Ruijie RG-WLAN Series Wireless Controllers

RGOS Command Reference, Release 11.9(0)B7

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)B7.

Audience

This manual is intended for:

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

Obtaining Technical Assistance

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

Related Documents

Documents	Description
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 ac-controller

Use this command to enter the AC configuration mode from the global configuration mode.

ac-controller

Parameter Description

Parameter	Description
N/A	N/A

Defaults N/A

Command Mode Global configuration mode

Usage Guide N/A

Configuration Examples The following example enters the AC configuration mode.

```
Ruijie(config)# ac-controller
Ruijie(config-ac)#
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

1.2 acctrl-trap

Use this command to control the switch of a specific trap on AC in AC configuration mode. Use the **no** form of this command to restore the default setting.

acctrl-trap [acap-updown-ctrl | acap-joinfail-ctrl | acap-decryeroreport-ctrl | acap-imageupdt-ctrl | acap-timestamp-ctrl | acsta-oper-ctrl]

no acctrl-trap [acap-updown-ctrl | acap-joinfail-ctrl | acap-decryeroreport-ctrl | acap-imageupdt-ctrl | acap-timestamp-ctrl | acsta-oper-ctrl]

Parameter Description

Parameter	Description
acap-updown-ctrl	Controls the forwarding of the trap message about up/down of the CAPWAP tunnel.
acap-joinfail-ctrl	Controls the forwarding of the trap message that AP failed to join AC.

acap-decryeroreport-ctrl	Controls the forwarding of the trap message that the decryption of CAPWAP messages is failed.
acap-imageupdt-ctrl	Controls the forwarding of the trap message about bin file updating of AP.
acap-timestamp-ctrl	Controls the forwarding of the trap message about synchronization.
acsta-oper-ctrl	Controls the forwarding of the trap message about login and logout of STA.

Defaults This function is disabled by default.

Command Mode AC configuration mode

Usage Guide The command is used to control the switch of a specified trap on AC.

Configuration Examples The following example enables the forwarding of the trap message about login and logout of STA on AC.

```
Ruijie(config-ac)# acctrl-trap acsta-oper-ctrl
```

Related Commands

Command	Description
N/A	N/A

Platform Description

1.3 ac-name

Use this command to configure an AC name for users to identify the AC. Use the **no** form of this command to restore the default setting.

ac-name *ac-name*

no ac-name

Parameter Description

Parameter	Description
ac-name	Indicates an AC name, which can consist of up to 63 characters, excluding any space.

Defaults The default is the last six bits of the MAC address. For example. the default name for the AC with the MAC address 001a.a916.e7b8 is Ruijie_Ac_16e7b8.

Command Mode AC configuration mode

Usage Guide Configure different names for different ACs to make it easy for users to manage.

Configuration Examples The following example sets the AC name to ruijie-ac.

```
Ruijie(config-ac)# ac-name ruijie-ac
```

Related Commands

Command	Description
N/A	N/A

Platform Description

1.4 ac-ip

Use this command to configure the IP address of the AC to which a virtual AP is to be connected. Use the **no** form of this command to restore the default setting.

ac-ip *ipv4*

no ac-name

Parameter Description

Parameter	Description
ipv4	Specifies the IPv4 address of the AC to which a virtual AP is to connect.

Defaults The AC IP address is not configured by default.

Command Mode AP virtualization template configuration mode

Usage Guide The configured IP address cannot be the IP address of the active AC, and can only be the IP address of the AC to be connected and the address of the loopback 0 interface or the CAPWAP control IP address if any.

Configuration Examples The following example configures AC IP address 1.1.1.1.

```
Ruijie(config)#virtual-ap VAP-1

Ruijie(config-virtual-ap)# ac-ip 1.1.1.1
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

1.5 ap-auth

Use this command to enable a specified AP with the access authentication function. Use the **no** form of this command to restore the default setting.

ap-auth { **serial** *serial-string* | **password** *password* | **ac-cert** *ac-cert-name* | **ap-cert** *ap-cert-name* }

no ap-auth { **serial** | **password** | **ac-cert** | **ap-cert** }

Parameter Description

Parameter	Description
serial-string	The serial number of the specified AP.
password	The password of the specified AP.
ac-cert-name	The certificate name of the specified AC.
ap-cert-name	The certificate name of the specified AP.

Defaults This function is disabled by default.

Command Mode AP configuration mode

Usage Guide The access authentication only occurs when the AP goes online. If the AP is already online, authentication occurs the next time the AP gets access.

The **ap-auth-serial** command is not supported in **all** modes for every AP has different serial number.

The certificate configured by the **ap-auth ap-cert** command is saved as **cert.crt** uniformly on the AP and the name cannot be changed.

Configuration Examples The following example sets the serial number for AP1 to 123456.

```
Ruijie# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Ruijie(config)# ap-config AP1
Ruijie(config-ap)# ap-auth serial 123456
```

The following example restores the default setting.

```
Ruijie# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Ruijie(config)# ap-config AP1
Ruijie(config-ap)# no ap-auth serial
```

Related Commands

Command	Description
N/A	N/A

Platform Description

1.6 ap-auth enable

Use this command to enable a specified AP with the access authentication function. Use the **no** form of this command to restore the default setting.

ap-auth [**serial** | **password** | **certificate**] **enable**

no ap-auth [**serial** | **password** | **certificate**] **enable**

Parameter Description

Parameter	Description
serial	Serial-number-based authentication.
password	Password-based authentication.
certificate	Certificate-based authentication.

Defaults This function is disabled by default.

Command Mode AC configuration mode

Usage Guide N/A

Configuration Examples The following example enables the AP with the serial-number-based authentication.

```
Ruijie(config)# ac-controller
Ruijie(config-ac)# ap-auth serial enable
```

The following example restores the default setting.

```
Ruijie(config)# ac-controller
Ruijie(config-ac)# no ap-auth serial enable
```

Related Commands

Command	Description
N/A	N/A

Platform Description

1.7 ap-auth serial-update

Use this command to enable all online APs to update their serial numbers.

ap-auth serial-update

Parameter Description

Parameter	Description
N/A	N/A

Defaults This function is disabled by default.

Command Mode AC configuration mode

Usage Guide N/A

Configuration Examples The following example enables all online APs to update their serial numbers.

```
Ruijie(config)# ac-controller
Ruijie(config-ac)# ap-auth serial-update
```

Related Commands

Command	Description
N/A	N/A

Platform Description

1.8 ap-backup group

Use this command to configure an AP backup group in AC configuration mode. Use the **no** form of this command to delete an AP backup group.

ap-backup group *name*

no ap-backup group *name*

Parameter Description

Parameter	Description
name	AP backup group name. “default” is system reserved, namely, “default” cannot be used for backup group configuration.

Defaults By default, the AC device has only one AP backup group named “default”, which takes no effect on the backup function.

Command Mode AC configuration mode

Usage Guide If an AP backup group is deleted, the AP device in this group will be added to the “default” group. The “default” group takes no effect on the backup function.

Configuration Examples The following example configures an AP backup group named apbackup-test-group.

```
Ruijie(config)# ac-controller
Ruijie(config-ac)# ap-backup group apbackup-test-group
```

The following example deletes an AP backup group named apbackup-test-group.

```
Ruijie(config)# ac-controller
Ruijie(config-ac)# no ap-backup group apbackup-test-group
```

Related Commands

Command	Description
N/A	N/A

Platform Description

1.9 ap-backup group

Use this command to configure an AP backup group in AP configuration mode. Use the **no** form of this command to remove an AP device from the AP backup group or disable its master AP role.

ap-backup-group *name* [**master**]

no ap-backup-group [*name*] [**master**]

Parameter Description

Parameter	Description
name	AP backup group name
master	(Optional) Designates the AP device as a master AP in the backup group.

Defaults By default, the “default” backup group does not have any AP.

Command Mode AP configuration mode

Usage Guide The backup group must exist before you add an AP device into it.

The **master** parameter designates the AP device as a master AP in the backup group. There is only one master AP in a backup group. If you want to designate a new master AP, use the **no** form of this command to disable the old master AP.

Configuration Examples The following example adds an AP into backup group “backup-test-group” and designates it as a master AP.

```
Ruijie(config)# ap-config AP0001
Ruijie(config-ap)# ap-backup-group backup-test-group master
```

The following example disables a master AP in the backup group.

```
Ruijie(config)# ap-config AP0001
Ruijie(config-ap)# no ap-backup-group backup-test-group master
```

The following example removes an AP from the backup group.

```
Ruijie(config)# ap-config AP0001
Ruijie(config-ap)# no ap-backup-group
```

Related Commands

Command	Description
N/A	N/A

Platform Description

1.10 ap-config

Use this command to enter the configuration mode of a specified AP, which must have been added into an AC. Use the **no** form of this command to restore the default setting.

ap-config *ap-name*

no ap-config *ap-name*

Parameter Description

Parameter	Description
ap-name	Indicates the name of the AP to be configured.

Defaults N/A

Command Mode Global configuration mode

Usage Guide

To enter the configuration mode of a specified AP, ensure this AP must have been added into an AC. The **ap-config all** command can be used to enter the configuration mode of all APs, and the configuration in this mode will be applicable to all APs associated with the AC. The **ap-config** *ap-name* command prevails over the **ap-config all** command.
The **no ap-config** *ap-name* command is used to remove the specified AP configuration. If the target AP is online, it will go offline and then online upon configuration change,

Configuration Examples

The following example configures the AP that has been added with a name AP0001.

```
Ruijie(config-ap)# ap-config AP0001
```

The following example configures the AP that has been offline with a name AP0001.

```
Ruijie(config-ap)# no ap-config AP0001
```

Related Commands

Command	Description
N/A	N/A

Platform Description

1.11 ap-group(AP Configuration Mode)

Use this command to add the AP to a specified AP group. Use the **no** form of this command to restore the default setting.

ap-group *ap-group-name*

no ap-group

Parameter Description

Parameter	Description
ap-group-name	AP group name.

Defaults The AP joins in the default group by default.

Command Mode AP configuration mode

Usage Guide When the AP group is deleted, the member APs of this group are switched to the default group.

Configuration Examples The following example adds the AP to test-group.

```
Ruijie(config)# ap-group test-group
Ruijie(config-ap-group)#
Ruijie(config)# ap-config AP0001
Ruijie(config-ap)# ap-group test-group
```

The following example restores the default setting.

```
Ruijie(config)# ap-config AP0001
Ruijie(config-ap)# no ap-group test-group
```

Related Commands

Command	Description
N/A	N/A

Platform Description

1.12 ap-group(Hot Backup Instance Configuration Mode)

Use this command to configure the AP group that associates with the hot backup instance. Use the **no** form of this command to restore the default setting.

ap-group *ap-group-name*

no ap-group *ap-group-name*

Parameter

Parameter	Description

Description

ap-group-name	AP group name.

Defaults N/A

Command Mode Hot backup instance configuration mode

Usage Guide One single hot backup instance can be associated with multiple AP groups.

Configuration Examples The following example associates hot backup instance context 10 with ap-group apg-a and apg-b.

```
Ruijie(config-hotbackup)# context 10
Ruijie(config-hotbackup-ctx)# ap-group apg-a
Ruijie(config-hotbackup-ctx)# ap-group apg-b
```

Related Commands

Command	Description
N/A	N/A

Platform Description

1.13 ap-group

All APs added into an AC always belong to one and only one specific AP group in a certain moment. Any newly added AP belongs to the default AP group: **default**. Use this command to create a new AP group or enter the configuration mode of an existing AP group. If you use this command to create an AP group, you will enter the configuration mode of this AP group once created. Use the **no** form of this command to restore the default setting.

[no] ap-group *ap-group-name*

Parameter Description

Parameter	Description
ap-group-name	Indicates an AP group name, which consists of up to 150 characters or 64 bytes, excluding any space.

Defaults By default, the system, once started, will create automatically a default AP group (called **default**), which cannot be created or deleted manually.

Command Mode AP configuration mode.

Usage Guide N/A

Configuration Examples

The following example creates an AP group named ***test-group.***

```
Ruijie(config)# ap-group test-group
Ruijie(config-ap-group)#
```

The following example deletes an AP group named ***test-group***.

```
Ruijie(config)#no ap-group test-group
```

The following example enters an AP group named **default**.

```
Ruijie(config)# ap-group default
```

Related Commands

Command	Description
N/A	N/A

Platform Description

1.14 ap-idle-timeout

Use this command to configure the duration for a virtual AP to continue service provision after the connection between the AP and active AC is down. Use the **no** form of this command to restore the default setting.

ap-idle-timeout *num*

no ap-idle-timeout

Parameter Description

Parameter	Description
num	Sets the duration (in the unit of day) for a virtual AP to continue service provision after he connection between the AP and active AC is down, in the range from 0 to 14d.

Defaults

The default time is one day.

Command Mode

AP configuration mode

AP group configuration mode

All-AP configuration mode

Usage Guide

If the **num** parameter is set to **0** to prevent tunnel instability, the tunnel between the virtual AP and corresponding AC is not torn down immediately but retained for two minutes.

After an AP disconnects from the active AC and the time specified in **ap-idle-timeout** has not expired, a virtual AP no longer connects to an AC if the tunnel between the virtual AP and corresponding AC is disconnected, and connects to the AC again only when the connection between the AP and active AC is re-established.

Configuration Examples The following example sets the duration for a virtual AP to continue service provision after the connection between the AP and active AC is down to three days.

```
Ruijie(config)# ap-config test
Ruijie(config-ap)# ap-idle-timeout 3
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

1.15 ap-mac

Use this command to configure MAC-address-binding. Use the **no** form of this command to remove the configuration.

ap-mac *ap-mac*

no ap-mac

Parameter Description

Parameter	Description
ap-mac	MAC address of the AP.

Defaults N/A

Command Mode AP configuration mode

Usage Guide

- With this command configured, the AP configuration takes affect only on the AP whose MAC address is bound.
- In general, MAC-address-binding has a higher priority over name-binding. As long as the AP MAC address is consistent with the preset bound MAC address, the AP adopts the configuration after it goes online.
- Automatic MAC-address-binding: If the specified AP is not configured with MAC-address-binding, when it goes online, the MAC address is bound automatically. The binding is still effective when the AP goes offline.
- MAC-address-binding is also used for AP access control. See the **bind-ap-mac** command for details.
- MAC-address-binding can be performed only on the offline AP.
- In hot backup environment, binding MAC address ensures the consistency of configuration on two ACs.

Configuration The following example sets the MAC address bound with ap test to 00ff.ffff.1111.

Examples

```
Ruijie(config)# ap-config test
Ruijie(config-ap)# ap-mac 00ff.ffff.1111
```

Related Commands

Command	Description
N/A	N/A

Platform Description

1.16 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.

1.17 ap-name

Use this command to configure the AP name. Use the **no** form of this command to remove the configuration.

ap-name *ap-name*

no ap-name

Parameter Description

Parameter	Description
ap-name	AP name, containing up to 63 characters without blank space.

Defaults N/A

Command Mode AP configuration mode

Usage Guide If the specified AP is online, the AP name configuration takes effect immediately. The name of the AP configuration mode (the string after **ap-config**) is replaced by the new name.

If the specified AP is offline, the AP name configuration takes effect when it goes online. The name of the AP configuration mode does not change until the AP goes online.

After configuring the AP name, you don't need to exit AP configuration mode before continuing configuration.

If the specified AP is online, the **no** form of this command is not supported

If the specified AP is offline, the **no** form of this command is used to remove the configuration.

If the new name is in use, the configuration fails.

The AP name contains up to 63 characters without blank space.

The AP name cannot be set to **all** or **AP**.

Don't configure the same name for multiple offline APs. If multiple different offline APs are configured with the same name, the first online AP adopts the new name while the other APs keep the old names.

Configuration Examples The following example sets the AP0001 name to AP_NEW on an AC.

```
Ruijie(config)# ap-config AP0001
Ruijie(config-ap)# ap-name AP_NEW
```

The following example sets the AP name to AP_TEST.

```
Ruijie(config)# ap-name AP_ TEST
```

Related Commands

Command	Description
N/A	N/A

Platform Description The command is supported on ACs and fit APs.

1.18 ap-priority

Use this command to enable or disable the support for the Failover priority of APs on an AC.

ap-priority { **enable** | **disable** }

Parameter Description

Parameter	Description
enable	Enables the support for the Failover priority of APs
disable	Disables the support for the Failover priority of APs

Defaults This function is disabled by default.

Command Mode AP configuration mode

Usage Guide N/A

Configuration Examples The following example establishes a connection between AP0001 and AC1. Configure the priority of AP0001 to 3, and enable the support for the Failover priority of AC1.

```
Ruijie(config)# ap-config AP0001
Ruijie(config-ap)# priority 3
Ruijie(config-ap)# exit
Ruijie(config)# ac-controller
Ruijie(config-ac)# ap-priority enable
```

Related Commands

Command	Description
N/A	N/A

Platform

Description

1.19 backup-controller-primary

Use this command to specify the preferred backup AC for all APs connected to the current AC. Use the **no** form of this command to delete the preferred backup AC.

backup-controller-primary *ac-name* { *ip-address* | *ipv6-address* } [**switch-back**]

no backup-controller-primary

Parameter Description

Parameter	Description
ap-name	Indicates the name of the AP to be configured.
ip-address	Indicates the IP address of the preferred backup AC In the format of A.B.C.D.
ipv6-address	Indicates the IPv6 address of the preferred backup AC in the format of X;Y::Z.
switch-back	Indicates the switch-back function.

Defaults N/A

Command Mode AP configuration mode

Usage Guide The configuration is based on all APs on the AC.

Configuration Examples The following example configures the preferred backup AC of AP ap1. The IP address of the preferred backup AC is 192.168.1.4.

```
Ruijie#config terminal
Ruijie(config)#ap-config ap1
Ruijie(config-ap)#backup-controller-primary ap1 192.168.1.4
```

The following example configures the preferred IPv6 backup AC of all APs as ac1 and the IPv6 address of ac1 as 2001:1234::100.

```
Ruijie#config terminal
Ruijie(config)#ap-config all
Ruijie(config-ap)#backup-controller-primary ac1 2001:1234::100
```

Related Commands

Command	Description
backup-controller-secondary	Configures the secondary backup controller.
backup-controller-tertiary	Configures the tertiary backup controller.

Platform Description N/A

1.20 backup-controller-secondary

Use this command to specify the secondary backup AC for all APs connected to the current AC. Use the no form of this command to delete the secondary backup AC.

backup-controller-secondary *ac-name* { *ip-address* | *ipv6-address* } [**switch-back**]

no backup-controller-secondary

Parameter Description

Parameter	Description
ap-name	Indicates the name of the AP to be configured
ip-address	Indicates the IP address of the secondary backup AC In the format of A.B.C.D.
ipv6-address	Indicates the IPv6 address of the secondary backup AC in the format of X;Y::Z.
switch-back	Enables switch-back function. The default is disabled.

Defaults N/A

Command Mode AP configuration mode

Usage Guide The configuration is based on all APs on the AC.

Configuration Examples The following example configures the secondary backup AC of AP ap1. The IP address of the secondary backup AC is 192.168.2.4.

```
Ruijie#config terminal
Ruijie(config)#ap-config ap1
Ruijie(config-ap)#backup-controller-secondary ap1 192.168.2.4
```

The following example configures the secondary IPv6 backup AC of all APs as ac2 and the IPv6 address of ac2 as 2001:1234::200.

```
Ruijie#config terminal
Ruijie(config)#ap-config all
Ruijie(config-ap)#backup-controller-secondary ac2 2001:1234::200
```

Related Commands

Command	Description
backup-controller-primary	Configures the preferred backup controller
backup-controller-tertiary	Configures the tertiary backup controller

Platform Description N/A

1.21 backup-controller-tertiary

Use this command to specify the tertiary backup AC for all APs connected to the current AC. Use the **no** form of this command to delete the tertiary backup AC.

backup-controller-tertiary *ac-name* { *ip-address* | *ipv6-address* } [**switch-back**]

no backup-controller-tertiary

Parameter Description

Parameter	Description
ap-name	Indicates the name of the AP to be configured
ip-address	Indicates the IP address of the secondary backup AC In the format of A.B.C.D.
ipv6-address	Indicates the IPv6 address of the secondary backup AC in the format of X;Y::Z.
switch-back	Enable switch-back function. The default is disabled.

Defaults N/A

Command Mode AP configuration mode

Usage Guide The configuration is based on all APs on the AC.

Configuration Examples The following example configures the tertiary backup AC of AP ap1. The IP address of the tertiary backup AC is 192.168.3.4.

```
Ruijie#config terminal
Ruijie(config)#ap-config ap1
Ruijie(config-ap)#backup-controller-tertiary ap1 192.168.3.4
```

The following example configures the tertiary IPv6 backup AC of all APs as ac3 and the IPv6 address of ac3 as 2001:1234::300.

```
Ruijie#config terminal
Ruijie(config)#ap-config all
Ruijie(config-ap)#backup-controller-tertiary ac3 2001:1234::300
```

Related Commands

Command	Description
backup-controller-primary	Configures the preferred backup controller.
backup-controller-tertiary	Configures the tertiary backup controller.

Platform Description N/A

1.22 bind-ap-mac

Use this command to enable AP validity check. Use the **no** form of this command to restore the default setting.

bind-ap-mac

no bind-ap-mac

Parameter Description

Parameter	Description
N/A	N/A

Defaults This function is disabled by default.

Command Mode AC configuration mode

Usage Guide When the AP validity check is enabled, only the AP with offline configurations that binds the MAC address can associate the AC. You can configure the command **ap-mac** to binds the MAC address to the offline AP in the AP configuration mode.

Configuration Examples

The following example enables AP validity check.

```
Ruijie(config)# ac-controller
Ruijie(config-ac)# bind-ap-mac
```

The following example disables AP validity check.

```
Ruijie(config)# ac-controller
Ruijie(config-ac)# no bind-ap-mac
```

Related Commands

Command	Description
ap-mac	Binds the MAC address to the offline AP.

Platform Description

1.23 credential

Use this command to configure a username and a password for an AP. Use the **no** form of this command to restore the default setting.

[no] credential *user-name password*

Parameter Description

Parameter	Description
user-name	Indicates a username to be used on an AP, which can consist of up to 255 characters, excluding any space.
password	Indicates a password to be set on an AP, which can consist of up to 255 characters, excluding any space.

Defaults N/A

Command Mode AP configuration mode or AP group configuration mode

Usage Guide N/A

Configuration Examples

The following example configures a username **first-ap** and a password **123456** for AP0001.

```
Ruijie(config)# ap-config AP0001
Ruijie(config-ap)# credential first-ap 123456
```

The following example configures a username **first-ap** and a password **123456** for all APs in the AP group (default).

```
Ruijie(config)# ap-group default
Ruijie(config-ap-group)# credential first-ap 123456
```

Related Commands

Command	Description
N/A	N/A

Platform Description

1.24 enable-broad-ssid

Use this command to enable SSID broadcast in the WLAN configuration mode. Use Tthe **no** form of this command to disable this function.

[no] enable-broad-ssid

Parameter Description

Parameter	Description
N/A	N/A

Defaults This function is enabled by default.

Command Mode WLAN configuration mode

Usage Guide When you configure the Suppress SSID information of this WLAN, the configuration will take effect only if completed before the WLAN is applied.

Configuration Examples

The following example enables SSID broadcast on this WLAN.

```
Ruijie(config-wlan)#enable-broad-ssid
```

The following example disables SSID broadcast on this WLAN.

```
Ruijie(config-wlan)#no enable-broad-ssid
```

Related Commands	Command	Description
	N/A	N/A

Platform Description

1.25 factory-reset

Use this command to restore the factory setting of a specified AP, that is, to reset this AP.

factory-reset *ap-name*

Parameter Description	Parameter	Description
	ap-name	indicates the name of the AP that needs to restore factory setting.

Defaults N/A

Command Mode AC configuration mode

Usage Guide The configuration will restore the factory setting of a specified AP, and as a result, the operation will reset this AP.

Configuration Examples The following example configures AP0001 to restore its factory setting.

```
Ruijie(config-ac)# factory-reset AP0001
```

Related Commands	Command	Description
	N/A	N/A

Platform Description

1.26 interface-mapping

Use **interface-mapping** in AP group configuration mode to map **wlan-vlan** or **wlan-vlan-group mapping** (the mapping in all descriptions of this cli refers to map wlan-vlan or wlan-vlan-group mapping) to the radios of all the APs in an AP group. The related WLAN configuration can be applied to the specified radio through such mapping. Use the **no** form this command to remove the related mapping configuration.

interface-mapping *wlan-id* [*vlan-id* I **group** *vlan-group-id*] [**radio** {*radio-id* | [*802.11b* | *802.11a*]}] [**ap-wlan-id** *ap-wlan-id*]

no interface-mapping *wlan-id* [*vlan-id* I **group** *vlan-group-id*] [**radio** {*radio-id* | [*802.11b* | *802.11a*]}] [**ap-wlan-id** *ap-wlan-id*]

Parameter Description

Parameter	Description
wlan-id	ID of the WLAN to be mapped. This WLAN must be created already. Its ID ranges from 1 to 4094.
vlan-id	ID of the VLAN to be mapped. This VLAN must be created already. Its ID ranges from 1 to 4094.
vlan-group-id	ID of the VLAN-group to be mapped. This VLAN-group must be created already. Its ID ranges from 1 to 128.
radio-id	An AP's radio to which the specified mapping is applied. Its reserved range is the standard, defined 1 to 96. Currently, the product should use the range of 1 to 2. If no radio-id is specified, the mapping will be applied to all the radios of all the APs in the AP group.
802.11b	Applies the mapping to 2.4G radio.
802.11a	Applies the mapping to 5.8G radio.
ap-wlan-id	Specifies the WLAN ID on the AP, in the range from 1 to 64. If the WLAN ID is not specified, the mapping selects an available ID automatically.

Defaults N/A

Command Mode AP group configuration mode

Usage Guide N/A

Configuration Examples

The following example configures VLAN 2 and a WLAN with its ID of 4094, and apply the mapping of wlan4094-vlan2 to radio 1 of all the APs in the default AP group.

```
Ruijie(config)#vlan 2
Ruijie(config)#wlan-config 4094 pro-4094 ssid-4094
Ruijie(config-wlan)#exit
Ruijie(config)#ap-group default
Ruijie(config-ap-group)#interface-mapping 4094 2 radio 1
```

The following example configures VLAN-group 3 and a WLAN with its ID of 4094, and apply the mapping of wlan4094-vlan-group3 to all the radios of all the APs in the default AP group.

```
Ruijie(config)#vlan-group 3
Ruijie(config)#wlan-config 4094 pro-4094 ssid-4094
Ruijie(config-wlan)#exit
Ruijie(config)#ap-group default
Ruijie(config-ap-group)#interface-mapping 4094 group 3
```

The following example configures the default AP group and delete the configured wlan4094-vlan2 mapping.

```
Ruijie(config)# ap-group default
Ruijie(config-ap-group)# no interface-mapping 4094 2 radio 1
```

Related Commands	Command	Description
	N/A	N/A

Platform Description

1.27 license-idle-timeout

Use this command to configure the shared aging time of a license in a license sharing network after the AC stops using the license. Use the **no** form of this command to restore the default setting.

license-idle-timeout *timeout*

no license-idle-timeout

Parameter Description	Parameter	Description
	timeout	Configures the shared aging time of a license, in the range from 1h to 336h.

Defaults The default time is 168h.

Command Mode AC configuration mode

Usage Guide This command applies to the license sharing scenarios, for example, AC virtualization scenarios.

Configuration Examples The following example sets the shared aging time of a license to 240h.

```
Ruijie(config-ac)# license-idle-timeout 240
```

Related Commands	Command	Description
	N/A	N/A

Platform Description N/A

1.28 link-interface

Use this command to configure the uplink interface used by a virtual AP to connect to an AC. Use the **no** form of this command to restore the default setting.

link-interface { **other** | *id* }

no link-interface

Parameter Description

Parameter	Description
other	A virtual AP uses an uplink interface different from that used by the active AC. This parameter is specified when there are two uplink interfaces and virtual AP and active AC use them for connection.
id	Specifies the number of uplink interface used by a virtual AP.

Defaults No uplink interface is configured by default.

Command Mode AP virtualization template configuration mode

Usage Guide

The **other** parameter is configured only when there are two uplink interfaces and the virtual AP and active AC use them for connection. Otherwise, the virtual AP cannot establish a CAPWAP connection to the corresponding AC.

If the configured uplink interface number does not exist, the virtual AP cannot establish a connection to the corresponding AC.

Configuration Examples The following example specifies uplink interface 2 for VAP-1.

```
Ruijie(config)#virtual-ap VAP-1
Ruijie(config-virtual-ap)# link-interface 2
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

1.29 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 by default.

Command Mode AP configuration mode

Usage Guide

Configuration Examples The following example disables the log display on the device.

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

Related Commands

Command	Description
logging buffered	Records the logs to a memory buffer.
logging	Sends logs to the Syslog server.
logging file flash:	Records logs on the extended FLASH.
logging console	Allows the log level to be displayed on the console.
logging monitor	Allows the log level to be displayed on the VTY window (such as telnet window) .
logging trap	Sets the log level to be sent to the Syslog server.

Platform Description

1.30 logging server

Use this command to record the logs in the specified Syslog Sever. Use the **no** form of the command to restore the default setting.

logging server *ip-address* [**udp-port** *num*]

no logging server *ip-address*

Parameter Description

Parameter	Description
ip-address	IP address of the host that receives log information.
num	Port number of the host that receives log information.

Defaults N/A

Command Mode AP configuration mode/All APs 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
```

Related Commands

Command	Description
logging on	Turns on the log switch.
show logging	Views log messages and related log configuration parameters in the buffer.
logging trap	Sets the level of logs allowed to be sent to Syslog server.

Platform Description

1.31 master-group

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

master-group *master-group-name*

no master-group *master-group-name*

Parameter Description

Parameter	Description
master-group-name	Specifies a role name, in the range from 1 to 64 characters.

Defaults N/A

Command Mode Global configuration mode

Usage Guide When the **no** form of this command is used to delete a role, APs, AP groups, and WLANs assigned to the role are restored to the unassigned state and the administrator of this role is restored to the default role-free state.

Configuration Examples

The following example creates a role named test-group.

```
Ruijie(config)# master-group test-group
Ruijie(config-master-group)#
```

The following example creates a role named test-group and enters the role configuration mode.

```
Ruijie(config)# master-group test-group
Ruijie(config-master-group)#
```

The following example deletes a role named test-group.

```
Ruijie(config)#no master-group test-group
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

1.32 master-group (AP Configuration Mode)

Use this command to assign an AP to a specific role. Use the **no** form of the command to restore the default setting.

master-group *master-group-name*

no master-group

Parameter Description

Parameter	Description
master-group-name	Specifies a role name.

Defaults The AP is not assigned to any role by default.

Command Mode AP configuration mode

Usage Guide After a role is deleted, APs assigned to the role are restored to the default unassigned state.

Configuration Examples The following example assigns an AP to role test-group.

```
Ruijie(config)# master-group test-group
Ruieji(config-master-group)# exit
Ruijie(config)# ap-config AP0001
```

```
Ruijie(config-ap)# master-group test-group
```

The following example restores the AP to the default setting.

```
Ruijie(config)# ap-config AP0001
Ruijie(config-ap)# no master-group
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

1.33 master-group (AP Group Configuration Mode)

Use this command to assign an AP group to a specific role. Use the **no** form of the command to restore the default setting.

master-group *master-group-name*

no master-group

Parameter Description

Parameter	Description
master-group-name	Specifies a role name.

Defaults The AP group is not assigned to any role by default.

Command Mode AP group configuration mode

Usage Guide After a role is deleted, AP groups assigned to the role are restored to the default unassigned state.

Configuration Examples The following example assigns an AP group to role test-group.

```
Ruijie(config)# master-group test-group
Ruieji(config-master-group)# exit
Ruijie(config)# ap-group default
Ruijie(config-group)# master-group test-group
```

The following example restores the AP group to default setting.

```
Ruijie(config)# ap-group default
Ruijie(config-group)# no master-group
```

Related Commands

Command	Description
N/A	N/A

Platform N/A

Description

1.34 master-group (WLAN Configuration Mode)

Use this command to assign a WLAN to a specific role. Use the **no** form of the command to restore the default setting.

master-group *master-group-name*

no master-group

Parameter Description

Parameter	Description
master-group-name	Specifies a role name.

Defaults The WLAN is not assigned to any role by default.

Command Mode WLAN configuration mode

Usage Guide After a role is deleted, WLANs assigned to the role are restored to the default unassigned state.

Configuration Examples The following example assigns a WLAN to role test-group.

```
Ruijie(config)# master-group test-group
Ruieji(config-master-group)# exit
Ruijie(config)# wlan-config 1
Ruijie(config-wlan)# master-group test-group
```

The following example restores the WLAN to default setting.

```
Ruijie(config)# wlan-config 1
Ruijie(config-wlan)# no master-group
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

1.35 nas-id

Use this command to set the access ID for the WLAN user or AC. Use the **no** form of this command to restore the default setting.

nas-id *nas-id*

no nas-id

Parameter Description

Parameter	Description
nas-id	Access ID, containing 32 characters without blank space.

Defaults The default WLAN user access ID is an empty string.
The default AC access ID is the AC MAC address in dotted format.

Command Mode WLAN configuration mode/AC configuration mode

Usage Guide N/A

Configuration Examples The following example sets the access ID for the WLAN user to 0000059159100460.

```
Ruijie(config-wlan)# nas-id 0000059159100460
```

The following example restores the default access ID of the WLAN user.

```
Ruijie(config-wlan)# no nas-id
```

The following example sets the AC access ID to 123456789.

```
Ruijie(config-ac)# nas-id 123456789
```

The following example restores the default AC access ID.

```
Ruijie(config-ac)# no nas-id
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

1.36 offline-ssid

Use this command to provide WLAN access service when a CAPWAP tunnel is not set up or torn down. Use the **no** form of the command to restore the default setting.

offline-ssid *ssid* [**hide**]

no offline-ssid

Parameter Description

Parameter	Description
ssid	SSID signal is broadcasted when the AP is started or the tunnel is torn down.
hide	No SSID signal is broadcasted.

Defaults No SSID is configured by default.

Command Mode AP configuration mode
AP group configuration mode
All-AP configuration mode

Usage Guide If RIPT is configured and the tunnel is torn down, signals are not sent.
When the AP is restarted, the configurations will be saved.

Configuration Examples The following example sets default SSID of AP1 to my-def-ssid.

```
Ruijie(config)#ap-config AP1
Ruijie(config-ap)#offline-ssid my-def-ssid
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

1.37 peer-ip

Use this command to set the address of the peer AC device connected with an AP belonging to the instance. So that the AP can use this address to build a second CAPWAP tunnel with the AC device.
Use the **no** form of this command to restore the default setting.
peer-ip *ipv4-address*
no peer-ip

Parameter Description

Parameter	Description
ipv4-address	Use the IP address configured by users as the peer AC address.

Defaults Use the configured IP address as the peer AC address.

Command mode Hot-backup instance configuration mode

Usage Guide In non-NAT environments, use the default configuration, which is the configured IP address as the peer AC address.
In NAT environments, configure the address based on environments where the AP locates:
If the AP is in NAT intranet, use the configured IP address as the peer AC address.
If the AP is in NAT extranet, use the IP address notified by the peer AC device as its address.

Configuration Examples The following example uses the IP address notified by the peer AC device as its address.

```
Ruijie(config-hotbackup)# context 10
Ruijie(config-hotbackup-ctx)# peer-ip real-ip
```

Related Commands

Command	Description
N/A	N/A

Platform Description

1.38 peer-ipv6

Use this command to set the IPv6 address of the peer AC associated with the AP in the current hot backup instance. Use the **no** form of this command to restore the default setting.

peer-ipv6 *ipv6-address*

no peer-ipv6

Parameter Description

Parameter	Description
ipv6-address	The IPv6 address of the peer AC.

Defaults The default is the source address of the CAPWAP tunnel.

Command Mode Hot backup instance configuration mode

Usage Guide In the non-NAT environment, it is recommended to use the default setting.

In the NAT environment, perform configuration according to the actual scenario. When the AC is within the NAT network, it has a private address unreachable for the AP. Therefore, the AC should be configured with a public address.

- If the AP and the AC are within the same NAT network, it is recommended to use the default setting.
- If the AP is not within the NAT network, it is recommended to use the configured IPv6 address as the peer AC address.

Use the **peer-ipv6 enable** command to enable the function of creating IPv6 hot backup dual-tunnel through CAPWAP.

Configuration Examples The following example sets the public IPv6 address to the AC address.

```
Ruijie(config-hotbackup)# context 10
Ruijie(config-hotbackup-ctx)# peer-ipv6 2001::1
```

Related Commands

Command	Description
N/A	N/A

Platform Description

1.39 peer-ipv6 enable

Use this command to create a dual-tunnel between the AP of the hot backup instance and two hot backup ACs. Use the **no** form of this command to restore the default setting.

peer-ipv6 enable

no peer-ipv6 enable

Parameter Description

Parameter	Description
N/A	N/A

Defaults This function is disabled by default.

Command Mode Hot backup instance configuration mode

Usage Guide When an IPv6 CAPWAP tunnel between an AP and a hot backup AC is created, this command must be configured to enable the creation of an IPv6 CAPWAP tunnel between the AP and another hot backup AC.

Configuration Examples The following example enables the AP with the capwapv6 hot backup dual-tunnel function.

```
Ruijie(config-hotbackup)# context 10
Ruijie(config-hotbackup-ctx)# peer-ipv6 enable
```

Related Commands

Command	Description
N/A	N/A

Platform Description

1.40 permit enable

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

permit enable

no permit enable

Parameter Description

Parameter	Description

N/A	N/A

Defaults AC virtualization is disabled by default.

