.

```
Ruijie#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Ruijie(config)#cwmp
Ruijie(config-cwmp)#acs url http://www.test.com/service/tr069servlet
```

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

**Related Commands**

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

**Platform Description** N/A

## 9.3 acs username

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

**acs username** *username*

**no acs username**

**Parameter Description**

| Parameter | Description |
| --- | --- |
| *username* | Configures the ACS username to be authenticated for the CPE to connect to the ACS. |

**Defaults** N/A

**Command Mode** CWMP configuration mode

**Usage Guide** Configures the ACS username to be authenticated for the CPE to connect to the ACS.

**Configuration Examples** The following example configures the ACS username to be authenticated for the CPE to connect to the ACS to admin.

```
Ruijie#config terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Ruijie(config)#cwmp
Ruijie(config-cwmp)#acs username admin
Ruijie(config-cwmp)#
```

**Related Commands**

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

| | |
|---|---|
| | ACS. |

**Platform Description** N/A

## cpe back-up

Use this command to configure the backup and restoration of the main program and configuration file of the CPE.

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

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

**no cpe back-up**

**Parameter Description**

| Parameter | Description |
|---|---|
| *seconds* | Specifies the delay for backup and restoration of the main program and configuration file of the CPE, in the range from 30 to 10,000 in the unit of seconds |

**Defaults** The default is 60 seconds.

**Command Mode** CWMP configuration mode

**Usage Guide** You can configure the restoration function on a CPE, so that the CPE can restore itself from exceptions of its main program or configuration file. Then when the CPE fails to connect to the ACS and breaks away from the NMS after its main program or configuration file is upgraded, the previous main program or configuration file of the CPE can be restored in time for the ACS to manage the CPE. This kind of exception is generally caused by delivery of a wrong main program or configuration file.

**Configuration Examples** The following example disables the backup and restoration of the main program and configuration file of the CPE.

```
Ruijie#config terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Ruijie(config)#cwmp
Ruijie(config-cwmp)#no cpe back-up
Ruijie(config-cwmp)#
```

**Related Commands**

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

**Platform Description** N/A

## 9.4 cpe back-up

Use this command to enable the CPE backup function.

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

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

**no cpe back-up**

**Parameter Description**

| Parameter | Description |
|---|---|
| *seconds* | Sets the backup delay time (30-10,000 seconds). |

**Defaults** The default is 60 seconds.

**Command Mode** CWMP configuration mode

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

**Configuration Examples** The following example disables the CPE backup function.

```
Ruijie#config terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Ruijie(config)#cwmp
Ruijie(config-cwmp)#no cpe back-up
Ruijie(config-cwmp)#
```

**Platform Description** N/A

## 9.5 cpe inform

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

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

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

**no cpe inform**

**Parameter**

| Parameter | Description |
|---|---|

**Description**

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

**Defaults** The default is 600 seconds.

**Command Mode** CWMP configuration mode

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

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

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

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

```
Ruijie#config terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Ruijie(config)#cwmp
Ruijie(config-cwmp)#cpe inform interval 60
Ruijie(config-cwmp)#
```

**Related Commands**

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

**Platform Description** N/A

## 9.6 cpe password

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

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

**no cpe password**

**Parameter Description**

| Parameter | Description |
|---|---|
| *password* | Configures the CPE user password to be authenticated for the ACS to connect to the CPE. |
| *encryption-type* | Specifies the encryption type, which can be set to 0 (indicating that no encryption is used) or 7 (indicating that simple encryption is used). |
| *encrypted-password* | Specifies the password in encrypted form. |

**Defaults**

encryption-type: 0

encrypted-password: N/A

**Command Mode**

CWMP configuration mode

**Usage Guide**

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

- The command contains English letters in upper or lower case and numeric characters.
- Blanks are allowed at the beginning of the password but will be ignored. Intermediate and ending blanks, however, are regarded as a part of the password.

**Configuration Examples**

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

```
Ruijie#config terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Ruijie(config)#cwmp
Ruijie(config-cwmp)#cpe password 123
Ruijie(config-cwmp)#
```

**Related Commands**

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

| | |
|---|---|
| **acs username** | Configures the CPE username to be authenticated for the ACS to connect to the CPE. |

**Platform Description** N/A

## 9.7 cpe url

Use this command to configure the URL of the CPE to which the ACS will connect.

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

**cpe url** *url*

**no cpe url**

**Parameter Description**

| Parameter | Description |
|---|---|
| *url* | Specifies the URL of the CPE. |

**Defaults** N/A

**Command Mode** CWMP configuration mode

**Usage Guide** Use this command to configure the URL of the CPE to which the ACS will connect. If no CPE URL is manually specified but a dynamic CPE URL is obtained through DHCP, the ACS initiates a connection to the CPE using the dynamically obtained CPE URL. The URL of the CPE should meet the following format requirements:

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

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

```
Ruijie#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Ruijie(config)#cwmp
Ruijie(config-cwmp)#cpe url Hhttp://10.10.10.1:7547/
Ruijie(config-cwmp)#
```

**Related Commands**

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

**Platform Description** N/A

## 9.8 cpe username

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

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

**cpe username** *username*

**no cpe username**

**Parameter Description**

| Parameter | Description |
|---|---|
| *username* | Configures the CPE username to be authenticated for the ACS to connect to the CPE. |

**Defaults** N/A

**Command Mode** CWMP configuration mode

**Usage Guide** Configures the CPE username to be authenticated for the ACS to connect to the CPE.

**Configuration Examples** The following example configures the CPE username to be authenticated for the ACS to connect to the CPE to admin.

```
Ruijie#config terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Ruijie(config)#cwmp
Ruijie(config-cwmp)#cpe username admin
Ruijie(config-cwmp)#
```

**Related Commands**

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

**Platform Description** N/A

## 9.9 cwmp

Use this command to enable the CWMP function.

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

**cwmp**
**no cwmp**

**Parameter Description**

| Parameter | Description |
|---|---|
| N/A | N/A |

**Defaults** By default, this function is enabled.

**Command Mode** Global configuration mode

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

**Configuration Examples** The following example disables the CWMP function.

```
Ruijie#config terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Ruijie(config)#no cwmp
Ruijie(config)#
```

**Related Commands**

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

**Platform Description** N/A

## 9.10 disable download

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

**Parameter Description**

| Parameter | Description |
|---|---|
| N/A | N/A |

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

**Command Mode** CWMP configuration mode

**Usage Guide** N/A

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

```
Ruijie#config terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Ruijie(config)#cwmp
Ruijie(config-cwmp)#disable download
Ruijie(config-cwmp)#
```

**Related Commands**

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

**Platform Description** N/A

## 9.11 disable upload

Use this command to disable the function of uploading configuration and log files to the ACS.
Use the **no** form of this command to restore the default setting.
**disable upload**
**no disable upload**

**Parameter Description**

| Parameter | Description |
|---|---|
| N/A | N/A |

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

**Command Mode** CWMP configuration mode

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

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

```
Ruijie#config terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Ruijie(config)#cwmp
Ruijie(config-cwmp)#disable upload
Ruijie(config-cwmp)#
```

**Related**

| Command | Description |
|---|---|

| Commands | | |
|---|---|---|
| | **show cwmp configuration** | Displays the current configuration of CWMP. |
| | **show cwmp status** | Displays the running status of CWMP. |

**Platform Description** N/A

## 9.12 show cwmp configuration

Use this command to display the current configuration of CWMP.

**show cwmp configuration**

| Parameter Description | Parameter | Description |
|---|---|---|
| | N/A | N/A |

**Defaults** N/A

**Command Mode** Privilege EXEC mode

**Usage Guide**

**Configuration Examples** The following example displays the current configuration of CWMP.

```
Ruijie(config-cwmp)#show cwmp configuration
CWMP Status                  : enable
ACS URL                      : http://www.ruijie.com.cn/acs
ACS username                 : admin
ACS password                 : ******
CPE URL                      : http://10.10.10.2:7547/
CPE username                 : ruijie
CPE password                 : ******
CPE inform status            : disable
CPE inform interval          : 60s
CPE inform start time        : 0:0:0 0 0 0
CPE wait timeout             : 50s
CPE download status          : enable
CPE upload status            : enable
CPE back up status           : enable
CPE back up delay time       : 60s
```

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

| Field | Description |
|---|---|
| CWMP Status | Running status of CWMP. |
| ACS URL | URL of the ACS。 |

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

**Related Commands**

| Command | Description |
|---|---|
| **show cwmp status** | Displays the running status of CWMP. |

**Platform Description** N/A

## 9.13 show cwmp status

Uses this command to display the running status of CWMP

**show cwmp status**

**Parameter Description**

| Parameter | Description |
|---|---|
| N/A | N/A |

**Defaults** N/A

**Command Mode** Privileged EXEC mode

**Usage Guide** N/A

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

```
Ruijie#show cwmp status
CWMP Status                  : enable
Session status               : Close
Last success session          : Unknown
Last success session time      : Thu Jan  1 00:00:00 1970
Last fail session             : Unknown
Last fail session time         : Thu Jan  1 00:00:00 1970
Session retry times           : 0
```

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

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

**Related Commands**

| Command | Description |
|---|---|
| **show cwmp configuration** | Displays the current configuration of CWMP. |

**Platform Description** N/A

## 9.14 timer cpe-timeout

Uses this command to configure the session timeout period of the CPE.