Command Mode AC configuration mode

Usage Guide AC virtualization function takes effect only to web management. Users can log in to the web management page using different administrator accounts to check and configure different WLANs, AP groups, and APs.

Configuration Examples The following example enables AC virtualization.

```
Ruijie(config)# ac-controller
Ruijie(config-ac)# permit enable
```

The following example disables AC virtualization.

```
Ruijie(config)# ac-controller
Ruijie(config-ac)# no permit enable
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

1.41 primary-base

Use this command to enter the configuration mode of a specific AP connected to the current AC and to specify the preferred AC for the specific AP.

primary-base *ap-name {ip-address | ipv6-address}*

no primary-base

Parameter Description

Parameter	Description
ap-name	Indicates the name of the AP to be configured
ip-address	Indicates the IP address of the primary AC In the format of A.B.C.D.
ipv6-address	Indicates the IPv6 address of the preferred IPv6 AC in the format of X;Y::Z.

Defaults N/A

Command Mode AP configuration mode/All APs configuration mode

Usage Guide Configure the preferred control AC of the AP. The configuration is based on a single AP.

Configuration Examples The following example sets the preferred AC of AP ap1. The IP address of the preferred AC is 192.168.1.1.

```
Ruijie#config terminal
Ruijie(config)#ap-config ap1
Ruijie(config-ap)#primary-base ap1 192.168.1.1
```

The following example configures the preferred IPv6 AC of ap1 as ac1 and the IPv6 address of ac1 as 2001:abcd::100.

```
Ruijie#config terminal
Ruijie(config)#ap-config ap1
Ruijie(config-ap)#primary-base ac1 2001:abcd::100
```

Related Commands

Command	Description
secondary-base	Configures the secondary AC.
tertiary-base	Configures the tertiary AC.

Platform Description

1.42 priority

Use this command to set the Failover priority of APs. After you enable the support for the Failover priority of APs on an AC, the AC can accept the access of APs according to their priority order.

priority *priority-value*

Parameter Description

Parameter	Description
priority-value	The parameter indicates the Failover priority of APs. The allowed value is 1, 2, 3, and 4.

Defaults The default is 1.

Command Mode AP configuration mode

Usage Guide Configure the Failover priority of devices. **1** indicates the lowest priority, and **4** indicate the highest priority. Add the AC sequence (priority of APs) to the AP. The configurations are saved in the AP. When the AP is associated next time, the configurations take effect.

Configuration Examples The following example sets the Failover priority of the AP group named **apgroup** to 3.

```
Ruijie#config terminal
Ruijie(config)#ap-config apgroup
```

```
Ruijie(config-ap)#priority 3
```

Related Commands

Command	Description
N/A	N/A

Platform Description

1.43 reload at

Use this command to enable AP restart as scheduled every day. Use the **no** form of this command to remove the configuration.

reload at *time*

no reload at

Parameter Description

Parameter	Description
time	AP restart time every day, in the format of hh:mm:ss.

Defaults N/A

Command Mode AP configuration mode

Usage Guide N/A

Configuration Examples The following example enables AP restart at 1:00:00 every day.

```
Ruijie(config)#ap-config Ruijie-AP1
Ruijie(config-ap)#reload at 1:00:00
```

Related Commands

Command	Description
N/A	N/A

Platform Description

1.44 reset

In the AC configuration mode, use this command to reset all APs, reset any AP with an updated software version, and reset any specified AP.

reset{all | |single *ap-name*}

Parameter Description

Parameter	Description
all	Indicates that all APs will be reset.
single *ap-name*	Indicates that a specified AP will be reset.

Defaults N/A

Command Mode AC configuration mode

Usage Guide N/A

Configuration Examples

The following example resets all APs.

```
Ruijie(config-ac)# reset all
```

The following example resets the AP named AP0001.

```
Ruijie(config-ac)# reset AP0001
```

Related Commands

Command	Description
N/A	N/A

Platform Description

1.45 secondary-base

Use this command to enter the configuration mode of a specific AP connected to the current AC and to specify the secondary AC for the specific AP.

secondary-base *ac-name* { *ip-address* | *ipv6-address* } [**switch-back**]

no secondary-base

Parameter Description

Parameter	Description
ap-name	Indicates the name of the AP to be configured
ip-address	Indicates the IP address of the secondary AC in the format of A.B.C.D.
ipv6-address	Indicates the IPv6 address of the secondary IPv6 AC in the format of X;Y::Z.
switch-back	Enables switch-back function. The default is disabled.

Defaults N/A

Command Mode AP configuration mode/All APs configuration mode

Usage Guide Configure the secondary AC of the AP. The configuration is based on a single AP.

Configuration Examples The following example configures the secondary AC of AP ap1. The IP address of the secondary AC is 192.168.2.1.

```
Ruijie#config terminal
Ruijie(config)#ap-config ap1
Ruijie(config-ap)#secondary-base ap1 192.168.2.1
```

The following example configures the secondary IPv6 AC of ap1 as ac2 and the IPv6 address of ac2 as 2001:abcd::200.

```
Ruijie#config terminal
Ruijie(config)#ap-config ap1
Ruijie(config-ap)#secondary-base ac2 2001:abcd::200
```

Related Commands

Command	Description
primary-base	Configures the preferred AC.
tertiary-base	Configures the tertiary AC.

Platform Description

1.46 set license

Use this command to add a license to a device. A license authorizes an AC to control the number of online APs. The license is overlaid during upgrade. Use the **no** form of this command to deactivate a license.

set license *activation-key*

no set license *activation-key*

Parameter Description

Parameter	Description
activation-key	Specifies the key of a license. The format of the key varies with specific conditions, for example, AAAA-BBBB-CCCC-DDDD-EEEE-FFFF-GGGG-HHHH.

Defaults N/A

Command mode Global configuration mode

Usage Guide A license can be configured only on one device for one time.

1) After being configured, a license takes effect forever.

2) After being deactivated, the license cannot be installed on the device again. But you can apply for a new license for another device using this license, the old SN, the deactivation key and a new SN.

3) After you deactivate a license, the number of APs allowed to be online reduces immediately. The APs that are already online are not affected.

> The number of online APs specified in a license cannot exceed the upper limit supported by an AC. Otherwise, "The support of APs reaches the max." is displayed.

> The value of *activation-key* may vary with license types. Therefore, you must select it based on specific conditions

Configuration Examples The following example adds a license to a device.

```
Ruijie#config terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Ruijie(config)#set license ABCD-1234-ABCD-5678-ABCD-1234-ABCD-5678
```

The following example deactivates a license.

```
Ruijie#config terminal
Ruijie(config)# no set license 4A3F-16AB-330C-B254-42C4-E18A-24F3-15CA
After unbinding, you cannot install the corresponding license again. Are you sure to continue[y/n]:y
The verification string is: xxxxxxxxxx
```

Related Commands

Command	Description
show license	Displays information about all configured licenses.

Platform Description

1.47 show ac-config

Use this command to display the basic configuration information about the current AC.

show ac-config

Parameter Description

Parameter	Description
N/A	N/A

Defaults N/A

Command Mode Any mode

Usage Guide N/A

Configuration Examples

The following example displays the basic configuration information of the current AC.

```
Ruijie(config)#show ac-config
AC Configuration info:
max_wtp         :128
sta_limit       :4096
license wtp max  :128
license sta max  :4096
serial auth     :Disable
password auth    :Disable
certificate auth :Disable
Bind AP MAC     :Disable
AP Priority     :Disable
ac_name         :Ruijie_Ac_231455
ac location     :Ruijie_COM

AC State info:
sta_num         :0
act_wtp         :12
used wtp            :8( 4 normal 8 half)
remain wtp       :120 normal 240 half
HW Ver          :1.0
SW Ver          :AC_RGOS 11.1(1)B1
Mac address     :001a.9923.1455
Product ID      :WS5708
NET ID          :9876543210012345
NAS ID          :001a.9923.1455
```

Related Commands

Command	Description
N/A	N/A

Platform Description

1.48 show ac-config ap-backup-group

Use this command to display the AP backup group.

show ac-config ap-backup-group [*group-name*]

Parameter Description

Parameter	Description
group-name	AP backup group name. The “default” group is not displayed.

Defaults N/A

Command Mode Any mode

Usage Guide N/A

Configuration Examples

The following example displays the all AP backup groups.

```
Ruijie#show ac-config ap-backup-group
Cnt    Group-Name              Master-AP cnt   Standby-AP cnt
Master-AP-Name    Working
------ ---------------------------------- ------------ -----------
------------  -----------
1     AP-BACKUP-GROUP1         1             2              AP4210-1
false
```

The following example displays details of backup group “AP-BACKUP-GROUP1”.

```
Ruijie#show ac-config ap-backup-group AP-BACKUP-GROUP1
Cnt     Ap-Name                 Ap-Mac            Online    Is-Master
Inherit-Wlan Cnt
------- ------------------------ -------------------- ------- ------------
-----------------
1     AP4210-1                8832.0000.1111     true      Yes       0
2     APD-M-1                     -            false     No        0
3     APD-M-2                 0011.4477.8833     true      No        0
```

Related Commands

Command	Description
N/A	N/A

Platform Description

1.49 show ap-config bssid

Use this command to display the BSSID list.

show ap-config bssid

Parameter Description

Parameter	Description
N/A	N/A

Defaults N/A

Command Any mode

Mode

Usage Guide N/A

Configuration Examples

The following example displays the BSSID list.

```
Ruijie(config)#show ap-config bssid
AP Mac          AP Name                                 Radio ID WLAN ID  AP WLAN ID BSSID
--------------- --------------------------------------- -------- -------- ----------
--------------
001a.a97e.a799 AAA                      1        8        1          061b.b121.c037
001a.a97e.a799 AAA                      1        4        2          0a1b.b121.c037
001a.a97e.a799 AAA                      1        6        3          121b.b121.c037
001a.a97e.a799 AAA                      1        5        4          161b.b121.c037
001a.a97e.a799 AAA                      2        4        2          0a1b.b121.bfaa
001a.a97e.a799 AAA                      2        6        3          121b.b121.bfaa
001a.a97e.a799 AAA                      2        5        4          161b.b121.bfaa
001a.a97e.a799 AAA                      2        7        5          221b.b121.bfaa
0074.9c02.33a8 AAA                      1        8        1          0a69.6c9e.9e8d
0074.9c02.33a8 AAA                      1        4        2          0e69.6c9e.9e8d
0074.9c02.33a8 AAA                      1        6        3          1269.6c9e.9e8d
0074.9c02.33a8 AAA                      1        5        4          1a69.6c9e.9e8d
0074.9c02.33a8 AAA                      2        4        2          0a69.6c9e.9e8e
```

Related Commands

Command	Description
N/A	N/A

Platform Description

1.50 show ap-config bssid cb

Use this command to display the BSSID list and the mappings between the AC WLAN ID and AP WLAN ID.

show ap-config bssid cb *ap-name*

Parameter Description

Parameter	Description
ap-name	Specifies an AP name.

Defaults N/A

Command Mode Any mode

Usage Guide N/A

Configuration Examples The following example displays the BSSID list and the mappings between the AC WLAN ID and AP WLAN ID.

```
Ruijie#show ap-config bssid cb ap1
Radio ID WLAN ID  AP WLAN ID BSSID
-------- -------- ---------- --------------
1       101     1         06d0.f822.3355
1       102     2         0ad0.f822.3355
2       101     1         06d0.f822.3356
2       102     2         0ad0.f822.3356
3       101     1         06d0.f822.3357
3       102     2         0ad0.f822.3357
Ruijie#
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

1.51 show ap-config cb

Use this command to display the status information of an AP.

show ap-config cb *ap-name*

Parameter Description

Parameter	Description
ap-name	Indicates the name of the AP to be queried.

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide N/A

Configuration Examples The following example displays the status information of an AP.

```
ac#show ap-config cb wlan-ap-0001
Configuration:
ap name             :wlan-ap-0001
ap id               :1
discovery timer       :20
```

```
echo request timer    :30
error report timer     :120
client timeout timer    :300
statistisc time        :120
ap fallback           :1
image id            :RGOS 10.4 (1t7)(1T7), Release(73413)
group name          :default
dhcp_option          :standard
Core dump server ip    :0.0.0.0
Core dump file name   :

Status:
local ipv4           :192.168.120.2
Tran protocol         :udp
Discovery type        :unknow
ECN Support         :0
location data         :Not Setting
mtu                :0
session id            :0x0f075476,0x0f075476,0x0f075476,0x0f075476
tunnel mode         :0xe(NELR)
mac type           :full support
WTP Name          :wlan-ap-0001
STA Limit           :30
STA num            :2
radio num           :1
```

Related Commands	Command	Description
	N/A	N/A

Platform Description

1.52 show ap-config inherit-wlan

Use this command to display the WLAN inherited by the specified AP device in backup group.

show ap-config inherit-wlan *ap-name*

Parameter Description	Parameter	Description
	ap-name	AP name

Defaults N/A

Command Mode Any mode

Usage Guide N/A

Configuration Examples

The following example displays the WLAN inherited by the specified AP in the backup group.

```
ac#show ap-config inherit-wlan wlan-ap-0001
WLAN ID  SSID               VLAN-Id/VLAN-Group ID    Radio ID
AP WLAN ID
-------- ---------------------- -------------------------
-------------------------- ----------
1       ruijie-wifi          1100                  ALL
```

Related Commands	Command	Description
	N/A	N/A

Platform Description

1.53 show ap-config product

Use this command to display the AP device list.

show ap-config product

Parameter Description	Parameter	Description
	N/A	N/A

Defaults N/A

Command Mode Any mode

Usage Guide N/A

Configuration Examples

The following example displays the AP device list.

```
Ruijie#show ap-config product
Product ID         Hardware Version Count    Used Wtp
-------------------- ---------------- -------- --------
AP120                          1.0      10     5.0
AP220-E                        1.0       5     5.0
AP320                          2.0       8     8.0
AP530-PPC                      1.5       2     2.0
```

Related Commands	Command	Description
	N/A	N/A

Platform Description

1.54 show ap-config summary

Use this command to display the AP list.

show ap-config 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 AP list.

```
Ruijie#show ap-config summary
========= show ap status =========
Radio: Radio ID or Band: 2.4G = 1#, 5G = 2#
      E = enabled, D = disabled, N = Not exist, V = Virtual AP
      Current Sta number
      Channel: * = Global
      Power Level = Percent

Online AP number: 2
Offline AP number: 1

AP Name                              IP Address     Mac Address    Radio
Radio             Up/Off time   State
---------------------------------------- --------------- --------------
------------------- ------------------- ------------- -----
AP220E-2                              22.22.22.11    00d0.1414.3f67 1  E   0
11*  100 2  E   0  153*  100    0:00:37:34 Run
xh-ap                                10.21.121.4    00d0.f822.33d6 1# N   0
-    - 2# N   0    -    -    0:23:56:05 Run
AP220E_V2.0_19                            -       1414.4b13.96f7 1  N   -
-    - 2  N   -    -    -    0:00:14:07 Quit
```

Related

Command	Description

Commands	N/A	N/A

Platform Description

1.55 show ap-config summary ap-auth

Use this command to display authentication information on all APs.

show ap-config summary ap-auth

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 authentication information on all APs.

```
Ruijie#sh ap-config summary ap-auth
AP Name                 Mac Address    Bind  bind-ap-serial   Bind
bind-ap-cert            Bind  bind-ap-password Bind  State
------------------------- -------------- ----- ---------------- -----
------------------------- ----- ---------------- ----- -----
ap220                   1414.4b13.9ff3 FALSE               TRUE
FALSE               TRUE  Run
0011.0000.0101                      FALSE               TRUE
FALSE               TRUE  Quit
0011.0000.0201                      FALSE               TRUE
FALSE               TRUE  Quit
```

Related Commands

Command	Description
N/A	N/A

Platform Description

1.56 show ap-config summary deny-ap

Use this command to display the list of APs that are refused in attempt to associate with the AC.

show ap-config summary deny-ap

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 list of APs that are refused in attempt to associate with the AC.

```
Ruijie#sh ap-config summary deny-ap
AP Name      IP Address         Mac Address    Reason
-----------  -----------------  -------------- --------------
AP1          192.168.10.10    1414.4b13.9ff3  By bind-ap-mac
AP2          192.168.10.11    00d0.f822.33b0  By bind-ap-mac
```

Related Commands

Command	Description
N/A	N/A

Platform Description

1.57 show ap-config summary hot-backup

Use this command to display the AP hot backup configuration and master AC.

show ap-config summary hot-backup

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 AP hot backup configuration and master AC.

```
Ruijie#sh ap-config summary hot-backup
AP NAME                         AP GROUP                        CONTEXT NAME
AC SELECT    CHANNEL STATE       AC DESCRIPTION
------------------------------ ------------------------------
------------------------------ -------------------- ----------------
tttt                            apg-10                          6.6.6.6-10
UNKNOWN      SINGLE             AC-110
ap2                             apg-810                          8.8.8.8-10
OTHER        DOUBLE             AC-810
ap3                             apg-820                          8.8.8.8-20
ME           DOUBLE             AC-820
```

Field	Description
AP NAME	AP name.
AP GROUP	AP group.
CONTEXT NAME	Hot backup instance.
AC SELECT	Master AC. ● ME: The local AC as the master AC. ● OTHER: The peer AC as the master AC. ● UNKNOWN: The AP does not announce the master AC or the announcement times out.
CHANNEL STATE	Number of tunnels. ● SINGLE: One tunnel is created. ● DOUBLE: Two tunnels are created. ● NULL: No tunnel is created.
AC DESCRIPTION	AC description.

Related Commands

Command	Description
N/A	N/A

Platform Description

1.58 show ap-config summary virtual-ap-role

Use this command to display whether to support AP virtualization and the AP status.

show ap-config summary virtual-ap-role

Parameter Description

Parameter	Description
N/A	N/A

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide N/A

Configuration Examples The following example displays whether to support AP virtualization and the AP status.

```
Ruijie#show ap-config summary virtual-ap-role
========= show virtaul ap role =========
Master  AP number: 1
Virtual AP number: 1
Normal  AP number: 1
Nonsupport AP number: 1
AP Name                              IP Address     Mac Address    Virtual AP
Role
-------------------------------------   ---------------   --------------
---------- ----------
AP1                                 11.11.11.5     00d0.f822.3366 Nonsupport
-
AP2                                   11.11.11.2     00d0.f822.3352 Support
Master
AP3                                   11.11.11.6     00d0.f822.3442 Support
Virtual
AP4                                   11.11.11.4     00d0.f822.3648 Support
Normal
Ruijie#
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

1.59 show ap-config virtual-ap detail

Use this command to display virtual AP details.

show ap-config virtual-ap detail *ap-name*

Parameter Description

Parameter	Description
ap-name	Specifies an AP.

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide N/A

Configuration Examples The following example displays virtual AP status.

```
Ruijie(config)# show ap-config virtual-ap detail ap1
AP(ap1) is Master
  WLAN capacity: 16
  Max stations : 256
  Master AP:
    WLAN   : 1 - 8
Max STA: 128
Link ID: 1
  Virtual AP 1:
    Address: 2.2.2.2
    State  : Run
    WLAN   : 9 - 16
Max STA: 128
Link ID: 2
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

1.60 show ap-config virtual-ap summary

Use this command to display virtual AP summary.

show ap-config virtual-ap 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 virtual AP summary.

```
Ruijie#show ap-config virtual-ap summary
AP Name                              Virtual AP Numbers   Active Numbers
-------------------------------------               --------------------
---------------
Ap1                                 1                1
Ruijie#
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

1.61 show ap-group aps

Use this command to display the list of APs connected to a specified AP group.

show ap-group aps *ap-group-name*

Parameter Description

Parameter	Description
ap-group-name	Indicates an AP group name.

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide N/A

Configuration Examples The following example displays the basic configuration information of the current AC.

```
Ruijie(config)#show ap-group aps default
Ap Name            Mac Addr       Pid
-------------------- --------------- --------------------
```

```
rrm-ap              0011.1122.3333 AP220E
```

Related Commands

Command	Description
N/A	N/A

Platform Description

1.62 show ap-group aps summary

Use this command to display the APs of all AP groups.

show ap-group aps 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 APs of all AP groups.

```
Ruijie(config)#show ap-group aps summary
AP Group Name       AP Name            Mac Addr
-------------------- -------------------- ---------------
default             rrm-ap             0011.1122.3333
default             ap0001             0011.1122.4444
```

Related Commands

Command	Description
N/A	N/A

Platform Description

1.63 show virtual-ap detail

Use this command to display AP virtualization template details.

show ap-config virtual-ap detail *sub-ap--name*

Parameter Description

Parameter	Description
sub-ap-name	Specifies the AP virtualization template name.

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide N/A

Configuration Examples The following example displays AP virtualization template details.

```
Ruijie#show virtual-ap detail ac3322
Module Name        :ac3322
AC IPV4           :2.2.2.2
Wlan Capacity      :0
Sta Capacity       :4
Link Interface     :
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

1.64 show virtual-ap summary

Use this command to display AP virtualization template summary.

show virtual-ap 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 AP virtualization template summary.

```
Ruijie#show virtual-ap summary
Module Name                              AC IPV4        Wlan  Sta   Interface
----------------------------------------   ---------------   -----   -----
---------
ac101                                  192.168.201.119 0     0     0
ac20                                   192.168.201.201 0     0     0
ac3322                                  2.2.2.2        0     4     0
ap550                                   2.2.2.2        0     3     2
clf_ac20                                192.168.201.20  5     0     0
test2                                   20.2.2.3       0     0     0
test3                                   23.3.3.21      0     32    0
test4                                   20.3.3.2       0     0     0
test5                                   20.3.3.1       0     2     2
test51                                  3.2.3.1        0     64    0
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

1.65 show ap-group cb

Use this command to display the basic configuration information of a specified AP group.

show ap-group cb *ap-group-name*

Parameter Description

Parameter	Description
ap-group-name	Indicates an AP group name.

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide N/A

Configuration Examples The following example displays the basic configuration information of the default AP group.

```
Ruijie(config)#show ap-group cb default

Ap Group info:
```

```
apg_name          :default
discovery_timer    :20
echo_req_timer     :30
error_report_timer  :120
sta_time_out       :300
stati_time         :120
ap_fallback        :Enable
image_id           :
```

Related Commands	Command	Description
	N/A	N/A

Platform Description

1.66 show ap-group intf-wlan-map

Use this command to display the WLAN-to-VLAN mapping table of a specified AP group.

show ap-group intf-wlan-map *ap-group-name*

Parameter Description	Parameter	Description
	ap-group-name	Indicates an AP group name.

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide N/A

Configuration Examples The following example displays the basic configuration information of the current AC.

```
Ruijie(config)#show ap-group intf-wlan-map default
WlAN ID   SSID           Vlan Id         Radio id   Mib index
--------- ---------------- ---------------- ---------- ----------------
500      ssid-500        2              ALL       1
```

Related Commands	Command	Description
	N/A	N/A

Platform Description

1.67 show ap-group summary

Use this command to display the list of all AP groups configured for the current AC.

show ap-group 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 list of all AP groups configured for the current AC.

```
Ruijie(config)#show ap-group summary
Total Ap Group Num : 2
Ap Group Name
1. default
2. test-group
```

Related Commands

Command	Description
N/A	N/A

Platform Description

1.68 show ap-mode

Use this command to display the AP mode.

show ap-mode

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 AP mode.

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

Related Commands

Command	Description
N/A	N/A

Platform Description

1.69 show license

Use this command to display license information.

show license

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 license information.

```
Ruijie#show license
Serial Number    : xxxxxxxxxxxx

 No. Activation Key                          AP Number
------------------------------------------------------------------------
  1. AAAA-BBBB-CCCC-DDDD-EEEE-FFFF-GGGG-HHHH     128
------------------------------------------------------------------------
Total 272 access points are supported, old version 128, new version 16.
Ruijie#
```

Related Commands

Command	Description
N/A	N/A

Platform N/A

Description

1.70 show virtual-ac balance-info

Use this command to display the virtual AC member list.

show virtual-ac balance-info

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 virtual AC member list.

```
Ruijie#show virtual-ac balance-info
Dev ID    AP Num AP License    STA Num
--------- -------- ---------- ----------
2             0       0.0         0
1             1       0.0         0
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

1.71show wlan hot-backup

Use this command to display the instance list of the peer end. Use the **no** form of the command to restore the default setting.

show wlan hot-backup [*peer-ip*] **summary**

Parameter Description

Parameter	Description
peer-ip	Specifies the IP address of the peer end.

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide N/A

Configuration Examples The following example displays the instance list of all peer ends.

```
Ruijie#show wlan hot-backup summary
Context Name                AC DESCRIPTION               AP Num   STA Num
------------------------------ ------------------------------ --------
--------
192.168.201.76-11            AC-76                       1       0
192.168.201.77-1             AC-77                       2       1
192.168.201.78-1             AC-78                       11      30
192.168.201.81-100           AC-100                      5       24
```

The following example displays the instance list of a specified peer end.

```
Ruijie#show wlan hot-backup 192.168.201.76 summary
Ruijie#show wlan hot-backup summary
Context Name                AC DESCRIPTION               AP Num   STA Num
------------------------------   ------------------------------   --------
--------
192.168.201.76-11            AC-76                       1       0
192.168.201.77-1             AC-77                       2       1
192.168.201.78-1             AC-78                       11      30
192.168.201.81-100           AC-100                      5       24
```

The following example displays the instance list of all peer ends on the AC.

```
Ruijie#show wlan hot-backup summary
Context Name                AC DESCRIPTION               AP Num   STA Num
Assigned Lic Backups Lic
------------------------------ ------------------------------ --------
-------- ------------ ------------
192.168.201.76-11            AC-76                       1       0       32
64
192.168.201.77-1             AC-77                       2       1       16
32
192.168.201.78-1             AC-78                       11      30      NA
NA
192.168.201.81-100           AC-100                      5       24      NA
NA
```

The following example displays the instance list of a specified peer end on the AC.

```
Ruijie#show wlan hot-backup 192.168.201.76 summary
Context  AC DESCRIPTION               AP Num   STA Num  Assigned Lic Backups Lic
-------- ------------------------------ -------- -------- ------------ ------------
11       AC-76                       1        2        32           64
```

Related Commands	Command	Description
	N/A	N/A

Platform Description N/A

1.72 show wlan-config cb

Use this command to display the configuration details of a specified WLAN.

show wlan-config cb *wlan-id*

Parameter Description	Parameter	Description
	N/A	N/A

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide N/A

Configuration Examples

The following example displays the configuration of WLAN 512.

```
Ruijie(config)#show wlan-config cb  512
WLAN ID.................................. 512
SSID..................................... ssid-512
Profile.................................. <NULL>
Short Preamble........................... Disable
Spectrum Management...................... Disable
QoS...................................... Disable
Short Slot Time.......................... Disable
APSD..................................... Disable
Delayed Block ACK........................ Disable
Immediate Block ACK...................... Disable
MAC Mode................................. Local
Tunnel Mode.............................. 802.3 Tunnel
Suppress SSID............................ Enable
RTS Threshold............................ 2347
Long Retry............................... 4
Short Retry.............................. 7
```

Related Commands	Command	Description
	N/A	N/A

Platform Description

1.73 show wlan-config summary

Use this command to display the WLAN configuration list on the AC.

show wlan-config 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 WLAN configuration list on the AC.

```
Ruijie(config)#show wlan-config summary
Total Wlan Num : 3
Wlan id  Profile Name        SSID               STA NUM
-------- -------------------- -------------------- --------
1       pro-1              ssid-1             0
2       pro-2              ssid-2             0
4095    <NULL>            ssid-4095          0
```

Related Commands

Command	Description
N/A	N/A

Platform Description

1.74 ssid

Use this command to set SSID.

ssid *ssid-string*

Parameter Description

Parameter	Description
ssid-string	SSID character string, consisting of up to 32 characters.

Defaults N/A

Command Mode WLAN configuration mode

Usage Guide If a WLAN is deployed, changing SSID will disconnected the STAs associated with WLAN.

Configuration Examples The following example changes the SSID of WLAN1 to ruijie.

```
Ruijie(config)#wlan-config 1
Ruijie(config-wlan)#ssid ruijie
```

Related Commands

Command	Description
N/A	N/A

Platform Description

1.75 ssid-code

Use this command to configure coded character set for the SSID.

ssid-code { **gbk** | **utf-8** }

Parameter Description

Parameter	Description
gbk	Configures gbk.
utf-8	Configures utf-8.

Defaults No SSID-code is configured by default.

Command Mode WLAN configuration mode

Usage Guide If the WLAN is deloyed, running this command will force the users of this WLAN offline.

Configuration Examples The following example configures t utf-8 for the SSID of WLAN 1.

```
Ruijie(config)#wlan-config 1
Ruijie(config-wlan)#ssid-code utf-8
```

Related Commands

Command	Description
N/A	N/A

Platform N/A

Description

1.76 sta-capacity

Use this command to configure the number of STAs supported by a virtual AP. Use the **no** form of the command to restore the default setting.

sta-capacity *sta-cap*

no sta-capacity

Parameter Description

Parameter	Description
sta-cap	Configures the number of STAs supported by a virtual AP

Defaults The number of STAs supportable by a virtual AP is not configured by default. If the number of STAs supportable by a virtual AP is not configured, it is calculated as follows:
(Total number of STAs supportable by the AP – Number of STAs configured for virtual APs)/Number of virtual APs with the number of supportable STAs not configured

Command Mode AP virtualization template configuration mode

Usage Guide N/A

Configuration Examples The following example sets the number of STAs supported by a virtual AP to 16.

```
Ruijie(config)#virtual-ap VAP-1
Ruijie(config-virtual-ap)# sta-capacity 16
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

1.77 statistics-timer

Use this command to configure statistics timer for a specified AP or all APs in a specified AP group. Use the **no** form of this command to restore the default configuration.

statistics-timer *timer-num*

no statistics-timer

Parameter Description

Parameter	Description
timer-num	Indicates a timer interval to be configured, in the range

	from 1 to 65535 in the unit of seconds.

Defaults The default is 120 seconds.

Command Mode AP configuration mode or AP group configuration mode

Usage Guide The command is used to set statistics timer for a specified AP. This command prefixed with no can be used to restore the default value.

Configuration Examples

The following example enters the configuration mode of AP0001 to configure its statistics timer to 200 seconds.

```
Ruijie(config)# ap-config AP0001
Ruieji(config-ap)# statistics-timer 200
```

The following example enters the configuration mode of AP0001 to restore the default setting.

```
Ruijie(config)# ap-config AP0001
Ruieji(config-ap)# no statistics-timer
```

The following example enters the default AP group to configure its statistics timer to 200 seconds.

```
Ruijie(config)# ap-group default
Ruijie(config-ap-group)# statistics-timer 200
```

The following example enters the default AP group to restore the default setting.

```
Ruijie(config)# ap-group default
Ruijie(config-ap-group)# no statistics-timer
```

Related Commands

Command	Description
N/A	N/A

Platform Description

1.78 switch2fat

Use this command to switch a specified AP to the fat AP mode, resulting in departure of the specified AP from the AC.

switch2fat ap-name

Parameter Description

Parameter	Description
ap-name	Indicates an AP name.

Defaults By default, all fit APs are controlled by their associated AC. A fit AP can be switched to a fat AP, and will have self-control ability.

Command Mode AC configuration mode

Usage Guide The command is used to switch a specified AP to the fat AP mode. As a result, the specified AP will leave the AC.

Configuration Examples The following example switches AP0002 to the fat mode.

```
Ruijie(config-ac)# switch2fat AP0002
```

Related Commands

Command	Description
N/A	N/A

Platform Description

1.79 tertiary-base

Use this command to enter the configuration mode of a specific AP connected to the current AC and to specify the tertiary AC for the specific AP.

tertiary-base *ac-name* { *ip-address* | *ipv6-address* } [**switch-back**]

Parameter Description

Parameter	Description
ap-name	Indicates the name of the AP to be configured
ip-address	Indicates the IP address of the secondary AC in the format of A.B.C.D.
ipv6-address	Indicates the IPv6 address of the secondary IPv6 AC in the format of X;Y::Z.
switch-back	Enables switch-back function. The default is disabled.

Defaults N/A

Command Mode AP configuration mode

Usage Guide Configure the tertiary AC of the AP. The configuration is based on a single AP.

Configuration Examples The following example configures the tertiary AC of AP ap1. The IP address of the tertiary AC is 192.168.3.1.

```
Ruijie#config terminal
Ruijie(config)#ap-config ap1
Ruijie(config-ap)#tertiary-base ap1 192.168.3.1
```

The following example configures the tertiary IPv6 AC of ap1 as ac3 and the IPv6 address of ac3 as 2001:abcd::300.

```
Ruijie#config terminal
Ruijie(config)#ap-config ap1
```

```
Ruijie(config-ap)#tertiary-base ac3 2001:abcd::300
```

Related Commands

Command	Description
primary-base	Configures the preferred AC.
secondary-base	Configures the secondary AC.

Platform Description

1.80 virtual-ap

Use this command to create an AP virtualization template. Use the **no** form of the command to restore the default setting.

virtual-ap *sub-ap-name*

no virtual-ap *sub-ap-name*

Parameter Description

Parameter	Description
sub-ap-name	Specifies an AP virtualization template name.

Defaults No AP virtualization template is created by default.

Command Mode Global configuration mode

Usage Guide N/A

Configuration Examples The following example creates an AP virtualization template.

```
Ruijie(config)#virtual-ap VAP-1
Ruijie(config-virtual-ap)#
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

1.81 virtual-ap

Use this command to configure a virtual AP. Use the **no** form of the command to restore the default setting.

virtual-ap *sub-ap-name* { **id** *num* }
no virtual-ap *sub-ap-name*

Parameter Description

Parameter	Description
sub-ap-name	Specifies the name of an AP virtualization template.
id *num*	Specifies the number of a virtual AP on the AP

Defaults No virtual AP is configured by default.

Command Mode AP configuration mode
AP group configuration mode
All-AP configuration mode

Usage Guide N/A

Configuration Examples The following example configures a virtual AP named VAP-1.

```
Ruijie(config)# ap-config AP1
Ruijie(config-ap)# virtual-ap VAP-1 id 1
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

1.82 wlan-capacity

Use this command to configure the number of WLANs supported by a virtual AP. Use the **no** form of the command to restore the default setting.
wlan-capacity *wlan-cap*
no wlan-capacity

Parameter Description

Parameter	Description
wlan-cap	Sets the number of WLANs supported by a virtual AP

Defaults The number of WLANs supported by a virtual AP is not configured by default. If the number of WLANs supportable by a virtual AP is not configured, it is calculated as follows:
(Total number of WLANs supported by the AP – Number of WLANs configured for virtual APs)/Number of virtual APs with the number of supported WLANs not configured

Command AP virtualization template configuration mode

Mode

Usage Guide N/A

Configuration Examples The following example sets the number of WLANs supported by a virtual AP to 6.

```
Ruijie(config)#virtual-ap VAP-1
Ruijie(config-virtual-ap)# wlan-capacity 6
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

1.83 webmaster

Use this command to add an administrator. Use the **no** form of the command to delete an administrator.

webmaster *webmaster-name*

no webmaster *webmaster-name*

Parameter Description

Parameter	Description
webmaster-name	Specifies the administrator name.

Defaults N/A

Command Mode Role configuration mode

Usage Guide N/A

Configuration Examples The following example adds administrator test-admin to role test-group.

The following example deletes administrator test-admin from role test-group.

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

1.84 wlan-config

Use this command create a WLAN and enter the WLAN configuration mode. Use the **no** form of this command to remove the configuration.

wlan-config *wlan-id* [*profile-string*] [*ssid-string*]

no wlan-config *wlan-id*

Parameter Description

Parameter	Description
wlan-id	Indicates an ID for the WLAN to be created, ranging from 1 to 4094.
profile-string	Indicates a descriptor for the WLAN, which can be omitted.
ssid-string	Indicates the SSID character string corresponding to the WLAN.

Defaults N/A

Command Mode WLAN configuration mode

Usage Guide

To create a WLAN, you must specify **ssid-string** but can omit **profile-string** as mentioned in the command description. When a WLAN is created, cli will automatically enter the configuration mode of this WLAN.
To enter the configuration mode of a WLAN, you only need to specify the existing ID of this WLAN. One SSID can correspond to more than one WLAN, but one WLAN cannot be associated with multiple SSIDs at the same time.

Configuration Examples

The following example creates a WLAN with an ID of 2048 and a SSID of **ssid-test**.

```
Ruijie(config)# wlan-config 2048 profile-test ssid-test
Ruijie(config-wlan)# exit
Ruijie(config)#
```

The following example enters the configuration mode of the WLAN with the ID of 2048.

```
Ruijie(config)# wlan-config 2048
Ruijie(config-wlan)# exit
```

Related Commands

Command	Description
interface-mapping wlan-id vlan-id [**radio** *radio-id*]	Applies this WLAN to a specified radio.

Platform Description

1.85 wtp-limit

Use this command to configure the maximum number of AP supported on the AC. Use the **no** form of this command to restore the default setting.

wtp-limit *wtp-num*

no wtp-limit

Parameter Description

Parameter	Description
wtp-num	The parameter indicates the maximum number of AP connected to the AC.

Defaults The default is **16** for WS5302 , and **128** for WS5708.

Command Mode AC configuration mode

Usage Guide

The command is used to configure the maximum number of AP supported on the AC. This number can exceed neither the maximum number supported by the AC nor the maximum number allowed by the license.

Different model of AP product has the different weight of supported number, for example, two wall APs occupy one of the maximum number. The AC device will calculate the real number of occupied APs according to the weight ratio. This command is used to configure the weight number of APs instead of real number of APs.