**timer cpe- timeout** *seconds*

**no timer cpe-timeout**

**Parameter Description**

| Parameter | Description |
|---|---|
| *seconds* | Sets the session timeout, in the range from 5 to 600 in the unit of seconds. |

**Defaults** By default, the session timeout period is 5 seconds.

**Command** CWMP configuration mode

**Mode**

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

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

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

```
Ruijie#config terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Ruijie(config)#cwmp
Ruijie(config-cwmp)#timer cpe-timeout 50
Ruijie(config-cwmp)#
```

**Related Commands**

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

**Platform Description** N/A

# 10 LED Commands

## 10.1 quiet-mode session

Use this command to configure LED quiet mode.

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

**quiet-mode session** *session-num*

**no quiet-mode session** *session-num*

**Parameter Description**

| Parameter | Description |
|---|---|
| *session-num* | Session ID. |

**Defaults** This function is disabled by default.

**Command Mode** AP configuration mode

**Usage Guide** Use this command to turn off all LEDs on the AP.

**Configuration Examples** The following example configures LED quiet mode from 23:00 that night to 7:00 next day.

```
Ruijie(config)#schedule session 1
Ruijie(config)#schedule session 1 time-range 1 period Mon time 23:00 to 7:00
Ruijie(config)#ap-config 00d0.f822.33bc
Ruijie(config-ap)#quiet-mode session 1
```

The following example disables LED quiet mode.

```
Ruijie(config)#ap-config 00d0.f822.33bc
Ruijie(config-ap)#no quiet-mode session 1
```

**Platform Description** N/A

# 11 USB Commands

## 11.1 show usb

Use this command to display the information about the inserted USB device in the system.

**show usb**

**Parameter Description**

| Parameter | Description |
|---|---|
| N/A | N/A |

**Defaults** N/A

**Command Mode** Privileged EXEC mode.

**Usage Guide** Device information is displayed if there is a USB device. Otherwise, there is no output. If the USB disk is connected to the USB port on the device, the ID displayed by running the **show usb** command is X, the USB port number. If the USB disk is connected to the USB port on the device via a HUB, the ID displayed by running the **show usb** command is X-Y, in which X stands for the USB port number and Y for the HUB slot number.

**Configuration Examples** The following example displays the information about the USB device:

```
Ruijie# show usb
Device: Mass Storage:
ID: 0
URL prefix: usb0
Disk Partitions:
usb0(type:FAT32)
Size : 131,072,000B(125MB)
Available size: 1,260,020B(1.2MB)
```

In above information, the Mass Storage Device is the name of the device.

The meaning of the information is as below:

Table 1: the description of the field.

| Field | Description |
|---|---|
| URL | Prefix used to access the USB device. |
| Size | Accessible size of the USB device. |
| Available size | Available size of the USB device. |

**Related Commands**

| Command | Description |
|---|---|
| N/A | N/A |

**Platform Description** N/A

## 11.2 usb remove

Use this command to remove the USB device.

**usb remove** *device_id*

**Parameter Description**

| Parameter | Description |
| --- | --- |
| *device_id* | Device ID of USB to be removed. |

**Defaults** N/A

**Command Mode** Privileged EXEC mode.

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

**Configuration Examples** The following example removes the USB device.

```
Ruijie# usb remove 0
OK, now you can pull out the device 0.
```

At this moment, the USB device can be plugged out.

**Related Commands**

| Command | Description |
| --- | --- |
| N/A | N/A |

**Platform Description** N/A

# 12 PKG_MGMT Commands

## 12.1 patch active

Use this command to activate a patch to take effect.

**patch active**

**Parameter Description**

| Parameter | Description |
| --- | --- |
| N/A | N/A |

**Defaults** N/A

**Command Mode** Privileged EXEC mode

**Default Level** 2

**Usage Guide** Activating operation can be performed only on the device already installed with a patch, after which the patch really takes effect. This command can be used to activate a hot patch temporarily. The activated patch becomes invalid after device restart.

**Configuration Examples** The following example activates a patch on the box device.

```
Ruijie#patch active
 Active the patch package success
```

The following example activates a patch on the chassis device.

```
Ruijie#patch active slot 8
[Slot 8]:
 Active the patch package success
```

**Verification** Use the **show patch** command to display patch information.

**Prompt Messages** The patch is activated successfully.

```
Active the patch package success
```

The running fails and a patch package needs to be installed at first.

```
Patch not installed
```

There is no need to run the command for the patch in the activated or running status.

```
The patch status is already active or running
```

Contact the service center to solve the package problem.

```
Cannot find the package's scripts file
```

**Common Errors**

There is no hot patch installed on current device.

The hot patch on current device is already activated.

**Platforms**

N/A

## 12.2 patch deactive

Use this command to deactivate a patch.

**patch deactive**

**Parameter Description**

| Parameter | Description |
| --- | --- |
| N/A | N/A |

**Command Mode**

Privileged EXEC mode

**Default Level**

2

**Usage Guide**

This commandcan be performed to deactivate a patch only after the patch is in the activated status.

**Configuration Examples**

The following example deactivates a patch on the box device.

```
Ruijie#patch deactive
 Deactive the patch package success
```

The following example deactivates a patch on the chassis device.

```
Ruijie#patch deactive slot 8
 [Slot 8]:
Deactive the patch package success
```

**Verification**

Use the **show patch** command to display patch information.

**Prompt Messages**

The patch is deactivated successfully.

```
Deactive the patch package success;
```

The running fails and a patch package needs to be installed at first.

```
Patch not installed
```

There is no need to run the command for the patch in the deactivated status.

```
The patch is not in active or running status
```

Contact the service center to solve the package problem.

```
Cannot find the package's scripts file
```

**Common Errors**

There is no hot patch installed on current device.

The hot patch on current device is already invalid.

## 12.3 patch delete

Use this command to uninstall a patch.

**patch delete**

**Parameter Description**

| Parameter | Description |
| --- | --- |
| N/A | N/A |

**Command Mode**

Privileged EXEC mode

**Default Level**

2

**Usage Guide**

This command is used to remove the existing hot patch package on the device.

**Configuration Examples**

The following example removes the installed hot patch package from the box device.

```
Ruijie# patch delete
Clear the patch patch_bridge success
Clear the patch success
```

The following example removes the installed hot patch package from the chassis device.

```
Ruijie# patch delete slot M1
[Slot M1]:
Clear the patch patch_bridge success
Clear the patch success
```

**Verification**

Use the **show patch** command to display patch status.

**Prompt Messages**

The patch is uninstalled successfully.

```
Clear the patch success
```

A hot patch package should be installed at first for it has not been installed.

```
Patch not installed
```

**Common Errors** There is no hot patch installed on current device.

## 12.4 patch running

Use this command to activate a patch permanently.

**patch running**

**Parameter Description**

| Parameter | Description |
|---|---|
| N/A | N/A |

**Command Mode** Privileged EXEC mode

**Default Level** 2

**Usage Guide** Activating operation can be performed only on the device already installed with a patch, after which the patch really takes effect. This command can be used to activate a hot patch permanently.

**Configuration Examples** The following example activates a patch on the box device.

```
Ruijie#patch running
The patch on the system now is in running status
```

The following example activates a patch on the chassis device.

```
Ruijie#patch running slot M1
[Slot M1]:
The patch on the system now is in running status
```

**Verification** Use the **show patch** command to display the patch information.

**Prompt Messages** The patch is activated permanently.

```
The patch on the system now is in running status
```

The running fails and a patch package needs to be installed at first.

```
Patch not installed
```

There is no need to run the command for the patch is in the deactivated status.

```
The patch is not in active or running status
```

Contact the service center to solve the package problem.

```
Cannot find the package's scripts file
```

**Common** There is no hot patch on current device.

**Errors** The hot patch is already activated on current device.

## 12.5 show component

Use this command todisplay all components already installed on current device and their information.

**show component** [ *component _name* ]

**Parameter Description**

| Parameter | Description |
|---|---|
| *component _name* | Name of the components<br>When this parameter value is N/A, the command is used to display all components already installed on the device and basic information of these components.<br>When this parameter value is not N/A, the command is used to display detailed information of the corresponding component, check whether the component isintact, and check whether this component works properly. |

**Command Mode** Privileged EXEC mode

**Default Level** 2

**Usage Guide** This command includes one with *component_name* and one without *component_name*. During upgrade, it requires users to understand all components installed on current device and their version information before components deletion. This needs to use the **show component** command without *component_name*. The **show component** command with *component_name* is used to obtain details of the corresponding component. The detailed information enables users to easily realize components' operation and damage. It is significant to insure their troubleshooting, security and reliability.