Configuration Examples

The following example configures the AC to connect 100 APs at most.

```
Ruijie(config-ac)# wtp-limit 100
```

The following example configures the AC to connect a default maximum of 128 APs.

```
Ruijie(config-ac)# no wtp-limit
```

Related Commands

Command	Description
sta-limit	Configures the maximum number of clients supported by the AC.

Platform Description

2 WLAN STAMP 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 This command is supported only on ACs.

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 Description

Parameter	Description
N/A	N/A

Defaults This function is disabled by default.

Command Global configuration mode

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 This command is supported only on ACs.

2.3 client-kick

Use this command to delete the MAC address of a specified wireless user.

client-kick *sta-mac*

Parameter Description

Parameter	Description
sta-mac	Indicates the MAC address of a wireless user.

Defaults N/A

Command Mode AC configuration mode

Usage Guide N/A

Configuration Examples The following example deletes the wireless user with the MAC address aaaa.bbbb.cccc.

```
Ruijie(config)# ac-controller
Ruijie(config-ac)# client-kick aaaaa.bbbbb.ccccc
```

Related Commands

Command	Description
N/A	N/A

Platform Description This command is supported only on ACs.

2.4 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 N/A

Command mode Global configuration mode

Usage Guide Up to 300 association control zones can be configured on an AC. 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 This command is supported only on ACs.

2.5 flow-balance-group add

Use this command to add a specified AP to a specified load balancing group.

flow-balance-group add *group-name ap-name*

Parameter Description

Parameter	Description
group-name	Indicates the name of the specified balancing group. Each flow-based load balancing group supports 10 APs at the most.
ap-name	Indicates the AP’s name to be added

Defaults N/A

Command Mode AC configuration mode

Usage Guide N/A

Configuration Examples

The following example adds ap1 and ap2 to the balancing group named test-group

```
Ruijie(config)# ac-controller
Ruijie(config-ac)# flow-balance-group add test-group ap1
Ruijie(config-ac)# flow-balance-group add test-group ap2
```

Related Commands

Command	Description
N/A	N/A

Platform Description This command is supported only on ACs.

2.6 flow-balance-group base

Use this command to configure the traffic base value for load balancing. Use the **no** form of this command to restore the default setting.

flow-balance-group base *number*

no flow-balance-group base

Parameter Description

Parameter	Description
number	Traffic base value. The range is from 1 to 100.

Defaults The traffic base value is 10 Mbps by default.

Command Mode AC configuration mode

Usage Guide N/A

Configuration Examples

The following example sets the traffic base value for load balancing to 50 Mbps

```
Ruijie(config)# ac-controller
Ruijie(config-ac)# flow-balance-group base 50
```

Related Commands

Command	Description
N/A	N/A

Platform Description This command is supported only on ACs.

2.7 flow-balance-group create

Use this command to configure the load-balancing group based on the flow. Use the **no** form of this command to remove the configuration.

flow-balance-group create *group-name*

no-flow-balance-group create *group-name*

Parameter Description

Parameter	Description
group-name	The name of a load balancing group, allows a maximum of 55 characters and excludes space. It supports 80 flow-balancing groups at most.

Defaults N/A

Command Mode AC configuration mode

Usage Guide The **no** option of this command is used to delete configuration of a specific balancing group.

Configuration Examples

The following example creates a load balancing group named test-group.

```
Ruijie(config)# ac-controller
Ruijie(config-ac)# flow-balance-group create test-group
```

The following example deletes the load balancing group named test-group.

```
Ruijie(config)# ac-controller
Ruijie(config-ac)# no flow-balance-group create test-group
```

Related Commands

Command	Description
N/A	N/A

Platform Description This command is supported only on ACs.

2.8 flow-balance-group del

Use this command to delete a specified AP from a specified load balancing group.

flow-balance-group del *group-name ap-name*

Parameter Description

Parameter	Description
group-name	The load balancing group for operation.
ap-name	The name of AP to be deleted from the load balancing group.

Defaults N/A

Command Mode AC configuration mode

Usage Guide N/A

Configuration Examples The following example deletes ap1 from balancing group named test-group.

```
Ruijie(config)# ac-controller
Ruijie(config-ac)# flow-balance-group del test-group ap1
```

Related Commands

Command	Description
N/A	N/A

Platform Description This command is supported only on ACs.

2.9 flow-balance-group enable

Use this command to configure a threshold value for the traffic of associated AP devices to enable load balancing. Use the **no** form of this command to restore the default threshold value.

flow-balance-group enable *group-name number*

no flow-balance-group enable *group-name number*

Parameter Description

Parameter	Description
group-name	The load balancing group for operation.
number	The traffic threshold value. The unit is %. The range is from 0 to 500. “0” indicates load balancing is disabled.

Defaults The default traffic threshold is 5%.

Command Mode AC configuration mode

Usage Guide N/A

Configuration Examples The following example sets the traffic threshold of load balancing group test-group to 100 Kbps.

```
Ruijie(config)# ac-controller
Ruijie(config-ac)# flow-balance-group enable test-group 1
```

Related Commands

Command	Description
N/A	N/A

Platform Description This command is supported only on ACs.

2.10 flow-balance-group flow

Use this command to configure the load threshold of the balancing group. Use the **no** form of this command to remove the configuration.

[no] flow-balance-group flow *group-name ap-name*

Parameter Description

Parameter	Description
group-name	Name of load balancing group for operation.
number	The threshold of the balancing group, the unit is 100 Kbps, the default is 500 Kbps, and the scope is 0-100000 kbps. 0 indicates this balancing group does not enable flow-based load balancing function.

Defaults The default traffic threshold is 5%.

Command Mode AC configuration mode

Usage Guide N/A

Configuration Examples The following example configures the threshold of balancing group named test-group as 100 Kbps.

```
Ruijie(config)# ac-controller
Ruijie(config-ac)# flow-balance-group flow test-group 1
```

Related Commands

Command	Description
N/A	N/A

Platform Description This command is supported only on ACs.

2.11 flow-balance-group radio-flow

Use this command to configure the load balancing group based on the traffic reported by the AP periodically. Use the **no** form of this command to remove the configuration.

flow-balance-group radio-flow *group-name*

no flow-balance-group radio-flow *group-name*

Parameter Description

Parameter	Description
group-name	Load balancing group name.

Defaults By default, the traffic calculated from the CAPWAP data channel on the AC device is used.

Command mode AC configuration mode

Usage Guide N/A

Configuration Examples The following example configures the load balancing group based on the traffic reported by the AP periodically.

```
Ruijie(config)# ac-controller
Ruijie(config-ac)# flow-balance-group radio-flow test-group
```

Related Commands

Command	Description
N/A	N/A

Platform Description This command is supported only on ACs.

2.12 hide-ssid sta-reach-limit

Use this command to configure the intelligent SSID hiding function. When the number of STAs on an AP or a radio reaches the upper limit, new STAs are not allowed to go online but the STAs can still scan the SSID and attempt to perform association. After the intelligent SSID hiding function is enabled, new STAs cannot detect the signal and will not attempt to perform association. 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	Specifies a radio on which the intelligent SSID hiding function is enabled. If this parameter is not specified, the intelligent SSID hiding function is enabled on all radios.
2.4g	The intelligent SSID hiding function is enabled on the 2.4G radio.
5g	The intelligent SSID hiding function is enabled on the 5G radio.

Defaults The intelligent SSID function is disabled by default.

Command mode AP configuration mode

Usage Guide After the intelligent SSID function is enabled and the numbers of STAs on all APs in an area reach the upper limit, new STAs cannot detect the SSID in this area.

Configuration Examples The following example enables the intelligent SSID hiding function on the 5G radio.

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

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

2.13 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.

2.14 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.

2.15 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.

2.16 inter-radio-balance num-balance dual-band

Use this command to configure the enabling threshold and balancing threshold for STA 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 num-balance dual-band enable-load *en-num* **threshold** *thrs-num*

no inter-radio-balance num-balance dual-band

Parameter Description

Parameter	Description
en-num	The enabling threshold value. Load balancing is enabled only when

	the number of STAs associated with the radio exceeds the threshold. The range is from 1 to 20.
thrs-num	The balancing threshold value. The STA will be disassociated with the radio when the STA number difference between the associated radio and lowest load radio. The range is from 1 to 20.

Defaults By default, the enabling threshold is 8 and the balancing threshold is 8.

Command mode AP /AP group configuration mode

Usage Guide When the load balancing between radios is enabled, if the number of STAs associated with the radio exceeds the enabling threshold and the STA number difference between the associated radio and lowest load radio exceeds the balancing threshold, the STA will be disassociated with the radio and the STAs 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 num-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 10 and 10 respectively for the different radios on AP0001.

```
Ruijie(config)# ap-config AP0001
Ruijie(config-ap)# inter-radio-balance num-balance dual-band enable-load 10
threshold 10
```

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 num-balance dual-band
```

The following example configures the enabling threshold and balancing threshold to 4 and 5 respectively for different radios of AP devices in the AP group.

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

The following example configures the enabling threshold and balancing threshold to 5 and 5 respectively for different radios on all AP devices.

```
Ruijie(config)# ap-config all
Ruijie(config-ap)# inter-radio-balance num-balance dual-band enable-load 5
threshold 5
```

Related Commands

Command	Description
N/A	N/A

Platform Description	This command is supported only on ACs.

2.17 inter-radio-balance num-balance enable

Use this command to enable load balancing for the number of STAs 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 num-balance enable

no inter-radio-balance num-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 STA number difference between radios on the AP device not exceed the threshold value.

Configuration Examples

The following example enables load balancing for the number of STAs between radios on AP0001.

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

The following example disables load balancing for the number of STAs between radios on AP0001.

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

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

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

The following example enables load balancing for the number of STAs between radios on all AP devices.

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

Related

Command	Description

Commands		
	N/A	N/A

Platform Description This command is supported only on ACs.

2.18 inter-radio-balance num-balance same-band

Use this command to configure the enabling threshold and balancing threshold for STA 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 num-balance same-band enable-load *en-num* **threshold** *thrs-num*

no inter-radio-balance num-balance same-band

Parameter Description

Parameter	Description
en-num	The enabling threshold value. Load balancing is enabled only when the number of STAs associated with the radio exceeds the threshold. The range is from 1 to 20.
thrs-num	The balancing threshold value. The STA will be disassociated with the radio when the STA number difference between the associated radio and lowest load radio. The range is from 1o to 20.

Defaults By default, the enabling threshold is 2 and the balancing threshold is 2.

Command mode AP /AP group configuration mode

Usage Guide When the load balancing between radios is enabled, if the number of STAs associated with the radio exceeds the enabling threshold and the STA number difference between the associated radio and lowest load radio exceeds the balancing threshold, the STA will be disassociated with the radio and the STAs 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 num-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 3 and 3 respectively for the same radios on AP0001.

```
Ruijie(config)# ap-config AP0001
Ruijie(config-ap)# inter-radio-balance num-balance same-band enable-load 3
threshold 3
```

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 num-balance same-band
```

The following example configures the enabling threshold and balancing threshold to 3 and 5 respectively for the same radios of AP devices in the AP group.

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

The following example configures the enabling threshold and balancing threshold to 5 and 5 respectively for the same radios on all AP devices.

```
Ruijie(config)# ap-config all
Ruijie(config-ap)# inter-radio-balance num-balance same-band enable-load 5 threshold 5
```

Related Commands

Command	Description
N/A	N/A

Platform Description This command is supported only on ACs.

2.19 inter-radio-balance radio weight

Use this command to configure the load ratio of radios. 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 number, in the range from 1 to 100.

Defaults The radio weight is 100, and load is balanced between radios based on the 1:1 ratio by default.

Command mode

AP configuration mode

AP group configuration mode

Usage Guide if weight of radio 1 is set to 50 and that of radio 2 is set to 100, the load ratio between radio 1 and radio 2 is 1:2.

Configuration Examples

The following example sets the load ratio of radios to 1:2.

```
Ruijie(config)# ap-config AP0001
Ruijie(config-ap)# inter-radio-balance radio 1 weight 50
```

The following example restores the default settings.

```
Ruijie(config)# ap-config AP0001
Ruijie(config-ap)# no inter-radio-balance radio 1 weight
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

2.20 num-balance-group add

Use this command to add a specified AP to a specified load balancing group.

num-balance-group add *group-name ap-name*

Parameter Description

Parameter	Description
group-name	The name of the specified balancing group. Each number-based balancing group supports 10 APs at the most.
ap-name	The name of the AP to be added

Defaults N/A

Command Mode AC configuration mode

Usage Guide N/A

Configuration Examples The following example adds ap1 to the balancing group test-group.

```
Ruijie(config)# ac-controller
Ruijie(config-ac)# num-balance-group add test-group ap1
```

Related Commands

Command	Description
N/A	N/A

Platform Description This command is supported only on ACs.

2.21 num-balance-group create

Use this command to create load balancing group based on number. Use the no form of this command to remove the configuration.

num-balance-group create *group-name*

no num-balance-group create *group-name*

Parameter	Description
group-name	The name of the load balancing group, allows a maximum of 55 characters, blank space is not included. It supports 80 number-based balancing groups at most.

Parameter Description

Defaults N/A

Command Mode AC configuration mode

Usage Guide N/A

Configuration Examples

The following example creates a load balancing group named test-group.

```
Ruijie(config)# ac-controller
Ruijie(config-ac)# num-balance-group create test-group
```

The following example deletes a load balancing group named test-group.

```
Ruijie(config)# ac-controller
Ruijie(config-ac)# no num-balance-group create test-group
```

Command	Description
N/A	N/A

Related Commands

Platform Description This command is supported only on ACs.

2.22 num-balance-group del

Use this command to delete a specified AP from a specified load balancing group.

num-balance-group del *group-name ap-name*

Parameter	Description
group-name	The load balancing group for operation.
ap-name	The name of the AP to be deleted from the balancing group.

Parameter Description

Defaults N/A

Command Mode The AC configuration mode

Usage Guide N/A

Configuration Examples

The following example deletes ap1 from the balancing group named test-group.

```
Ruijie(config)# ac-controller
Ruijie(config-ac)# num-balance-group del test-group ap1
```

Related Commands

Command	Description
N/A	N/A

Platform Description

This command is supported only on ACs.

2.23 num-balance-group enable

Use this command to configure a threshold value for the number of STAs associated with AP devices to enable load balancing. Use the **no** form of this command to restore the default threshold value.

num-balance-group enable *group-name number*

no num-balance-group enable *group-name number*

Parameter Description

Parameter	Description
group-name	The load balancing group for operation.
ap-name	The enabling threshold value. The range is from 0 to 10. “0” indicates load balancing for the number of STAs is disabled.

Defaults

The default enabling threshold is 3.

Command Mode

AC configuration mode

Usage Guide

N/A

Configuration Examples

The following example sets the enabling threshold for the number of STAs associated to 1.

```
Ruijie(config)# ac-controller
Ruijie(config-ac)# num-balance-group enable test-group 1
```

Related Commands

Command	Description
N/A	N/A

Platform Description

This command is supported only on ACs.

2.24 num-balance-group mode

Use this command to configure the mode of load balancing group. Use the **no** form of the command to restore the default setting.

num-balance-group mode *group-name* { **radio-mode** | **ap-mode** }

no num-balance-group mode *group-name*

Parameter Description

Parameter	Description
group-name	The name of the load balancing group for operation.
radio-mode	The radio-based mode of the load balancing group.
ap-mode	The AP-based mode of the load balancing group.

Defaults The default is AP-based mode.

Command Mode AC configuration mode.

Usage Guide N/A

Configuration Examples The following example configures the radio-based mode for the balancing group named test-group

```
Ruijie(config)# ac-controller
Ruijie(config-ac)# num-balance-group mode test-group radio-mode
```

Related Commands

Command	Description
N/A	N/A

Platform Description This command is supported only on ACs.

2.25 num-balance-group num

Use this command to configure the load threshold of the load balancing group. Use the **no** form of this command to remove the configuration.

[no] flow-balance-group flow *group-name ap-name*

Parameter Description

Parameter	Description
group-name	The name of the load balancing group for the operation.
number	The threshold of balancing group. The range is from 0 to 20. 0 indicates this balancing group disables the flow-based load balancing function..

Defaults The default threshold is 3

Command Mode The AC configuration mode

Usage Guide N/A

Configuration Examples The following example configures the threshold of the balancing group named test-group as 1.

```
Ruijie(config)# ac-controller
Ruijie(config-ac)# num-balance-group flow test-group 1
```

Related Commands

Command	Description
N/A	N/A

Platform Description This command is supported only on ACs.

2.26 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 Up to 300 terminal packages can be configured on an AC. 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 This command is supported only on ACs.

2.27 prevent-jitter

Use this command to enable the STA jitter prevention function and the STA jitter prevention time. Use the **no** form of this command to restore the default setting.

prevent-jitter { **enable | time** *keep-time* }

no prevent-jitter { **enable | time** }

Parameter Description

Parameter	Description
enable	Enables or disables the STA jitter prevention function.
time	Indicates the STA jitter prevention time.
keep-time	Configures the STA jitter prevention time in seconds. The value ranges from **1** to **86400**.

Defaults The default STA jitter prevention time is 60s.

Command mode WLAN configuration mode

Usage Guide During the STA jitter prevention time, if the STA goes online from the same WLAN of the AP again, it is regarded that the STA has never gone offline. If the STA goes online from the same WLAN of another AP, it is regarded that the STA roams to the AP with the same SSID. If the STA goes online from another WLAN, it is regarded that the STA is switched to another AP with a different SSID. If the AP or authentication server proactively forces an STA to go offline, the STA jitter prevention function does not take effect and the STA goes offline immediately.

Configuration Examples

The following example enables the STA jitter prevention function for WLAN1.

```
Ruijie(config)#wlan-config 1
Ruijie(config-wlan)#prevent-jitter enable
```

The following example sets the STA jitter prevention time to 300s.

```
Ruijie(config)#wlan-config 1
Ruijie(config-wlan)#prevent-jitter time 300
```

The following example disables the STA jitter prevention function for WLAN1.

```
Ruijie(config)#wlan-config 1
Ruijie(config-wlan)#no prevent-jitter enable
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

2.28 primary-sta

	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	See table below
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”.

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

```
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	This command is supported only on ACs .

2.29 secondary-sta

	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	See table below
Defaults	N/A
Command mode	Terminal package configuration 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	The following example configures a secondary STA with MAC address of 00d0.f800.0002 for the

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

Examples 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 This command is supported only on ACs.

2.30 show ac-config client

Use this command to display the information about all the STAs connected with the current AC.

show ac-config client [**by-ap-name** | **802.11a** | **802.11b** | **802.11n** | **802.11g** | **802.11ac | 802.11ax | other**]

Parameter Description

Parameter	Description
by-ap-name	Indicates that the STAs are sorted by AP name.
802.11a	Displays information about users of 802.11a.
802.11b	Displays information about users of 802.11b.
802.11n	Displays information about users of 802.11n.
802.11g	Displays information about users of 802.11g.
802.11ac	Displays information about users of 802.11ac.
802.11ax	Displays information about users of 802.11ax.
other	Displays information about unknown users.

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide N/A

Configuration Examples The following example displays the information about all the STAs connected with the current AC.

```
AC#show ac-config client
========= show sta status =========
AP    : ap name/radio id
Status: Speed/Power Save/Work Mode, E = enable power save, D = disable power
save

Total Sta Num : 1
STA MAC       IP Address     AP                                  Wlan Vlan
Status     Asso Auth Link Auth Up time
-------------- --------------- ---------------------------------------
```

```
---- ---- ----------- --------- --------- -------------
78e4.00d3.1183 192.168.248.2   te/1                              1    1
65.0M/D/bn  Open     Open       0:00:08:10
```

Related Commands	Command	Description
	N/A	N/A

Platform Description This command is supported only on ACs.

2.31 show ac-config client detail

Use this command to display the details of a specified wireless user.

show ac-config client detail *mac-addr*

Parameter Description	Parameter	Description
	mac-addr	Indicates the MAC address of a wireless user.

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide N/A

Configuration Examples The following example displays the details of a specified wireless user.

```
AC#show ac-config client detail 0023.cdae.5260
Mac Address        :0023.cdae.5260
IP Address          :0.0.0.0
Wlan Id            :123
Vlan Id            :2
Roam State         :Local
Association ID       :0

Associated Ap Information:
AP Name           :youzt
AP IP              :10.1.1.2
```

Related Commands	Command	Description
	N/A	N/A

Platform Description This command is supported only on ACs.

2.32 show ac-config client hot-backup

Use this command to display the wireless client backup information.

show ac-config client hot-backup

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 wireless client backup information.

```
AC# show ac-config client hot-backup
STA MAC        IPV4 Address    Context Name                  Status AC DESCRIPTION
-------------- --------------- ----------------------------- ------ ---------------
---------------
0001.2fe1.5022 192.168.121.2   2.2.2.2-1                     Active AC1
0001.21f2.3dac 192.168.135.28  3.3.3.3-10                           Backup AC10
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

2.33 show ap-config client-statistic

Use this command to display online/offline times and total roaming times in different. time.

show ap-config client-statistic

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 about the specified wireless user.

```
AC# #show ac-config client statistic
========= show sta statistic =========
STA online  times in 5 second: 13
STA offline times in 5 second: 10
STA roaming times in 5 second: 2

STA online  times in 1 minute: 30
STA offline times in 1 minute: 25
STA roaming times in 1 minute: 10

STA online  times in 1 hour:  200
STA offline times in 1 hour:  300
STA roaming times in 1 hour:  100

Maxinum rate of STA-online in 1 hour: 20/s
```

Related Commands

Command	Description
N/A	N/A

Platform Description This command is supported only on ACs.

2.34 show ac-config flow-balance summary

Use this command to display detailed configuration information of flow-based load balancing group.

show ap-config flow-balance 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 detailed configuration information of flow-based load balancing group.

```
Ruijie(config)#show ac-config flow-balance summary
Group          Threshold     AP NAME
---------------- --------------
-------------------------------------------------------------------------------
-------
test-group1         5*100kbps ap1, ap2, ap3
test-group2         6*200kbps ap4, ap5, ap6
```

Related Commands	Command	Description
	N/A	N/A

Platform Description This command is supported only on ACs.

2.35 show ac-config num-balance summary

Use this command to display the detailed configuration information of the number-based load balancing group.

show ap-config num-balance 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 detailed configuration information of the number-based load balancing group.

```
Ruijie(config)#show ac-config num-balance summary
Group           Threshold AP NAME
---------------- --------- -------------------------
test-group1      1       ap1, ap2, ap3
test-group2      2       ap4, ap5, ap6
```

Related Commands	Command	Description
	N/A	N/A

Platform Description	This command is supported only on ACs.

2.36 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	This command is supported only on ACs.

2.37 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	The following example displays all association control zones.

Examples

```
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	This command is supported only on ACs.

2.38 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 This command is supported only on ACs.

2.39 show sta-blacklist

Use this command to display the STA blacklist.

show sta-blacklist

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 STA blacklist.

```
Ruijie#show sta-blacklist
Num       STA MAC       Add time
---------- -------------- --------------------
1         0080.1111.1111 2013-07-02 13:56:22
2         0090.2222.3333 2013-07-02 13:56:35
3         0070.1111.2233 2013-07-02 13:57:08
```

Related Commands

Command	Description
N/A	N/A

Platform Description This command is supported only on ACs.

2.40 sta-balance num-limit enable

Use this command to enable the STA to terminate load balancing automatically after association failures. Use the **no** form of this command to restore the default setting.

sta-balance num-limit enable

no sta-balance num-limit enable

Parameter Description

Parameter	Description
N/A	N/A

Defaults This function is disabled by default.

Command mode AC configuration mode

Usage Guide By default, the STA keeps attempting to associate e with the AP selected by load balancing. After the sta-balance function is enabled, the maximum number of its attempts is five times. If the association fails for five times, the STA will terminate load balancing next time.

Configuration Examples

The following example enables the sta-balance function.

```
Ruijie(config)# ac-controller
Ruijie(config-ap)# sta-balance num-limit enable
```

Related Commands

Command	Description
N/A	N/A

Platform This command is supported only on ACs.

Description

2.41 sta-blacklist

Use this command to enable the STA blacklist function, set aging time for the blacklisted STAs and identify the STA as the attack source. Use the **no** form of this command to restore the default setting.

sta-blacklist { **enable** | **lifetime** | **detect-time** | **fail-limit** } [*seconds* | *number*]

no sta-blacklist { **enable** | **lifetime** | **detect-time** | **fail-limit** } [*seconds* | *number*]

Parameter Description

Parameter	Description
enable	Enables the STA blacklist function.
lifetime	Sets aging time for the blacklisted STAs.
detect-time	Detection time. Once the STA fails to associate with the AP, it is identified as the attack source. If the STA association failure count reaches **fail-limit** within **detect-time**, the STA is added to the blacklist.
fail-limit	Limits the STA access failure count within **detec-time**.
seconds	In the unit of seconds. **lifetime**: in the range from 60 to 1200. **detect-time**: in the range from 5 to 60.
number	Sets the STA access failure count, in the range from 1 to 100.

Defaults

The STA blacklist function is disabled by default.

The default *lifetime* is 300 seconds.

The default *detect-time* is 60 seconds.

The default *number* is 5 seconds.

Command mode

AC configuration mode

Usage Guide

N/A

Configuration Examples

The following example enables the STA blacklist function.

```
Ruijie(config)# ac-controller
Ruijie(config-ac)# sta-blacklist enable
```

The following example disables the STA blacklist function.

```
Ruijie(config)# ac-controller
Ruijie(config-ac)# no sta-blacklist enable
```

The following example sets the blacklisted STA aging time to 60 seconds.

```
Ruijie(config)# ac-controller
Ruijie(config-ac)# sta-blacklist lifetime 60
```

The following example sets detect-time to 10 seconds.

```
Ruijie(config)# ac-controller
Ruijie(config-ac)# sta-blacklist detect-time 10
```

The following example limits association failure count.

```
Ruijie(config)# ac-controller
Ruijie(config-ac)# sta-blacklist fail-limit 20
```

Related Commands

Command	Description
N/A	N/A

Platform Description This command is supported only on ACs.

2.42 sta-idle-timeout

Use this command to configure aging time for a wireless user in a specified AP or AP group. Use the **no** form of this command to restore the default setting.

sta-idle-timeout *timer-num*

no sta-idle-timeout

Parameter Description

Parameter	Description
timer-num	Indicates that you set the aging time, in the range from 60 to 86400 in the unit of seconds.

Defaults The default is 300 seconds.

Command Mode AP configuration mode/AP group configuration mode

Usage Guide If no information is received from a wireless user within the setting time, the wireless user will be regarded to have left the WLAN, and will be deleted from the network by the system.

Configuration Examples

The following example enters the configuration mode of AP0001 to configure its client timeout timer to 600 seconds.

```
Ruijie(config)# ap-config AP0001
Ruijie(config-ap)# sta-idle-timeout 600
```

The following example enters the configuration mode of AP0001 to restore its client timeout timer to the default setting.

```
Ruijie(config)# ap-config AP0001
Ruijie (config-ap)# no sta-idle-timeout-timer
```

The following example enters the default AP group to configure its client timeout timer to 600 seconds.

```
Ruijie(config)# ap-group default
Ruijie (config-ap-group)# sta-idle-timeout 600
```

The following example enters the default AP group to restore its client timeout timer to the default setting.

```
Ruijie(config)# ap-group default
Ruijie(config-ap-group)# no sta-idle-timeout-timer
```

Related Commands	Command	Description
	N/A	N/A

Platform Description This command is supported only on ACs.

2.43 sta-limit

Use this command to configure the maximum number of wireless users that can be connected. In the AC configuration mode, this command can provide global configuration. In the AP group and AP configuration mode , this command can be used to configure the maximum number of wireless users that can be connected to a specified AP. In the WLAN configuration mode,this command can be used to configure the maximum number of wireless users that can be connected to a specified WLAN.Use the **no** form of this command to restore the default setting.

sta-limit *client-num*

no sta-limit *client-num*

Parameter Description

Parameter	Description
client-num	Indicates the maximum number of wireless users that can be connected. In the AC configuration mode: The value is equal to 32 multipled by the number of APs suppprted by the AC (depending on lincense limit) In the AP group configuration mode, the value is 512. In the AP configuration mode, for offline APs or ap-config all mode, the value is 512. For online APs, the value depends on the product model. In the WLAN configuration mode, the value is equal to 32 multipled by the number of APs suppprted by the AC (depending on lincense limit).

Defaults

In the AC configuration mode:
The default is equal to 32 multipled by the number of APs suppprted by the AC .
In theAP group configuration mode, the default is 32.
In the AP configuration modem, the default for the offline APs or ap-config all mode is 32 and the default for the online APs is determined by the AP model.
In the WLAN configuration mode, the default is no limit.

Command Mode

AC configuration mode
AP group configuration mode
AP configuration mode
WLAN configuration mode

Usage Guide

This command is used to configure how many clients the device can serve at most. This value should not exceed the maximum number supported by an AC or the maximum number limited by the license. The maximum number of wireless users that can be supported varies with AC products.
For the ap-config all, ap-group and off-line AP configuration, the range is from 1 to 512. If the value configured by the user exceed the STA number supported by an AP, it will automatically adjust the value to the maximum STA number supported by the AP when the AP is online.
For online APs, the maximum value is number of STAs supported by the AP.

Configuration Examples

The following example configures an AC to provide service for 2400 clients at most.

```
Ruijie(config-ac)# sta-limit 2400
```

The following example configures all APs in the AP group (Default) to admit 20 wireless users at most.

```
Ruijie(config)# ap-group default
Ruijie(config-ap-group)# sta-limit 20
```

Related Commands

Command	Description
N/A	N/A

Platform Description

This command is supported only on ACs.

2.44 sta-limit per-ap

Use this command to configure the maximum number of STAs associated with each AP. Use the **no** form of this command to restore the default setting.
sta-limit per-ap *client-num*
no sta-limit per-ap

Parameter Description

Parameter	Description
client-num	Sets the maximum number of STAs associated with each AP in the range from 1 to 1536.

Defaults

The default is no limit.

Command mode

WLAN configuration mode

Usage Guide

If the configured value exceeds the AP capacity, the AP capacity prevails.

Configuration Examples

The following example sets the maximum number of STAs associated with each AP in WLAN 1 to 10.

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

```
Ruijie(config-wlan)# sta-limit per-ap 10
```

Related Commands	Command	Description
	N/A	N/A

Platform Description N/A

2.45 sta-limit radio

Use this command to configure the maximum number of wireless users that can be connected. In the AP group and AP configuration mode, you can specify the maximum number of wireless users connected on a specific radio of an AP. Use the **no** form of this command to restore the default setting.

sta-limit *client-num* **radio** *radio_id*

no sta-limit *client-num* **radio** *radio_id*

Parameter Description	Parameter	Description
	client-num	Indicates the maximum number of wireless users that can be connected, in the range from 1 to 156 (or the maximum number of users supported by the AP).
	radio-id	Indicates the radio identifier.

Defaults By default, there is no limit.

Command Mode AP configuration mode/ AP group configuration mode

Usage Guide

The limit number of user in this command has no dependence on that of the sta-limit command. In other words, the limit number of user in this command can be greater than that of the sta-limit command.

For the ap-config all, ap-group and off-line AP configuration, the range is from 1 to 156. If the value configured by the user exceed the STA number supported by an AP, it will automatically adjust the value to the maximum STA number supported by the AP when the AP is online.

For online APs, the maximum value is number of STAs supported by the AP.

Configuration Examples

The following example configures the maximum number of wireless users that can be added into radio 1 of an AP to 20.

```
Ruijie(config)# ap-config ap1
Ruijie(config-ap)# sta-limit 20 radio 1
```

Related	Command	Description

Commands	N/A	N/A

Platform Description This command is supported only on ACs.

2.46 sta-logging rate-limit

Use this command to set the maximum number of syslogs printed per second, including STA online/offline information and STA change messages. Use the **no** form of this command to restore the default setting.

sta-logging rate-limit *limit-num*

no sta-logging rate-limit

Parameter Description

Parameter	Description
limit-num	Sets the maximum number of syslogs printed per second, in the range from 0 to 10000.

Defaults The default is 5.

Command mode AC configuration mode

Usage Guide N/A

Configuration Examples The following example sets the maximum number of syslogs printed per second to 100,

```
Ruijie(config)# ac-controller
Ruijie(config-ac)# sta-logging rate-limit 100
```

Related Commands

Command	Description
N/A	N/A

Platform Description This command is supported only on ACs.

3 WLAN CAPWAP Commands

3.1 ac-domain-name

Use this command to enable the AP to discover the AC domain name. Use the **no** form of this command to restore the default setting.

ac-domain-name *ac-domain-name*

no ac-domain-name

Parameter Description

Parameter	Description
ac-domain-name	Configures the AC domain name that the AP is to be discovered. The maximum length of the AC domain name is 64 characters, containing no spaces.

Defaults By default, the AC domain name is ac.ruijie.com.cn.

Command Mode AP configuration mode/AP group configuration mode

Usage Guide AP is able to discover the AC through DNS. You can use this command to revise the AC domain name to be discovered by the AP, so as to allow the AP to discover different APs.

Configuration Examples The following example enables the AP to discover the AC with the domain name as ruijie-ac.com.

```
Ruijie(config)# ap-config AP001
Ruijie(config-ap)# ac-domain-name ruijie-ac.com
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

3.2 acip ipv4

Use this command to configure the AP to join a specified AC. Use the **no** form of this command to remove the configuration.

acip ipv4 *ip-address* [*ip-address*]

no acip ipv4

Parameter Description

Parameter	Description
ip-address	Indicates the static IP address. Up to six static addresses can be configured.

Defaults N/A

Command Mode AP global configuration mode/AP configuration mode on the AC

Usage Guide

In general, the fit AP has no configuration. You can find AC through broadcast, multicast, DHCP and DNS or joining AC through the AC address configured by the static address. AP sends a discovery request packet to these IP addresses to detect whether AC is valid, and then add an AC.

If this command is configured for the fit AP and the AC connected with it, then the final configuration is the AC configuration.

Configuration Examples

The following example configures the static IP address list for the fit AP to join AC as 192.168.1.1 and 192.168.2.1.

```
Ruijie(config)# acip ipv4 192.168.1.1 192.168.2.1
```

The following example configures the static IP address list for AP0001 to join AC as 192.168.1.1 and 192.168.2.1.

```
Ruijie(config)# ap-config AP0001
Ruijie(config-ap)# acip ipv4 192.168.1.1 192.168.2.1
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

3.3 acip ipv6

Use this command to configure an AP to join an AC with a specific IPv6 address. Use the **no** form of this command to remove the configuration.

acip ipv6 *ipv6-address* [*ipv6-address*]

no acip ipv6

Parameter Description

Parameter	Description
ipv6-address	Specifies the IPv6 address of the AC to be connected with

	the AP. Up to six static addresses can be configured.

Defaults N/A

Command Mode AP global configuration mode/AP configuration mode on the AC

Usage Guide

An AP can find ACs through IPv6 multicast, DHCPv6, or DNSv6 packets or join an AC with a specific static IPv6 address. After this command is configured, the AP sends discovery request packets to the static IPv6 address of the AC to detect whether the address is valid. If the address is valid, the AP will join the AC.

If this command is configured on a fit AP and an AC connected with the AP, only the configuration on the AC takes effect.

Configuration Examples

The following example configures a fit AP to join an AC with static IPv6 address 2001:1a2b::1234.

```
Ruijie(config)# acip ipv6 2001:1a2b::1234
```

The following example configures AP0001 to join an AC with static IPv6 address 2001:1a2b::1234.

```
Ruijie(config)# ap-config AP0001
Ruijie(config-ap)# acip ipv6 2001:1a2b::1234
```

Related Commands

Command	Description
acip ipv4	Specifies the IPv4 address of an AC to be connected with the AP.

Platform Description N/A

3.4 active-bin-file

Use this command to activate an AP software version on an AC, and only the activated AP software version can be used to upgrade. Use the **no** form of this command to remove the configuration.

active-bin-file *filename* [**rgos10**]

no active-bin-file *filename* [**rgos10**]

Parameter Description

Parameter	Description
filename	Specifies software version name, including the suffix. This command can activate up to five software versions.

rgos10	Activates the transition version between RGOS 10 to RGOS 11. The software only applies to the AP.

Defaults N/A

Command Mode AC configuration mode

Usage Guide To configure an AC as the upgraded version of the specified AP product series, finish these three steps first: creating AP product series, configuring the software version corresponding to the specified AP, and activating the software version. Moreover, before the configuration, ensure this software version is available in the AC system files.

Configuration Examples

The following example activates an AP software version file ap.bin on the AC.

```
Ruijie(config-ac)# active-bin-file ap.bin
Ruijie(config-ac)#
```

The following example removes the activated AP software version file ap.bin from the AC.

```
Ruijie(config-ac)# no active-bin-file ap.bin
```

Related Commands

Command	Description
ap-serial	Creates an AP product series name and specify which hardware version AP product models belong to this series.
ap-image	Upgrades a specified AP software version with a specified activated file.

Platform Description N/A

3.5 ap-image

Use this command to configure AC upgrade to use a specified file to upgrade a specified series of APs. This command applies to all APs connected to the current AC. Use the **no** form of this command to remove the configuration.

ap-image { **auto-upgrade** | *filename serial-name* }

no ap-image { **auto-upgrade** | *filename serial-name* }

Parameter Description

Parameter	Description
auto-upgrade	Automatically matches the proper AP for upgrade.
filename	Indicates a software version name, including the suffix.
serial-name	Indicates the AP model series to be upgraded.

Defaults N/A

Command Mode AC configuration mode

Usage Guide This command is intended to use a specified file to upgrade a specified series of APs. This command applies to all APs connected to the current AC. To configure an AC as the upgraded version of the specified AP product series, finish these three steps first: creating AP product series, configuring the software version corresponding to the specified AP, and activating the software version. Moreover, before configuration, ensure this software version exists in the AC system files.

Configuration Examples The following exmaple configures the product series name as **test-serial**, and upgrades it with the **ap.bin** file.