Some components in use will change their defaults files. Though this is more possibly normal than malicious, the **show component** command is used only to judge whether component files change in use. It is unable to distinguish natural damage from malicious one. It depends on users to make a further judgment.

**Configuration Examples** The following example displays all components already installed on the box device and their information.

```
Ruijie# show component
Package :sysmonit
    Version:1.0.1.23cd34aa      Build time: Wed Dec  7 00:58:56 2013
    Size:12877  Install time :Wed   Mar 5 14:23:12 2012
    Description: this is a system monit package
    Required packages: None
```

```
------------------------------------------------------------------
Package:bridge
    Version:2.0.1.37cd5cda     Build time: Wed Dec  7 00:54:56 2013
    Size:23245  Install time :Wed   Mar 5 14:30:12 2012
    Description: this is a bridge package
    Required packages: None
------------------------------------------------------------------
```

This command is used to obtain all components already installed on the device and theirbasic information. The information offers a basis for users to decide whether to upgrade or delete components.

| Field | Description |
|---|---|
| Package | Name of the component |
| Version | Version number of the component |
| Build time | Compilation time of the component on the server |
| Size | Content size of the component |
| Install time | Installation time of the component |
| Description | Simple functional description of the component |
| Required packages | Name of required packages |

The following example displays the information of all feature components already installed on the chassis device.

```
Ruijie#show component slot 8
Ruijie#*
[Slot 8]:
Package : utils-system
    Version: 1.0.0.433ef8d       Build time: Sun May 19 19:22:54 2013
    Size: 823936   Install time: Sun May 19 19:27:04 2013
    Description: utils system compile
    Required packages: None
----------------------------------
Package : tcl-expect
    Version: 1.0.0.433ef8d       Build time: Sun May 19 19:19:18 2013
    Size: 3474153        Install time: Sun May 19 19:27:04 2013
    Description: tcl & expect packages
    Required packages: None
----------------------------------
```

The following example displays the information of specified components already installed on the box device.

```
Ruijie# show componentbridge
package:bridge
    Version: 2.3.1.1252ea      Build time: Wed Dec  7 00:54:56 2013
    Size:26945  Install time : Wed  Mar 19:23:15 2012
```

```
    Description:this is a bridge package
    Required packages: None
    Package files:
       /lib64
       /lib64/libbridge.so
       /sbin
    /sbin/bridge

   Package file validate: [OK]
   Required relationship verify: [OK]
```

The other information except the basic information of components is listed as follows.

| Field | Description |
|---|---|
| Package file validate | Checks whether the component filesare intact. “OK” is displayed when all component files work properly; “ERR” is displayed together with their names when some component files are lost or revised. |
| Required package | Lists all required packages of the component. “OK” is labeled if required components are already installed; “ERR” is labeled if not together with detailed description about their names and versions. |
| Package files | Lists all files contained in the package. |

**Prompt Messages** The execution is successful with all components information displayed.

```
Package :sysmonit
    Version:1.0.1.23cd34aa     Build time: Wed Dec  7 00:58:56 2013
    Size:12877  Install time :Wed   Mar 5 14:23:12 2012
    Description: this is a system monit package
    Required packages: None
--------------------------------------------------------------------
Package:bridge
    Version:2.0.1.37cd5cda     Build time: Wed Dec  7 00:54:56 2013
    Size:23245  Install time :Wed   Mar 5 14:30:12 2012
    Description: this is a bridge package
    Required packages: None
--------------------------------------------------------------------
```

## 12.6 show patch

Use this command to display the information of a hot patch package already installed on the device.

**show patch** [ *patch _name* ]

**Parameter Description**

| Parameter | Description |
| --- | --- |
| *patch _name* | Name of the patches<br>When this parameter value is N/A, the command is used to display all components already installed on the device and basic information of these components.<br>When this parameter value is not N/A, the command is used to display detailed information of the corresponding component, check whether the component is intact, and check whether this component works properly. |

**Command Mode** Privileged EXEC mode

**Default Level** 2

**Usage Guide** This command is used to check all patches already installed on the device and their information.

**Configuration Examples** The following example displays all patches already installed on the box device.

```
Ruijie# show patch
patch package patch_install installed in the system, version:pa1
Package : patch_bridge
status:running
Version: pa1      Build time: Mon May 13 09:03:07 2013
Size: 277     Install time: Tue May 21 03:07:17 2013
    Description: a patch for bridge
    Required packages: None
```

This command is used to obtain the basic information of all patches already installed on the device.

| Field | Description |
| --- | --- |
| Package | Name of the patch |
| status | Status of the patch |
| Version | Version of the patch |
| Build time | Compilation time of the patch on the server |
| Size | Content size of the patch |
| Install time | Installation time of the patch |
| Description | Simple functional description of the patch |

The following example displays the information of all patches installed on the chassis device.

```
Ruijie#show patch slot 8
[Slot 8]:
Patch package patch_install installed in the system, version:pa1
Package : patch_test
Status: running
    Version: 1.0.0.05151504
```

```
    Build time: Wed May 15 07:04:28 2013
    Size: 1804
    Install time: Thu Jan  1 00:56:43 1970
    Description: Experimentation
    Required packages: None
-----------------------------------
```

The following example displays the information of particular patches installed on the box device.

```
Ruijie# show componentbridge
package:bridge
    Version: 2.3.1.1252ea      Build time: Wed Dec  7 00:54:56 2011
    Size:26945  Install time : Wed  Mar 19:23:15 2012
    Description:this is a bridge package
    Required packages: None
    Package files:
       /lib64
       /lib64/libbridge.so
       /sbin
    /sbin/bridge

   Package file validate: [OK]
```

The other information except the basic information of the patch is listed as follows:

| Field | Description |
|---|---|
| Package file validate | Checks whether the patch files are intact. “OK” is displayed when all patch files work properly; “ERR” is displayed together with their names when some files are lost or revised. |
| Package files | Lists all files contained in the patch package. |

**Prompt Messages** The information of the patch is displayed after successful running.

```
Patch package patch_install installed in the system, version:pa1
Package : patch_bridge
 Status:running
 Version: pa1      Build time: Mon May 13 09:03:07 2013
Size: 277     Install time: Tue May 21 03:07:17 2013
    Description: a patch for bridge
    Required packages: None
```

## 12.7 show upgrade file

Use this command to display the information of the installation package files in the device file system.

**show upgrade file** *url*

**Parameter**

| Parameter | Description |
|---|---|

**Description**

| | |
|---|---|
| *url* | The local *url* path indicates where an installation package file is stored. |

**Command Mode** Privileged EXEC mode

**Default Level** 2

**Usage Guide** This command is used to preview main messages of an installation package after it is downloaded into local file system.

This command is not applied to a chassis package.

**Configuration Examples** The following example displays the information of an installation package file.

```
Ruijie# show upgrade file flash://bridge_eg1000m_2.3.1.1252ea-1.mips.rpm
Name    : bridge
Version:1.0.1.23cd34aa
Package type     : common component
Support target   : eg1000m
Size            : 26945
Build time       : Wed Dec  7 00:54:56 2013
Install date     : (not installed)
Description      : this is a bridge package
Package files :
    Package files:
       /lib64
       /lib64/libbridge.so
       /sbin
       /sbin/bridge
```

This command is used to obtain the information in the package.

| Field | Description |
|---|---|
| Name | Name of the package |
| Version | Version of the package |
| Package type | Type of the package |
| Support target | Supported product description |
| Size | Content size of the package |
| Build time | Compilation time of the package |
| Install date | Installation time of the package |
| Description | Description of the package |
| Package files | All contents in the package |

**Prompt Messages** The package information is displayed after running.

```
Name    : bridge
```

```
Version:1.0.1.23cd34aa
Package type     : common component
Support target   : eg1000m
Size            : 26945
Build time       : Wed Dec  7 00:54:56 2013
Install date     : (not installed)
Description      : this is a bridge package
Package files :
    Package files:
       /lib64
       /lib64/libbridge.so
       /sbin
   /sbin/bridge
```

## 12.8 show upgrade history

Use this command to display the upgrade history.

**show upgrade history**

**Parameter Description**

| Parameter | Description |
|---|---|
| N/A | N/A |

**Command Mode** Privileged EXEC mode

**Default Level** 2

**Configuration Examples** The following example displays the upgrade history.

```
Ruijie#show upgrade history
Last Upgrade Information:
   Time:        2014-08-31 12:15:03
   Method:      LOCAL
Package Name: N18000_RGOS11.0(1)B1_CM_01200616_install.bin
Package Type: Distribution
```

**Prompt Messages** N/A

**Platforms** N/A

# 12.9 upgrade

Use this command to install and upgrade an installation package in the local file system.