```
Ruijie(config-ac)# ap-serial test-serial AP210-E, AP210, AP220-E, AP220
hw-ver 1.0
Ruijie(config-ac)#
Ruijie(config-ac)# ap-image ap.bin test-serial
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

3.6 ap-image

Use this command to upgrade a specified AP with a specified file. This command does not support the ap-config all mode. Use the **no** form of this command to remove the settings.

ap-image *filename*

no ap-image

Parameter Description

Parameter	Description
filename	Specifies an AP software version filename for upgrade, including the suffix.

Defaults N/A

Command Mode AP configuration mode

Usage Guide N/A

Configuration Examples

The following exmaple upgrades AP0001 with the file **ap.bin**.

```
Ruijie(config-ac)# ap-serial test-serial 1.0 AP220-E hw-ver 1.0
Ruijie(config-ac)# active-bin-file ap.bin
Ruijie(config-ac)# exit
Ruijie(config)# ap-config AP0001
Ruijie(config-ap)# ap-image ap.bin
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

3.7 apip ipv4

Use this command to configure a static IP address for a specified AP. Use the **no** form of the command to remove the configuration.

apip ipv4 *ip-address network-mask gateway*

no apip ipv4

Parameter Description

Parameter	Description
ip-address	The static IP address.
network-mask	The subnet mask.
gateway	The gateway address.

Defaults N/A

Command Mode AP global configuration mode

Usage Guide

In general, the fit AP has no configuration. Its IP address and gateway can be dynamically obtained by DHCP. When the CAPWAP tunnel between AP and AC is established, AC delivers the static IP address for AP, so that the address of AP maintains unchanged after AP is rebooted. In special application scenario, you can configure this command in AP global configuration mode to manually set the static IP address for the fit AP.

1. With the AP address configured as static, the DHCP is disabled, and the AC address cannot be obtained through the OPTION of DHCP. Therefore, after this command is configured, you

need to configure the AC address using the command “acip” on the AP so that the AP can find and join the AC when the AP and the AC are not in the same subnet.

2. The configuration of this command will be automatically saved after the AP configuration. No command of saving is required to be executed.

3. This command serves the same purpose as the command “ip address” on the AC in the AP configuration mode. However, when the AP joins the AC, if the command “ip address” exists in the AP configuration mode of the AC and conflicts with the command “apip”, the static address of the AP will be updated and the CAPWAP tunnel will be re-created.

Configuration Examples

The following example configures the static IP address of the fit AP as 192.168.1.2, the subnet mask as 255.255.255.0, and the gateway as 192.168.1.1..

```
Ruijie(config)# apip ipv4 192.168.1.2 255.255.255.0 192.168.1.1
```

Related Commands

Command	Description
acip	Specifies the AC address to be connected with by an AP.
ip address	Configures the static address of the AP.

Platform Description

N/A

3.8 apip ipv6

Use this command to configure a static IPv6 address for a specified AP. Use the **no** form of the command to remove the configuration.

apip ipv6 *ipv6-address-with-mask gateway*

no apip ipv6

Parameter Description

Parameter	Description
ipv6-address-with-mask	The IPv6 address with the mask length, for example. X:X:X:X::X/24.
gateway	Gateway address.

Defaults

N/A

Command Mode

AP global configuration mode

Usage Guide

This command is used to configure a static IPv6 address for the AP.

1. With the AP IPv6 address configured as static, the DHCPv6 is disabled, and the AC address cannot be obtained through the OPTION of DHCPv6. Therefore, after this command is configured, you need to configure the AC IPv6 address using the **acip ipv6** command on the AP and enable IPv6 support for the AP using the **apip ipv6 enable** command so that the AP can find and join the IPv6 AC when the AP and the AC are not in the same subnet.

2. The configuration of this command will be automatically saved.

3. This command serves the same purpose as the **ipv6 address** command on the AC in the AP configuration mode. However, when the AP joins the AC, the **ipv6 address** command in the AP configuration mode on the AC will conflict with the **apip ipv6** command, the static IPv6 address of the AP will be updated and the CAPWAP tunnel will be re-created.

Configuration Examples The following example configures the static IPv6 address of the fit AP as 2001:1a2b:1234::5566/48, and the gateway as 2001:1a2b:1234::1.

```
Ruijie(config)# apip ipv6 address 2001:1a2b:1234::5566/48 2001:1a2b:1234::1
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

3.9 apip ipv6 address autoconfig

Use this command to configure an AP to obtain a static IPv6 address through the automatic IPv6 address configuration mechanism. Use the **no** form of this command to remove the configuration.

apip ipv6 address autoconfig default

no apip ipv6 address autoconfig default

Parameter Description

Parameter	Description
N/A	N/A

Defaults N/A

Command Mode AP global configuration mode

Usage Guide You can run this command to configure a static IPv6 address for the AP. The configuration is similar to static IPv4 address configuration by running the **apip** command.

Configuration Examples The following example sets static IPv6 address 2001:1a2b:1234::5566/48 for the fit AP and specifies gateway address 2001:1a2b:1234::1.

```
Ruijie(config)# apip ipv6 2001:1a2b:1234::5566/48 2001:1a2b:1234::1
```

Related Commands

Command	Description
acip ipv6	Specifies the IPv6 address of the AC to be connected with the AP.
apip ipv6 enable	Enables IPv6 support on the AP.
ipv6 address	Specifies the static AP IPv6 address configured on the AC.

Platform Description N/A

3.10 apip ipv6 enable

Use this command to enable IPv6 support on a specific AP. Use the **no** form of this command to remove the configuration.

apip ipv6 enable

no apip ipv6 enable

Parameter Description

Parameter	Description
N/A	N/A

Defaults IPv6 support is enabled on the AP by default.

Command Mode AP global configuration mode

Usage Guide You can run this command to enable IPv6 support or run the **no** form of this command to disable IPv6 support. If an AP enabled with IPv6 support has no static IPv6 address, it will dynamically obtain an IPv6 address through DHCPv6. If IPv6 support is disabled from the AP, DHCPv6 is also disabled, but configuration about the static IPv6 address is not deleted.

Configuration Examples The following example enables IPv6 support on the fit AP.

```
Ruijie(config)# apip ipv6 enable
```

Related Commands

Command	Description
apip ipv6 address	Specifies the IPv6 address of the AC to be connected with the AP.
ipv6 enable	Enables IPv6 support on the specific AP on the AC in AP configuration mode.

Platform Description N/A

3.11 apip pppoe

Use this command to enable the AP to obtain the address through PPPoE. Use the **no** form of this command to restore the default setting.

apip pppoe

no apip pppoe

Parameter Description

Parameter	Description
N/A	N/A

Defaults This function is disabled by default.

Command Mode AP global configuration mode

Usage Guide After configuring this command, you should perform PPPoE and configure the default route to point to the dialer interface to enable communication between the AP and the AC.

CAPWAP can select only dialer 1 as the source port. Therefore, PPPoE dial requires dialer 1.

Configuration Examples The following example enables the fit AP to obtain the address through PPPoE.

```
Ruijie(config)# apip pppoe
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

3.12 ap-cfg erps raps-vlan

Use this command to configure ERPS single ring.

ap-cfg erps raps-vlan *vlan-id* **ring-port west** *interface-name1* **east** *interface-name2*

Use this command to configure RPL link and RPL owner node.

ap-cfg erps raps-vlan *vlan-id* **rpl-port** { **west** | **east** } **rpl-owner**

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

no ap-cfg erps raps-vlan

Parameter Description

Parameter	Description
vlan-id	Indicates the R-APS VLAN ID.
interface-name1	Indicates the name of the west port.
interface-name2	Indicates the name of the east port.
west	Specifies the west port to be the RPL owner.
east	Specifies the east port to be the RPL owner.

Defaults No ERPS is configured by default.

Command Mode AP configuration mode

Usage Guide A link needs to be disconnected or a port needs to be shut down during network planning. The ring topology can be built only after the ERPS link is configured.
Configure a Ring Protection Link (RPL) link on a device in the ERPS ring, so that traffic is balanced to dual upstream links. When one link fails or one device is faulty, the blocked RPL link is connected to prevent link failure.
The VLAN used by the ERPS will occupy the VLAN capacity of the device. Therefore, the VLAN cannot be set to VLAN 1 or VLAN 2444, both of which are default VLANs. It cannot be the same with the VLAN of an STA specified by the **Interface-mapping** command or the VLAN of a wired port specified by the **wired-VLAN** command. It cannot be the same with the VLAN specified by the **ap-vlan** command, neither.

Configuration Examples The following example configures ERPS single ring.

```
Ruijie(config)#ap-cfg erps raps-vlan 10 ring-port west gigabitEthernet 0/26 east gigabitEthernet 0/25
```

The following example configures RPL link and RPL owner node.

```
Ruijie(config)#ap-cfg erps raps-vlan 10 rpl-port east rpl-ower
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

3.13 ap-serial

Use this command to configure an AP series on an AC. Only when the AP hardware version and product model are configured to a series can its software version be upgraded through the AC. Use the **no** form of this command to remove the configuration.

ap-serial *serial-name hardware-version ap-pid1, ap-pid2, ..., ap-pidn* [**hw-ver** *hardware-version*]

no ap-serial *serial-name*

Parameter Description

Parameter	Description
serial-name	Indicates an AP series name to be created. The maximum character configuration number is 64, blank space is not included. The maximum number of the AP series that can be supported at the same time: WS5708 series: 16, WS5302 series:8
ap-pid1 ap-pid2 ... ap-pidn	Product models
hardware-version	Indicates the AP hardware version, the maximum configuration character is 64, blank space is not included. The hardware version name is a decimal, the mark is 'x' or 'X" which can be used to configure the following character.

Defaults N/A

Command Mode AC configuration mode

Usage Guide To configure an AC as the upgraded version of the specified AP product series, finish these three steps first: creating AP product series, configuring the software version corresponding to the specified AP, and activating the software version. Moreover, before configuration, ensure this software version exists in the AC system files.

Configuration Examples The following example creates an AP series named **test-serial** of which the designate AP hardware version is 1.0 on an AC, including these AP models: AP220-SE AP220-SH, AP220-E.

```
Ruijie(config-ac)# ap-serial test-serial 1.0 AP220-SE AP220-SH, AP220-E
hw-ver 1.0
Ruijie(config-ac)# active-bin-file ap.bin
Ruijie(config-ac)# ap-image test-serial ap.bin
```

The following exmaple removes the configuration from the AC to make the APs in the product series named **test-serial** no longer use the **ap.bin** file for upgrade.

```
Ruijie(config-ac)# no ap-image test-serial ap.bin
```

Related Commands

Command	Description
active-bin-file	Activates an AP software version file to upgrade an AP software version.

Platform N/A

Description

3.14 ap-upgrade bandwidth

Use this command to configure the upgrade bandwidth for AP devices. Use the **no** form of this command to restore the default setting.

ap-upgrade band-width *num*

no ap-upgrade band-width

Parameter Description

Parameter	Description
num	Bandwidth for AP upgrade, namely, the push rate for the AP upgrade file. The range is from 1 to 1,024. The unit is 1 KB. The default value is 0.

Defaults Upgrade bandwidth is not limited by default.

Command Mode AP configuration mode

Usage Guide During upgrading AP devices, the AC device occupies more transmission bandwidth to reduce upgrade time. However, in some small networks, the bandwidth for wired services should be guaranteed during AP upgrade to avoid impacting wired services. You can configure the upgrade bandwidth for AP devices to control the percentage of upgrade bandwidth.

The bandwidth limit configured

1. This command configuration controls the bandwidth for centralized upgrade of AP devices from the AC device, the distributed upgrade of AP devices is not impacted. As distributed upgrade data source is from central upgrade, the distributed upgrade is indirectly influenced.
2. The bandwidth unit is 1KB. For example, the minimum link bandwidth between AC and AP devices is 1 Mbps, the bandwidth value is 128.

Configuration Examples The following example sets the upgrade bandwidth for an AP device to 1 Mbps.

```
Ruijie(config-ac)# ap-upgrade band-width 128
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

3.15 ap-upgrade group

Use this command to add an AP device to the upgrade group. Use the **no** form of this command to remove the AP device from the upgrade group.

ap-upgrade group *group-name*

no ap-upgrade group

Parameter Description

Parameter	Description
group-name	Upgrade group name.

Defaults N/A

Command Mode AP configuration mode

Usage Guide The following configuration restrictions are applied on the AP devices which are added to a upgrade group:

1. The AP devices in the same group need to be configured with the **ap-grade band-width** command, so that the upgrade bandwidth of the AP devices is identical.
2. The **capwap upgrade group** command should be configured before this command.

Configuration Examples The following example adds an AP device to the upgrade group UPGRADE-GROUP1.

```
Ruijie(config-ac)# ap-upgrade group UPGRADE-GROUP1
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A.

3.16 capwap ctrl-ip

Use this command to set the IPv4 address for the CAPWAP tunnel between the AC and the AP. Use the **no** form of this command to restore the default setting.

capwap ctrl-ip *ip-address*

no capwap ctrl-ip

Parameter Description

Parameter	Description
ip-address	Specifies the IP address for the CAPWAP tunnel between the AC and

	the AP. It should be an interface IP address of the AC.

Defaults

Command Mode AC configuration mode

Usage Guide The AC generally uses a Loopback address to create the CAPWAP tunnel. This command enables the AC to create the CAPWAP tunnel with interface addresses in other three layers.

- This command may force the AP offline.
- Configuring an IP address not existing on the AC causes failure to create the CAPWAP tunnel.
- If the gateway of the AP is not on the AC, the AP address pool option should be set to the IP address in this command (if it is configured).
- In the AC hot backup environment, if this command is used to set the CAPWAP tunnel address, use the **peer-ip A.B.C.D** command to set the same IP address on the peer-to-peer backup AC.,

Configuration Examples The following example sets the IP address for the CAPWAP tunnel between the AC and the AP to 10.0.0.1..

```
Ruijie(config-ac)# capwap ctrl-ip 10.0.0.1
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

3.17 capwap discovery-type ac-referral

Use the **capwap discovery-type ac-referral allow** command to allow using ac-referral packets to discover an AC. Use the **capwap discovery-type ac-referral forbidden** command to forbid using ac-referral packets to discover an AC.

capwap discovery-type ac-referral allow

capwap discovery-type ac-referral forbidden

Parameter Description

Parameter	Description
N/A	N/A

Defaults An AP can use ac-referral packets to discover an AC by default.

Command Mode AC configuration mode

Usage Guide If the AC discovery mode is set to **forbidden**, an AP cannot connect to an AC using ac-referral packets.

Configuration Examples The following example forbids using ac-referral packets to discover an AC.

```
Ruijie(config-ac)# capwap discovery-type ac-referral forbidden
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

3.18 capwap discovery-type all

Use the **capwap discovery-type all allow** command to allow an AP to discover ACs using various kinds of packets. Use the **capwap discovery-type all forbidden** command to forbid using various kinds of packets to discover ACs.

capwap discovery-type all allow

capwap discovery-type all forbidden

Parameter Description

Parameter	Description
N/A	N/A

Defaults An AP can use various kinds of packets to discover an AC by default.

Command Mode AC configuration mode

Usage Guide An AP sends various kinds of packets, including ac-referral packets, DHCP packets, DNS packets, packets carrying the statically configured AC IP address, and packets of other types (for example, broadcast and multicast packets) to an AC. Only APs receiving responses from an AC can perceive that the AC is valid, and these APs can establish CAPWAP tunnels to the AC.

Configuration Examples The following example forbids using various kinds of packets to discover ACs.

```
Ruijie(config-ac)# capwap discovery-type all forbidden
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

3.19 capwap discovery-type dhcp

Use the **capwap discovery-type dhcp allow** command to allow an AP to discover ACs using DHCP packets. Use the **capwap discovery-type dhcp forbidden** command to forbid using DHCP packets to discover ACs.

capwap discovery-type dhcp allow

capwap discovery-type dhcp forbidden

Parameter Description

Parameter	Description
N/A	N/A

Defaults An AP can use DHCP packets to discover an AC by default.

Command Mode AC configuration mode

Usage Guide An AP sends DHCP packets to an AC. Only APs receiving responses from an AC can perceive that the AC is valid, and these APs can establish CAPWAP tunnels to the AC.

Configuration Examples The following example forbids using DHCP packets to discover ACs.

```
Ruijie(config-ac)# capwap discovery-type dhcp forbidden
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

3.20 capwap discovery-type dns

Use the **capwap discovery-type dns allow** command to allow an AP to discover ACs using DNS

packets. Use the **capwap discovery-type dns forbidden** command to forbid using DNS packets to discover ACs.

capwap discovery-type dns allow

capwap discovery-type dns forbidden

Parameter Description

Parameter	Description
N/A	N/A

Defaults An AP can use DNS packets to discover an AC by default.

Command Mode AC configuration mode

Usage Guide An AP sends DNS packets to an AC. Only APs receiving responses from an AC can perceive that the AC is valid, and these APs can establish CAPWAP tunnels to the AC.

Configuration Examples The following example forbids using DNS packets to discover ACs.

```
Ruijie(config-ac)# capwap discovery-type dns forbidden
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

3.21 capwap discovery-type static-config

Use the **capwap discovery-type static-config allow** command to allow an AP to discover ACs using packets carrying the static IP address of an AC. Use the **capwap discovery-type static-config forbidden** command to forbid using packets carrying the static IP address of an AC.

capwap discovery-type static-config allow

capwap discovery-type static-config forbidden

Parameter Description

Parameter	Description
N/A	N/A

Defaults An AP can use packets carrying the static IP address of an AC to discover the AC by default.

Command AC configuration mode

Mode

Usage Guide An AP sends packets carrying the static IP address of an AC to discover the AC. Only APs receiving responses from an AC can perceive that the AC is valid, and these APs can establish CAPWAP tunnels to the AC.

Configuration Examples The following example forbids using packets carrying the static IP address of an AC to discover the AC.

```
Ruijie(config-ac)# capwap discovery-type static-config forbidden
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

3.22 capwap discovery-type unknown

Use the **capwap discovery-type unknown allow** command to allow an AP to discover ACs using other packets. Use the **capwap discovery-type unknown forbidden** command to forbid using DNS packets to discover ACs.

capwap discovery-type unknown allow

capwap discovery-type unknown forbidden

Parameter Description

Parameter	Description
N/A	N/A

Defaults An AP can use other packets to discover an AC by default.

Command Mode AC configuration mode

Usage Guide An AP sends other packets to an AC. Only APs receiving responses from an AC can perceive that the AC is valid, and these APs can establish CAPWAP tunnels to the AC.

Configuration Examples The following example forbids using other packets to discover ACs.

```
Ruijie(config-ac)# capwap discovery-type unknown forbidden
```

Related

Command	Description

Commands

N/A	N/A

Platform Description N/A

3.23 capwap disc-concurrent

Use this command to configure CAPWAP packet processing capacity.

capwap disc-concurrent *num*

Parameter Description

Parameter	Description
num	The value varies with the device.

Defaults The default value varies with the device.

Command Mode AC configuration mode

Usage Guide If the number of CAPWAP packets exceeds the specified value, the packets will be discarded.

Configuration Examples The following example sets the CAPWAP packet processing capacity to 512pps.

```
Ruijie(config-ac)# capwap disc-concurrent 512
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

3.24 capwap dtls enable

Use this command to enable DTLS encryption for the CAPWAP tunnel. Use the **no** form of this command to disable this function.

capwap dtls enable

no capwap dtls enable

Parameter Description

Parameter	Description
N/A	N/A

Defaults This function is enabled by default.

Command Mode AC configuration mode

Usage Guide This function is enabled by default to ensure security of communication between the AC and the AP. This function is disabled in some cases, for example, for test purpose.

Configuration Examples The following example enables DTLS encryption for the CAPWAP tunnel.

```
Ruijie(config)# ac-controller
Ruijie(config-ac)# capwap dtls enable
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

3.25 capwap fragment enable

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

capwap fragment enable

no capwap fragment enable

Parameter Description

Parameter	Description
N/A	N/A

Defaults This function is disabled by default.

Command Mode AP configuration mode/AP group configuration mode

Usage Guide After the packets are encapsulated through the CAPWAP tunnel, its length may exceed IP MTU, causing IP fragmentation. If IP MTUs of multiple nodes on a link are inconsistent, the packet may go through fragmentation and defragmentation for many times, affecting packet forwarding. This command is used to enable CAPWAP fragmentation, that is, the packet is fragmented during CAPWAP encapsulation. The length of fragmented packets can be set to the minimum MTU using the **capwap mtu** command to avoid another IP fragmentation.

Configuration Examples The following example enables CAPWAP fragmentation on AP1.

```
Ruijie(config)# ap-config AP1
Ruijie(config-ap)# capwap fragment enable
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

3.26 capwap max-concurrent

Use this command to set the maximum number of concurrent online APs. Use the **no** form of this command to restore the default setting.

capwap max-concurrent *num*

no capwap max-concurrent

Parameter Description

Parameter	Description
num	The maximum number of concurrent online APs, in the range from 1 to 200.

Defaults The default is 50.

Command Mode AC configuration mode

Usage Guide If too many APs go online concurrently, AC CPU may increase even to 100%. This will cause the tunnel disconnection. Therefore, it is necessary to limit the number of concurrent online APs.

If you set a small value, the total online time of all APs associated to the AC will be long.

Configuration Examples The following example sets the maximum number of concurrent online APs to 100.

```
Ruijie(config-ac)#capwap max-concurrent 100
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

3.27 capwap max-retransmit

Use this command to set the maximum count of CAPWAP packet retransmission. Use the **no** form of this command to restore the default setting.

capwap max-retransmit *num*

no capwap max-retransmit

Parameter Description

Parameter	Description
num	Sets the maximum count of CAPWAP packet retransmission, in the range from 3 to 60.

Defaults The default is 5.

Command Mode AP configuration mode/AP group configuration mode

Usage Guide If the CAPWAP request packet is not responded, the packet is retransmitted, The retransmission interval increases by the initial retransmission interval (the smaller value between three seconds and half echo-interval) and the maximum retransmission interval should be no greater than the smaller value between half echo-interval and 60 seconds. If the device does not receive the response packet within the maximum count, the tunnel is considered disconnected. This command is only effective when the tunnel is in the Run state.

Configuration Examples The following example sets the maximum retransmission count to 20.

```
Ruijie(config)# ap-config AP1
Ruijie(config-ap)#capwap max-retransmit 20
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

3.28 capwap upgrade center enable

Use this command to enable the AP upgrade function on the center AC or disable the AP upgrade function on the branch AC. Use the **no** form of this command to restore the default setting.

capwap upgrade center enable

no capwap upgrade center enable

default capwap upgrade center enable

Parameter Description

Parameter	Description
N/A	N/A

Defaults The AP upgrade function is enabled on the center AC by default.

Command Mode AC configuration mode

Usage Guide

1. This command applies only to hierarchical AC scenarios.

2. When the AP upgrade function on an AC is changed from enabled to disabled, upgrade configurations (activated bin, automatic upgrade, sequential upgrade, and single AP upgrade) on the AC are automatically cleared.

3. After a branch AC connects to the center AC, the branch AC automatically synchronizes configurations of the center AC.

4. When a branch AC is in the connected state, configurations on the branch AC cannot be modified. The configurations can only be modified on the center AC and automatically synchronized to the branch AC.

5. When the branch AC is in the standalone state, configurations on the branch AC can be modified.

Configuration Examples

The following example enables the AP upgrade function on the center AC.

```
Ruijie(config-ac)# capwap upgrade center enable
```

The following example disables the AP upgrade function on the center AC.

```
Ruijie(config-ac)# no capwap upgrade center enable
```

The following example restores the default setting.

```
Ruijie(config-ac)# default capwap upgrade center enable
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

3.29 capwap upgrade group

Use this command to configure an AP upgrade group. Use the **no** form of this command to remove an AP upgrade group.

capwap upgrade group *group-name* [**max-concurrent** *num*]

no capwap upgrade group [*group-name* **max-concurrent**]

Parameter Description

Parameter	Description
num	The number of AP devices which can be upgraded concurrently in centralized mode. The range is from 1 to 200. The default is 5.
group-name	Upgrade group name

Defaults

Command Mode AC configuration mode

Usage Guide The AP number should be equal to the available bandwidth divided by max bandwidth of each AP.

Configuration Examples The following example creates an AP upgrade group Upgrade-Group1 and sets the concurrent number to 10.

```
Ruijie(config-ac)# capwap upgrade group Upgrade-Group1 max-current 10
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

3.30 capwap mtu

Use this command to set the Path MTU (PMTU) for the CAPWAP tunnel. Use the **no** form of this command to restore the default setting.

capwap mtu *num*

no capwap mtu

Parameter Description

Parameter	Description
num	Sets the PMTU for the CAPWAP tunnel, in the range from 68 to 1500 in the unit of bytes.

Defaults The default is 1500.

Command Mode AP configuration mode/AP group configuration mode

Usage Guide If the CAPWAP-encapsulated packet is longer than the PMTU, the packet is fragmented. Set the PMTU equal to the maximum IP MTU so as to avoid IP fragmentation and defragmentation.

A small PMTU will produce a large quantity of packet fragments, affecting packet forwarding or even leading to transmission failure. It is recommended to set a reasonable PMTU.

Configuration Examples The following example sets the PMTU for the CAPWAP tunnel to 1200 bytes.

```
Ruijie(config)# ap-config AP1
Ruijie(config-ap)# capwap mtu 1200
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A.

3.31 capwap upgrade max-concurrent

Use this command to set the maximum number of concurrently upgrading APs. Use the **no** form of this command to restore the default setting.

capwap upgrade max-concurrent *num*

no capwap upgrade max-concurrent

Parameter Description

Parameter	Description
num	The maximum number of concurrently upgrading APs, in the range from 1 to 200.

Defaults The default is 15.

Command Mode AC configuration mode

Usage Guide If too many APs upgrade concurrently, AC CPU may increase even to 100%. This will cause tunnel disconnection. Therefore, it is necessary to limit the number of concurrently upgrading APs.

Configuration Examples The following example sets the maximum number of concurrently upgrading APs to 10.

```
Ruijie(config-ac)#capwap upgrade max-concurrent 10
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

3.32 echo-interval

Use this command to configure the keep-alive interval for CAPWAP. Use the **no** form of this command to restore the default setting.

echo-interval *seconds*

no echo-interval

Parameter Description

Parameter	Description
seconds	This parameter indicates the keep-alive interval for CAPWAP, in the range from 5 to 255 in the unit of seconds.

Defaults The default is 30 seconds.

Command Mode AP configuration mode or AP group configuration mode

Usage Guide

In the fit AP network frame, AC and AP are connected through the CAPWAP tunnel. Echo Request and Echo Response are used to keep the validity of the link. In the case of no other request packets, AP sends the Echo Request packet to keep alive every echo interval. If AP does not receive a response, the packet will be retransmitted at the multiple original retransmission interval (3 seconds or half the echo interval, taking the smaller value) and the longest retransmission interval cannot exceed half the echo interval or 60 seconds (taking the smaller value). It is considered that the tunnel is interrupted if the AP does not receive the response packet within the maximum retransmit times, which means the failure time of keep alive of the tunnel is the keep-alive time plus retransmission intervals. This command only takes effect in the Run status of the tunnel. By default, the echo-interval is 30 seconds, the maximum retransmit times are 5. Namely, the AP device sends a request and does not receive a response after 0 second, the request packet will be retransmitted at the interval of 3 seconds, 6 seconds, 12 seconds, 15 seconds and 15 seconds.

In the deployment of wireless networks, you can adjust the echo interval based on network size to plan the convergence capability of the network. During the adjustment, make sure that you know the network size and the network does require the convergence capability to prevent impacts on the network environment due to too low value in the wireless network deployed by massive APs.

Configuration Examples

The following exmaple configures a 10-second echo interval for AP0001.

```
Ruijie(config)# ap-config AP0001
Ruijie(config-ap)# echo-interval 10
```

The following example configures a 10-second echo interval for all APs.

```
Ruijie(config)# ap-config all
Ruijie(config-ap)# echo-interval 10
```

The following example configures a 10-second echo interval for all APs in the default AP group.

```
Ruijie(config)# ap-group default
Ruijie(config-ap-group)# echo-interval 10
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

3.33 exec-cmd

Use this command to configure an AP to execute a command. Use the no form of this command to remove the setting.

exec-cmd mode *exec-mode* **cmd** *exec-cmd* **once**

no exec-cmd mode *exec-mode* **cmd** *exec-cmd*

Use this command to configure all APs in an AP group to execute a command.

exec-cmd *exec-cmd*

Parameter Description

Parameter	Description
exec-mode	Indicates the mode in which a command is executed on the AP.
exec-cmd	Indicates the command to be executed on the AP.
once	Indicates that the command is executed only once and is not saved.

Defaults N/A

Command Mode Single AP configuration mode/All APs configuration mode/AP group configuration mode

Usage Guide Some configuration commands are supported currently only by the AP and they are unavailable on the AC. To configure the commands for APs on the AC, run the **exec-cmd** command. To cancel or change the configuration of the **exec-cmd** command, run the **no exec-cmd** command to remove the configuration and then run the **exec-cmd** command to cancel or change the required configuration.

If **ap-config all** and **ap-config** are configured simultaneously, for online APs, the later configuration will take effect; for offline APs, **ap-config** has a higher priority than **ap-config all**.

Some configuration commands are available only in AP configuration mode and they are unavailable

in AP group configuration mode. To configure such a command for all APs in an AP group, run the **exec-cmd** command in the AP group. Note that the configuration is not saved in AP group configuration mode, that is, the command is executed only once on all APs in the current AP group.

Configuration Examples

The following example disables Eweb for an AP.

```
Ruijie(config)#ap-config AP1
Ruijie(config-ap)# exec-cmd mode configure cmd "no enable service web-server all"
```

The following example enables Eweb for an AP,

```
Ruijie(config-ap)# no exec-cmd mode configure cmd "no enable service web-server all"
Ruijie(config-ap)# exec-cmd mode configure cmd "enable service web-server all"
```

The following example configures Bluetooth iBeacon for all APs in the AP group.

```
Ruijie(config)#ap-group default
Ruijie(config-group)#exec-cmd ibeacon uuid ffffffffffffffffffffffffffffffff major ffff minor ffff
```

The following example disables Eweb for all APs in the AP group.

```
Ruijie(config-group)#exec-cmd exec-cmd mode configure cmd "no enable service web-server all"
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

3.34 install update

Use this command to update the installation status of Mini AP.

install updat

Parameter Description

Parameter	Description
N/A	N/A

Defaults N/A

Command Mode AP configuration mode

Usage Guide Once a Mini AP is installed to a Master AP, the Mini AP is considered as Offline if it is manually

removed. You can use this command to update the installation status of Mini APs to Uninstalled. This configuration is not saved.

Configuration Examples

The following exmaple updates the installation status of all Mini APs.

```
Ruijie(config)# ap-config all
Ruijie(config-ap)# install update
```

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

3.35 ip address

Use this command to configure the static IP address of a specified AP. Use the **no** form of this command to restore the default setting.

ip address *ip-address network-mask gateway*

no ip address

Parameter Description

Parameter	Description
ip-address	Interface address of the AP.
network-mask	Address mask of the AP.
gateway	Gateway of the AP.

Defaults

N/A

Command Mode

AP configuration mode

Usage Guide

The AP can obtain its IP address through static configuration or DHCP. If the AP has not a static IP address, it will obtain an address dynamically by DHCP and join the AC. In this case, you can use this command to configure the static address of the AP so that the address keeps unchanged after the AP restarts.

⚠ 1. With the AP address configured as static, the DHCP is disabled, and the AC address cannot be obtained through the OPTION of DHCP. Therefore, before this command is configured, you need to configure the address of the AC connected by using the command “acip” in AP configuration mode so that the AP can find and join the AC when the AP and the AC are not in the same subnet.

2. If the current address of the AP is not the same as the one specified through this command, the static address will be updated and the CAPWAP tunnel will be re-created.

Configuration Examples

The following example configures the address of AP0001 as 1.1.1.1, its mask as 255.255.255.0, and its next hop as 1.1.1.2.

```
Ruijie(config)# ap-config AP0001
Ruijie(config-ap)# ip address 1.1.1.1 255.255.255.0 1.1.1.2
```

Related Commands

Command	Description
apip	Configures the static address of an AP on the AP.
acip	Specifies the AC address to be connected with by an AP.

Platform Description

N/A

3.36 ipv6 address

Use this command to specify a static IPv6 address for an AP. Use the **no** form of this command to restore the default setting.

ipv6 address *ipv6-address-with-mask gateway*

no ipv6 address

Parameter Description

Parameter	Description
ipv6-address-with-mask	Specifies an interface IPv6 address of the AP, in the format similar to X:X:X:X::X/24.
gateway	Specifies an IPv6 gateway address of the AP.

Defaults

N/A

Command Mode

AP configuration mode

Usage Guide

An IPv6 address of an AP can be manually configured or obtained through DHCPv6. By default, the AP obtains an IPv6 address for itself through DHCPv6. If the AP has no static IPv6 address, it dynamically obtains an IPv6 address through DHCPv6 and joins an AC. You can run this command to set a static IPv6 address for the AP to ensure that the address of the AP remains unchanged after the AP is restarted.

1. If a static IPv6 address is set for the AP, DHCPv6 will be disabled. As a result, the AP cannot obtain IPv6 addresses of ACs through DHCPv6 OPTION. Therefore, before running this

command, you must use the **acip ipv6** command to specify the IPv6 address of the AC to be connected with the AP in AP configuration mode. After this configuration, the AP can discover and join the AC even if they are not on the same sub-network.
2. If the current IPv6 address of the AP is different from the static IPv6 address set by this command, the former will be overwritten by the latter. If the AP is enabled with IPv6 support, it will re-establish CAPWAP tunnels. If not, it will not re-establish CAPWAP tunnels.
3. If both IPv4 and IPv6 addresses are specified for the AP, and IPv6 support is enabled on it, the AP will search for IPv4 and IPv6 ACs at the same time.

Configuration Examples

The following example sets IPv6 address 2001:1a2b:1234::5566/48 for AP0001 and specifies gateway address 2001:1a2b:1234::1.

```
Ruijie(config)# ap-config AP0001
Ruijie(config-ap)# ipv6 address 2001:1a2b:1234::5566/48 2001:1a2b:1234::1
```

Related Commands

Command	Description
apip ipv6	Configures a static IPv6 address for the AP on itself.
apip ipv6 enable	Enables IPv6 support on the AP.
ipv6 enable	Enables IPv6 support for the AP on an AC in AP configuration mode.
acip ipv6	Specifies the IPv6 address of an AC connected with the AP.

Platform Description

N/A

3.37 ipv6 enable

Use this command to enable IPv6 support on a specific AP on an AC. 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

An AP is enabled with IPv6 support by default.

Command Mode

AP configuration mode

Usage Guide

An AP can search for IPv6 ACs based on IPv6 addresses only when it is enabled with IPv6 support. By default, the AP is disabled with IPv6 support. You can use this command to enable IPv6 support on the AP and use the **no** form of this command to disable IPv6 support from the AP.

1. If running this command changes the IPv6 support state of the AP, the AP will re-establish CAPWAP tunnels.
2. If the AP with both static IPv4 and IPv6 addresses is enabled with IPv6 support, the AP will re-establish CAPWAP tunnels and search for IPv4 and IPv6 ACs. It is not sure that the AP will join an IPv6 AC found by the AP. To allow the AP to search for only IPv6 APs, you can delete the static IPv4 address from the AP before enabling IPv6 support on the AP.

Configuration Examples

The following example enables IPv6 support on AP0001.

```
Ruijie(config)# ap-config AP0001
Ruijie(config-ap)# ipv6 enable
```

Related Commands

Command	Description
apip ipv6 enable	Enables IPv6 support for the AP on the AP itself.
ipv6 address	Sets an IPv6 address for the AP on the AC in AP configuration mode.

Platform Description

N/A

3.38 link-latency

Use this command to check the link status between an AC and the APs in a specified AP group. Use the **no** form of this command to remove the configuration.

[**no**] **link-latency**

Parameter Description

Parameter	Description
N/A	N/A

Defaults

N/A

Command Mode

AP configuration mode/AP group configuration mode

Usage Guide

N/A

Configuration

The following example enables inspection of the link status between specified AP-0001 and an AC,

Examples and check information about the corresponding link status.

```
Ruijie(config)#ap-config AP-0001
Ruijie(config-ap)#link-latency
```

The following example enables inspection of the link status between an AC and the APs in the **default** AP group, and check the link status information about the specified AP-0001.

```
Ruijie(config)# ap-group default
Ruijie(config-ap-group)# link-latency
```

Related Commands

Command	Description
show ap-config link-latency	Checks link status between AC and AP.

Platform Description N/A

3.39 location

Use this command to configure information about AC and AP location. Use the **no** form of this command to restore the default setting.

location *location-string*

no location

Parameter Description

Parameter	Description
location-string	Indicates AC location information, which can consist of up to 255 characters without any space.

Defaults By default, the AC location information is Ruijie_COM, the AP location information is null.

Command Mode AC configuration mode/AP configuration mode

Usage Guide N/A

Configuration Examples

The following example configures the location of a specific AC to the second floor of the computer department building (computer-layer2).

```
Ruijie(config-ac)# location computer-layer2
```

The following example configures AP0001 location information to AP-company.

```
Ruijie(config)# ap-config AP0001
Ruijie(config-ap)# location AP-company
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

3.40 reset slot

Use this command to reload a Mini AP installed to a Master AP.

reset slot *slot-id*

Parameter Description

Parameter	Description
slot-id	Slot number. The range is from 1 to 24.

Defaults N/A

Command Mode AP configuration mode

Usage Guide This command can take effect only on the Master AP and can enable reloading for only one Mini AP per execution.
This configuration is not saved.

Configuration Examples The following example reloads the Mini AP1 which is installed on slot1 of Master AP0001.

```
Ruijie(config)# ap-config AP0001
Ruijie(config-ap)# reset slot 1
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

3.41 set version

Use this command to set the version number.

set-version *string*

Parameter Description

Parameter	Description
string	Sets the version number.

Defaults N/A

Command Mode AC configuration mode

Usage Guide This command is used to set the version number and push version number to APs.

Configuration Examples The following example sets the version number to RGOS 10.4(2B17)-SP2.

```
Ruijie(config)# ac-controller
Ruijie(config-ac)# set-version RGOS 10.4(2B17)-SP2
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

3.42 show ac-config active-file

Use this command to display a list of activated files on the current AC. The **Used** field indicates how many APs are using this file, and the **Ready** field indicates whether this file has been activated completely.

show ac-config active-file

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 a list of activated files on the current AC.

```
Ruijie#show ac-config active-file
Cnt    File Name                       Image Id           Software number
Type      Used Cnt   DL Cnt Ready
------ ---------------------------------- --------------------
-------------------- ---------- ---------- ---------- --------
1     ap220ev1.1-mid(6-3).bin          RGOS 10.X-UPG       NA
```

```
rgos10     0          0          Init
2      ap220.bin                        1.0.0.017ed304      M09092708272014
main       0          0          Init
```

Related Commands	Command	Description
	N/A	N/A

Platform Description N/A

3.43 show ac-config serial-product

Use this command to display the correspondence association between the AP product series and product models configured of the AC, and display which files should be used to upgrade the corresponding product series.

show ac-config serial-product

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 AP product series and product models configured for the current AC.

```
Ruijie#show ac-config serial-product


Cnt    Serial Name     Hardware Version File Name    AP Product ID
------ --------------- ---------------- ------------ ---------------
1      ap-ser1.x       1.x              ap220-1.bin  AP220-E
                                                     AP220-SE
                                                     AP220-SH
                                                     AP620-H
```

```
                                                    AP220-E(M)
2     ap-ser2.x      2.x            ap220.bin    AP220-E
                                                    AP220-SH
                                                AP220-E(M)
```

Related Commands	Command	Description
	N/A	N/A

Platform Description N/A

3.44 show ac-config upgrade-group

Use this command to display the upgrade groups and AP devices on the AC device.

show ac-config upgrade-group [*group-name*]

Parameter Description	Parameter	Description
	group-name	AP upgrade group name.

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide N/A

Configuration Examples The following example displays AP upgrade groups.

```
Ruijie#show ac-config upgrade-group
Cnt    Group-Name              Max-Concurrent    Token cnt    Upgrading cnt
------ ---------------------------------- ------------ -----------
------------
1     UPGRADE-GROUP1            10             2         1
```

The following example displays the AP devices in the upgrade group.

```
Ruijie#show ac-config upgrade-group UPGRADE-GROUP1
Group have 2 ap, online 1 offline 1
Cnt     Ap-Name                Ap-Mac           Online    Upgrade
Band-width
------- ------------------------ -------------------- ------- ------------
---------
1     ap220e                 8832.0000.1111     true      true        128
```

```
2     ap330                        -           false     false       128
```

Related Commands	Command	Description
	N/A	N/A

Platform Description N/A

3.45 show ap-config board-data

Use this command to display the board data information of an AP.

show ap-config board-data *ap-name*

Parameter Description	Parameter	Description
	ap-name	Indicates the name of the AP to be queried.

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide N/A

Configuration Examples The following example displays the board data information of an AP.

```
ac#show ap-config board-data wlan-ap-0001
Ap(wlan-ap-0001)'s board data:
wtp model num      :
  wtp serial num     :1234567890123
  board id          :AP220E
  board reversion    :AP2
  base address      :0011.2233.4455
```

Related Commands	Command	Description
	N/A	N/A

Platform Description N/A

3.46 show ap-config inventory

Use this command to display the manufacturer information about an AP.

show ap-config inventory *ap-name*

Parameter Description	**Parameter**	**Description**
	ap-name	Indicates the name of the AP to be queried.

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide N/A

Configuration Examples

The following example displays the manufacturer information of an AP.

```
ac#show ap-config inventory wlan-ap-0001
AP Name: wlan-ap-0001
Location:
Product Id: AP220E
Vendor Id: 31762
SN: 1531991320
```

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

Platform Description N/A

3.47 show ap-config link-latency

Use this command to check the link status between AC and AP.

show ap-config link-latency {all | single *ap-name*}

Parameter Description	**Parameter**	**Description**
	all	Indicates that you check the link status information of all APs associated with the AC.
	single *ap-name*	Indicates that you check the link status information of a

	single AP.

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide N/A

Configuration Examples The following example displays the link status information of the specified AP-0001.

```
Ruijie(config)#show ap-config link-latency single AP-0001
AP Name   Status     Current    Maximum   Minimum
--------- ---------- ---------- --------- ---------
AP-0001   Enabled    4      ms 22    ms 2     ms
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

3.48 show ap-config reboot

Use this command to display the reboot information about an AP.

show ap-config reboot *ap-name*

Parameter Description

Parameter	Description
ap-name	Indicates the name of the AP to be queried.

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide N/A

Configuration Examples The following example displays the reboot information of an AP.

```
ac#show ap-config reboot wlan-ap-0001
Ap(wlan-ap-0001)'s reboot statistic:
Reboot Cnt         :0
AC Init Cnt        :0
```

```
Link Fail Cnt      :0
SW Fail Cnt        :0
HW Fail Cnt        :0
Other Fail Cnt     :0
Unknow Fail Cnt    :0
Last Fail Type     :0
```

Related Commands	Command	Description
	N/A	N/A

Platform Description N/A

3.49 show ap-config slot

Use this command to display the Mini APs in a specified Master AP.

show ap-config slot *ap-name*

Parameter Description	Parameter	Description
	ap-name	Indicates the name of the Master AP.

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide This command displays information of online Master APs only.

Configuration Examples The following example displays the Mini APs in Master AP AM5528.

```
Ruijie#show ap-config slot AM5528(EP)
Radio: Radio ID
      E = enabled, D = disabled, N = Not exist
      Current Sta number
      Channel: * = Global
      Power Level = Percent

Install Slot Number: 48
Online Slot Number: 11
Offline Slot Number: 37
Slot ID Role    Slot Name                    Model     Slot Mac      Radio
```

```
Radio            Up/Off time   State
------- ----   ------------------------------ --------- --------------
------------------ ------------------ ------------- -------
1      master   19#4F_wenmi                  MAP552    5869.6c36.e29b 1  E
3    9    50 2  E   6  165   100    0:04:18:03 online
2      master   19#4F_fangjian_1             MAP752(ST)5869.6c36.e22d 3
E   4   13    50 4  E   5  153   100    0:04:17:58 online
2      slave    19#4F_fangjian_2             MAP752(ST)5869.6c36.e32c 5
E   3    6    50 6  E   3   36   100    0:04:17:52 online
```

Related Commands	Command	Description
	N/A	N/A

Platform Description N/A

3.50 show ap-config static-ip

Use this command to display static address information on the AP.

show ap-config static-ip { **all** | **single** *ap-name* }

Parameter Description	Parameter	Description
	all	Displays all APs.
	single	Displays one single AP.
	ap-name	The AP name.

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide N/A

Configuration Examples The following example displays static address information, including the AP name. IP address, network mask and gateway.

```
Ruijie#show ap-config static-ip single 0034.5612.78a0
AP Name     Static IP   Net Mask         Getway
------------------------------------------------------------- ------------
---
0034.5612.78a0         Enabled 22.22.22.22  255.255.255.0  22.22.22.53
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

3.51 show ap-config summary location

Use this command to display location information on all APs.

show ap-config summary location

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 location information on all APs, including the AP name, MAC address, location, and status (online/offline).

```
Ruijie#show ap-config summary location
AP Name                              IP Address     Mac Address    Location
State
-------------------------------------- --------------- --------------
---------------------------------------- -----
ap220                                172.18.100.4    1414.4b13.9ff3
Bangongshi_4#                                    Run
ap3                                 172.18.100.16   001a.a94e.d40d  building
20#3F                        Run
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

3.52 show ap-config summary slot

Use this command to display the Mini APs in all Master APs.

show ap-config summary slot

Parameter Description

Parameter	Description
N/A	N/A

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide This command displays information of online Master APs only.

Configuration Examples The following example displays the Mini APs in all Master APs.

```
Ruijie#show ap-config summary slot
Radio: Radio ID
      E = enabled, D = disabled, N = Not exist
      Current Sta number
      Channel: * = Global
      Power Level = Percent

Total AP Number: 1
Total Install Slot Number: 48
Total Online Slot Number: 11
Total Offline Slot Number: 37

AP(AM5528EP)'s Slots Information
Install Slot Number: 48
Online Slot Number: 11
Offline Slot Number: 37
Slot ID Role    Slot Name                     Model     Slot Mac      Radio
Radio             Up/Off time   State
------- ----    ------------------------------- --------- --------------
------------------ ------------------- ------------- -------
1      master   19#4F_wenmi                    MAP552    5869.6c36.e29b 1  E
3   9    50 2  E   6  165   100    0:04:18:03 online
2      master   19#4F_fangjian_1               MAP752(ST)5869.6c36.e22d 3  E
4  13    50 4  E   5  153   100    0:04:17:58 online
2      slave    19#4F_fangjian_2               MAP752(ST)5869.6c36.e32c 5  E
3   6    50 6  E   3   36   100    0:04:17:52 online
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

3.53 show ap-config summary slot interface

Use this command to display all downlink ports of i-Share+ APs.

show ap-config summary slot interface

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 downlink ports of i-Share+ APs.

```
Ruijie#sh ap-config summary slot interface
AP(00d0.f822.33dc)'s information
AP mac        IP Address     Slot ID Role    Status  Duplex  Speed
------------- -------------- ------- -------- ------- ------- -------
00d0.f822.33dc 102.102.102.102 1      master   down    Unknown Unknown
00d0.f822.33dc 102.102.102.102 2      master   down    Unknown Unknown
00d0.f822.33dc 102.102.102.102 3      master   down    Unknown Unknown
00d0.f822.33dc 102.102.102.102 4      master   down    Unknown Unknown
00d0.f822.33dc 102.102.102.102 5      master   up     Full    1000M
00d0.f822.33dc 102.102.102.102 6      master   down    Unknown Unknown
00d0.f822.33dc 102.102.102.102 7      master   down    Unknown Unknown
00d0.f822.33dc 102.102.102.102 8      master   down    Unknown Unknown
00d0.f822.33dc 102.102.102.102 9      master   down    Unknown Unknown
00d0.f822.33dc 102.102.102.102 10     master   down    Unknown Unknown
00d0.f822.33dc 102.102.102.102 11     master   down    Unknown Unknown
00d0.f822.33dc 102.102.102.102 12     master   down    Unknown Unknown
00d0.f822.33dc 102.102.102.102 13     master   down    Unknown Unknown
00d0.f822.33dc 102.102.102.102 14     master   down    Unknown Unknown
00d0.f822.33dc 102.102.102.102 15     master   down    Unknown Unknown
00d0.f822.33dc 102.102.102.102 16     master   down    Unknown Unknown
```

```
00d0.f822.33dc 102.102.102.102 17     master   down    Unknown Unknown
00d0.f822.33dc 102.102.102.102 18     master   down    Unknown Unknown
00d0.f822.33dc 102.102.102.102 19     master   down    Unknown Unknown
00d0.f822.33dc 102.102.102.102 20     master   down    Unknown Unknown
00d0.f822.33dc 102.102.102.102 21     master   down    Unknown Unknown
00d0.f822.33dc 102.102.102.102 22     master   down    Unknown Unknown
00d0.f822.33dc 102.102.102.102 23     master   down    Unknown Unknown
00d0.f822.33dc 102.102.102.102 24     master   down    Unknown Unknown
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

3.54 show ap-config updating-list

Use this command to display upgrade information on the AP.

show ap-config updating-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 upgrade information on the AP.

```
Ruijie#show ap-config updating-list
AP NAME                      AP PID           File Tx  Time      AP Reset
Ready
-------------------------- --------------- -------- -------- ---------------
AP220-I                     AP220-I           100      00:00:45  Y
00d0.1414.3f67         AP220-E          98       00:00:48  N
```

Field	Description
AP NAME	AP name.
AP PID	AP ID.

File Tx	File transfer process.
Time	Upgrade duration.
AP Reset Ready	Resets after upgrade is complete.

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

3.55 show ap-config wtp-descriptor

Use this command to display the status description of an AP.

show ap-config wtp-descriptor *ap-name*

Parameter Description

Parameter	Description
ap-name	Indicates the name of the AP to be queried.

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide N/A

Configuration Examples

The following example displays the status description of an AP.

```
ac#show ap-config wtp-descriptor wlan-ap-0001
Ap(wlan-ap-0001)'s wtp descriptor:
max radio         :2
radio in used      :2

encrypt num        :2
Cnt  WBID    Encry Cap
1    0x1     0xc

sub descriptor num  :3
Cnt  vonder id version type   version len    version
1    0x7c12    BOOT Ver      28           MainVer10.SubVer4.SvnVer3634
2    0x7c12    ACT SW Ver     30           RGOS 10.4 (1t7)(1T7),
Release(73413)
```

```
3    0x7c12    HW Ver        3            1.0
```

Related Commands	Command	Description
	N/A	N/A

Platform Description N/A

3.56 show ap-config wtp-info

Use this command to display the AP device status.

show ap-config wtp-info *ap-name*

Parameter Description	Parameter	Description
	ap-name	AP device name

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide N/A

Configuration Examples The following example displays the AP device status.

```
Ruijie#show ap-config wtp-info ap220e
Ap(ap220e)'s status:
AC IP(status):     :101.101.101.101
AC IPV6(status):    :
AP IP(status):     :10.10.10.8 255.255.255.0 10.10.10.2
AP IPV6(status):    :::/0 ::
AP IPV4 ENABLE:    :enable
AP IPV6 ENABLE:    :disable
IPV6 AUTOCONFIG:    :disable
Location Data:     :
Session ID:        :88320000,111163fb,5c3b3cb3,2cac585a
mac type           :full support
WTP Name:          :ap220e
AP Domain Name:     :ac.ruijie.com.cn
wired vlan         :0 port id 1
wired vlan         :0 port id 2
wired vlan         :0 port id 3
wired vlan         :0 port id 4
Cw_interface_name   :BVI 1
```

```
Cw_wan_interface_ifx::1
Cw_wan_interface_ifx::0
Upgrading State    :Init
AP Image file      :NA
Real version       :1.0.0.641d31e6
Custom version     :AP_RGOS 11.1(2)B1
Upgrade version    :NA
Upgrade from AP    :FALSE
Upgrade for other AP:FALSE
Upgrade from AC    :FALSE
Wait for upgrade   :FALSE
Support distr-upg  :TRUE
Upgrade-banfwidth  :128
Upgrade group      :Upgrade-group1
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

3.57 show capwap detail

Use this command to display details about the CAPWAP tunnel.

show capwap [*index* | [*ip-address* [*port*]]] **detail**

Parameter Description

Parameter	Description
index	Tunnel index.
ip-address	Tunnel IP address.
port	Tunnel port number.

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide N/A

Configuration Examples The following example displays details about the CAPWAP tunnel whose address is 1.1.1.1.

```
Ruijie#show capwap 1.1.1.1 detail
CAPWAP process “capwap 1” with state Run
```

```
Process uptime is 3 days 0 hour 41 minutes
Echo interval is 30 secs, Dead interval is 81 secs
Current timers echo-interval
Peer address is 172.18.59.5
Peer control port is 10000, data port is 10001
My address is 55.55.55.60
The MAC of AP is 001a.a94e.d773
The Session ID of AP is 001a.a94e.d773.53e1.0801.53e1.0801.53e1
The Path MTU is 1500
Recent recieved request's sequence number 39
Recent recieved response's sequence number 11
Recent send request's sequence number 11
Retransmit Count 0, Discovery Count 0, Failed DTLS Session Count 0
Sending queue length 0, Receive queue length 0
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

3.58 show capwap state

Use this command to display the CAPWAP tunnel state.

show capwap state

Parameter Description

Parameter	Description
N/A	N/A

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide N/A

Configuration Examples The following example displays the CAPWAP tunnel state.

```
Ruijie#show capwap state
CAPWAP tunnel state, 3 peers, 2 is run:
```

```
Index  Peer IP              Peer Port  State        Mac Address
1    192.168.0.1           10000     Run          001a.a900.0001
2    192.168.0.2           10000     Run          001a.a900.0002
3    192.168.0.3           10000     DTLS Teardown   001a.a900.0003
```

Field	Description
Index	Tunnel index.
Peer IP	Peer IP address.
Peer Port	Peer port number.
State	Tunnel state.
Mac Address	AP MAC address, only displayed on ACs.

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

3.59 show capwap statistics

Use this command to display statistics about the CAPWAP tunnel packets.

show capwap [*index* | [*ip-address* [*port*]]] **statistics**

Parameter Description

Parameter	Description
index	Tunnel index.
ip-address	Tunnel IP address.
port	Tunnel port number.

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide N/A

Configuration Examples The following example displays packet statistics about the CAPWAP tunnel whose IP address is 1.1.1.1.

```
Ruijie#show capwap 1.1.1.1 statistics
```

Related Commands

Command	Description

N/A	N/A

Platform Description N/A

3.60 show version

Use this command to display the AP version.

show version { **all** | *ap-name* }

Parameter Description

Parameter	Description
all	All APs.
ap-name	Specifies an AP.

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide N/A

Configuration Examples The following example displays the version information on all APs.

```
Ruijie#show version all
AP(AP220E-0)'s version:
  Product ID         : AP220-E
  System uptime      : 0:3:9:32
  Hardware version    : 2.00
  Software version    : AP_RGOS 11.1(2)B1
  Patch number       : SP2
  Software number     : M05563609152014
  Serial number      : 1234942570005
  MAC address        : 00d0.f822.33b0

AP(AP220E-2)'s version:
  Product ID         : AP220-E
  System uptime      : 0:6:11:53
  Hardware version    : 2.00
  Software version    : AP_RGOS 11.1(2)B1
  Patch number       : SP2
  Software number     : M05563609152014
  Serial number      : 1234942570018
```

```
MAC address       : 001a.a9bd.0c1b
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

3.61 slot

Use this command to name a Mini AP. Use the **no** form of this command to delete the Mini AP name.

slot *slot-id* { *slot-name* [**secondary**] | **mac** *mac-address slot-name* }

no slot [{ *slot-name* [**secondary**] | **mac** *mac-address* }]

Parameter Description

Parameter	Description
slot-id	Slot number. The range is from 1 to 24.
ap-name	Mini AP name, containing up to 63 characters without spaces.
secondary	Applies to the secondary AP.
mac-address	MAC address of the Mini AP.

Defaults By default, a Mini AP is not named.

Command Mode AP configuration mode

Usage Guide

This command takes effect only for i-Share+ APs and cannot be configured for all APs.

If you want to name a secondary Mini AP, please add the **secondary** parameter.

Each slot can be configured with two MAC addresses.

Configuration Examples The following example sets the name of Mini AP1 to 1#101.

```
Ruijie(config)# ap-config AP0001
Ruijie(config-ap)# slot 1 1#101
```

The following example sets the name of AP0001, secondary Mini AP1 of slot 1, to 1#102.

```
Ruijie(config)# ap-config AP0001
Ruijie(config-ap)# slot 1 1#102 secondary
```

The following example sets the name of Mini AP (MAC address: 0001.0001.0001) of slot 1 to 1#101 and the name of Mini AP (MAC address: 0001.0001.0002) of slot 1 to 1#102.

```
Ruijie(config)# ap-config AP0001
Ruijie(config-ap)# slot 1 mac 0001.0001.0001 1#101
Ruijie(config-ap)# slot 1 mac 0001.0001.0002 1#102
```

Related Commands	Command	Description
	N/A	N/A

Platform Description N/A

3.62 timestamp

Use this command to configure a specified AP or all APs in a specified AP group to synchronize with the AC in time.

timestamp

Parameter Description	Parameter	Description
	N/A	N/A

Defaults N/A

Command Mode AP configuration mode/AP group configuration mode

Usage Guide N/A

Configuration Examples

The following example configures AP0001 to synchronize with the AC in time.

```
Ruijie(config)# ap-config AP0001
Ruijie(config-ap)# timestamp
```

The following example configures all APs in the AP group (Default) to synchronize with the AC in time.

```
Ruijie(config)# ap-group default
Ruijie(config-ap-group)# timestamp
```

Related Commands	Command	Description
	N/A	N/A

Platform Description N/A

3.63 tran-data-show

Use this command to display log information transmitted recently from a specified

AP to the AC.

tran-data-show *ap-name* { **exception | cpuinfo | memory | syslog** | **tech-support** }

Parameter Description

Parameter	Description
ap-name	Indicates the name of the specified AP.
exception	Indicates the crash log information of the specified AP.
cpuinfo	Indicates the CPU information of the specified AP.
memory	Indicates the memory information of the specified AP.
syslog	Indicates the general log information of the specified AP.
tech-support	Indicates the console information of the specified AP.

Defaults N/A

Command Mode AC configuration mode

Usage Guide N/A

Configuration Examples

The following example displays the crash log of AP0001.

```
Ruijie(config-ac)# tran-data-show AP0001 exception
```

The following example displays the CPU information of AP0001.

```
Ruijie(config-ac)# tran-data-show AP0001 cpuinfo
```

The following example displays the memory information of AP0001.

```
Ruijie(config-ac)# tran-data-show AP0001 memory
```

The following example displays the general log information of AP0001.

```
Ruijie(config-ac)# tran-data-show AP0001 syslog
```

The following example displays the console information of AP0001.

```
Ruijie(config-ac)# tran-data-show AP0001 tech-support
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

3.64 tran-data-start

Use this command to obtain log information about a specified AP.

tran-data-start *ap-name* { **exception** | **memory** | **tech-support** | **tech-package** }

Parameter Description

Parameter	Description
ap-name	Indicates the name of the specified AP.
exception	Indicates the crash log information sent by the specified AP.
memory	Indicates the device status information sent by the specified AP, including CPU information, memory information, and general log information (including port UP/DOWN information).
tech-support	Indicates the console information.
tech-package	Indicates the package information.

Defaults N/A

Command Mode AC configuration mode

Usage Guide N/A

Configuration Examples

The following example obtains the crash log information from AP0001, and saves it as ap_AP0001_exception.log in the AC file system.

```
Ruijie(config-ac)# tran-data-start AP0001 exception
```

The following example obtains the general log information from AP0001, and saves it as ap_AP0001_syslog.log, ap_AP0001_memory.log, and ap_AP0001_cpuinfo.log in the AC file system.

```
Ruijie(config-ac)# tran-data-start AP0001 memory
```

The following example obtains the console information from AP0001, and saves it as ap_AP0001_8832.0000.1111_tech-console.log in the AC file system.

```
Ruijie(config-ac)# tran-data-start AP0001 tech-support
```

The following example obtains the package information from AP0001, and saves it as ap_AP0001_8832.0000.1111_tech-package.tar.gz in the AC file system.

```
Ruijie(config-ac)# tran-data-start AP0001 tech-package
```

Related Commands

Command	Description
N/A	N/A

Platform N/A

Description

3.65 uninstall

Use this command to remove the Mini AP installation information.

uninstall *slot-id*

Parameter Description	**Parameter**	**Description**
	slot-id	Slot number, The range is from 1 to 24.

Defaults N/A

Command Mode AP configuration mode

Usage Guide

Once a Mini AP is installed to a Master AP, the Mini AP is considered as **Offline** if it is manually removed. You can use this command to remove the installation information of the Mini AP.

This command takes no effect on an online Mini AP.

This configuration is not saved and can remove the installation information for only one Mini AP per execution.

Configuration Examples

The following example removes the Mini AP installation information of slot 1 on Master AP1.

```
Ruijie(config)# ap-config AP1
Ruijie(config-ap)# uninstall 1
```

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

Platform Description N/A

4 WBS Commands

4.1 11asuport enable

Use the command to enable the specified radio to support 802.11a on 5 GHz. Use the **no** form of this command to disable the radio to support 802.11a on 5 GHz.

11asupport enable radio *radio-id*

no 11asupport enable radio *radio-id*

Parameter Description

Parameter	Description
radio-id	Radio ID. The range is from 1 to 96.

Defaults By default, 802.11a is supported.

Command mode AP configuration mode

Usage Guide N/A

Configuration Examples The following example enables radio1 to support 802.11a on 5 GHz.

```
Ruijie(config)# ap-config AP0001
Ruijie(config-ap)# 11asupport enable radio 1
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

4.2 11bsupport enable

Use the command to enable the specified radio to support 802.11b on 2.4 GHz. Use the **no** form of this command to disable the radio to support 802.11b on 2.4 GHz.

11bsupport enable radio *radio-id*

no 11bsupport enable radio *radio-id*

Parameter Description

Parameter	Description

radio-id	Radio ID. The range is from 1 to 96.

Defaults By default, 802.11b is supported.

Command mode AP configuration mode

Usage Guide N/A

Configuration Examples The following example enables radio1 to support 802.11b on 2.4 GHz.

```
Ruijie(config)# ap-config AP0001
Ruijie(config-ap)# 11bsupport enable radio 1
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

4.3 11gsupport enable

Use this command to enable the specified radio to support 802.11g on 2.4 GHz. Use the **no** form of this command to disable the radio to support 802.11g on 2.4 GHz.

11gsupport enable radio *radio-id*

no 11gsupport enable radio *radio-id*

Parameter Description

Parameter	Description
radio-id	Radio ID. The range is from 1 to 96.

Defaults By default, 802.11g is supported.

Command mode AP configuration mode

Usage Guide N/A

Configuration Examples The following example enables radio1 to support 802.11g on 2.4 GHz.

```
Ruijie(config)# ap-config AP0001
Ruijie(config-ap)# 11gsupport enable radio 1
```

Related Commands

Command	Description

N/A	N/A

Platform Description N/A

4.4 11nasupport enable

Use this command to enable the specified radio to support 802.11n on 5 GHz. Use the **no** form of this command to disable the radio to support 802.11n on 5 GHz.

11nasupport enable radio *radio-id*

no 11nasupport enable radio *radio-id*

Parameter Description

Parameter	Description
radio-id	Radio ID. The range is from 1 to 96.

Defaults By default, 802.11n is supported.

Command mode AP configuration mode

Usage Guide N/A

Configuration Examples The following example enables radio1 to support 802.11n on 5 GHz.

```
Ruijie(config)# ap-config AP0001
Ruijie(config-ap)# 11nasupport enable radio 1
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

4.5 11ngsupport enable

Use this command to enable the specified radio to support 802.11n on 2.4 GHz. Use the **no** form of this command to disable the radio to support 802.11n on 2.4 GHz.

11ngsupport enable radio *radio-id*

no 11ngsupport enable radio *radio-id*

Parameter Description

Parameter	Description

radio-id	Radio ID. The range is from 1 to 96.

Defaults By default, 802.11n is supported.

Command mode AP configuration mode

Usage Guide N/A

Configuration Examples The following example enables radio1 to support 802.11n on 2.4 GHz.

```
Ruijie(config)# ap-config AP0001
Ruijie(config-ap)# 11ngsupport enable radio 1
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

4.6 11acsupport enable

Use this command to enable the specified radio to support 802.11ac. Use the **no** form of this command to disable the radio to support 802.11ac.

11acsupport enable radio *radio-id*

no 11acsupport enable radio *radio-id*

Parameter Description

Parameter	Description
radio-id	Radio ID. The range is from 1 to 96.

Defaults By default, 802.11ac is supported when the radio ID is even.

Command mode AP configuration mode

Usage Guide N/A

Configuration Examples The following example enables radio1 to support 802.11ac.

```
Ruijie(config)# ap-config AP0001
Ruijie(config-ap)# 11acsupport enable radio 1
```

Related Commands

Command	Description

N/A	N/A

Platform Description N/A

4.7 11axsupport enable

Use this command to enable the specified radio to support 802.11ax. Use the **no** form of this command to disable the radio with 802.11ax.

11axsupport enable radio *radio-id*

no 11axsupport enable radio *radio-id*

Parameter Description

Parameter	Description
radio-id	Radio ID. The range is from 1 to 96.

Defaults By default, 802.11ax is supported.

Command mode AP configuration mode, all-AP configuration mode

Usage Guide N/A

Configuration Examples The following example enters AP0001 and disables radio 2 with 802.11ac.

```
Ruijie# configure terminal
Ruijie(config)# ap-config AP0001
Ruijie(config-ap)# no 11axsupport enable radio 2
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

4.8 802.11a network rate

Use this command to configure a RF rate list for the 802.11anetwork.

802.11a network rate { **6** | **9** | **12** | **18** | **24** | **36** | **48** | **54** } { **disabled** | **mandatory** | **supported** }

Parameter Description

Parameter	Description
6	Indicates 6Mbps rate.
9	Indicates 9Mbps rate.

12	Indicates 12Mbps rate.
18	Indicates 18Mbps rate.
24	Indicates 24Mbps rate.
36	Indicates 36Mbps rate.
48	Indicates 48Mbps rate.
54	Indicates 54Mbps rate.
disabled	Not supported
mandatory	Supported
supported	Optional

Defaults By default, the default value varies with the modes of the AP. For the 802.11a networks, the rates of 6, 12 and 24 are mandatory, and all others are supported.

Command Mode AC configuration mode/AP configuration mode/AP group configuration mode

Usage Guide None

Configuration Examples

The following example disables 6Mbps for 802.11a users.

```
Ruijie(config)# ac-controller
Ruijie(config-ac)# 802.11a network rate 6 disabled
```

The following example disables 6Mbps for 802.11a users on AP001.

```
Ruijie(config)# ap-config AP001
Ruijie(config-ap)# 802.11a network rate 6 disabled
```

The following example disables 6Mbps for 802.11a users on default group.

```
Ruijie(config)# ap-group default
Ruijie(config-group)# 802.11a network rate 6 disabled
```

Related Commands

Command	Description
-	-

Platform Description N/A

4.9 802.11b network rate

Use this command to configure a RF rate list for the 802.11b network.

802.11b network rate { **1** | **2** | **5** | **11** } { **disabled** | **mandatory** | **supported** }

Parameter Description

Parameter	Description
1	Indicates 1Mbps rate.

2	Indicates 2Mbps rate.
5	Indicates 5Mbps rate.
11	Indicates 11Mbps rate.
disabled	Not supported
mandatory	Supported
supported	Optional

Defaults By default, 1Mbps, 2Mbps, 5.5Mbps, 11Mbps are mandatory.

Command Mode AC configuration mode/AP configuration mode/AP group configuraiton mode

Usage Guide None

Configuration Examples

The following example disables 1Mbps for 802.11b users.

```
Ruijie(config)# ac-controller
Ruijie(config-ac)# 802.11b network rate 1 disabled
```

The following example disables 1Mbps for 802.11b users on AP0001.

```
Ruijie(config)# ap-config AP001
Ruijie(config-ap)# 802.11b network rate 1 disabled
```

The following example disables 1Mbps for 802.11b users on default group.

```
Ruijie(config)# ap-group default
Ruijie(config-group)# 802.11b network rate 1 disabled
```

4.10 802.11g network rate

Use this command to configure a RF rate list for the 802.11g network.

802.11g network rate { **1** | **2** | **5 | 6** | **9** | **11** | **12** | **18** | **24** | **36** | **48** | **54** } { **disabled** | **mandatory** | **supported** }

Parameter Description

Parameter	Description
1	Indicates 1Mbps rate.
2	Indicates 2Mbps rate.
5	Indicates 5Mbps rate.
6	Indicates 6Mbps rate.
9	Indicates 9Mbps rate.
11	Indicates 11Mbps rate.
12	Indicates 12Mbps rate.
18	Indicates 18Mbps rate.

24	Indicates 24Mbps rate.
36	Indicates 36Mbps rate.
48	Indicates 48Mbps rate.
54	Indicates 54Mbps rate.
disabled	Not supported
mandatory	Supported
supported	Optional

Defaults By default, 1Mbps, 2Mbps, 5.5Mbps, 11Mbps are mandatory. The others are optional.

Command Mode AC configuration mode/AP configuration mode/AP group configuration mode

Usage Guide None

Configuration Examples

The following example disables 1Mbps for 802.11g users..

```
Ruijie(config)# ac-controller
Ruijie(config-ac)# 802.11g network rate 1 disabled
```

The following example disables 1Mbps for 802.11g users on AP0001.

```
Ruijie(config)# ap-config AP001
Ruijie(config-ap)# 802.11b network rate 1 disabled
```

The following example disables 1Mbps for 802.11g users on default group.

```
Ruijie(config)# ap-group default
Ruijie(config-group)# 802.11b network rate 1 disabled
```

4.11 {802.11a | 802.11b} network [disable | enable]

Use this command to configure whether to enable or disable the 2.4GHz or 5GHZ network. When the 2.4GHz or 5GHZ network is disabled, all the wireless users connected with this wireless network will go offline.

{ **802.11a | 802.11b** } **network** [**disable** | **enable**]

Parameter Description

Parameter	Description

Defaults The default is **enable**.

Command Mode ac configuration mode.

Usage Guide None

Configuration Examples Example 1: Configure the 802.11a network disable

```
Ruijie(config-ac)# 802.11a network disable
```

Related Commands

Command	Description
-	-

Platform Description N/A

4.12 80.211n a-mpdu enable

Use this command to enable the specified radio to support AMPDU. Use the **no** form of this command to disable the radio to support AMPDU.

802.11n a-mpdu enable radio *radio-id*

no 802.11n a-mpdu enable radio *radio-id*

Parameter Description

Parameter	Description
radio-id	Radio ID. The range is from 1 to 96.

Defaults AMPDU is enabled by default.

Command mode AP configuration mode

Usage Guide This command takes effect only when the radio operates in 802.11n or 802.11ac,

Configuration Examples The following example enables radio1 to support AMPDU.

```
Ruijie(config)# ap-config AP0001
Ruijie(config-ap)# 802.11n a-mpdu enable radio 1
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

4.13 80.211n mcs support

Use this command to configure the modulation and coding scheme (MCS) index of 802.11n. Use the **no** form of this command to restore the default MCS of 802.11n.

802.11n mcs support *num* **radio** *radio-id*

no 802.11n mcs support radio *radio-id*

Parameter Description

Parameter	Description
num	MCS index. The range is from 0 to 31.
radio-id	Radio ID. The range is from 1 to 96.

Defaults The default MCS index of 802.11n is 31.

Command mode AP configuration mode

Usage Guide N/A

Configuration Examples The following example configures the MCS index to 15 of 802.11n for radio1.

```
Ruijie(config)# ap-config AP0001
Ruijie(config-ap)# 802.11n mcs support 15 radio 1
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

4.14 80.211ac mcs support

Use this command to configure the modulation and coding scheme (MCS) index of 802.11ac. Use the **no** form of this command to restore the default MCS of 802.11ac.

802.11ac mcs support *num* **radio** *radio-id*

no 802.11ac mcs support radio *radio-id*

Parameter Description

Parameter	Description
num	MCS index. The range is from 0 to 39.
radio-id	Radio ID. The range is from 1 to 96.

Defaults The default MCS index of 802.11ac is 39.

Command mode AP configuration mode

Usage Guide N/A

Configuration Examples The following example configures the MCS index to 19 of 802.11ac for radio1.

```
Ruijie(config)# ap-config AP0001
Ruijie(config-ap)# 802.11ac mcs support 19 radio 1
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

4.15 802.11ax mcs support

Use this command to configure the maximum 802.11ax MCS index value. Use the **no** form of this command to restore the default settings.

802.11ax mcs support *num* **radio** *radio-id*

no 802.11ax mcs support radio *radio-id*

Parameter Description

Parameter	Description
num	MCS index. The range is from 0 to 95.
radio-id	Radio ID. The range is from 1 to 96.

Defaults By default, the maximum 802.11 ax MCS index value is 95.

Command mode AP configuration mode, all-AP configuration mode

Usage Guide

1. The configuration takes effect only when the AP radios operate in 802.11ax mode.
2. Number of spatial streams = Maximum MCS index value/12 +1.

For example, if the maximum MCS index value is 31, the maximum number of spatial streams is 3.

Configuration Examples The following example sets the maximum 802.11ax MCS index value to 9 for radio 2.

```
Ruijie# configure terminal
Ruijie(config)# ap-config AP0001
Ruijie(config-ap)# 802.11ax mcs support 9 radio 2
```

Related Commands	Command	Description
	N/A	N/A

Platform Description N/A

4.16 ampdu-retries

In a wireless network, AMPDU software retransmission is adopted to reduce the sub-frame loss. The more retransmission attempts, the less the package loss. However excessive retransmission attempts increase the workload of air interfaces, which reduce the immediacy of other packages. So, it is recommended to configure more retransmission attempts when sub-frame loss frequently occurs.

ampdu-retries *times* **radio** *radio_id*

Parameter Description	Parameter	Description
	times	Retransmission times. The range is from 1 to 10.
	radio-id	Radio ID. The range is from 1 to 96.

Defaults By default, the retransmission times is 10.

Command Mode AP configuration mode

Usage Guide N/A

Configuration Examples The following example enters the configuration mode of AP0001 and sets the AMPDU software retransmission times to 2.