**upgrade** [*url* [ **force** ]

**Parameter Description**

| Parameter | Description |
|---|---|
| *url* | The local path indicates where an installation package is stored. This command is used to upgrade an installation package on the device. |
| **force** | Mandatory upgrade |

**Command Mode** Privileged EXEC mode

**Default Level** 2

**Usage Guide** This command is applicable to installation packages of all subsystem components, chassis devices, feature components and hot patches. Before its use, run the **copy** command to copy feature packages into the file system in the device.
When there is no specified range of parameters, the command is used to upgrade the matched system components according to the auto-sync configuration.

**Configuration Examples** The following example upgrades the main package on the device.

```
Ruijie#upgrade usb0:/eg1000m_main_1.0.0.0f328e91.bin
Upgrade processing is 10%
Upgrade processing is 60%
Upgrade processing is 90%
Upgrade info [OK]
Kernel version[2.6.32.91f9d21->2.6.32.9f8b56f]
Rootfs version[1.0.0.2ad02537->1.0.0.1bcc12e8]
Upgrade processing is 100%
Reload system to take effect!
```

The following example upgrades the chassis package on the device.

```
Ruijie# upgrade usb0:/ ca-octeon_11.0(1B2)_20131106_main_install.bin
[Slot M1]:Upgrade processing is 10%

 [Slot 1]:Upgrade processing is 10%

 [Slot M1]:Upgrade processing is 60%

 [Slot 1]:Upgrade processing is 60%
```

```
[Slot M1]:Upgrade processing is 90%

[Slot M1]:
Upgrade info [OK]
  Kernel version[2.6.32.abb2b41f170c81->2.6.32.abb2b415749f40]
  Rootfs version[1.0.0.d5f0de03->1.0.0.660e0085]

[Slot M1]:Restart to take effect !

[Slot M1]:Upgrade processing is 100%
[Slot 1]:Upgrade processing is 90%

[Slot 1]:
Upgrade info [OK]
  Kernel version[2.6.32.9f8b56f1d45ab2 ->2.6.32.0f48cb9f170c81]
  Rootfs version[1.0.0.2ad02537->1.0.0.1bcc12e8]

[Slot 1]:Restart to take effect !

[Slot 1]:Upgrade processing is 100%
[slot: M1]
  device_name: ca-octeon-cm
  status:     SUCCESS
[slot: 1]
  device_name: ca-octeon-lc
Status:     SUCCESS
```

**Verification** Run the **show version detail** command to check whether the upgrade of a subsystem component is successful.
Run the **show component** command to check whether the upgrade of a feature component is successful. upgrading a feature component
Run the **show patch** command to check whether the upgrade of a hot patch is successful.

**Prompt Messages** The prompt message of successful running is displayed.

```
Upgrade info [OK]
```

The installation package is invalid or damaged and needs to be regained for upgrade command.

```
Invalid package file
```

The installation package is not available on the device and needs to be regained for upgrade command.

```
Device don't support
```

There is no need to upgrade the device.

```
The version in device is newer or the same
```

When there is insufficient space for upgrade, check USB flash disk attached on the device.

```
No enough space for decompress
```

Contact the service center to solve the system problem.

```
No enough space,rootfs been destroyed. Please upgrade in uboot
```

The existing patch package needs to be uninstalled before upgrade.

```
Already exist patch, please uninstall before upgrade
```

The patch package is not applicable to this system and needs to be changed.

```
Patch compatibility err
```

The upgrade of a patch package is not available on this device and needs to be regained.

```
some origin cmpnt has change
```

## 12.10 upgrade download tftp

Use this command to download, install and upgrade installation packages from the tftp server.

**upgrade download tftp:**/*path* [ **force** ]

**Parameter Description**

| Parameter | Description |
|---|---|
| *path* | The path of installation packages on the tftp server<br>This command is downloaded and upgraded automatically from the server. |
| **force** | Enforces upgrade. |

**Command Mode** Privileged EXEC mode

**Default Level** 2

**Usage Guide** This command is applicable to installation packages of all subsystem components, chassis devices, feature components and hot patches. This command is used to perform automatic installation, copy and upgrade of files.

**Configuration Examples** The following example upgrades the main package.

```
Ruijie# upgrade download
tftp://192.168.201.98/eg1000m_main_1.0.0.0f328e91.bin
Accessing tftp://192.168.201.98/eg1000m_main_1.0.0.0f328e91.bin...
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
```

```
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!
Transmission finished, file length 21525888 bytes.
 Upgrade processing is 10%
 Upgrade processing is 60%
 Upgrade processing is 90%
 Upgrade info [OK]
       Kernel version[2.6.32.91f9d21->2.6.32.9f8b56f]
       Rootfs version[1.0.0.2ad02537->1.0.0.1bcc12e8]
 Upgrade processing is 100%
Reload to take effect!
```

**Verification** Run the **show version detail** command to check whether the upgrade of a subsystem component is successful.
Run the **show component** command to check whether the upgrade of a feature component is successful.
Run the **show patch** command to check whether the upgrade is successful of a hot patch package.

**Prompt Messages** The prompt message of successful running is displayed.

```
Upgrade info [OK];
```

The installation package is invalid or damaged and needs to be regained for upgrade command.

```
Invalid package file
```

The installation package is not available on the device and needs to be regained for upgrade command.

```
Device don't support
```

There is no need to upgrade the device.

```
The version in device is newer or the same
```

When there is insufficient space for upgrade, check USB flash disk attached on the device.

```
No enough space for decompress
```

Contact the service center to solve the system problem.

```
No enough space,rootfs been destroyed. Please upgrade in uboot
```

The existing patch package needs to be deleted.

```
Already exist patch, please uninstall before upgrade
```

The patch package is not compatible on this device. Replace the package..

```
Patch compatibility err
```

The upgrade of the patch package is not applied to the device. Regain the package.

```
Some origin component has change
```

## 12.11 upgrade rollback

Use this command to roll a subsystem back to the version before the upgrade.

**upgrade rollback**

**Parameter Description**

| Parameter | Description |
|---|---|
| N/A | N/A |

**Command Mode** Privileged EXEC mode

**Default Level** 2

**Usage Guide** This command is used when the device cannot work properly after subsystem upgrade. It takes effect only when the last upgrade of subsystem components is successful.

The command is valid after device restart. The recursive rollback cannot be executed through this command in succession.

**Configuration Examples** The following example rolls a subsystem back to the version before the upgrade on the box device.

```
Ruijie#upgrade rollback
kernel rollback version[2.6.32.9f8b56f->2.6.32.91f9d21][OK]
rootfs rollback version[1.0.0.1bcc12e8->1.0.0.2ad02537][OK]
Rollback success!
Reload system to take effect!
```

The following example rolls a subsystem back to the version before the upgrade on the chassis device.

```
Ruijie#upgrade rollback slot M1
[Slot M1]:
kernel rollback version[2.6.32.9f8b56f->2.6.32.91f9d21][OK]
rootfs rollback version[1.0.0.1bcc12e8->1.0.0.2ad02537][OK]
Rollback success!
Reload system to take effect!
```

**Verification** Run the **show version detail** command to check the result of rolling back subsystem components after device restart.

**Prompt Messages** The prompt message of successful running is displayed.

```
Rollback success!
Restart to take effect !
```

The rollback operation cannot be performed when subsystem components have not been upgraded last time.

```
Not subsys package last upgrade
```

The rollback operation cannot be performed for the last upgrade is not successful.

```
Last upgrade err or skip
```

The upgrade command has not been run or the rollback operation has been performed.

```
Monitor file lost
```

**Common Errors** The last upgrade is not for subsystem components, but for feature packages, hot patch packages and so on.
Run the rollback command for subsystem once.

## 12.12 clear storage

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

**Parameter Description**

| Parameter | Description |
|---|---|
| *url* | A local *url* directory or full path name indicates where the installation package is stored |

**Command Mode** Privileged EXEC mode

**Default Level** 2

**Usage Guide** This command is used to remove an installation package or all packages in a directory and all installation packages on the local device.

**Configuration Examples**

```
Ruijie#clear storage
Remove the whole storage directory?[y/n]y
Ruijie#clear storage usb0
Remove the file or directory usb0 from the storage?[y/n]y
Ruijie#
```

**Verification** Check specified *url*

**Platforms** N/A

# 13 SYS Commands

## 13.1 calendar set

Use this command to set the hardware calendar.