```
Ruijie(config)#ap-config AP0001
Ruiejie(config-ap)#ampdu-retries 2 radio 1
```

Related Commands	Command	Description
	N/A	N/A

Platform Description N/A

4.17 ampdu-rts

Use this command to enable the Request to Send (RTS) protection mode for the AMPDU packets.

Use the **no** form of this command to disable the RTS mode.

ampdu-rts radio { *radio-id* | *802.11b* | *802.11a* }

no ampdu-rts radio { *radio-id* | *802.11b* | *802.11a* }

Parameter Description

Parameter	Description
radio-id	Radio ID. The range is from 1 to 96.
802.11b	Configures radios on all 2.4 GHz frequency band.
802.11a	Configures radios on all 5.8 GHz frequency band.

Defaults This function is disabled by default.

Command Mode AP configuration mode

Usage Guide N/A

Configuration Examples The following example enters the configuration mode of AP0001 and enables the AMPDU RTS protection on the radio 1.

```
Ruijie(config)# ap- config AP0001
Ruieji(config-ap)# ampdu-rts radio 1
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

4.18 antenna receive

Use this command to configure the receiving antenna type of the specified radio for the specified AP or all APs of the specified AP group.

antenna receive *value* **radio** *radio-id*

Parameter Description

Parameter	Description
value	Antenna mask. The range is from 1 to 15.
radio-id	Radio ID. The range is from 1 to 96.

Defaults For AP configuration mode, the default receiving antenna type depends on device model.
For AP group configuration mode, there is no default setting.

Command Mode AP configuration mode/AP group configuration mode

Usage Guide This command takes effect only on the AP device operating in 802.11n.

Configuration Examples The following example configures the receiving antenna type to 5 for AP001.

```
Ruijie(config)# ap-config AP0001
Ruijie(config-ap)# antenna receive 5 radio 1
```

The following example configures the receiving antenna type to 5 for AP group.

```
Ruijie(config)# ap-group default
Ruijie(config-group)# antenna receive 5 radio 1
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

4.19 antenna transmit

Use this command to configure the transmitting antenna type of the specified radio or all APs of the specified AP group..

antenna transmit *value* **radio** *radio-id*

Parameter Description

Parameter	Description
value	Antenna mask. The range is from 1 to 15.
radio-id	Radio ID. The range is from 1 to 96.

Defaults For AP configuration mode, the default receiving antenna type depends on device model.
For AP group configuration mode, there is no default setting.

Command Mode AP configuration mode/AP group configuration mode

Usage Guide This command takes effect only on the AP device operating in 802.11n.

Configuration Examples The following example configures the transmitting antenna type to 7 on AP001.

```
Ruijie(config)# ap-config AP0001
Ruijie(config-ap)# antenna transmit 7 radio 1
```

The following example configures the transmitting antenna type to 7 on the AP group (default).

```
Ruijie(config)# ap-group default
Ruijie(config-group)# antenna transmit 7 radio 1
```

Related Commands	Command	Description
	N/A	N/A

Platform Description N/A

4.20 apsd

Use this command to enable the unscheduled-automatic power save delivery (U-APSD) mode for the specified radio of an AP device.

apsd { **enable** | **disable** } **radio** *radio-id*

Parameter Description	Parameter	Description
	enable	Enables the U-APSD mode.
	disable	Disables the U-APSD mode.
	radio-id	Radio ID. The range is from 1 to 96.

Defaults U-APSD mode is enabled by default.

Command mode AP configuration mode

Usage Guide N/A

Configuration Examples The following example enables the U-APSD mode for radio1.

```
Ruijie(config)# ap-config AP0001
Ruijie(config-ap)#apsd enable radio 1
```

Related Commands	Command	Description
	N/A	N/A

Platform Description N/A

4.21 autowifi

Use this command to enable one-click WLAN configuration on an unconfigured device. Use the **no** form of this command to remove the one-click WLAN configuration.

autowifi

no autowifi

Parameter Description	Parameter	Description
	N/A	N/A

Defaults N/A

Command Mode AC global configuration mode

Usage Guide One-click WLAN configuration function is provided for fast configuration on an unconfigured device,

⚠ In general, this function aims at helping the scenario investigator to improve efficiency and helping the channel distributors to test WLAN performance in a more convenient way.

Configuration Examples The following example configures one-click WLAN configuration.

```
Ruijie(config)# autowifi
```

Related Commands	Command	Description
	N/A	N/A

Platform Description N/A

4.22 assoc-rssi

Use this command to configure the minimum RSSI for the STA to associate with the specified AP.

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

response-rssi *rssi* **radio** *radio-id*

no response-rssi radio *radio-id*

Parameter Description	Parameter	Description
	rssi	Specifies the RSSI. The range is from 0 to 100. The unit is dBm.
	radio-id	Radio ID. The range is from 1 to 96.

Defaults The default RSSI is 0, namely, the STA any RSSI can associate with the AP.

Command mode AP configuration mode

Usage Guide This command is used to clear sticky STAs in roaming scenario, It is recommended to set RSSI to a

value in the range from 15 to 30.

Configuration Examples The following example enters AP0001 configuration mode and sets the minimum RSSI for the STA to associate with AP0001 to 15.

```
Ruijie(config)# ap-config AP0001
Ruijie(config-ap)# assoc-rssi 15 radio 1
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

4.23 beacon dtim-period

Use this command to configure the period of delivery transmission indication messages (DTIM) for the specified radio.

beacon dtim-period *period-num* **radio** *radio-id*

Parameter Description

Parameter	Description
period-num	DTIM period, which indicating the beacon periods. The range is from 1 to 255.
radio-id	Radio ID. The range is from 1 to 96.

Defaults The default DTIM period is 1 (namely, 1 beacon period).

Command Mode AP configuration mode.

Usage Guide N/A

Configuration Examples The following example configures the DTIM period of radio 1 of AP0001 to 30 beacon periods.

```
Ruijie(config)# ap-config AP0001
Ruijie(config-ap)# beacon dtim-period 30 radio 1
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

4.24 beacon period

Use this command to configure the beacon period forthe specified radio of the specified AP.

beacon period *milliseconds* **radio** *radio-id*

Parameter Description

Parameter	Description
milliseconds	Beacon period. The range is from 20 to 1,000. The unit is millisecond.
radio-id	Radio ID. The range is from 1 to 96.

Defaults The default is beacon period is 100 milliseconds.

Command Mode AP configuration mode.

Usage Guide N/A

Configuration Examples The following example configures the beacon period of radio 1 of AP0001 to 200 milliseconds.

```
Ruijie(config)# ap-config AP0001
Ruijie(config-ap)# beacon period 200 radio 1
```

Related Commands

Command	Description
-	-

Platform Description N/A

4.25 beacon rate

Use this command to configure the beacon rate for the specified radio. Use the **no** form of this command to restore the default beacon rate.

beacon rate *rate-Mbps* **radio** {*radio-id* | *802.11b* | *802.11a*}

no beacon rate radio {*radio-id* | *802.11b* | *802.11a*}

Parameter Description

Parameter	Description
rate-Mbps	Specifies the beacon rate. 1, The rate blocked in the rate set cannot be set as a beacon rate. 2. The rates of 1Mbps, 2Mbps, 5.5Mbps and 11 Mbps are not supported by the radios on 5 GHz.
radio-id	Radio ID. The range is from 1 to 96.
802.11b	Configures radios on all 2.4 GHz frequency band.
802.11a	Configures radios on all 5.8 GHz frequency band.

Defaults No beacon rate is configured by default.

Command mode AP configuration mode

Usage Guide N/A

Configuration Examples The following example configures the beacon rate of radio1 to 12Mbps.

```
Ruijie(config)# ap-config AP0001
Ruijie(config-ap)# beacon rate 12.0 radio 1
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

4.26 chan-width

Use this command to set the bandwidth of the specified radio.

chan-width { **20** | **40** | **80** | **160** } **radio** { *radio-id* | *802.11b* | *802.11a* }

Parameter Description

Parameter	Description
20	Sets the radio width to 20 Mbps.
40	Sets the radio width to 40 Mbps.
80	Sets the radio width to 80 Mbps.
160	Sets the radio width to 160 Mbps.
radio-id	Sets radio ID. The range is from 1 to 96.
802.11b	Configures radios on all 2.4 GHz frequency band.
802.11a	Configures radios on all 5.8 GHz frequency band.

Defaults The default channel bandwidth of 5.8G radio on 802.11ax new products is 40 Mbps.
The default channel bandwidth of the other radio is 20 Mbps.

Command mode AP configuration mode

Usage Guide The radio bandwidth configuration takes effect only for the AP device operating at 802.11n mode.

Configuration Examples The following example sets the radio width of radio1 to 40 Mbps.

```
Ruijie(config)# ap-config AP0001
Ruijie(config-ap)# chan-width 40 radio 1
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

4.27 channel

Use this command to configure a channel for the specified radio of the specified AP.

channel { **global** | *channel-id* } **radio** { *radio-id* | **802.11b | 802.11a** }

Parameter Description

Parameter	Description
chan-id	Specifies the channel ID.
global	Indicates that the channel is specified through the radio resource management (RRM) function.
radio-id	Sets radio ID. The range is from 1 to 96.
802.11b	Configures radios on all 2.4 GHz frequency band.
802.11a	Configures radios on all 5.8 GHz frequency band.

Defaults By default, the **global** parameter is used.

Command Mode AP configuration mode.

Usage Guide N/A

Configuration Examples The following example specifies channel 6 for radio 1.

```
Ruijie(config)# ap-config AP0001
Ruijie(config-ap)# channel 6 radio 1
```

Related Commands

Command	Description
-	-

Platform Description N/A

4.28 channel-switch

Use this command to specify two radio for channel switch.

channel-switch *radio-id1 radio-id2*

Parameter Description

Parameter	Description
radio-id1	Specifies the first radio ID, in the range from 1 to 96.
radio-id2	Specifies the first radio ID, in the range from 1 to 96.

Defaults N/A

Command Mode AP configuration mode.

Usage Guide N/A

Configuration Examples The following example enters AP0001 configuration mode and specifies radio 1 and radio 3 for channel switch.

```
Ruijie(config)# ap-config AP0001
Ruijie(config-ap)# channel-switch 1 3
```

Related Commands

Command	Description
-	-

Platform Description N/A

4.29 country

Use this command to specify a country code for an AC device. Use the **no** form of this command to remove the country code settings for an AC device.

country *country-code*

no country *country-code*

Use this command to specify a country code for the specified radio of an AP device.

country *country-code* **radio** *radio-id* | [**802.11b** | **802.11a**] }

Parameter Description

Parameter	Description
country-code	Country code.
radio-id	Sets radio ID. The range is from 1 to 48.
802.11b	Configures radios on all 2.4 GHz frequency band.

802.11a	Configures radios on all 5.8 GHz frequency band.

Defaults

By default, the country code supported by an AC device is **CN**, and the country code used by an AP device is **CN**.

Command Mode

AC/AP configuration mode.

Usage Guide

1. The country code "CN" supported by an AC cannot be deleted.
2. This command cannot be configured for all APs at the same time.
3. Before configuring a country code for an AP, add the country code to the country code set supported by the AC. If the country code used by an AP changes, the radio band, channel, and power of the AP change accordingly.
4. If **802.11b** is specified, the country code is configured for all 2.4 GHz radios; the configuration takes effect when the AP goes online for the first time, and it takes effect on the specified radios only. When **802.11a** is specified, the country code is configured for all 5.8 GHz radios; the configuration takes effect when the AP goes online for the first time and it takes effect on the specified radios only.
5. 2.4 GHz radios do not support channel 14.

Configuration Examples

The following example configures a country code supported by an AC device to US.

```
Ruijie(config)# ac-controller
Ruijie(config- ac)# country US
Ruijie(config- ac)# exit
```

The following example configures a country code for radio 1 of AP0001 to US.

```
Ruijie(config)# ap-config AP0001
Ruijie(config-ap)# country US radio 1
```

Related Commands

Command	Description
-	-

Platform Description

N/A

4.30 country-code

Use this command to specify a country code for an AC device. Use the **no** form of this command to remove the country code settings for an AC device.

country-code *country-code*

no country *country-code*

Parameter Description

Parameter	Description
country-code	Sets the country code.

Defaults By default, the country code supported by an AC device is **CN**, and the country code used by an AP device is **CN**.

Command mode Global configuration mode

Usage Guide The country codes that are currently supported include:

AE	United Arab Emirates
AM	Armenia
AR	Argentina
AT	Austria
AU	Australia
AZ	Azerbaijan
BE	Belgium
BG	Bulgaria
BH	Bahrain
BN	Brunei Darussalam
BO	Bolvia
BR	Brazil
BY	Belarus
BZ	Belize
CA	Canada
CH	Switzerland
CL	Chile
CN	China
CO	Colombia
CR	Costa Rica
CY	Cyprus
CZ	Czech Republic
DE	Germany
DK	Denmark
DO	Dominican Republic
EC	Ecuador
EE	Estonia
EG	Egypt
ES	Spain
FI	Finland
FR	France
GB	United Kingdom

GE	Georgia
GR	Greece
GT	Guatemala
HK	Hong Kong
HN	Honduras
HR	Croatia
HU	Hungary
ID	Indonesia
IE	Ireland
IL	Israel
IN	India
IQ	Iraq
IR	Iran
IS	Iceland
IT	Italy
JO	Jordan
JP	Japan
KP	North Korea
KR	Korea ROC
KW	Kuwait
KZ	Kazakhstan
LB	Lebanon
LI	Liechtenstein
LK	Sri Lanka
LT	Lithuania
LU	Luxembourg
LV	Latvia
MA	Morocco
MC	Monaco
MK	Macedonia
MO	Macau
MT	Malta
MX	Mexico
MY	Malaysia
NG	Nigeria
NL	Netherlands
NO	Norway
NZ	New Zealand
OM	Oman
PA	Panama
PE	Peru
PH	Philippines
PK	Pakistan

PL	Poland
PR	Puerto Rico
PT	Portugal
QA	Qatar
RO	Romania
RU	Russia
SA	Saudi Arabia
SE	Sweden
SG	Singapore
SI	Slovenia
SK	Slovak Republic
SV	El Salvador
SY	Syria
TH	Thailand
TN	Tunisia
TR	Turkey
TT	Trinidad & Tobago
TW	Taiwan
UA	Ukraine
US	United States
UY	Uruguay
UZ	Uzbekistan
VE	Venezuela
VN	Vietnam
YE	Yemen
ZA	South Africa
ZW	Zimbabwe

Radio, channel and transmit power vary with the country code.

Channel 14 is not supported for 2.4G.

Configuration Examples

The following example configures a country code supported by an AC device to US.

```
Ruijie(config)# country-code US
Ruijie(config)# exit
```

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

4.31 coverage-area-control

Use this command to set the coverage area control power. Use the **no** form of this command to restore the default coverage area control power.

coverage-area-control *power* [**radio** { *radio-id* | **802.11b | 802.11a** }]

no coverage-area-control [**radio** { *radio-id* | **802.11b | 802.11a** }]

Parameter Description

Parameter	Description
power	Specifies the coverage area control power. The unit is dBm. The range is from 0 to 32.
radio-id	Sets radio ID. The range is from 1 to 96.
802.11b	Configures radios on all 2.4 GHz frequency band.
802.11a	Configures radios on all 5.8 GHz frequency band.

Defaults The default value is 0.

Command mode AP configuration mode/AP group configuration mode

Usage Guide N/A

Configuration Examples The following example enters AP0001 configuration mode and sets the coverage area control power to 20.

```
Ruijie(config)# ap-config AP0001
Ruijie(config-ap)# coverage-area-control 20
```

The following example enters AP group configuration mode and sets the coverage area control power to 20.

```
Ruijie(config)# ap-group default
Ruijie(config-group)# coverage-area-control 20
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

4.32 ebag

Use this command to enable ebag network optimization. Use the **no** form of this command to disable ebag network optimization.

ebag

no ebag

Parameter Description

Parameter	Description
N/A	N/A

Defaults N/A

Command mode AP configuration mode

Usage Guide This command is generally used in e-bag scenario. Use this function with caution in other scenarios.

Configuration Examples The following example enables ebag network optimization.

```
Ruijie(config)# ap-config AP0001
Ruijie(config-ap)# ebag
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

4.33 enable-radio

Use this command to enable a/all radio for an AP device. Use the **no** form of this command to disable a/all radios.

enable-radio { *radio-id* | **all** }

no enable-radio { *radio-id* | **all** }

Parameter Description

Parameter	Description
radio-id	Radio ID. The range is from 1 to 96.
all	Enables all radios.

Defaults By default, all radios of the AP device are enabled.

Command Mode AP configuration mode.

Usage Guide

Note:

This operation may result in offline of all the wireless users connected to the specified radio.

Configuration Examples

The following example enters the configuration mode of AP0001 and disables radio 1.

```
Ruijie(config)# ap- config AP0001
Ruieji(config-ap)# no enable-radio 1
```

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

4.34 eth-schd

Use this command to configure maximum number of Ethernet packets received on the AP device for one time. Use the **no** form of this command to restore the default number of packets received for one time.

eth-schd *limit*

no eth-schd

Parameter Description

Parameter	Description
limit	The maximum number of Ethernet packets received for one time. The range is from 1 to 256.

Defaults

The default limit value varies by AP model.

Command Mode

AP configuration mode

Usage Guide

You can improve the network performance by raising the received Ethernet packets limit for every time on an AP, at the cost of reducing immediacy of packets of key services. With regard to applications which are multi-user concurrent and real-time sensitive, such as electronic schoolbag, requiring only ordinary networks, you are recommended to decrease the value of received Ethernet packets limit per time to 25.

Configuration Examples

The following example enters the configuration mode of AP0001 and sets the maximum number of the Ethernet packets received per time to 50.

```
Ruijie(config)# ap- config AP0001
Ruieji(config-ap)# eth-schd 50
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

4.35 external-antenna enable

Use this command to enable the external antenna and disable the built-in antenna on the AP device.

external-antenna enable radio *radio-id*

no external-antenna enable radio *radio-id*

Parameter Description

Parameter	Description
radio-id	Specifies the radio ID in the range from 1 to 96.

Defaults By default, the built-in antenna is enabled, and the external antenna is disabled.

Command mode AP configuration mode

Usage Guide N/A

Configuration Examples The following example enables the external antenna and disables the built-in antenna on AP001.

```
Ruijie(config)# ap-config AP0001
Ruijie(config-ap)# external-antenna enable radio 1
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

4.36 extra-coverage

Use this command to enable client access to the third radio. Use the **no** or **default** form of this command to restore the default settings.

extra-coverage enable

no extra-coverage enable

default extra-coverage enable

Parameter

Parameter	Description

Description

N/A	N/A

Defaults This function is disabled by default.

Command mode AP configuration mode/AP group configuration mode

Usage Guide N/A

Configuration Examples The following example enters AP0001 configuration mode and enables client access to the third radio.

```
Ruijie(config)# ap-config AP0001
Ruijie(config-ap)# extra-coverage enable
```

The following example enters AP0001 configuration mode and disables client access to the third radio.

```
Ruijie(config)# ap-config AP0001
Ruijie(config-ap)# no extra-coverage enable
```

The following example enters AP0001 configuration mode and restores the default settings.

```
Ruijie(config)# ap-config AP0001
Ruijie(config-ap)# default extra-coverage enable
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

4.37 fragment-threshold

Use this command to set a fragment threshold for a radio. Use the **no** form of this command to restore the default fragment threshold.

fragment-threshold *value* **radio** *radio-id*

no fragment-threshold radio *radio-id*

Parameter Description

Parameter	Description
value	Specifies the fragment threshold. The value is an even number ranging from 256 to 2.346.
radio-id	Radio ID. The range is from 1 to 96.

Defaults The default fragment threshold is 2,346.

Command mode AP configuration mode

Usage Guide N/A

Configuration Examples The following example sets the fragment threshold of radio1 to 1,538.

```
Ruijie(config)# ap-config AP0001
Ruijie(config-ap)# fragment-threshold 1538  radio 1
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

4.38 green-field enable

Use this command to enable the green-field protection mode for the specified radio. Use the **no** form of this command to disable the green-field protection mode.

green-field enable radio *radio-id*

no green-field enable radio *radio-id*

Parameter Description

Parameter	Description
radio-id	Radio ID. The range is from 1 to 96.

Defaults By default, the green-field protection mode is disabled.

Command mode AP configuration mode

Usage Guide This command is supported only for the radio on 2.4 GHz.

Configuration Examples The following example enables the green-field protection mode for radio1.

```
Ruijie(config)# ap-config AP0001
```

```
Ruijie(config-ap)# green-field enable radio 1
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

4.39 ldpc

Use this command to enable low density parity check (LDPC) coding for the specified radio. Use the **no** form of this command to disable LDPC coding.

ldpc radio *radio-id*

no ldpc radio *radio-id*

Parameter Description

Parameter	Description
radio-id	Radio ID. The range is from 1 to 96.

Defaults By default, LDPC coding is enabled.

Command Mode AP configuration mode

Usage Guide N/A

Configuration Examples The following example enters the configuration mode of AP0001 and enables LDPC coding on radio 1.

```
Ruijie(config)# ap-config AP0001
Ruieji(config-ap)# ldpc radio 1
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

4.40 link-check

Use this command to enable/disable link check.. Use the **no** form of this command to restore the

default setting.

link-check { **enable** | **disable** }

no link-check { **enable** | **disable** }

Parameter Description

Parameter	Description
enable	Enables link check.
disable	Disables link check.

Defaults Link check is disabled by default.

Command mode Global configuration mode

Usage Guide N/A

Configuration Examples The following example enables link check.

```
Ruijie(config)# link-check enable
```

The following example disables link check.

```
Ruijie(config)# link-check disable
```

or

```
Ruijie(config)# no link-check enable
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

4.41 linktest

Use this command to display the link information about a wireless client.

linktest *H.H.H*

Parameter Description

Parameter	Description
H.H.H	MAC address of the wireless client.

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide N/A

Configuration Examples

The following example displays the link information about a wireless client.

```
Ruijie# linktest cca2.2352.768d
Link test station(cca2.2352.768d):
   Signal strength in the form of RSSI :         55
   Signal quality in the form of SNR:           -37
   Total number of packets that are retried:     9
   Maximum retry count for a single packet:      16
   Number of lost packets:                    0
   Data rate of a successfully transmitted packet: 0
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

4.42 long-gi

Use this command to configure the long-gi for the specified radio. Use the **no** form of this command to restore the default settings.

long-gi { **0.8** | **1.6** | **3.2** } **radio** *radio-id*

no long-gi radio *radio-id*

Parameter Description

Parameter	Description
0.8	Sets the long-gi to 0.8us.
1.6	Sets the long-gi to 1.6us.
3.2	Sets the long-gi to 3.2us.
radio-id	Specifies the radio ID, in the range from 1 to 96.

Defaults The default long-gi is 0.8.

Command mode AP configuration mode, all-AP configraiton mode

Usage Guide long-gi applies to 802.11ax.

Configuration Examples The following example enters AP0001 configuration mode and sets long-gi for radio 2 to 3.2us.

```
Ruijie# configure terminal
Ruijie(config)# ap-config AP0001
```

```
Ruijie(config-ap)# long-gi 3.2 radio 2
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

4.43 mcast-rate

Use this command to configure the multicast rate for WLAN. Use the **no** form of this command to restore the default multicast rate of WLAN.

mcast-rate *mcast-num*

no mcast-rate

Parameter Description

Parameter	Description
mcast-num	WLAN multicast rate. The available rates: 1Mbps, 6Mbps, 11Mbps, 24Mbps, 54Mbps.

Defaults The default WLAN multicast rate is 24Mbps.

Command mode WLAN configuration mode

Usage Guide N/A

Configuration Examples The following example configures the multicast rate of WLAN2048 to 11Mbps.

```
Ruijie(config)# wlan-config 2048
Ruijie(config-wlan)# mcast-rate 11
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

4.44 mcell

Use this command to enable mcell for the specified radip. Use the **no** form of this command to remove the configuration.

mcell enable radio *radio-id*

no mcell enable radio *radio-id*

Parameter Description

Parameter	Description
radio-id	Specifies a radio ID, in the range from 1 to 96.

Defaults This function is disabled by default.

Command mode AP configuration mode

Usage Guide N/A

Configuration Examples The following example enables mcell for radio 1.

```
Ruijie(config)# ap-config AP0001
Ruijie(config-ap)# mcell enable radio 1
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

4.45 mu-mimo enable

Use this command to enable MU-MIMO for the specified radio. Use the **no** or **default** form of this command to restore the default setting.

mu-mimo enable radio *radio-id*

no mu-mimo enable radio *radio-id*

default mu-mimo enable radio *radio-id*

Parameter Description

Parameter	Description
radio-id	Specifies a radio, in the range from 1 to 96.

Defaults MU-MIMOis enabled by default.

Command Mode AP configuration mode/ All-AP configuration mode/AP group configuration mode

Usage Guide

Configuration Examples The following example enters AP0001 configuration mode and enable MU-MIMO for radio1.

```
Ruijie(config)# ap-config AP0001
Ruijie(config-ap)# mu-mimo enable radio 1
```

The following example enters AP0001 configuration mode and disables MU-MIMO for radio2.

```
Ruijie(config)# ap-config AP0001
Ruijie(config-ap)# no mu-mimo enable radio 2
```

The following example enters AP0001 configuration mode and restores MU-MIMO setting for radio3.

```
Ruijie(config)# ap-config AP0001
Ruijie(config-ap)# default mu-mimo enable radio 3
```

The following example enters All-AP configuration mode and enables MU-MIMO for radio1.

```
Ruijie(config)# ap-config all
Ruijie(config-ap)# mu-mimo enable radio 1
```

The following example enters default configuration mode and enables MU-MIMO for radio1.

```
Ruijie(config)# ap-group default
Ruijie(config-group)# mu-mimo enable radio 1
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

4.46 ofdma enable

Use this command to enable RF OFDMA. Use the **no** form of this command to restore the default settings.

ofdma enable radio *radio-id*

no ofdma enable radio *radio-id*

Parameter Description

Parameter	Description
radio-id	Specifies the IDs of the radios enabled with RF OFDMA. The value ranges from 1 to 96.

Defaults OFDMA is enabled by default.

Command mode AP configuration mode/all-AP configuration mode/AP group configuration mode

Usage Guide Only OFDMA-supported radio can be enabled with OFDMA.

Configuration Examples The following example enters AP001 configuration mode and disables OFDMA for radio2.

```
Ruijie# configure terminal
Ruijie(config)# ap-config AP0001
Ruijie(config-ap)# no ofdma enable radio 2
```

The following example enters all-AP configuration mode and disables OFDMA for radio2.

```
Ruijie# configure terminal
Ruijie(config)# ap-config all
Ruijie(config-ap)# no ofdma enable radio 2
```

The following example enters default configuration mode and disables OFDMA for radio2.

```
Ruijie# configure terminal
Ruijie(config)# ap-group default
Ruijie(config-group)# no ofdma enable radio 2
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

4.47 peer-distance

Use this command to configure the maximum distance between the specified radio and the peer.

peer-distance *val* **radio** *radio-id*

Parameter Description

Parameter	Description
val	The maximum distance between the radio and the peer. The range is from 1,000 to 25,000. The unit is meter.
radio-id	Radio ID. The range is from 1 to 96.

Defaults The default distance between the radio and the peer is 1,000 meters.

Command mode AP configuration mode

Usage Guide N/A

Configuration Examples The following example configures the maximum distance between radio and the peer to 3,000 meters.

```
Ruijie(config)# ap-config AP0001
Ruijie(config-ap)# peer-distance 3000 radio 1
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

4.48 power local

Use this command to configure trasmit power for the specified radio of the specified AP.

power local { **global** | *power* } **radio** { *radio-id* | *802.11b* | *802.11a* }

Parameter Description

Parameter	Description
power	Indicates the percentage of transmit power. The range is from 1 to 100.
Global	Indicates that the transmit power is specified through RRM for the specified AP or all APs of the specified AP group.
radio-id	Radio ID. The range is from 1 to 96.
802.11b	Configures 2.4GHz radio.
802.11a	Configures 5.8GHz radio.

Defaults By default, the **global** parameter is used.

Command Mode AP configuration mode/AP group configuration mode

Usage Guide N/A

Configuration Examples

The following example configures the transmit power of radio1 of AP0001 to 50%.

```
Ruijie(config)# ap-config AP0001
Ruijie(config-ap)# power local 50 radio 1
```

The following example configures the transmit power of radio 1 of AP group (default) to 50%.

```
Ruijie(config)# ap-group default
Ruijie(config-group)# power local 50 radio 1
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

4.49 preamable

Use this command configure the preamable attribute for the specified radio of the specified AP.

preamable { **long** | **short** } **radio** *radio-id*

Parameter Description

Parameter	Description
radio-id	Radio ID. The range is from 1 to 96.
long	Indicates that the AP transmits only frames of long preamable.
short	Indicates that the AP transmits frames of short or long preamable.

Defaults By default, is **short** parameter is used.

Command Mode AP configuration mode.

Usage Guide N/A

Configuration Examples

The following example configures the preamable attribute of radio 1 of AP0001 to **long**.

```
Ruijie(config)# ap-config AP0001
Ruijie(config-ap)# preamable long radio 1
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

4.50 radio-type

Use this command to configure the RF mode for the specified radio of the specified AP.

radio-type *radio-id* {**802.11a | 802.11b**}

Parameter Description

Parameter	Description
radio-id	Radio ID. The range is from 1 to 96.
802.11a	Indicates the 5GHz band is used.
802.11b	Indicates the 2.4GHz band is used.

Defaults By default, the AP device with single radio (namely, radio1) operates in 2.4 GHz, while the AP device with dual radios can operate in 2.4 GHz (radio1) and 5 GHz (radio2).

Command Mode AP configuration mode.

Usage Guide N/A

Configuration Examples The following example configures radio 1 of AP0001 to operates in 2.4 GHz.

```
Ruijie(config)# ap-config AP0001
Ruijie(config-ap)# radio-type 1 802.11a
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

4.51 response-rssi

Use this command to set the minimum received signal strength indication (RSSI) for wireless client to associate with the AP. Use the **no** form of this command to restore the default setting.

response-rssi *rssi* **radio** { *radio-id* | *802.11b* | *802.11a* }

no response-rssi radio *radio-id* { *radio-id* | **802.11b** | **802.11a** }

Parameter Description

Parameter	Description
rssi	Specifies the RSSI. The range is from 0 to 100. The unit is dBm.
radio-id	Radio ID. The range is from 1 to 96.
802.11b	Configures radios on all 2.4 GHz frequency band.
802.11a	Configures radios on all 5.8 GHz frequency band.

Defaults The default RSSI is 0, namely, the wireless client of any RSSI can associate with the AP.

Command mode AP configuration mode

Usage Guide N/A

Configuration Examples The following example configures the minimum access RSSI to 20.

```
Ruijie(config)# ap-config AP0001
Ruijie(config-ap)# response-rssi 20 radio 1
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

4.52 rts-threshold

Use this command to configure the RTS threshold of the specified radio. Use the **no** form of this command to restore the default RTS threshold.

rts-threshold *value* **radio** *radio-id*

no rts-threshold radio *radio-id*

Parameter Description

Parameter	Description
value	RTS threshold. The unit is byte. The range is from 257 to 2,347.
radio-id	Radio ID. The range is from 1 to 96.

Defaults The default RTS threshold is 2,347.

Command mode AP configuration mode

Usage Guide N/A

Configuration Examples The following example configures the RTS threshold of radio1 to 1,539.

```
Ruijie(config)# ap-config AP0001
Ruijie(config-ap)# rts-threshold 1539 radio 1
```

Related Commands

Command	Description

N/A	N/A

Platform Description N/A

4.53 short-gi

Use this command to enable the radio to support short-gi. Use the **no** form of this command to disable the radio to support short-gi.

short-gi enable radio *radio-id* **chan-width** { **20** | **40** | **80** |**160** }

no short-gi enable radio *radio-id* **chan-width** { **20** | **40** | **80** |**160** }

Parameter Description

Parameter	Description
radio-id	Radio ID. The range is from 1 to 96.
20	Configures the channel bandwidth to 20 Mbps.
40	Configures the channel bandwidth to 40 Mbps.
80	Configures the channel bandwidth to 80 Mbps.
160	Configures the channel bandwitdth to 160 Mbps.

Defaults By default, 20Mbps, and 40Mbps at 2.4GHz radio are enabled. 20Mbps, 40Mbps, 80Mbps and 160Mbps at 5.8GHz radio are enabled.

Command Mode AP configuration mode

Usage Guide N/A

Configuration Examples

The following example enables radio1 to support the short-gi of 20Mbps.

```
Ruijie(config)# ap-config AP0001
Ruijie(config-ap)# short-gi enable radio 1 chan-width 20
```

The following example disables radio2 to support the short-gi of 40Mbps.

```
Ruijie(config)#ap-config AP0001
Ruijie(config-ap)# no short-gi enable radio 2 chan-width 40
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

4.54 short-slot-time

Use this command to enable short slot time for the AP device. Use the **no** form of this command to disable short slot time.

short-slot-time radio *radio-id*

no short-slot-time radio *radio-id*

Parameter Description

Parameter	Description
radio-id	Radio ID. The range is from 1 to 96.

Defaults By default, short slot time is enabled on the AP device.

Command mode AP configuration mode

Usage Guide Short slot time takes effect only on the AP working in 5GHz.

Configuration Examples The following example enables short slot time on radio1.

```
Ruijie(config)#ap-config AP0001
Ruijie(config-ap)# short-slot-time radio 1
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

4.55 stbc

Use this command to enable space-time block code (STBC) for the specified radio. Use the **no** form of this command to disable STBC.

stbc radio *radio-id*

no stbc radio *radio-id*

Parameter Description

Parameter	Description
radio-id	Radio ID. The range is from 1 to 96.

Defaults By default, STBC is enabled.

Command Mode AP configuration mode

Usage Guide N/A

Configuration Examples The following example enters the configuration mode of AP0001 and enable STBC for radio1.

```
Ruijie(config)# ap- config AP0001
Ruieji(config-ap)# stbc radio 1
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

4.56 show ac-config { 802.11a | 802.11b } summary

Use this command to display the AP devices supporting in 802.11a/b on the AC device.

show ac-config { **802.11a** | **802.11b** } **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 AP devices supporting 802.11a on the AC device.

```
Ruijie#show ac-config 802.11a summary
Index  Ap name                              slot id  Radio Base MAC  state
load(%)  noise(dBm) interfere(%)
------ ------------------------------------ -------- ---------------
-------- -------- ---------- ---------------
1     ap320v1.0                            2       0000.0000.0000  Enable
0       -110      0
2     00d0.fb88.7812                        2       00d0.fb88.7815  Enable
0       -110      0
```

Related

Command	Description

Commands	N/A	N/A

Platform Description N/A

4.57 show antenna all

Use this command to display antenna status of all APs.

show antenna all

Parameter Description

Parameter	Description
N/A	N/A

Defaults N/A

Command Mode Privileged EXEC Mode.

Usage Guide Use this command to display the antenna status.

Configuration Examples The following example displays the antenna status of all APs.

```
Ruijie# show antenna all
ap's antenna state                                          R1       R2
R3       R4       R5       R6
                        ap                                0 1 2 3   0 1 2 3   0
1 2 3   0 1 2 3   0 1 2 3   0 1 2 3
-------------------------------------------------------------------   -------
-------   -------   -------   -------   -------
APD-M4                                                    - N N -   - N Y -   -
N N -   - N N -   - - - -   - - - -
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

4.58 show antenna single

Use this command to display antenna status of the specified AP.

show antenna single *ap-name*

Parameter Description

Parameter	Description
ap-name	AP device name.

Defaults N/A

Command Mode Privileged EXEC Mode.

Usage Guide Use this command to display the antenna status of the specified AP..

Configuration Examples The following example displays the antenna status of “APD-M4”:

```
Ruijie# show antenna single APD-M4
```

```
ap[APD-M4] antenna state

R1-1: N

R1-2: N

R2-1: N

R2-2: N

R3-1: N

R3-2: N

R4-1: N

R4-2: N
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

4.59 show ap-config radio

Use this command to display the radio configuration of all APs .

show ap-config radio

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 radio configuration of all AP devices.

```
Ruijie#show ap-config radio
Show all AP radios:
AP Name                              MAC Address        Radio MAC
Radio MAC
---------------------------------------- ------------------
------------------- -------------------
AP0001                               N/A              N/A              N/A
```

Field	Description
AP Name	AP Name
MAC Address	AP MAC address
Radio MAC	MAC address of odd Radio ID
Radio MAC	MAC address of even Radio ID

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

4.60 show ap-config radio ap-name

Use this command to display the radio configuration of all APs.

show ap-config radio ap-name *ap-name*

Parameter Description

Parameter	Description
ap-name	AP device name

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide N/A

Configuration Examples

The following example displays the radio configuration of all APs.

```
Ruijie#show ap-config radio ap-name
Radio ID Radio Type      STA NUM  Channel  Power  Radio Base MAC  Status
-------- --------------- -------- -------- ------ --------------- -------
1        802.11b/g/n     10       6*       100    000c.3067.fbd7  Enable
2        802.11a/n/ac/ax  0       149*     100    000c.3067.fbd8  Disable
```

Field	Description
Radio ID	RF port ID
Radio Type	Radio band
STA NUM	STA number
Channel	Channel
Power	Power
Radio Base MAC	MAC address of RF port
Status	RF port status

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

4.61 show ap-config radio config

Use this command to display the radio configuration of the specified AP.

show ap-config radio *radio-id* **config** *ap-name*

Parameter Description

Parameter	Description
ap-name	AP device name
radio-id	Radio ID. The range is from 1 to 96.

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide N/A

Configuration The following example displays the radio configuration of the specified AP.