**calendar set** [ *month* [ *day* [ *year* ] ] ]

**Parameter Description**

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

**Defaults**

-

**Command Mode**

Privileged EXEC mode

**Default Level**

-

**Usage Guide**

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

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

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

**Configuration Examples**

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

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

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

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

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

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

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

**Check Method** -

**Platform Description** -

## 13.2 clock read-calendar

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

**clock read-calendar**

**Parameter Description**

| Parameter | Description |
|---|---|
| - | - |

**Defaults** -

**Command Mode** Privileged EXEC mode

**Default Level** -

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

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

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

**Check Method** -

**Platform Description** -

## 13.3 clock set

Use this command to set the system software clock.

**clock set** [ *month* [ *day* [ *year* ] ] ]

**Parameter Description**

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

**Defaults** -

**Command Mode** Privileged EXEC mode

**Default Level** -

**Usage Guide**

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

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

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

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

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

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

```
Ruijie# clock set 6
```

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

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

```
Ruijie# clock set 6:42
06:42:31 CST Fri, Mar 2, 2012
```

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

```
Ruijie# clock set 18 3 2
18:42:48 CST Fri, Mar 2, 2012
```

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

**Check Method** -

**Platform Description** -

## 13.4 clock summer-time

Use this command to set the summer time.
**clock summer-time** *zone* **start** *start-month* [*week*|**last**] *start-date hh:mm* **end** *end-month* [*week*| **last**] *end-date hh:mm* [ **ahead** *hours-offset* [*minutes-offset* ]

Use this command to disable the summer time.
**no clock summer-time**

**Parameter Description**

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

**Defaults** -

**Command Mode** configuration mode

**Default Level** -

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

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

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

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

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

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

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

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

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

The following example disables summer time.

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

**Check Method** -

**Platform Description** -

# 13.5 clock timezone

Use this command to set the time zone.

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

Use this command to remove the time zone settings.

**no clock timezone**

**Parameter Description**

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

**Defaults**

-

**Command Mode**

configuration mode

**Default Level**

-

**Usage Guide**

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

**Configuration Examples**

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

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

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

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

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

The following example removes the time zone settings.

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

```
Set no clock timezone.
```

**Check Method** -

**Platform Description** -

## 13.6 clock update-calendar

Use this command to enable the system to synchronize the hardware time with the software time.
**clock update-calendar**

**Parameter Description**

| Parameter | Description |
| --- | --- |
| - | - |

**Defaults** -

**Command Mode** Privileged EXEC mode

**Default Level** -

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

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

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

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

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

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

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

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

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

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

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

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

**Check Method** -

**Platform Description** -

## 13.7 cpu high-watermark set

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

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

Use this command to disable CPU usage monitoring.

**no cpu high-watermark set**

Use this command to restore the default settings.

**default cpu high-watermark set**

**Parameter Description**

| Parameter | Description |
| --- | --- |
| **high** *high-value* | Sets the high watermark of the CPU usage. The range is from 2 to 99. |
| **range** *range-value* | Sets the watermark fluctuation range. The range is from 1 to 20. |

**Defaults**

By default, the watermark of the CPU usage is 80% and the watermark fluctuation range is 5% (namely, the range of the CPU usage watermark is from 75% and 85%).

**Command Mode**

configuration mode

**Default Level**

-

**Usage Guide**

This command is supported only in VSD0 mode. Multiple VSDs are not supported.
You can use this command to set the high watermark of the CPU usage and enable CPU usage monitoring. When detecting that the CPU usage exceeds the fluctuation range of the highest watermark, the system prints prompts.

**Configuration Examples**

The following example sets the CPU usage watermark to the default value and enables CPU usage monitoring (if it is disabled).

```
Ruijie(config)# default cpu high-watermark set
Reset default cpu watermark monitor
set system cpu watermark high 80%(75%~85%)
```

The following example disables CPU usage monitoring.

```
Ruijie(config)# no cpu high-watermark set
Close cpu watermark monitor
```

The following example enables CPU usage monitoring. Keep the defined watermark value.

```
Ruijie(config)# cpu high-watermark set
Open cpu watermark monitor
set system cpu watermark high 80%(75%~85%)
```

The following example enables CPU usage monitoring and sets the high watermark to 88% and fluctuation range to 3%.

```
Ruijie(config)# cpu high-watermark set high 88 range 3
Open cpu watermark monitor
set system cpu watermark high 88%(85%~91%)
```

In this case, the high watermark is set to 88%. The upper limit of the high watermark is 91% (88%+3%) and the lower limit is 85% (88%-3%).

**Check Method**

-

**Prompt Message**

If the high watermark of the CPU usage is allowed to fluctuate from 85% to 91%, the system will print the following warning message when the CPU usage exceeds the upper limit of the high watermark:

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

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

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

**Platform Description** -

## 13.8 memory low-watermark set

Use this command to set the low watermark threshold of the memory and enable the memory low watermark detection.
**memory low-watermark set** *mem-value*

Use this command to disable the detection of memory low watermark.
**no memory low-watermark set**

**Parameter Description**

| Parameter | Description |
|---|---|
| *mem-value* | Memory watermark threshold. The range is from 1 KB to 4,294,967,295 KB. |

**Defaults** By default, the detection of memory low watermark is disabled.

**Command Mode** Global configuration mode

**Default Level** -

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

**Configuration Examples** The following example sets the low watermark threshold of the memory to 500,000 KB and enables detection.

```
Ruijie(config)#memory low-watermark 500000
```

**Check Method** -

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

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

**Platform Description** -

## 13.9 memory history clear

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

**memory history clear** [ **one-forth | half | all** ]

**Parameter Description**

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

**Defaults** -

**Command Mode** Global configuration mode

**Default Level** -

**Usage Guide** -

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

```
Ruijie# show memory history

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

Time Thu Jan  1 00:24:41 1970
Used(k) 148492
Maxinum memory users for this period
Process Name    Holding
tcpip.elf       270028
cli-memory      52408
rg_syslogd      36640

Time Thu Jan  1 00:24:41 1970
Used(k) 148444
```

```
Maxinum memory users for this period
Process Name    Holding
tcpip.elf       270028
cli-memory      44088
rg_syslogd      36640

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

**Check Method** -

**Prompt Message** -

**Platform Description** -

## 13.10 reload

Use this command to reload the device.

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

**Parameter Description**

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

**Defaults** -

**Command Mode** Privileged EXEC mode

**Default Level** -

**Usage Guide** -

**Configuration Examples** The following example reloads the device.

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

```
Restarting system...
```

**Check Method** -

**Prompt Message** -

**Platform Description** -

## 13.11 show calendar

Use this command to display the hardware calendar.

**show calendar**

**Parameter Description**

| Parameter | Description |
| --- | --- |
| - | - |

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

**Default Level** -

**Usage Guide** -

**Configuration Examples** The following example displays the hardware calendar.

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

**Prompt Message** -

**Platform Description** -

## 13.12 show clock

Use this command to display the system software clock.

**show clock**

**Parameter Description**

| Parameter | Description |
| --- | --- |

| | |
|---|---|
| - | - |

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

**Default Level** -

**Usage Guide** -

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

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

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

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

**Prompt Message** -

**Platform Description** -

## 13.13 show memory

Use this command to display the system memory.

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

**Parameter Description**

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

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

**Default Level** -

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

history entries.

**Configuration Examples**

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

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

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

Description of some keywords in the command:

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

Description of the displayed information on each task:

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

**Prompt Message** -

**Platform Description** -

## 13.14 show memory vsd

Use this command to display memory information.

**show memory vsd** *vsd_id*

**Parameter Description**

| Parameter | Description |
|---|---|
| *vsd_id* | VSD ID is a digit. You can use the **show vsd** command to display the ID of each VSD. The ID range is from 0 to 16. |

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

**Default Level** -

**Usage Guide**

This command is supported only in VSD0 mode.

**Configuration Examples**

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

```
Ruijie#show memory vsd 1
PID     Text    Rss     Data    Stack   Total   Process
1408    244     1192    25400   84      32164   tty_secu_enable
1385    104     16288   648     84      18648   gvpd
1384    304     3872    17084   84      24728   wbamain
1382    376     17708   33656   84      53308   snooping.elf
1381    84      2156    16736   84      22956   password_policy
1380    72      1096    404     84      3848    dns_client.elf
1379    168     2580    472     84      5352    rg-rmond
1378    652     3504    9768    84      15964   rg-snmpd
1376    208     1452    10672   84      14872   rg-fsui
1375    116     2020    33464   84      37288   rg-telnetc
1373    24      844     220     84      2824    rg-telnetd
1372    724     2364    17016   84      24380   rg-sshd
1371    244     2996    35780   84      42544   rg-tty-admin
1365    132     2168    9004    84      13796   vrrp_plus.elf
1364    312     16944   764     84      20368   vrrp.elf
1363    124     16988   500     84      19744   lacp.elf
1358    24      1380    320     84      3536    ftpc_cli.elf
1357    124     1944    8552    84      14976   ftp_server.elf
```

```
1352    340     3032    74704   84      80768   dhcp6.elf
1351    312     1960    988     84      6116    dhcp.elf
1350    388     17808   920     84      21600   mstp.elf
1349    240     3876    976     84      9536    rpi.elf
1348    1316    4656    1004    84      10764   isis.elf
1347    212     4220    872     84      9368    ripng.elf
1345    460     4284    876     84      9656    rip.elf
1344    1800    5568    1572    84      12156   bgp.elf
1340    1084    4700    1024    84      10928   ldp.elf
1339    288     17684   556     84      21472   msf.elf
1338    208     3604    42712   84      47708   rg-syslogd
--More--
```

**Prompt Message** -

**Platform Description** -

## 13.15 show pci-bus

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

**show pci-bus**

**Parameter Description**

| Parameter | Description |
| --- | --- |
| - | - |

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

**Default Level** -

**Usage Guide** -

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

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

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

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

**Prompt Message** -

**Platform Description** -

## 13.16 show processes cpu

Use this command to display system task information.

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

**Parameter Description**

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

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

**Default Level** -

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

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

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

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

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


--More--
```

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

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

Description of the information displayed in this command:

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

The task running statuses are listed below:

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

Description of each task:

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

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

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

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

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

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

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

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

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

Example:

```
Ruijie#show processes cpu history


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

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

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



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

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

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

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

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

Example:

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

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

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

**Prompt Message** -

**Platform Description** -

## 13.17 show processes cpu detailed

Use this command to display the details of the specified task.

**show processes cpu detailed** { *process-id* | process-*name* }

**Parameter Description**

| Parameter | Description |
|---|---|
| *process-id* | Displays the information on the task of the specified task ID. |
| *process-name* | Displays the information on the task of the specified task name. |

**Command Mode** Privileged EXEC mode/ global configuration mode

**Default Level** -

**Usage Guide** This command is supported only in VSD0 mode. Multiple VSDs are not supported.

**Configuration Examples** The following example displays the information on the task of the specified task name.

```
Ruijie# show processes cpu detailed demo
Process Id    : 1820
Process Name  : demo
Vsdid         : 0
Process Ppid  : 1

State         : R(running)
On CPU        : 0
Priority      : 20
Age Time      : 24:06.5
Run Time      : 00:01.0
Cpu Usage     :
    Lass  5 sec    0.3% (0.6%)
    Lass  1 min    0.3% (0.6%)
    Lass  5 min    0.3% (0.6%)
    Lass 15 min    0.3% (0.6%)
Tty           : ?
```

Code Usage: 209.6 KB. If the specified task name is not unique, the system displays the following message:

```
Ruijie# show processes cpu detailed demo
duplicate process, choose one by id not name.
name: demo, id: 1089, state: S(sleeping)
name: demo, id: 1091, state: R(running)
process name: monitor_procps, do NOT exist, or NOT only one.
```

Description of the displayed information:

| Field | Description |
|---|---|
| Process Id | Task ID |
| Vsdid | VSD ID of the task |
| Process Name | Task name |
| Process Ppid | Parent process task ID |
| State | Task running status |
| On CPU | CPU where the task is running |
| Priority | Task priority |
| Age Time | Duration for the task from self-startup to now |
| Run Time | Duration for the task from self-startup to being executed |

| | |
|---|---|
| Cpu Usage | CPU usage of the task within the last five seconds, one minute, five minutes, and 15 minutes.<br>The value in the round brackets is the CPU usage that is not divided by the total number of cores where the task runs. For example, the demo task is running on No.0 core, which is the control core and the system has two control cores. In this case, the CPU usage is 0.3% (0.6%). |
| Tty | Tty ID, in the format of "Primary device ID, secondary device ID". If it is 0, the value is **?**. |
| Code Usage | Size occupied by the task code segment |

The following example displays the information on the task of the specified task ID.

```
Ruijie# show process cpu detailed 1715
```

**Prompt Message** -

**Platform Description** -

## 13.18 show processes vsd

Use this command to display system task of the specified VSD.

**show process vsd** *vsd_id* **cpu**

**Parameter Description**

| Parameter | Description |
|---|---|
| *vsd_id* | VSD ID is a digit. You can use the **show vsd** command to display the ID of each VSD. The range is from 0 to 16. |

**Command Mode** Privileged EXEC mode/ global configuration mode

**Default Level** -

**Usage Guide**

This command is supported only in VSD0 mode. Multiple VSDs are not supported.

**Configuration Examples** The following example displays the system task information in VSD1 mode.

```
Ruijie#show processes vsd 1 cpu
```

**Prompt Message** -

**Platform Description** -

## 13.19 show usb-bus

Use this command to display the information on the device mounted to the USB bus.

**show usb-bus**

**Parameter Description**

| Parameter | Description |
| --- | --- |
| - | - |

**Command Mode** Privileged EXEC mode/ global configuration mode

**Default Level** -

**Usage Guide** -

**Configuration Examples** 1: The following example displays the information on the device mounted to the USB bus.

```
Ruijie# show usb-bus
Device: Linux Foundation 2.0 root hub
  Bus 001 Device 001: ID 1d6b:0002
```

**Prompt Message** -

**Platform Description** -

## 13.20 show version

Use this command to display the system version information.

**show version**

**Parameter Description**

| Parameter | Description |
| --- | --- |
| - | - |

**Command Mode** Privileged EXEC mode/ global configuration mode

**Default Level** -

**Usage Guide** -

**Usage Guide** The following example displays the system version information.

```
Ruijie# show version
System description      : Ruijie Indoor AP320-I (802.11a/n and 802.11b/g/n) By Ruijie Networks
System start time       : 2012-12-06 00:00:00
System uptime           : 0:03:20:07
System hardware version : 1.0.0
System software version : AP_RGOS11.0(1B1)
System serial number    : 1234942570018
System boot version     : 1.0.0
```

**Prompt Message** -

**Platform Description** -

## 13.21 show cpu

Use this command to display the information on the system task running on the control core instead of the non-virtual core.

**show cpu**

**Parameter Description**

| Parameter | Description |
|---|---|
| - | - |

**Command Mode** Privileged EXEC mode/ global configuration mode

**Default Level** -

**Usage Guide** This command is supported only in VSD0 mode. Multiple VSDs are not supported.
If the system is equipped with a virtual core, you can use the **show processes cpu** command to check the CPU usage of the virtual core.

**Configuration Examples** The following example displays the information on the system task running on the control core instead of the non-virtual core.

```
Ruijie#show cpu
=============================================
CPU Using Rate Information
CPU utilization in five seconds:  4.80%
CPU utilization in one minute:  4.10%
CPU utilization in five minutes:  4.00%

 NO      5Sec    1Min    5Min Process
```

```
    1    0.00%    0.00%    0.00% init
    2    0.00%    0.00%    0.00% kthreadd
    3    0.00%    0.00%    0.00% ksoftirqd/0
    4    0.00%    0.00%    0.00% events/0
--More--
```

**Prompt Message**

-

**Platform Description**

-

# 14 NTP Commands

## 14.1 no ntp

Use this command to disable Network Time Protocol (NTP), and clear all NTP configuration.

**no ntp**

**Parameter Description**

| Parameter | Description |
|---|---|
| N/A | N/A |

**Defaults** NTP is disabled by default.

**Command mode** Global configuration mode.

**Usage Guide** By default, NTP is disabled. However, once the NTP server or the NTP authentication is configured, the NTP service will be enabled.

**Configuration Examples** The following example disables NTP.

```
Ruijie(config)#no ntp
```

**Related Commands**

| Command | Description |
|---|---|
| **ntp server** | Specifies an NTP server. |

**Platform Description** N/A

## 14.2 ntp access-group

Use this command to configure an access group to control NTP access. Use the **no** form of this command to remove the peer access group.

**ntp access-group** { **peer** | **serve** | **serve-only** | **query-only** } *access-list-number* | *access-list-name*

**no ntp access-group** { **peer** | **serve** | **serve-only** | **query-only** } *access-list-number* | *access-list-name*

**Parameter Description**

| Parameter | Description |
|---|---|
| **peer** | Allows the device to receive time requests and NTP control queries to synchronize itself to the servers specified in the access list. |

| | |
|---|---|
| **serve** | Allows the device to receive time requests and NTP control queries from the servers specified in the access list but not to synchronize itself to the specified servers. |
| **serve-only** | Allows the device to receive only time requests from the servers specified in the access list. |
| **query-only** | Allows the device to receive only NTP control queries from servers specified in the access list. |
| *access-list-number* | Access control list number, ranging from 1 to 99 and 1300 to 1999. |
| *access-list-name* | Access control list name. |

**Defaults** No access rule to control NTP access is configured by default, namely, NTP access is granted to all devices.

**Command mode** Global configuration mode.

**Usage Guide** Use this command to configure an access group to control NTP access, providing a minimal security measures (more secure way is to use the NTP authentication mechanism).
The NTP service enables the access group options to be scanned in the following order, from least restrictive to most restrictive: **peer**, **serve**, **serve-only**, **query-only**.
If you do not configure any access groups, NTP access is granted to all devices. However, once you configure the access rule, NTP access is granted only to the devices specified in the access list.

⚠ NTP control query is not supported in the current system. Although it matches with the order in accordance with the above rules, the related requests about the control and query are not supported.

**Configuration Examples** The following example shows how to allow the device to only receive time requests from the device of 192.168.1.1.