Examples

```
Ruijie# show ap-config radio 1 config 220em
Admin State.............................. Enable
Current Tx Power......................... Global
Num of BSSIDs............................ 1
DTIM Period.............................. 1
Beacon Period(milliseconds)............... 100
Country Code............................. CN
Current Channel.......................... Global
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

4.62 show ap-config radio info

Use this command to display radio information of the specified AP.

show ap-config radio info *ap-name*

Parameter Description

Parameter	Description
ap-name	Specifies an AP

Defaults N/A

Command mode Privileged EXEC mode

Usage Guide N/A

Configuration Examples The following example displays radio information of all APs.

```
Ruijie#show ap-config radio info ap-name
Radio ID Radio Type      MU-MIMO    OFDMA      Radio Base MAC  Status
-------- --------------- ---------- ---------- --------------- -------
1        802.11b/g/n     Nonsupport Nonsupport 000c.3067.fbd7  Enable
2        802.11a/n/ac/ax DL         DL/UL      000c.3067.fbd8  Disable
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

4.63 show ap-config radio radio-id status

Use this command to display details about the radio configuration of the specified AP device.

show ap-config radio *radio-id* **status** *ap-name*

Parameter Description

Parameter	Description
radio-id	Radio ID. The range is from 1 to 96.
ap-name	AP device name.

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide N/A

Configuration Examples

The following example displays details about the radio configuration of the specified AP.

```
Ruijie# show ap-config radio 1 s 220em
Admin State.............................. Enable
Oper State............................... Normal
WTP Radio Statistics
 Last Fail Type......................... Statistic Not Supported
 Reset Count............................ 0
 SW Failure Count....................... 0
 HW Failure Count....................... 0
 Other Failure Count.................... 0
 Unknown Failure Count.................. 0
 Config Update Count.................... 0
 Channel Change Count................... 2
 Band Change Count...................... 197
 Current Noise Floor.................... -102
Assigned WTP BSSID
 WLAN ID................................ 0
 MAC Address............................ 0000.0000.0000
MIC Countermeasures
 WLAN ID................................ 0
 MAC Address............................ 0000.0000.0000
RSNA Error Report From Station
 Client MAC Address..................... 0000.0000.0000
```

```
 Radio Base MAC..................... 0000.0000.0000
 Radio ID........................... 1
 WLAN ID............................ 0
 TKIP ICV Errors.................... 0
 TKIP Local MIC Failures............ 0
 TKIP Remote MIC Failures........... 0
 CCMP Replays....................... 0
 CCMP Decrypt Errors................ 0
 TKIP Replays....................... 0
Statistics
 Tx Fragment Count.................. 0
 Multicast Tx Count................. 0
 Failed Count....................... 0
 Retry Count........................ 0
 Multiple Retry Count............... 0
 Frame Duplicate Count.............. 0
 RTS Success Count.................. 0
 RTS Failure Count.................. 0
 ACK Failure Count.................. 0
 Rx Fragment Count.................. 0
 Multicast RX Count................. 0
 FCS Error Count.................... 0
 Tx Frame Count .................... 0
 Decryption Errors.................. 0
 Discarded QoS Fragment Count....... 0
 Associated Station Count........... 0
 QoS CF Polls Received Count........ 0
 QoS CF Polls Unused Count.......... 0
 QoS CF Polls Unusable Count........ 0
Current Tx Power.................... 100
Current Tx Power Value.............. 28
Tx Power Level Num.................. 0
WebAuth online sta Count..............0
DOT1x online sta Count................0
Security sta Count....................0
WTP Radio Fail Alarm Indication
 Type............................... Unknown
 Status............................. 0
 Pad................................ 0
WTP Radio Information
Radio Type.......................... 802.11b
WTP Radio Config
 Short Preamble..................... 0
 Number of BSSIDs................... 1
```

```
 DTIM Period.............................. 0
 Radio Base MAC........................... 00d0.f822.33da
 Beacon Period(milliseconds)............. 100
 Country String........................... CNI
Direct Sequence Control
 Current Channel.......................... 11
 Current CCA.............................. 1
 Energy Detect Threshold.................. 1
MAC Operation
 RTS Threshold............................ 2347
 Short Retry.............................. 7
 Long Retry............................... 4
 Fragmentation Threshold.................. 2346
 Tx MSDU Lifetime......................... 0
 Rx MSDU Lifetime......................... 0
Multi-Domain Capability
 First Channel............................ 0
 Number of Channels....................... 0
 Max Tx Power Level....................... 0
OFDM Control
 Current Channel.......................... 0
 Band Supported........................... 0
 TI Threshold............................. 0
Capability
 Power Default............................ 28
 Power Max................................ 28
 Power Min................................ 1
 Power Per Default........................ 100
 Power Per Max............................ 100
 Power Per Min............................ 4
```

Related Commands	Command	Description
	N/A	N/A

Platform Description N/A

4.64 show ap-config radio status

Use this command to display the radio list of an AP device.

show ap-config radio status *ap-name*

Parameter	Parameter	Description

Description	*ap-name*	AP device name.

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide N/A

Configuration Examples The following example displays the radio list of the specified AP.

```
Ruijie# show ap-config radio status 220em
Radio Slot  Radio Type     Sub Band   Admin Status    Oper Status     Regulary
Domain     Radio Base MAC
----------- --------------- ---------- --------------- ---------------
-------------------- --------------------
1          802.11b/g/n         -        Enable          -
Supported          00d0.f822.33da
2          802.11a/n         -        Enable          -            Supported
00d0.f822.33db
```

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

Platform Description N/A

4.65 show ap-config summary radio

Use this command to display all APs on the specified radio.

show ap-config summary radio [*radio-id*]

Parameter Description	**Parameter**	**Description**
	radio-id	Specifies a radio, in the range from 1 to 96.

Defaults N/A

Command mode Privileged EXEC mode

Usage Guide N/A

Configuration The following example displays all APs on radio 1.

Examples

```
Ruijie#sh ap-config summary radio 1
Ap Name                                Radio Base MAC  STA NUM  Radio Type   AP IP
---------------------------------------      ---------------      --------
------------ ---------------
AP530-I1.01                                 0014.4b74.d427  0        802.11b
172.18.57.195
APfloor1                                 0014.4b6d.e18f  8       802.11b/n/ax
172.18.57.227
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

4.66 show client details

Use this command to display the information of the specified wireless client.

show client details *sta-mac*

Parameter Description

Parameter	Description
sta-mac	MAC address of the wireless client. The format is H.H.H.

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide N/A

Configuration Examples

The following example displays the information of wireless client “0025.9c9b.aeb5”.

```
Ruijie# show client details 0025.9c9b.aeb5
The Details of Client 0025.9c9b.aeb5:
   RSSI..................... 28
   SNR...................... -67
   AID...................... 1
   RX Data.................. 51
   RX Management............ 0
   RX Control............... 0
   RX Unicast............... 25
   RX Multicast............. 0
   RX Bytes................. 6174
   TX Data.................. 3
```

```
TX Management.......... 0
TX Unicast............. 3
TX Multicast........... 0
TX Bytes............... 228
TX Probe............... 0
TX Assoc............... 0
TX Assoc Fail.......... 0
TX Auth................ 0
TX Auth Fail........... 0
TX Deauth.............. 0
TX Disassoc............ 0
Packet Load............ 51216
```

Related Commands	Command	Description
	N/A	N/A

Platform Description N/A

4.67 show smart bad radio

Use this command to display the bad radio on AP5280.

show smart bad radio

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 bad radio on AP5280.

```
AC#show smart bad radio

Ap-name               ap-mac               radio
-------------------     ---------------        ----------------
AP5280-1              00d0.1234.4565         1,2,3,4,
AP5280-2              00d0.1234.4568         7,8,
```

Field description

Field	Description
Ap name	AP Name
Ap-mac	AP MAC Address
radio	Bad Radio ID

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

4.68 update-key-tsc enable

Use this command to enable the AP device to update key TSC during 802.1x reauthentication. Use the **no** form of this command to disable the AP device to update the key TSC..

update-key-tsc enable

no update-key-tsc enable

Parameter Description

Parameter	Description
N/A	N/A

Defaults N/A

Command Mode AP configuration mode/ AP group configuration mode.

Usage Guide N/A

Configuration Examples The following example enables the AP device to update key TSC during 802.1x reauthentication.

```
Ruijie(config)# ap-config AP0001

Ruijie(config-ap)# update-key-tsc enable
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

5 EF-DHCP Commands

5.1 central dhcp enable

Use this command to forward the DHCP packet through the wireless access controller in local forwarding mode. Use the **no** form of this command to restore the default setting.

central dhcp enable

no central dhcp enable

Parameter Description

Parameter	Description
N/A	N/A

Defaults By default, the DHCP packets are sent in local forwarding mode, namely the packets are forwarded through the access point.

Command mode WLAN configuration mode

Usage Guide Ruijie recommends enabling this function for easy management of the DHCP address pool in WLAN and simplification of the DHCP topology.

Configuration Examples The following example enables this function.

```
Ruijie(config)#wlan-config 100 ruijie_wlan
Ruijie(config-wlan)#tunnel local
Ruijie(config-wlan)#central dhcp enable
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

5.2 local fw ip

Use this command to specify the local forwarding mode for the data of the specified user. Use the **no** form of this command to restore the default setting.

local fw ip [*ip address*]

no local fw ip [*ip address*]

Parameter

Parameter	Description

Description

ip address	IP address of the specified user.

Defaults No IP address is specified by default. The forwarding mode is the same as that of the tunnel configuration.

Command mode AC-controller configuration mode

Usage Guide The flexible forwarding function can identify the data access condition automatically to adopt either local forwarding or centralized forwarding. With this command configured, the forwarding mode is determined by the user IP address.

Configuration Examples The following example specifies the local forwarding mode for the data of user192.168.1.1.

```
ruijie(config)#ac-controller
ruijie(config-ac)#local fw ip192.168.1.1
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

5.3 tunnel

Use this command to configure separate MAC mode or local MAC mode for the WLAN tunnel. Use the **no** form of this command to restore the default setting.

tunnel { **8023** | **local** | **local-auth** }

no tunnel

Parameter Description

Parameter	Description
8023	The AP encapsulates the wireless data into the 802.3 frame and forwards the frame to the AC.
local	The AP adopts local forwarding.
local-auth	The AP adopts local forwarding and the STA performs authentication on the AP end.

Defaults The default is **8023**.

Command mode WLAN configuration mode

Usage Guide The **local-auth** command can be used only in the RIPT scenario. Otherwise, WLAN is not available.

Configuration Examples The following example sets the tunnel mode to **local**.

```
Ruijie(config-wlan)#tunnel local
```

The following example sets the tunnel mode to **8023**.

```
Ruijie(config-wlan)#tunnel 8023
```

The following example restores the tunnel mode to the default setting.

```
Ruijie(config-wlan)#no tunnel
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

5.4 tunnel 8023 wlan

Use this command to specify the centralized forwarding mode for the packets of a specified VLAN.

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

tunnel 8023 wlan [*wlan-id*] **vlan** [*vlan-id*]

no tunnel 8023 wlan [*wlan-id*] **vlan** [*vlan-id*]

Parameter Description

Parameter	Description
wlan-id	The ID of the WLAN for centralized forwarding, in the range from 1 to 4094. The WLAN must have been created,
vlan-id	The ID of the VLAN for centralized forwarding, in the range from 1 to 4094. The VLAN must have been created,

Defaults No VLAN is specified by default. The forwarding mode is the same as that of the tunnel configuration.

Command mode AP-group configuration mode

Usage Guide The **tunnel-local** command is used to specify the local forwarding mode for the whole WLAN. The **tunnel 8023 wlan** command is used to specify the centralized forwarding mode for a certain VLAN.

Configuration Examples The following example specifies the centralized forwarding mode for VLAN 2 in WLAN1. The other VLAN packets apply local forwarding.

```
Ruijie(config)#wlan-config 1
Ruijie(config-wlan)#tunnel local
Ruijie(config-wlan)#exit
Ruijie(config)#ap-group default
```

```
Ruijie(config-ap-group)#tunnel 8023 wlan 1 vlan 2
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

5.5 tunnel local wlan

Use this command to specify the local forwarding mode for the packets of a specified VLAN. Use the **no** form of this command to restore the default setting.

tunnel local wlan [*wlan-id*] **vlan** [*vlan-id*]

no tunnel local wlan [*wlan-id*] **vlan** [*vlan-id*]

Parameter Description

Parameter	Description
wlan-id	The ID of the WLAN for local forwarding, in the range from 1 to 4094. The WLAN must have been created,
vlan-id	The ID of the VLAN for local forwarding, in the range from 1 to 4094. The VLAN must have been created,

Defaults No VLAN is specified by default. The forwarding mode is the same as that of the tunnel configuration.

Command mode AP-group configuration mode

Usage Guide The **tunnel-8023** command can be used to specify the centralized forwarding mode for the whole WLAN. The **tunnel local wlan** command can be used to specify the local forwarding mode for a certain VLAN.

Configuration Examples The following example specifies the local forwarding mode for VLAN 2 in WLAN1. The other VLAN packets apply centralized forwarding.

```
Ruijie(config)#wlan-config 1
Ruijie(config-wlan)#tunnel 8023
Ruijie(config-wlan)#exit
Ruijie(config)#ap-group default
Ruijie(config-ap-group)#tunnel local wlan 1 vlan 2
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

6 ETH-MNG Commands

6.1 ap-subif

Use this command to enable the AP to create the sub interface of the WAN port. Use the **no** form of this command to remove the configuration.

ap-subif enable

no ap-subif enable

Parameter Description

Parameter	Description
N/A	N/A

Defaults N/A

Command Mode AP configuration mode

Usage Guide If the AP obtains its address through PPPoE, the sub interface of the WAN port is removed automatically. This command cannot enable the AP to create the sub interface of the WAN port in PPPoE mode.

Configuration Examples The following example enables AP1 to remove the sub interface from the WAN port.

```
Ruijie(config)# ap-config AP1
Ruijie(config-ap)# no ap-subif enable
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

6.2 ap-vlan

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

ap-vlan *vlan-id*

no ap-vlan

Parameter

Parameter	Description

Description

vlan-id	Specifies the VLAN on the wired network port, in the range from 1 to 4094.

Defaults The default is 1.

Command Mode AP configuration mode

Usage Guide The AP untags the frame of the Native VLAN before forwarding it. In local forwarding mode, if the user VLAN is the same as the Native VLAN, the frame is forwarded untagged and the access switch determines the VLAN where the user resides.

- This command forces the online AP to go offline and enables reconnection.
- In WDS deployment, when ROOT-BRIDGE and NONROOT-BRIDGE devices are configured with local forwarding, they should reside in the same AP-VLAN. Otherwise, the NONROOT-BRIDGE device cannot share the address pool with the ROOT-BRIDGE device; packet forwarding on the NONROOT-BRIDGE device may even be affected.
- This command needs to be configured only in the following case: In local forwarding mode, STAs and an AP belong to a same subnet and VLANs have been configured for the STAs and the AP. This command is not required in other cases.
- If the static DHCP address pool is configured, and BVI 1 port number is used as client ID, this configuration will bring changes to the BVI port. In this case, the DHCP server configuration should be modified. Otherwise, the address cannot be obtained.
- When the AP obtains the address through PPPoE and CAPWAP selects dialer 1 as the source port, the STA traffic is forwarded untagged even if this command is configured.

Configuration Examples The following example sets the Native VLAN for AP 1 to 20.

```
Ruijie(config)# ap-config AP1
Ruijie(config-ap)# ap-vlan 20
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

6.3 pass-vlan

Use this command to configure the transmission VLAN for the AP. Use the **no** form of this command to remove the setting.

pass-vlan *vlan-range*

no pass-vlan *vlan-range*

Parameter Description

Parameter	Description
vlan-range	Indicates the VLAN ID range. Multiple VLAN IDs can be specified. Separate two VLAN IDs by a comma (,) and separate two VLAN ID ranges by a hyphen (-).

Defaults No transmission VLAN is configured by default.

Command Mode AP configuration mode

Usage Guide

1. This command can be configured for all APs but takes effect only on the i-Share+ master AP.
2. When this command is run, the transmission VLAN will be created on the i-Share+ master AP, so that the master AP can forward packets based on the transmission VLAN. In addition, the transmission VLAN will be automatically pruned on the downlink port of the master AP, to prevent broadcast and multicast packets of other master APs from being flooded to mini APs connected to the master AP.

The transmission VLAN cannot conflict with the VLANs specified by the **interface-mapping**, **ap-vlan**, and **wired-vlan** commands, and cannot be VLAN 2444.

Configuration Examples The following example sets the transmission VLAN to 20 for AP1.

```
Ruijie(config)# ap-config AP1
Ruijie(config-ap)# pass-vlan 20
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

6.4 show port-mode

Use this command to display the port mode.

show port-mode

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 port mode.

```
Ruijie#show port-mode
Current port mode:    mixed
Configure port mode:   copper
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

6.5 switch port-mode

Use this command to switch the port mode.

switch port-mode { **copper** | **fiber** | **mixed** }

Parameter Description

Parameter	Description
copper	4 Gigabit copper mode
fiber	40 Gigabit fiber mode
mixed	2 Gigabit copper & 20 Gigabit fiber port

Defaults The default port mode is **mixed**.

Command Mode Privileged EXEC mode

Usage Guide 4 Gigabit copper mode applies to port 25-28. 40 Gigabit fiber mode applies to port 29-32. Mixed mode applies to port 27, 28, 31, 32.

Configuration Examples The following example switches the port to **fiber**.

```
Ruijie# switch port-mode fiber
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

6.6 wired-interface

Use this command to enable the wired network port on the AP. Use the **no** form of this command to disable the wired port. Use the **default** form of this command to restore the default setting.

wired-interface [**slot** *slot-id* [**secondary**]] [**port** *port-id*] **enable**

no wired-interface [**slot** *slot-id* [**secondary**]] [**port** *port-id*] **enable**

default wired-interface [**slot** *slot-id* [**secondary**]] [**port** *port-id*] **enable**

Parameter Description

Parameter	Description
slot	Indicates the slot to which a Mini AP belongs.
slot-id	Indicates the slot ID. The value ranges from 1 to 24.
secondary	Applies to the secondary device.
port	Configures the wired network port.
port-id	Specifies the wired network port number, in the range from 1 to 4.
enable	Enables the wired network port.

Defaults The wired network port is enabled by default.

Command Mode AP configuration mode/all-AP configuration mode/AP group configuration mode

Usage Guide

1. This command can be configured on all APs, but it takes effect only on the APs with wired network port.
2. If this command involves no port configuration, all wired network ports share the same configuration; if the four ports are disabled, no port configuration is displayed.The **slot** parameter takes effect only for i-Share+ APs. If no slot is specified, the configuration applies to all Mini APs.
3. The fit AP obtains its configuration from the AC. The AP saves the wired port configuration automatically. When disconnected from the AC, the AP can restore the configuration after restart. If the wired port is disabled through configuration, the port remains disabled even after AP restart.

If the wired port on the AP is disabled, you cannot manage the AP through the wired port even after AP restart. It is recommended to long press the reset button on the AP to restore the factory setting.

Configuration Examples The following example disables the wired network port on AP1.

```
Ruijie(config)# ap-config AP1
Ruijie(config-ap)# no wired-interface
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

6.7 wired-rate

Use this command to configure the maximum bandwidths for various LAN interfaces and slots.

wired-rate *value* [**port** *port-id*] [**slot** *slot-id* [**secondary**]]

Parameter Description

Parameter	Description
value	Specifies the maximum bandwidth in the unit of 1Mbps. The default for AC, AP120-W and AP130-W are 1000, 100 and 1000 respectively.
port-id	Specifies the interface, in the range from 1to 4.There is no default and this parameter is not available on the fat AP.
slot-id	Specifies the slot, in the range from 1 to 24. There is no default and this parameter is only available on the i-Share+ AP.
secondary	Applies to the secondary device.

Defaults The maximum bandwidths of various LAN interfaces are not limited by default.

Command Modes AP configuration mode/AP group configuration mode

Usage Guide If no port is specified, all LAN port bandwidths are configuredd

The **slot** parameter takes effect only for i-Share+ APs. If no slot is specified, the configuration applies to all Mini APs.

Configuration Examples The following example sets the maximum bandwidth for interface0/2of an AP to 50 Mbps.

```
Ruijie(config)#ap-config [ap-name]
Ruijie(config-ap)# wired-rate 50 interface 2
```

The following example sets the maximum bandwidth for interface 0/3for all APs to 30 Mbps.

```
Ruijie(config)#ap-config all
Ruijie(config-ap)# wired-rate 30 interface 3
```

The following example sets the maximum bandwidth for interface0/1 of an AP group to 80 Mbps.

```
Ruijie(config)#ap-group default
Ruijie(config-group)#wired-rate 80 port 1
```

The following example sets the maximum bandwidth for all LAN ports of an AP group to 90 Mbps.

```
Ruijie(config)#ap-group default
Ruijie(config-group)#wired-rate 90
```

The following example sets the maximum bandwidth for slot 3 of the i-Share+ AP to 90 Mbps.

```
Ruijie(config)#ap-config am5528
Ruijie(config-ap)#wired-rate 90 slot 3
```

Related Commands

Command	Description
show run	Displays the current configuration.

Platform Description N/A

6.8 wired-vlan

Use this command to configure the VLAN for the for the wired network port on the AP. Use the **no** form of this command to restore the default setting.

wired-vlan *vlan-id* [**slot** *slot-id* [**secondary**]] [**port** *port-id*] **auto-save**

no wired-vlan [*vlan-id* [**slot** *slot-id* [**secondary**]] [**port** *port-id*]] **auto-save**

Parameter Description

Parameter	Description
vlan-id	Specifies the VLAN where the wired network port resides, in the range from 1 to 4094.
slot	Indicates the slot to which a Mini AP belongs.
slot-id	Indicates the slot ID. The value ranges from 1 to 24.
secondary	Applies to the secondary device.
port	Configures the wired network port.
port-id	Specifies the wired network port number, in the range from 1 to 4.
auto-save	Saves the configuration. The AP restores the configuration after restart.

Defaults The wired network port and the AP are in the same VLAN by default.

Command Mode AP configuration mode/ AP group configuration mode

Usage Guide

1. This command can be configured on all APs, but it takes effect only on the APs with wired network port.
2. If this command involves no port configuration, all wired network ports are in the same VLAN; if

the four ports are configured in the same VLAN, no port configuration is displayed. The **slot** parameter takes effect only for i-Share+ APs. If no slot is specified, the configuration applies to all Mini APs.

3. In access AP mode (the AP does not assign IP addresses), when the wired network port and the AP are configured in the same VLAN, the VLAN where the wired network port resides is determined by the access switch rather than by this configuration. If the packet on the wired network port should be tagged, the Native VLAN of the access switch must be different from the VLAN where the wired network port resides. Otherwise, the packet cannot be forwarded to the wired network port.
4. In wireless routing mode (the AP assigns IP addresses), wired users obtain IP addresses from the DHCP address pool on the AP. The VLAN where the address pool interface resides must be consistent with the VLAN specified in this command.
5. The fit AP obtains its configuration from the AC. The **auto-same** parameter enables the AP to save the wired port configuration automatically. When disconnected from the AC, the AP can restore the configuration after restart to enable users to access the network through wired network port.

When the wired network port is enabled with the **auto-same** function and the VLAN where the wired network port resides is different from the Native VLAN of the AP, the AP cannot obtain the IP address after restart. It is recommended to long press the reset button on the AP to restore the factory setting.

Configuration Examples

The following example configures VLAN 20 for the wired network port on AP1.

```
Ruijie(config)# ap-config AP1
Ruijie(config-ap)# wired-vlan 20
```

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

7 DATA-PLANE Commands

7.1 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.
	`Ruijie(config)#data-plane queue-weight 100 50 50 25 25`
	`Ruijie(config)#data-plane token 10 10`
	`Ruijie(config)#data-plane wireless-broadcast enable`

Platform Description	N/A.

8 WLOG Commands

8.1 show wlan diag ap

Use this command to display AP records on an AC.

show wlan diag ap [**ap-mac** *AP_MAC*] [**number** *NUMBER*]

Parameter Description

Parameter	Description
AP_MAC	Specifies the MAC address of an AP to be displayed.
NUMBER	Specifies the maximum number of records to be displayed.

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide N/A

Configuration Examples The following example displays AP records.

```
Ruijie# show wlan diag ap ap-mac 00d0.f822.33b0 number 10

ap_record: ruijieAP[00d0.f822.33b0/1.1.1.2],down/up:2

IP Address:1.1.1.2
2012-05-28 09:30:00  [TIMER]     AP UP Time:00:00:18:54
Wired port five in rate/out rate stat:612kbits/sec(in) 1208kbits/sec(out)
   Unicast:    84595   bytes(in) 86625   bytes(out)
   Multicast:  7        bytes(in) 4       bytes(out)
   Broadcast:  2145    bytes(in) 117     bytes(out)
   Error Frame:0       bytes(in) 0       bytes(out)
Radio    channel power      Active STA WEB_Auth   DOT1X      Rssi     ErrorPkt
RetryPkt
-------- ------- ----------- ---------- ---------- ----------  --------
---------- ----------
1     11    100       2        1        0         0      0        0
2     157   100       0        0        0         0      0        0

IP Address:1.1.1.2
2012-05-28 09:49:18  [CW-DOWN]    AP UP Time:00:00:38:12
Wired port five in rate/out rate stat:187kbits/sec(in) 905kbits/sec(out)
   Unicast:    84789   bytes(in) 86810   bytes(out)
   Multicast:  7        bytes(in) 5      bytes(out)
```

```
   Broadcast:  2148    bytes(in) 133     bytes(out)
   Error Frame:0       bytes(in) 0       bytes(out)
Radio    channel power       Active STA WEB_Auth   DOT1X      Rssi     ErrorPkt
RetryCnt
-------- ------- ----------- ---------- ---------- ----------  --------
---------- ----------
1      11      100       2        1         0         0        0         0
2      157     100       0        0         0         0        0         0
CAPWAP DOWN REASON:echo expired
```

Field	Description
ap_record	Specifies AP records.
IP Address	Specifies the IP address of an AP whose information is collected.
TIMER	Specifies information collected by a timer.
CW-DOWN	Specifies information collected when a CAPWAP connection is interrupted.
Wired port five in rate/out rate stat	Specifies the input or output rate on a wired port for the recent five minutes.
Unicast	Specifies statistics about unicast packets on a wired port.
Multicast	Specifies statistics about multicast packets on a wired port.
Broadcast	Specifies statistics about broadcast packets on a wired port.
Error Frame	Specifies statistics about incorrect frames on a wired port.
Radio	Specifies a radio ID.
channel	Specifies the working channel of the radio.
power	Specifies the emission frequency of the radio.
Active STA	Specifies the number of STAs associated with the radio.
WEB_AUTH	Specifies the number of STAs associated with the radio and get online through the web interface.
DOT1X	Specifies the number of STAs associated with the radio and get online through 802.1X authentication.
ErrorPkt	Specifies the number of incorrect frames received by the radio.
RetryCnt	Specifies the number of times that packets from the radio are retransmitted.
CAPWAP DOWN REASON	Specifies the reason for CAPWAP disconnection. This item is displayed only when **CW_DOWN** is set.

Related Commands

Command	Description
N/A	N/A

Platform Description This command is supported on AC devices.

8.2 show wlan diag network

Use this command to display the record information about the entire network.

show wlan diag network

Parameter Description

Parameter	Description
N/A	N/A

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide N/A

Configuration Examples

```
Ruijie# show wlan diag network
Time:2012-05-28 09:10:00
AC uptime: 1 h
Online AP:1
Online AP Version:
   PID[AP220-E]:hwver[2.00] AP Number:1
Offline AP:7
ssid          Active STA WEB Auth   Dot1x     Free STA
----------------------------- ---------- ---------- ---------- ----------
1T17-wlog-test1                0         0         0         0
1T17-wlog-test2                0         0         0
```

Field	Description
Time	Specifies the time for colleting a record.
AC Running Time	Specifies the running time of an AC connection.
Current Online Number of AP	Specifies the number of online APs.
Online AP Version	Specifies the version of online APs.
Offline Number of AP	Specifies the number of pre-configured but offline APs.

ssid	Specifies the SSID of a WLAN.
Active STA	Specifies the total number of active STAs.
WEB Auth	Specifies the number of STAs that get online through web authentication.
Dot1x	Specifies the number of STAs that get online through 802.1x authentication.
Free STA	Specifies the number of STAs free of authentication.

Related Commands

Command	Description
N/A	N/A

Platform Description This command is supported on AC devices.

8.3 show wlan diag sta

Use the following command to display STA statistics on an AC:
show wlan diag sta [**sta-mac** *STA_MAC*] [**ip-range** *IP_PREFIX*] [**action** *ACTION* [**result** *RESULT*]] [**number** *NUMBER*]
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.
IP_PREFIX	Specifies the range of IP addresses for the STA, which is limited by an IP prefix.
ACTION	Specifies the type of STA action records.
RESULT	Specifies the result of STA action records.
NUMBER	Specifies the maximum number of records to be displayed.

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide N/A

Configuration Examples This example displays STA statistics on an AC:

```
Ruijie# show wlan diag sta
sta_record: c83a.35c6.0c72
[STA-DOWN]   STA UP Time: 2018-04-19 22:06:05     STA DOWN Time: 2018-04-19
```

```
22:11:17
Time        IP  Address         RSSI/Link  Rate   DEV  ID/AP  MAC/SSID/Radio
Action             Result  Reason
--------                   ---------------                   ---------------
-------------------------------------------------    --------------------
------- --------------------
09:59:28  0.0.0.0            0/0.0M             1/00d0.f822.33b0/lxh-ssid/1
STA UP BY APMG      SUCCESS
```

10:12:07 192.168.248.2 -88/13.0M 1/00d0.f822.33b0/lxh-ssid/1 STA DOWN BY APMG AP circular AC user is offline 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 This command is supported on ACs.

8.4 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 ACs and APs.

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 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 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 This command is supported on ACs.

8.5 web-server enable api-path assoc-sta url

Use this command to configure the Elog server URL for the associated STA. Use the **no** form of this command to remove the setting.

web-server enable api-path assoc-sta url *url*

no web-server enable api-path assoc-sta url

Parameter Description

Parameter	Description
url	Sets the Elog server URL

Defaults No Elog server is configured by default.

Command Mode Global configuration mode

Usage Guide N/A

Configuration Examples The following example configures the Elog server URL for the associated STA and removes the setting.

```
Ruijie# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Ruijie(config)#web-server enable api-path assoc-sta url
http://172.18.155.14:8080/elog/service/dc/updateSta
Ruijie(config)#no web-server enable api-path assoc-sta url
```

Related Commands

Command	Description
N/A	N/A

Platform Description This command is supported on ACs.

9 Roaming Commands

9.1 keepalive-count

Use this command to set the maximum number of times that the keep-alive request is can be sent. Use the **no** form or **default** form of this command to restore the default keep-alive count.

keepalive-count *counts*

no keepalive-count

default keepalive-count

Parameter Description

Parameter	Description
counts	Indicates the keep-alive count. The range is from 2 to 30.

Defaults The default keepalive count is 4.

Command Mode Mobility group configuration mode.

Usage Guide In an unstable network, the keepalive request times can be increased to avoid interruption.

Configuration Examples The following example configures the keepalive request times to 5.

```
Ruijie(config)#mobility-group mgroup_name
Ruijie(config-mobility)# keepalive-count  5
```

Related Commands

Command	Description
keepalive-interval	Indicates the interval of sending a keep-alive request.

Platform Description N/A

9.2 keepalive-interval

Use this command to set the interval of sending a keep-alive request. Use the **no** form or **default** form of this command to restore the default keep-alive interval.

keepalive-interval *seconds*

no keepalive-interval

default keepalive-interval

Parameter

Parameter	Description

Description

seconds	Indicates the interval of sending a keep-alive request. The range is from 1 to 30. The unit is second.

Defaults The default interval is 10 seconds.

Command Mode Mobility group configuration mode.

Usage Guide If there are many mobility members, you can increase the keepalive request interval to reduce the times of sending keepalive request.

Configuration Examples The following example sets a mobility group named Mgroup_name. The mobility group sends a keep-alive request to another AC in the mobility group at a regular interval of 20 seconds.

```
Ruijie(config)#mobility-group mgroup_name
Ruijie(config-mobility)#keepalive-interval 20
```

Related Commands

Command	Description
keepalive-count	Configures the keepalive request times.

Platform Description N/A

9.3 list

Use this command to configure members of a mobility list. Use the **no** form or **default** form of this command to delete a member of the mobility list.

list (*ip-address* | *ipv6-address*)

no list (*ip-address* | *ipv6-address*)

default list { *ip-address* | *ipv6-address* }

Parameter Description

Parameter	Description
ip-address	Indicates the IP address of the member AC of mobility group. The IP address is the loopback 0 interface address of the AC.
ipv6-address	IPv6 address of the member AC of the mobility group, which is the IPv6 address of loopback 0 interface of the AC.

Defaults N/A

Command Mode Mobility group configuration mode.

Usage Guide

The mobility list is configured based on a mobility group. To configure a mobility list, you need to create a mobility group first and then enter mobility group configuration mode to add members of the mobility list in the mobility group. You can configure multiple mobility list members on the AC. Usually, these members do not belong to the same mobility group as the AC because the subscribers connected to the AC in the same mobility group can roam more efficiently. Therefore, the ACs configured in the mobility list and the current AC should belong to different mobility groups. You can add a maximum of 72 mobility list members to each AC. If the IPv4 or IPv6 address on the loopback 0 interface of the AC is changed, the multicast tunnel interface (MTI) established with the former IP address will disconnect in the next keep-alive interval, and a new MTI tunnel will be established with a new IP address.

When configuring an AC as both an IPv4 and IPv6 member, the roaming only accepts one MTI tunnel, and the other one is not effective. When an abnormality occurs and the MTI tunnel is disconnected, the AC will automatically switch to the other MTI tunnel.

When configuring the IPv6 member list of a mobility group, if the current AC has no IPv6 control address, the establishment of the IPv6 roaming tunnel will fail.

Configuration Examples

The following example configures a mobility list in the mobility group Mgroup_name on the current AC. The mobility list comprises the AC1 and AC2 members. The IP address of AC1 is 192.168.2.1, and the IP address of AC2 is 192.168.2.2 and the IPv6 address of AC3 is 2002:1::1.

```
Ruijie# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Ruijie(config)# mobility-group mgroup_name
Ruijie(mobility- mobility)# list 192.168.2.1
Ruijie(mobility- mobility)# list 192.168.2.2
Ruijie(mobility- mobility)# list 2002:1::1

Ruijie# show mobility status mgroup_name
Mobility Group mgroup_name
Multicast Mode ................................. Disable
Multicast Address.............................. 0.0.0.0
Mobility Keepalive Interval..................... 10
Mobility Keepalive Count........................ 3
Mobility Group Status........................... Fast Mode

Mobility Members:
IP Address         Client/Server   Data Tunnel    Ctrl Tunnel    192.168.1.1
Client          OK             OK
192.168.1.2        Client           OK             OK
Mobility List Members:
IP Address         Client/Server   Data Tunnel    Ctrl Tunnel
192.168.2.2        Client          OK             OK
IP Address         Client/Server   Data Tunnel    Ctrl Tunnel
192.168.2.1        Client          OK             OK
IP Address         Client/Server   Data Tunnel    Ctrl Tunnel
```

```
2002:1::1          Client          OK              OK
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

9.4 member

Use this command to add AC members to the mobility group. Use the **no** form or **default** form of this command to delete the specified AC members.

member (*ip-address* | *ipv6-address*)

no member (*ip-address* | *ipv6-address*)

default member { *ip-address* | *ipv6-address* }

Parameter Description

Parameter	Description
ip-address	Indicates the IP address of the member AC of the mobility group. The IP address is the loopback 0 interface address of the AC.
ipv6-address	IPv6 address of the member AC of the mobility group, which is the IPv6 address of loopback 0 interface of the AC.

Defaults N/A

Command Mode Mobility group configuration mode.

Usage Guide To configure a mobility group, perform the two steps: 1) Create a mobility group; 2) Add the corresponding AC members to the mobility group. You need to configure every AC in the mobility group. The address of a member of the mobility group is the IPv4 or IPv6 address of the loopback 0 interface of the corresponding AC. If the IPv4 or IPv6 address of the loopback 0 interface of the current AC is changed, the MTI tunnel established with the former IP address will disconnect in the next keep-alive interval, and a new MTI tunnel will be established with a new IP address.

When configuring an IPv4 or IPv6 roaming AC, if the AC is not configured with an corresponding IPv4 or IPv6 address on the loopback 0 interface, the establishment of the roaming tunnel will fail.

When configuring an AC as both an IPv4 and IPv6 member, the roaming only accepts one MTI tunnel, and the other one is not effective. When an abnormality occurs and the MTI tunnel is disconnected, the AC will automatically switch to the other MTI tunnel.

Configuration The following example creates the mobility group named **mgroup_name**, and add members to the

Examples mobility group.

```
Ruijie# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Ruijie(config)#mobility-group mgroup_name
Ruijie(config-mobility)#member 192.168.1.1
Ruijie(config-mobility)#member 2002:1::1
```

Related Commands

Command	Description
N/A	N/A

Platform Description The command is supported only on ACs.

9.5 mobility-fast

Use this command to enable active information exchange of the mobility group. Use the **no** form or **default** form of this command to disable active information exchange of the mobility group.

mobility-fast

no mobility-fast

default mobility-fast

Parameter Description

Parameter	Description
N/A	N/A

Defaults By default, active information exchange is disabled.

Command Mode Mobility group configuration mode.

Usage Guide You can enable active information exchange to reduce time cost of mobility when there are a very few STAs. However, enabling active information exchange may increase the workload of AC devices when there are many STAs.