```
Ruijie(config)# access-list 1 permit 192.168.1.1
Ruijie(config)# ntp access-group serve-only 1
```

**Related Commands**

| Command | Description |
|---|---|
| **ip access-list** | Creates an IP access control list. |

**Platform Description** N/A

## 14.3 ntp authenticate

Use this command to enable NTP authentication. Use the **no** form of this command to disable NTP authentication.
**ntp authenticate**

**no ntp authenticate**

**Parameter Description**

| Parameter | Description |
| --- | --- |
| N/A | N/A |

**Defaults** Disabled.

**Command mode** Global configuration mode.

**Usage Guide** If NTP authentication is disabled, the synchronization communication is not encrypted. To enable encrypted communication on the server, enable the NTP authentication and configure other keys globally.
NTP authentication is implemented through the trusted key specified by the **ntp authentication-key** and **ntp trusted-key** commands.

**Configuration Examples** After an authentication key is configured and specified as the global trusted key, enable NTP authentication.

```
Ruijie(config)#ntp authentication-key 6 md5 wooooop
Ruijie(config)#ntp trusted-key 6
Ruijie(config)#ntp authenticate
```

**Related Commands**

| Command | Description |
| --- | --- |
| **ntp authentication-key** | Sets the global authentication key. |
| **ntp trusted-key** | Configures the global trusted key. |

**Platform Description** N/A

## 14.4 ntp authentication-key

Use this command to configure an NTP authentication key. Use the **no** form of this command to remove the NTP authentication key.
**ntp authentication-key** *key-id* **md5** *key-string* [*enc-type*]
**no ntp authentication-key** *key-id*

**Parameter Description**

| Parameter | Description |
| --- | --- |
| *key-id* | Key ID, ranging from 1 to 4294967295. |
| *key-string* | Key string |
| *enc-type* | (Optional) Whether this key is encrypted, where, 0 indicates the key is |

| | |
|---|---|
| | not encrypted, 7 indicates the key is encrypted simply. The key is not encrypted by default. |

**Defaults** NTP authentication key is not configured by default.

**Command mode** Global configuration mode.

**Usage Guide** Use this command to configure an NTP authentication key and enables the **md5** algorithm for authentication. Each key presents a unique key ID, which can be configured as a trusted key using the **ntp trusted-key** command..
You can configure up to 1024 NTP authentication keys. However, each server can support only one key.

**Configuration Examples** The following example configures an NTP authentication key.

```
Ruijie(config)ntp authentication-key 6 md5 wooooop
```

**Related Commands**

| Command | Description |
|---|---|
| **ntp authenticate** | Enables NTP authentication. |
| **ntp trusted-key** | Configures an NTP trusted key. |
| **ntp server** | Specifies an NTP server. |

**Platform Description** N/A

## 14.5 ntp disable

Use this command to disable the device to receive NTP packets on the specified interface.
**ntp disable**

**Parameter Description**

| Parameter | Description |
|---|---|
| N/A | N/A |

**Defaults** All NTP packets can be received by default.

**Command mode** Interface configuration mode.

**Usage Guide** By default, the device receives NTP packets on all interfaces, and adjust clock for the client. You can use this command to disable the device to receive NTP packets on the specified interface.

⚠ This command is configured only the interface that can receive and send IP packets.

**Configuration Examples** The following example disables the device to receive the NTP packets.

```
Ruijie(config-if)# no ntp disable
```

**Related Commands**

| Command | Description |
| --- | --- |
| N/A | N/A |

**Platform Description** N/A

## 14.6 ntp master

Use this command to configure the device to act as an authoritative NTP server, synchronizing time to other devices. Use the **no** form of this command to remove the device as an authoritative NTP server.

**ntp master** [ *stratum* ]

**no ntp master**

**Parameter Description**

| Parameter | Description |
| --- | --- |
| *stratum* | Stratum level. The range is from 1 to 15. The default is 8. |

**Defaults** N/A

**Command mode** Global configuration mode.

**Usage Guide** In general, the local device synchronizes time from the external time source directly or indirectly. However, if the time synchronization fails due to network connection trouble, you can use this command to configure the local device to act as an authoritative NTP server to synchronize time to t other devices. Once configured, the device will not perform time synchronization with the time source which is of a higher stratum.

Configuring the device to act as an authoritative NTP server (in particular, specify a lower stratum level), may be likely to overwrite the effective time. If multiple devices in the same network are configured with this command, the time synchronization may be instable due to the time difference between the devices.

Before configuring this command, you need to manually correct the system clock to avoid too much bias if the device has never performed time synchronization with the external clock source.

**Configuration Examples** The following example configures the device to act as an authoritative NTP server, and sets the stratum level to 12:

```
Ruijie(config)# ntp master 12
```

**Related Commands**

| Command | Description |
| --- | --- |
| N/A | N/A |

**Platform Description** N/A

## 14.7 ntp server

Use this command to specify a NTP server for the NTP client. Use the **no** form of this command to delete the specified NTP server.

**ntp server** { *ip-addr* | *domain* | **ip** *domain* | **ipv6** *domain* } [ **version** *version* ] [ **source** *if-name* ] [ **key** *keyid* ] [ **prefer** ]

**no ntp server** *ip-addr*

**Parameter Description**

| Parameter | Description |
| --- | --- |
| *ip-addr* | Sets the IP address of the NTP server. The address can be in IPv4 or IPv6 format. |
| *domain* | Sets the domain name of the NTP server, supporting IPv4 and IPv6. |
| *version* | (Optional) Specifies the NTP version (1-3). The default is NTPv3. |
| *if-name* | (Optional) Specifies the source interface from which the NTP message is sent (L3 interface). |
| *keyid* | (Optional) Specifies the encryption key adopted when communication with the corresponding server. The key ID range is from 1 to 4,294,967,295. |
| **prefer** | (Optional) Specifies the given NTP server as the preferred one. |

**Defaults** No NTP server is configured by default.

**Command mode** Global configuration mode.

**Usage Guide** At present, RGOS system only supports clients other than servers. Up to 20 servers can be synchronized.

To carry out the encrypted communication with the server, set the global encryption key and global trusted key firstly, and then specify the corresponding key as the trusted key of the server to launch the encrypted communication of the server. It requires the server presents identical global encryption key and global trust key to complete the encrypted communication with the server.

In the same condition (for instance, precision), the prefer clock is used for synchronization.

⚠ The source interface of NTP packets must be configured with the IP address and can be

communicated with the peer.

**Configuration Examples** The following example configures an NTP server.

For IPv4: `Ruijie(config)# ntp server 192.168.210.222`

For IPv6: `Ruijie(config)# ntp server 10::2`

**Related Commands**

| Command | Description |
|---|---|
| **no ntp** | Disables NTP. |

**Platform Description** N/A

## 14.8 ntp trusted-key

Use this command to set a global trusted key. Use the **no** form of this command to remove the global trusted key.

**ntp trusted-key** *key-id*

**no ntp trusted-key** *key-id*

**Parameter Description**

| Parameter | Description |
|---|---|
| *key-id* | Global trusted key ID, ranging from 1 to 4294967295. |

**Defaults** N/A

**Command mode** Global configuration mode.

**Usage Guide** The NTP communication parties must use the same trusted key. The key is identified by ID and is not transmitted to improve security.

**Configuration Examples** The following example configures an authentication key and sets it as a trusted key.

```
Ruijie(config)#ntp authentication-key 6 md5 wooooop
Ruijie(config)#ntp trusted-key 6
Ruijie(config)#ntp server 192.168.210.222 key 6
```

**Related Commands**

| Command | Description |
|---|---|
| **ntp authenticate** | Enables NTP authentication. |
| **ntp authentication-key** | Configures an NTP authentication key. |
| **ntp server** | Configures an NTP server. |

**Platform Description** N/A

## 14.9 ntp update-calendar

Use this command to enable the NTP client to periodically update the device clock with the time synchronized from the external source clock. Use the **no** form of this command to remove this function.

**ntp update-calendar**

**no ntp update-calendar**

**Parameter Description**

| Parameter | Description |
| --- | --- |
| N/A | N/A |

**Defaults** By default, update the calendar periodically is not configured.

**Command mode** Global configuration mode.

**Usage Guide** By default, the NTP update-calendar is not configured. After configuration, the NTP client updates the calendar at the same time when the time synchronization of external time source is successful. It is recommended to enable this function for keeping the accurate calendar.

**Configuration Examples** The following example configures the NTP update calendar periodically.

```
Ruijie(config)# ntp update-calendar
```

**Related Commands**

| Command | Description |
| --- | --- |
| N/A | N/A |

**Platform Description** N/A

## 14.10 show ntp server

Use this command to display the NTP server configuration.

**show ntp server**

**Parameter Description**

| Parameter | Description |
| --- | --- |
| N/A | N/A |

**Defaults** N/A

**Command mode** Privileged EXEC mode, global configuration mode, interface configuration mode, VLAN configuration mode

**Usage Guide** N/A

**Configuration Examples** The following example displays the NTP server.

```
Ruijie# show ntp server
ntp-server                              source    keyid       prefer  version
---------------------------------------  --------  -----------  ------
-------
10::2                                  None     None        FALSE   3
192.168.210.222                          None      None        FALSE   3
```

**Related Commands**

| Command | Description |
| --- | --- |
| N/A | N/A |

**Platform Description** N/A

## 14.11 show ntp status

Use this command to display the NTP configuration.

**show ntp status**

**Parameter Description**

| Parameter | Description |
| --- | --- |
| N/A | N/A |

**Defaults** N/A

**Command mode** Privileged EXEC mode, global configuration mode, interface configuration mode, VLAN configuration mode

**Usage Guide** Use this command to display the NTP configuration. No configuration is displayed before the synchronization server is configured for the first time.

**Configuration Examples** The following example displays the NTP configuration.

```
Ruijie# show ntp status
Clock is synchronized, stratum 8, reference is 127.127.1.1
nominal freq is 250.0000 Hz, actual freq is 250.0000 Hz, precision is 2**24
reference time is D4BD819B.433892EE (01:27:55.000 UTC )
```

```
clock offset is 0.00000 sec, root delay is 0.00000 sec
root dispersion is 0.00002 msec, peer dispersion is 0.00002 msec
```

**Related Commands**

| Command | Description |
| --- | --- |
| N/A | N/A |

**Platform Description** N/A

# 15 SNTP Commands

## 15.1 sntp enable

Use this command to enable the SNTP function. Use the **no** form of this command to restore the default value.

**sntp enable**

**no sntp enable**

**Parameter Description**

| Parameter | Description |
|---|---|
| N/A | N/A |

**Defaults** SNTP is disabled by default.

**Command mode** Global configuration mode.

**Usage Guide** N/A

**Configuration Examples** The following example enables SNTP.

```
Ruijie(config)# sntp enable
```

**Related Commands**

| Command | Description |
|---|---|
| **show sntp** | Displays the SNTP configuration. |

**Platform Description** N/A

## 15.2 sntp interval

Use this command to set the interval for the SNTP client to synchronize its clock with the NTP/SNTP server. Use the **no** form of this command to restore the default synchronization interval.

**sntp interval** *seconds*

**no sntp interval**

**Parameter Description**

| Parameter | Description |
|---|---|
| *seconds* | Synchronization interval. The unit is second, and the range is from 60 to 65,535. |

**Defaults** The default synchronization interval is 1,800 seconds.

**Command mode** Global configuration mode.

**Usage Guide** To make the synchronization interval configuration effective, run the **sntp enable** command.

**Configuration Examples** The following example configures the synchronization interval to 3,600 seconds.

```
Ruijie(config)# sntp interval 3600
```

**Related Commands**

| Command | Description |
|---|---|
| **sntp enable** | Enables SNTP. |
| **show sntp** | Displays the SNTP configuration. |

**Platform Description** N/A

## 15.3 sntp server

Use this command to specify an SNTP server. Use the **no** form of this command to remove the SNTP server.

**sntp server** *ip- address*

**no sntp server**

**Parameter Description**

| Parameter | Description |
|---|---|
| *ip-address* | IP address of the SNTP server. |

**Defaults** No SNTP server is configured by default.

**Command mode** Global configuration mode.

**Usage Guide** As SNTP is fully compatible with NTP, the SNTP server can be used as an NTP server in Internet.

**Configuration Examples** The following example specifies an NTP server in Internet.

```
Ruijie(config)# sntp server 192.168.4.12
```

**Related Commands**

| Command | Description |
|---|---|
| **show sntp** | Displays the SNTP configuration. |
| **sntp enable** | Enables SNTP. |

**Platform Description** N/A

## 15.4 show sntp

Use this command to display the SNTP configuration.

**show sntp**

**Parameter Description**

| Parameter | Description |
| --- | --- |
| N/A | N/A |

**Defaults**

**Command mode** Privileged EXEC mode, global configuration mode, interface configuration mode.

**Usage Guide** N/A

**Configuration Examples** The following example displays the SNTP configuration.

```
Ruijie# show  sntp
SNTP state          : Enable
SNTP server         : 192.168.4.12
SNTP sync interval   : 60
Time zone            : +8
```

**Related Commands**

| Command | Description |
| --- | --- |
| **sntp enable** | Enables SNTP. |

**Platform Description** N/A

# 16 Time Range Commands

## 16.1 absolute

Use this command to configure an absolute time range.
**absolute** { [ **start** *time date* ] [ **end** *time date* ] }

Use the **no** form of this command to remove the absolute time range.
**no absolute**

**Parameter Description**

| Parameter | Description |
|---|---|
| **start** *time date* | Indicates the start time of the range. |
| **end** *time date* | Indicates the end time of the range. |

**Defaults** No absolute time range is configured by default.

**Command Mode** Time range configuration mode

**Default Level** 14

**Usage Guide** Use the **absolute** command to configure a time absolute time range between a start time and an end time to allow a certain function to take effect within the absolute time range.

**Configuration Examples** The following example creates a time range and enters time range configuration mode.

```
Ruijie(config)# time-range no-http
Ruijie(config-time-range)#
```

The following example configures an absolute time range.

```
Ruijie(config-time-range)# absolute start 1:1 1 JAN 2013 end 1:1 1 JAN 2014
```

**Check Method** Use the **show time-range** [ *time-range-name* ] command to display the time range configuration.

**Prompt Message** -

**Platform Description** -

## 16.2 periodic

Use this command to configure periodic time.
**periodic** *day-of-the-week time* **to** [ *day-of-the-week* ] *time*

Use the **no** form of this command to remove the configured periodic time.
**no periodic** *day-of-the-week time* **to** [ *day-of-the-week* ] *time*

**Parameter Description**

| Parameter | Description |
|---|---|
| *day-of-the-week* | Indicates the week day when the periodic time starts or ends. |
| *time* | Indicates the exact time when the periodic time starts or ends. |

**Defaults** No periodic time is configured by default.

**Command Mode** Time range configuration mode

**Default Level** 14

**Usage Guide** Use the **periodic** command to configure a periodic time interval to allow a certain function to take effect within the periodic time.

**Configuration Examples** The following example creates a time range and enters time range configuration mode.

```
Ruijie(config)# time-range no-http
Ruijie(config-time-range)#
```

The following example configures a periodic time interval.

```
Ruijie(config-time-range)# periodic Monday 1:1 to Tuesday 2:2
```

**Check Method** Use the **show time-range** [ *time-range-name* ] command to display the time range configuration.

**Prompt Message** -

**Platform Description** -

## 16.3 show time-range

Use this command to display the time range configuration.
**show time-range** [ *time-range-name* ]

**Parameter Description**

| Parameter | Description |
| --- | --- |
| *time-range-name* | Displays a specified time range. |

**Command Mode** Privileged EXEC mode

**Default Level** 14

**Usage Guide** Use this command to check the time range configuration.

**Configuration Examples** The following example displays the time range configuration.

```
Ruijie# show time-range
time-range entry: test (inactive)
  absolute end 01:02 02 February 2012
```

**Prompt Message** -

**Platform Description** -

## 16.4 time-range

Use this command to create a time range and enter time range configuration mode.
**time-range** *time-range-name*

Use the **no** form of this command to remove the configured time range.
**no time-range** *time-range-name*

**Parameter Description**

| Parameter | Description |
| --- | --- |
| *time-range-name* | Time range name |

**Defaults** No time range is configured by default.

**Command Mode** Global configuration mode

**Default Level** 2

**Usage** Some applications (such as ACL ) may run based on time. For example, an ACL can be effective within

| | |
|---|---|
| **Guide** | certain time ranges of a week. To this end, first you must configure a time range. After the time range is created, you can configure relevant time control in time range mode. |
| **Configuration Examples** | The following example creates a time range.<br>`Ruijie(config)# time-range no-http`<br>`Ruijie(config-time-range)#` |
| **Check Method** | Use the **show time-range** [ *time-range-name* ] command to display the time range configuration. |
| **Prompt Message** | - |
| **Platform Description** | - |