Configuration Examples The following example enables active information exchange of the mobility group.

```
Ruijie# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Ruijie(config)#mobility-group mgroup_name
Ruijie(config-mobility)# mobility-fast
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

9.6 mobility-group

Use this command to add a mobility group and enter mobility group configuration. Use the **no** form or **default** form of this command to remove a mobility group.

mobility-group *group-name*

no mobility-group *group-name*

default mobility-group *group-name*

Parameter Description

Parameter	Description
group-name	Mobility group name containing up to 63 characters.

Defaults No mobility group is configured by default.

Command Mode Global configuration mode.

Usage Guide The mobility group must be created when AC mobility is performed.

Configuration Examples The following example creates a mobility group named **mgroup_name**:

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

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

9.7 mti-ping

Use this command to check the connectivity between mobility members.

mti-ping (*ip-address* | *ipv6-address*)

Parameter Description

Parameter	Description
ip-address	The format is A.B.C.D. The parameter indicates the IP address of the

	destination AC to be pinged. The format is A.B.C.D. The IP address is the loopback 0 interface address of the AC.
ipv6-address	IPv6 address of the destination AC to be pinged. The address is the IPv6 address of loopback 0 interface of the AC.

Defaults N/A

Command Mode Mobility group configuration mode.

Usage Guide You can use this command to check the tunnel connectivity between the mobility members.

Configuration Examples The AC with the IP address of 192.168.1.1 is a member of the same mobility group. Check whether the AC is reachable through the MTI.

```
Ruijie(config)#mobility-group my_group_name
Ruijie(config-mobility)#mti-ping 192.168.1.1
Sending 4, MTI packet to  192.168.1.1, timeout is 2 seconds:
!!!!
Success rate is 100 perc
```

The AC with the IP address of 2001::1 is a member of the same mobility group. Check whether the AC is reachable through the MTI.

```
Ruijie(config)#mobility-group my group name
Ruijie(config-bobility)#mit-oing 2001::1
Sending 4, MTI packet to 2001::1, timeout is 2 seconds:
!!!!
Success rate is 100 perc
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

9.8 roaming logging rate-limit

Use this command to configure the maximum number of roaming syslogs displayed per second. Use the **no** or **default** form of this command to restore the default setting.

roaming logging rate-limit *limit-num*

no roaming logging rate-limit

default roaming logging rate-limit

Parameter Description

Parameter	Description

limit-num	The maximum number of roaming syslogs displayed per second. The range is from 1 to 10,000.

Defaults By default, the maximum number of roaming syslogs displayed per second is 5.

Command Mode Global configuration mode.

Usage Guide N/A

Configuration Examples The following example configures the maximum number of roaming syslogs displayed per second to 100.

```
Ruijie(config)# roaming logging rate-limit 100
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

9.9 roaming support wlan

Use this command to allow or deny STA roaming within the target WLAN. Use the **no** or **default** form of this command to restore the default setting.

No roaming support wlan *wlan-id*

roaming support wlan *wlan-id*

default roaming support wlan *wlan-id*

****

Parameter Description

Parameter	Description
wlan-id	The target WLAN, in the range from 1 to 4094.

Defaults STA roaming is allowed by default.

Command Mode Global configuration mode

Usage Guide N/A

Configuration Examples The following example denies STA roaming within WLAN1.

```
Ruijie(config)# no roaming support wlan 1
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

9.10 show mobility statistics

Use this command to display the roaming statistics.

show mobility statistics

Parameter Description

Parameter	Description
N/A	N/A

Defaults N/A

Command Mode Privileged EXEC mode, global configuration mode and mobility group configuration mode.

Usage Guide N/A

Configuration Examples The following example displays information about roaming statistics.

```
Ruijie#show mobility statistics
Global Mobility Statistics
Rx Errors.....................................0
Tx Errors.....................................0
Response Retransmitted........................0
Handoff Requests Received.....................0
Handoff End Requests Received.................0
State Transitions Disallowed..................0
Resource Unavailable..........................0

Mobility Initiator Statistics
Handoff Request Sent..........................0
Handoff Reply Received........................0
Handoff As Local Received.....................0
Handoff As Foreign Received...................0
Anchor Request Sent...........................0
Anchor Deny Received..........................0
Anchor Grant Received.........................0
Anchor Transfer Received......................0
```

```
Mobility Responder Statistic
Handoff Request Ignored.....................0
Handoff Request Dropped.....................0
Handoff Request Deny........................0
Client Handoff As Local.....................0
Client Handoff As Foreign...................0
Anchor Request Received.....................0
Anchor Requests Deny........................0
Anchor Requests Granted.....................0
Anchor Transfered...........................0
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

9.11 show mobility status

Use this command to display the status of the specified mobility group.

show mobility status *group-name*

Parameter Description

Parameter	Description
group-name	Mobility group name.

Defaults N/A

Command Mode Privileged EXEC mode, global configuration mode and mobility group configuration mode.

Usage Guide N/A

Configuration Examples The following example displays the status of a mobility group named *mgroup name*.

```
Ruijie# show mobility status mgroup_name
Mobility Group mgroup_name
Mobility Keepalive Interval..................... 10
Mobility Keepalive Count........................ 3
Mobility Group Status........................... normal

Mobility Members:
```

```
IP Address        Client/Server   Data Tunnel    Ctrl Tunnel
192.168.1.2       Client          OK             OK
Mobility List Members:
IP Address        Client/Server   Data Tunnel    Ctrl Tunnel
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

9.12 show mobility summary

Use this command to display the summary of mobility groups.

show mobility summary

Parameter Description

Parameter	Description
N/A	N/A

Defaults N/A

Command Mode Privileged EXEC mode, global configuration mode and mobility group configuration mode.

Usage Guide N/A

Configuration Examples The following example displays the summary of mobility groups.

```
Ruijie# show mobility summary
Mobility Group mgroup_name
Mobility Keepalive Interval..................... 10
Mobility Keepalive Count........................ 3
Mobility Group Status........................... normal
Mobility Members:
IP Address        Client/Server   Data Tunnel    Ctrl Tunnel
192.168.1.2       Client          OK             OK
Mobility List Members:
IP Address        Client/Server   Data Tunnel    Ctrl Tunnel

Mobility Group mgroup_name2
Mobility Keepalive Interval..................... 10
Mobility Keepalive Count........................ 3
```

```
Mobility Group Status.......................... normal
Mobility Members:
IP Address        Client/Server   Data Tunnel    Ctrl Tunnel
Mobility List Members:
IP Address        Client/Server   Data Tunnel    Ctrl Tunnel
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

9.13 show mobility user

Use this command to display the information about mobility users.

show mobility user [*mac*]

Parameter Description

Parameter	Description
mac	Specifies the MAC address of the mobility user. This parameter is optional.

Defaults N/A

Command Mode Privileged EXEC mode, global configuration mode and mobility group configuration mode.

Usage Guide N/A

Configuration Examples The following example displays information about the specified STA.

```
Ruijie# show mobility user 00:26:0c:ef:6d:12
MAC: 0026.0cef.6d12
IPv4-Address: 20.0.0.2
IPv6-Address: 2001::2
WLAN: 1
TYPE: LRC
ROC-AC: N/A
ROC-AP: 004c.0cef.6d11
ROC-VLAN: 2
RIC-AC: N/A
RIC-AP: 004c.0cef.6d12
```

```
RIC-VLAN: 3
```

The following example displays information about all STAs.

```
Ruijie# show mobility user
STA-MAC            IPv4-Address    IPv6-Address        WLAN   TYPE   ROC-VLAN
RIC-VLAN
--------------    -----------    -------------        ----   ----   --------
--------
0026.0cef.6d12   20.0.0.2     N/A              1     LRC    2       2
0040.0cef.6d33   20.0.0.5     N/A              2     RIC    3       3
0040.0cef.6d44   20.0.0.6     N/A              3     ROC    2       4
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

9.14 show mobility user roam-track

Use this command to display the information of mobility user track.

show mobility user roam-track *mac*

Parameter Description

Parameter	Description
mac	Specifies the MAC address of the mobility user.

Defaults N/A

Command Mode Privileged EXEC mode, global configuration mode, mobility group configuration mode.

Usage Guide N/A

Configuration Examples The following example displays the track information of mobility user d85d.4c7e.d4c0.

```
Ruijie#show mobility user roam-track d85d.4c7e.d4c0
------ --------------- ---------------- --------------------
ID      AC-Info         AP-Info      Online-time(d:h:m:s)
------ --------------- ---------------- --------------------
1     -LOCAL-         001a.a94e.d41E/1  0:00:00:12
2     192.168.170.12   001a.a94e.d40d/1  0:00:00:24
3     -LOCAL-         001a.a94e.d42A/1  0:00:00:24
```

Related

Command	Description

Commands

N/A	N/A

Platform Description N/A

WLAN RF Commands

1 RRM Commands

1.1 advanced 802.11 channel

Use this command to add or delete a channel for the DCA algorithm.

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

advanced { **802.11a** | **802.11b** } **channel** { **add** | **delete** } *channel-id*

no advanced { **802.11a** | **802.11b** } **channel** { **add** | **delete** }

default advanced { **802.11a** | **802.11b** } **channel** { **add | delete** }

Parameter Description

Parameter	Description
802.11a	A 5GHz network.
802.11b	A 2.4GHz network.
add	Adds a channel for the DCA algorithm.
delete	Deletes a channel for the DCA algorithm.
channel-id	Channel number. The range for a 5GHz network is as follows: 36, 40, 44, 48, 52, 56, 60, 64, 100, 104, 108, 112, 116, 120, 124, 128, 132, 136, 140, 149, 153, 157, 161, and 165. The range for a 2.4GHz network is as follows: 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, and 13.

Defaults See the Limitation and Specifications manual.

Command Mode Global configuration mode

Usage Guide The command can be used to add or delete only one channel value. If the subscriber knows that a radio client cannot support a specific channel number, the subscriber can modify the scope of optional channels in the environment by running this command.

Configuration Examples The following example adds channel 4 and channel 8 for the DCA algorithm on a 2.4GHz network.

```
Ruijie(config)# advanced 802.11b channel add 4
Ruijie(config)# advanced 802.11b channel add 8
```

The following example deletes channel 6 for the DCA algorithm on a 2.4GHz network.

```
Ruijie(config)# advanced 802.11b channel delete 6
```

Related Commands

Command	Description
advanced 802.11 channel dca interval	Configures the interval of the DCA algorithm.
show advanced 802.11 channel	Displays the related information of the DCA

	algorithm.

Platform Description N/A

1.2 advanced 802.11 channel clients

Use this command to configure the client number threshold for the DCA algorithm.

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

advanced { **802.11a** | **802.11b** } **channel clients** *clients-num*

no advanced { **802.11a** | **802.11b** } **channel clients**

default advanced { **802.11a** | **802.11b** } **channel clients**

Parameter Description

Parameter	Description
802.11a	A 5 GHz network.
802.11b	A 2.4 GHz network.
clients-num	Sets the client number threshold, in the range from 0 to 128. When the client number in a frequency band exceeds the client number threshold on the AP, the channel remains unchanged to prevent clients from getting offline.

Defaults The default is 0, that is, the channel remains unchanged when any client is associated with AP.

Command Mode Global configuration mode

Usage Guide N/A

Configuration Examples The following example sets the client number threshold for the DCA algorithm on a 2.4 GHz network to 5.

```
Ruijie(config)#advanced 802.11b channel clients 5
```

Related Commands

Command	Description
show advanced { 802.11a | 802.11b } channel	Displays the current client threshold for the DCA algorithm.

Platform Description N/A

1.3 advanced 802.11 channel countered-switch

Use this command to configure the AP to switch channels through the DCA algorithm when it is

contained.

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

advanced { **802.11a** | **802.11b** } **channel countered-switch** { **enable** | **disable** }

no advanced { **802.11a** | **802.11b** } **channel countered-switch**

default advanced { **802.11a** | **802.11b** } **channel countered-switch**

Parameter Description

Parameter	Description
802.11a	A 5 GHz network.
802.11b	A 2.4 GHz network.
enable	Enables the DCA channel switch when AP is contained.
disable	Disables the DCA channel switch when AP is contained.

Defaults This function is disabled by default.

Command Mode Global configuration mode

Usage Guide N/A

Configuration Examples The following example enables the AP to switch channels through the DCA algorithm when it is contained.

```
Ruijie(config)#advanced 802.11b channel countered-switch enable
```

Related Commands

Command	Description
**show advanced { 802.11a	802.11b } channel**	Checks whether the DCA channel switch is enabled.

Platform Description N/A

1.4 advanced 802.11 channel dca anchor-time

Use this command to set the start time and duration for the DCA algorithm.

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

advanced { **802.11a** | **802.11b** } **channel dca anchor-time** *start-hour duration*

no advanced { **802.11a** | **802.11b** } **channel dca anchor-time**

default advanced { 802.11a | 802.11b } channel dca anchor-time

Parameter Description

Parameter	Description
802.11a	A 5GHz network.
802.11b	A 2.4GHz network.

start-hour	Sets the hour at which the DCA algorithm begins to run in a day, in the range from 0 to 23.
duration	The period during which the DCA algorithm runs consecutively, in the range from 1 to 24 in the unit of hours.

Defaults The default *start-hour* is 02:00, and the default *duration* is 2 hours, indicating that the DCA algorithm runs consecutively from 02:00 to 04:00.

Command Mode Global configuration mode

Usage Guide The command can be used to specify the start hour and duration of the DCA algorithm in a day. The start hour value is 0 to 23, indicating 00:00am to 11:00pm. The duration value ranges from 1 to 24. If *duration* is set to 24, it indicates that the DCA algorithm runs consecutively around the clock.

Configuration Examples The following example sets the start hour of the DCA algorithm on the 2.4GHz network to 08:00, and the duration to 4 hours.

```
Ruijie(config)# advanced 802.11b channel dca anchor-time 8 4
```

Related Commands

Command	Description
advanced 802.11 channel period	Specifies the running period of the DCA algorithm.
advanced 802.11 channel interval	Configures the interval of the DCA algorithm.
show advanced 802.11 channel	Displays the related information of the DCA algorithm.

Platform Description N/A

1.5 advanced 802.11 channel dca chan-width-11n

Use this command to configure the frequency band used by the DCA algorithm in an 802.11n network. Use the **no** or **default** form of the command to restore the default setting.

advanced { **802.11a** | **802.11b** } **channel dca chan-width-11n** { **20** | **40** }

no advanced { **802.11a** | **802.11b** } **channel dca chan-width-11n**

default advanced { **802.11a** | **802.11b** } **channel dca chan-width-11n**

Parameter Description

Parameter	Description
802.11a	A 5GHz network.
802.11b	A 2.4GHz network.
20	Configures the frequency band of 20 MHz for the channels in the

	DCA algorithm.
40	Configures the frequency band of 40 MHz for the channels in the DCA algorithm.

Defaults The default is 20 MHz.

Command Mode Global configuration mode

Usage Guide To use the frequency band of 40 MHz in an 802.11n network, run the **advanced 802.11{a | b} channel dca chan-width-11n** command. In addition, ensure that there are two consecutive channels (for example, 149 and 153) among the channels used by the DCA algorithm.

Configuration Examples The following example configures the frequency band used by the DCA algorithm in a 5GHz network to be 40 MHz.

```
Ruijie(config)#advanced 802.11a channel add 149
Ruijie(config)#advanced 802.11a channel add 153
Ruijie(config)#advanced 802.11a channel dca chan-width-11n 40
```

Related Commands

Command	Description
advanced 802.11 channel	Indicates the channels used for the DCA algorithm are added or deleted.
show advanced 802.11 channel	Displays the related information of the DCA algorithm.

Platform Description N/A

1.6 advanced 802.11 channel dca interval

Use this command to specify the running interval of the DCA algorithm. Use the **no** or **default** form of this command to restore the default setting.

advanced { **802.11a** | **802.11b** } **channel dca interval** *value*

no advanced { **802.11a** | **802.11b** } **channel dca interval**

default advanced { **802.11a** | **802.11b** } **channel dca interval**

Parameter Description

Parameter	Description
802.11a	A 5GHz network.
802.11b	A 2.4GHz network.
value	Configures the running interval of the DCA algorithm in the range from 3 to 1440 in the unit of minutes.

Defaults The default is 20 minutes.

Command Mode Global configuration mode

Usage Guide

The interval value here is also used as the running interval of the TPC algorithm.

Configuration Examples The following example configures the DCA algorithm in a 2.4GHz network to run once an hour.

```
Ruijie(config)# advanced 802.11b channel dca interval 60
```

Related Commands

Command	Description
advanced 802.11 channel period	Specifies the running period of the DCA algorithm.
advanced 802.11 channel dca anchor-time	Configures the time at which the DCA algorithm is enabled.
show advanced 802.11 channel	Displays the related information of the DCA algorithm.

Platform Description N/A

1.7 advanced 802.11 channel dca period

Use this command to specify the running period of the DCA algorithm. Use the **no** or **default** form of this command to restore the default setting.

advanced { **802.11a** | **802.11b** } **channel dca period** *day0-of-the-week* [**to** *day1-of-the-week*]

no advanced { **802.11a** | **802.11b** } **channel dca period**

default advanced { 802.11a | 802.11b } channel dca period

Parameter Description

Parameter	Description
802.11a	A 5GHz network.
802.11b	A 2.4GHz network.
day-of-the-week0	The day on which the DCA algorithm begins to run in a week. The valid value is as follows: {Sunday | Monday | Tuesday | Wednesday | Thursday | Friday | Saturday}
day-of-the-week1	The day on which the DCA algorithm stops running in a week. The valid value is as follows: {Sunday | Monday | Tuesday | Wednesday | Thursday | Friday | Saturday}

Defaults By default, the DCA algorithm runs all over the week (from Sunday through to Saturday).

Command Mode Global configuration mode

Usage Guide The command can be used to specify the running period of the DCA algorithm in a week. The command can be configured repeatedly, and the seven days of a week can be combined at will. If you use the default configurations, the DCA algorithm runs every day.

Configuration Examples The following example configures the running period of the DCA algorithm in the 2.4GHz network to Monday, Wednesday, and Friday.

```
Ruijie(config)# advanced 802.11b channel dca period Monday
Ruijie(config)# advanced 802.11b channel dca period Wednesday
Ruijie(config)# advanced 802.11b channel dca period Friday
```

The following example configures the running period of the DCA algorithm in the 2.4GHz network to Monday, Tuesday, Wednesday, Thursday, and Friday.

```
Ruijie(config)# advanced 802.11b channel dca period Monday to Friday
```

Related Commands

Command	Description
advanced 802.11 channel interval	Configures the interval of the DCA algorithm.
show advanced 802.11 channel	Displays the related information of the DCA algorithm.

Platform Description N/A

1.8 advanced 802.11 channel dca sensitivity

Use this command to specify the sensitivity of the DCA algorithm to the environmental changes when channel allocation is considered. Use the **no** or **default** form of this command to restore the default setting.

advanced { **802.11a** | **802.11b** } **channel dca sensitivity** { **low** | **medium** | **high** }

no advanced { **802.11a** | **802.11b** } **channel dca sensitivity**

default advanced { **802.11a** | **802.11b** } **channel dca sensitivity**

Parameter Description

Parameter	Description
802.11a	A 5GHz network.
802.11b	A 2.4GHz network.
low	Indicates that the DCA algorithm is of low sensitivity to the environmental changes.

medium	Indicates that the DCA algorithm is of medium sensitivity to the environmental changes.
high	Indicates that the DCA algorithm is of high sensitivity to the environmental changes.

Defaults The DCA algorithm is of medium sensitivity to the environmental changes by default.

Command Mode Global configuration mode

Usage Guide N/A

Configuration Examples The following example configures the DCA algorithm in a 2.4GHz network to be highly sensitive to the environmental changes.

```
Ruijie(config)# advanced 802.11b channel dca sensitivity high
```

Related Commands

Command	Description
show advanced 802.11 channel	Displays the related information of the DCA algorithm.

Platform Description N/A

1.9 advanced 802.11 channel foreign

Use this command to determine whether the external AP interference is considered or ignored when the DCA algorithm allocates channels. Use the **no** form of this command to delete the configuration. Use the **default** form of this command to restore the default setting.

advanced { **802.11a** | **802.11b** } **channel foreign** { **enable** | **disable** }

no advanced { **802.11a** | **802.11b** } **channel foreign**

default advanced { **802.11a** | **802.11b** } **channel foreign**

Parameter Description

Parameter	Description
802.11a	A 5GHz network.
802.11b	A 2.4GHz network.
enable	Indicates that the AP interference factor is considered by the DCA algorithm.
disable	Indicates that the AP interference factor is ignored by the DCA algorithm.

Defaults This function is enabled by default.

Command Mode Global configuration mode

Usage Guide N/A

Configuration Examples The following example configures the DCA algorithm in a 2.4GHz network to consider the AP interference factor.

```
Ruijie(config)# advanced 802.11b channel foreign enable
```

Related Commands

Command	Description
advanced 802.11 channel load	Determines whether the load factor is considered by the DCA algorithm.
advanced 802.11 channel noise	Determines whether the noise factor is considered by the DCA algorithm.
show advanced 802.11 channel	Displays the related information of the DCA algorithm.

Platform Description N/A

1.10 advanced 802.11 channel global

Use this command to configure the running mode of the DCA algorithm. Use the **no** or **default** form of this command to restore the default setting.

advanced { **802.11a** | **802.11b** } **channel global** { **auto** | **once** | **off** }

no advanced { **802.11a** | **802.11b** } **channel global**

default advanced { **802.11a** | **802.11b** } **channel global**

Parameter Description

Parameter	Description
802.11a	A 5GHz network.
802.11b	A 2.4GHz network.
auto	Configures the running mode of the DCA algorithm as periodical.
once	Configures the running mode of the DCA algorithm as triggered.
off	Indicates that the DCA algorithm is disabled.

Defaults The running mode of the DCA algorithm is specified as periodical running by default.

Command Mode Global configuration mode

Usage Guide The DCA algorithm can be run in three modes: periodical, triggered, and disabled. The command can be used to modify the running mode of the DCA algorithm according to the needs of channel allocation. The DCA algorithm is run in triggered mode by default. When AP gents online or radio of the AP is enabled, the radio is triggered to adjust the channel. It will not change the AP's channel afterwards. After the DCA algorithm is configured to run in periodical mode, channel allocation is performed on all APs every 20 minutes by default.

Configuration Examples The following example disables the DCA algorithm in a 2.4GHz network.

```
Ruijie(config)# advanced 802.11b channel global off
```

Related Commands

Command	Description
show advanced 802.11 channel	Displays information related to the DCA algorithm.

Platform Description N/A

1.11 advanced 802.11 channel load

Use this command to determine whether the load factor is considered or ignored when the DCA algorithm allocates channels. Use the **no** or **default** form of this command to restore the default setting.

advanced { **802.11a** | **802.11b** } **channel load** { **enable** | **disable** }

no advanced { **802.11a** | **802.11b** } **channel load**

default advanced { **802.11a** | **802.11b** } **channel load**

Parameter Description

Parameter	Description
802.11a	A 5GHz network.
802.11b	A 2.4GHz network.
enable	Indicates the load factor is considered by the DCA algorithm.
disable	Indicates the load factor is ignored by the DCA algorithm.

Defaults This function is disabled by default.

Command Mode Global configuration mode

Usage Guide N/A

Configuration Examples The following example configures the DCA algorithm in a 2.4GHz network to consider the load factor.

```
Ruijie(config)# advanced 802.11b channel load enable
```

Related Commands

Command	Description
advanced 802.11 channel interference	Determines whether the interference factor is considered by the DCA algorithm.
advanced 802.11 channel noise	Determines whether the noise factor is considered by the DCA algorithm.
show advanced 802.11 channel	Displays the related information of the DCA algorithm.

Platform Description N/A

1.12 advanced 802.11 channel noise

Use this command to determine whether the ambient noise is considered or ignored when the DCA algorithm allocates channels. Use the **no** or **default** form of this command to restore the default setting.

advanced { **802.11a** | **802.11b** } **channel noise** { **enable** | **disable** }

no advanced { **802.11a** | **802.11b** } **channel noise**

default advanced { **802.11a** | **802.11b** } **channel noise**

Parameter Description

Parameter	Description
802.11a	A 5GHz network.
802.11b	A 2.4GHz network.
enable	Indicates the noise factor is considered by the DCA algorithm.
disable	Indicates the noise factor is ignored by the DCA algorithm.

Defaults This function is disabled by default.

Command Mode Global configuration mode

Usage Guide N/A

Configuration Examples The following example configures the DCA algorithm in a 2.4GHz network to consider the noise factor.

```
Ruijie(config)# advanced 802.11b channel noise enable
```

Related Commands

Command	Description
advanced 802.11 channel interference	Determines whether the interference factor is

	considered by the DCA algorithm.
advanced 802.11 channel load	Determines whether the load factor is considered by the DCA algorithm.
show advanced 802.11 channel	Displays the related information of the DCA algorithm.

Platform Description N/A

1.13 advanced 802.11 channel pkt-loss-rate-threshold

Use this command to configure the threshold of packet loss rate on the air interface for the DCA algorithm during channel allocation. Use the **no** or **default** form of this command to restore the default setting.

advanced { **802.11a** | **802.11b** } **channel pkt-loss-rate-threshold** *threshold*

no advanced { **802.11a** | **802.11b** } **channel pkt-loss-rate-threshold**

default advanced { **802.11a** | **802.11b** } **channel pkt-loss-rate-threshold**

Parameter Description

Parameter	Description
802.11a	A 5 GHz network.
802.11b	A 2.4 GHz network.
threshold	Sets the threshold of packet loss rate on the air interface, in the range from 0 to 100. When the packet loss rate in a frequency band exceeds the threshold, the AP switched to another channel through the DCA algorithm to avoid high packet loss rate. The range is from 0 to 100.

Defaults The default is 100, that is, the threshold of packet loss rate is not configured by default.

Command Mode Global configuration mode

Usage Guide N/A

Configuration Examples The following example sets the threshold of packet loss rate on the air interface for the DCA algorithm on a 2.4GHz network to 10%.

```
Ruijie(config)#advanced 802.11b channel pkt-loss-rate-threshold 10
```

Related Commands

Command	Description
show advanced { 802.11a | 802.11b } channel	Displays the threshold of packet loss rate on the air interface for the DCA algorithm.

Platform Description N/A

1.14 advanced 802.11 channel update

Use this command to enable the DCA algorithm once manually and select channels automatically through the DCA algorithm.

advanced { **802.11a** | **802.11b** } **channel update**

Parameter Description

Parameter	Description
802.11a	A 5GHz network.
802.11b	A 2.4GHz network.

Defaults N/A

Command Mode Global configuration mode

Usage Guide The command takes effect only when the running mode of the DCA algorithm is configured to **triggered**. When the running mode of the DCA algorithm is configured to **triggered**, you can run this command to enable the DCA algorithm once and the running time of the DCA algorithm is the next running period.

Configuration Examples The following example configures the running mode of the DCA algorithm in a 2.4GHz network to **once** and enables the DCA algorithm once.

```
Ruijie(config)# advanced 802.11b channel global once
Ruijie(config)# advanced 802.11b channel update
```

Related Commands

Command	Description
advanced 802.11 channel global	Configures the running mode of the DCA algorithm.
show advanced 802.11 channel	Displays the related information of the DCA algorithm.

Platform Description N/A

1.15 advanced 802.11 coverage

Use this command to enable or disable the blind spot detection and repair algorithm. Use the **no** form of this command to delete the configuration. Use the **default** form of this command to restore the

default setting.

advanced { **802.11a** | **802.11b** } **coverage** { **enable** | **disable** }

no advanced { 802.11a | 802.11b } coverage

default advanced { 802.11a | 802.11b } coverage

Parameter Description

Parameter	Description
802.11a	A 5GHz network.
802.11b	A 2.4GHz network.
enable	Indicates the blind spot detection and repair function is enabled.
disable	Indicates the blind spot detection and repair function is disabled.

Defaults This function is enabled by default.

Command Mode Global configuration mode

Usage Guide If the blind spot detection and repair algorithm is enabled, the radio AC judges whether there exists a weak-signal coverage area in the current environment according to the signal status of the mobile subscriber.

Configuration Examples The following example enables the blind spot detection and repair algorithm in a 2.4GHz network.

```
Ruijie(config)# advanced 802.11b coverage enable
```

Related Commands

Command	Description
advanced 802.11 coverage exception global	Sets the limit of subscriber failure rate in the blind spot detection algorithm.
advanced 802.11 coverage fail-rate	Sets the limit of packet failure rate in the blind spot detection algorithm.
advanced 802.11 coverage level global	Sets the limit of subscriber failure count in the blind spot detection algorithm.
advanced 802.11 coverage packet-count	Sets the limit of packet failure count in the blind spot detection algorithm.
advanced 802.11 coverage rssi-threshold	Sets the packet signal limit in the blind spot detection algorithm.
show advanced 802.11 coverage	Displays the related information of the blind detection algorithm.

Platform Description N/A

1.16 advanced 802.11 coverage exception global

Use this command to specify the limit of the subscriber failure rate in the blind spot detection and repair algorithm. Use the **no** or **default** form of this command to restore the default setting.

advanced { 802.11a | 802.11b } coverage exception global *percent*

no advanced { 802.11a | 802.11b } coverage exception global

default advanced { 802.11a | 802.11b } coverage exception global

Parameter Description

Parameter	Description
802.11a	A 5GHz network.
802.11b	A 2.4GHz network.
percent	Indicates the percentage of the failed subscribers in the range from 1% to 100%.

Defaults The default *percent* is 25%.

Command Mode Global configuration mode

Usage Guide If the strength of signals transmitted by a mobile subscriber is lower than the specified limit or if the count/rate of voice/data packets reaches the limit, the blind spot detection and repair algorithm considers the mobile subscriber to be a failed subscriber. In the running period of the blind spot detection and repair algorithm: If the subscriber failure count/rate reaches the specified limit, the blind spot detection and repair algorithm determines that there exists a blind spot in the current environment; if the transmit power does not reach the maximum level, the blind spot detection and repair algorithm increments the transmit power of the radio AP by one level.

Configuration Examples The following example configures the limit of subscriber failure rate in the blind spot detection and repair algorithm in a 2.4GHz network to 50%.

```
Ruijie(config)# advanced 802.11b coverage exception global 50
```

Related Commands

Command	Description
advanced 802.11 coverage	Enables or disables the blind spot detection and repair algorithm.
advanced 802.11 coverage fail-rate	Sets the limit of packet failure rate in the blind spot detection algorithm.
advanced 802.11 coverage level global	Sets the limit of subscriber failure count in the blind spot detection algorithm.
advanced 802.11 coverage packet-count	Sets the limit of packet failure count in the blind spot detection algorithm.
advanced 802.11 coverage rssi-threshold	Sets the packet signal limit in the blind spot

	detection algorithm.
show advanced 802.11 coverage	Displays the related information of the blind detection algorithm.

Platform Description N/A

1.17 advanced 802.11 coverage fail-rate

Use this command to specify the limit of data/voice packet failure rate in the blind spot detection and repair algorithm. Use the **no** or **default** form of this command to restore the default setting.
advanced { 802.11a | 802.11b } coverage { data | voice } fail-rate *percent*
no advanced { 802.11a | 802.11b } coverage { data | voice } fail-rate
default advanced { 802.11a | 802.11b } coverage { data | voice } fail-rate

Parameter Description

Parameter	Description
802.11a	A 5GHz network.
802.11b	A 2.4GHz network.
data	Specifies the limit of failure rate for data packets.
voice	Specifies the limit of failure rate for voice packets.
percent	Indicates the percentage of failure rate in the range from 1% to 100%.

Defaults The default is 20%.

Command Mode Global configuration mode

Usage Guide If the strength of signals transmitted by a mobile subscriber is lower than the limit or if the count/rate of voice/data packets reaches the specified limit, the blind spot detection and repair algorithm considers the mobile subscriber to be a failed subscriber. In the running period of the blind spot detection and repair algorithm: If the subscriber failure count/rate reaches the specified limit, the blind spot detection and repair algorithm determines that there exists a blind spot in the current environment; if the transmit power does not reach the maximum level, the blind spot detection and repair algorithm increments the transmit power of the radio AP by one level.

Configuration Examples The following example configures the limit of data packet failure rate in the blind spot detection and repair algorithm in a 2.4GHz network to 50%.

```
Ruijie(config)# advanced 802.11b coverage data fail-rate 50
```

The following example configures the limit of voice packet failure rate in the blind spot detection and repair algorithm in a 5GHz network to 30%.

```
Ruijie(config)# advanced 802.11a coverage voice fail-rate 30
```

Related Commands

Command	Description
advanced 802.11 coverage	Enables or disables the blind spot detection and repair algorithm.
advanced 802.11 coverage exception global	Sets the limit of subscriber failure rate in the blind spot detection algorithm.
advanced 802.11 coverage level global	Sets the limit of failed subscriber count in the blind spot detection algorithm.
advanced 802.11 coverage packet-count	Sets the limit of failed packet count in the blind spot detection algorithm.
advanced 802.11 coverage rssi-threshold	Sets the packet signal limit in the blind spot detection algorithm.
show advanced 802.11 coverage	Displays the related information of the blind detection algorithm.

Platform Description N/A

1.18 advanced 802.11 coverage level global

Use this command to specify the limit of subscriber failure count in the blind spot detection and repair algorithm. Use the **no** or **default** form of this command to restore the default setting.
advanced { 802.11a | 802.11b } coverage level global *clients-num*
no advanced { 802.11a | 802.11b } coverage level global
default advanced { 802.11a | 802.11b } coverage level global

Parameter Description

Parameter	Description
802.11a	A 5GHz network.
802.11b	A 2.4GHz network.
clients-num	Specifies the limit of the failed subscriber count in the rangefrom 1 to 75.

Defaults The default is 3.

Command Mode Global configuration mode

Usage Guide If the strength of signals transmitted by a mobile subscriber is lower than the limit or if the count/rate of voice/data packets reaches the specified limit, the blind spot detection and repair algorithm considers the mobile subscriber to be a failed subscriber. In the running period of the blind spot detection and repair algorithm: If the subscriber failure count/rate reaches the specified limit, the blind spot detection and repair algorithm determines that there exists a blind spot in the current

environment; if the transmit power does not reach the maximum level, the blind spot detection and repair algorithm increments the transmit power of the radio AP by one level.

Configuration Examples The following example configures the limit of failed subscriber count in the blind spot detection and repair algorithm in a 2.4GHz network to 10.

```
Ruijie(config)# advanced 802.11b coverage level global 10
```

Related Commands

Command	Description
advanced 802.11 coverage	Enable or disables the blind spot detection and repair algorithm.
advanced 802.11 coverage exception global	Sets the limit of subscriber failure rate in the blind spot detection algorithm.
advanced 802.11 coverage fail-rate	Sets the limit of packet failure rate in the blind spot detection algorithm.
advanced 802.11 coverage packet-count	Sets the limit of failed packet count in the blind spot detection algorithm.
advanced 802.11 coverage rssi-threshold	Sets the packet signal limit in the blind spot detection algorithm.
show advanced 802.11 coverage	Displays the related information of the blind detection algorithm.

Platform Description N/A

1.19 advanced 802.11 coverage packet-count

Use this command to specify the limit of data/voice packet failure count in the blind spot detection and repair algorithm. Use the **no** or **default** form of this command to restore the default setting.

advanced { 802.11a | 802.11b } coverage { date | voice } packet-count *packets*

no advanced { 802.11a | 802.11b } coverage { date | voice } packet-count

default advanced { 802.11a | 802.11b } coverage { date | voice } packet-count

Parameter Description

Parameter	Description
802.11a	A 5GHz network.
802.11b	A 2.4GHz network.
data	Specifies the limit of failure rate for data packets.
voice	Specifies the limit of failure rate for voice packets.
packets	Specifies the limit of failed packets in the range from 1 to 255.

Defaults The default is 10.

Command Mode Global configuration mode

Usage Guide If the strength of signals transmitted by a mobile subscriber is lower than the limit or if the count/rate of voice/data packets reaches the specified limit, the blind spot detection and repair algorithm considers the mobile subscriber to be a failed subscriber. In the running period of the blind spot detection and repair algorithm: If the subscriber failure count/rate reaches the specified limit, the blind spot detection and repair algorithm determines that there exists a blind spot in the current environment; if the transmit power does not reach the maximum level, the blind spot detection and repair algorithm increments the transmit power of the radio AP by one level.

Configuration Examples The following example configures the limit of failed data packet count in the blind spot detection and repair algorithm in a 2.4GHz network to 30.

```
Ruijie(config)# advanced 802.11b coverage data packet-count 30
```

Related Commands

Command	Description
advanced 802.11 coverage	Enables or disables the blind spot detection and repair algorithm.
advanced 802.11 coverage exception global	Sets the limit of subscriber failure rate in the blind spot detection algorithm.
advanced 802.11 coverage fail-rate	Sets the limit of packet failure rate in the blind spot detection algorithm.
advanced 802.11 coverage level global	Sets the limit of failed subscriber count in the blind spot detection algorithm.
advanced 802.11 coverage rssi-threshold	Sets the packet signal limit in the blind spot detection algorithm.
show advanced 802.11 coverage	Displays the related information of the blind detection algorithm.

Platform Description N/A

1.20 advanced 802.11 coverage profile

Use this command to specify the limit of SNR for a subscriber that the blind spot detection and repair algorithm considers to be at a blind spot. Use the **no** or **default** form of this command to restore the default setting.

advanced { 802.11a | 802.11b } coverage profile *value*

no advanced { 802.11a | 802.11b } coverage profile

default advanced { 802.11a | 802.11b } coverage profile

Parameter Description

Parameter	Description

802.11a	A 5GHz network.
802.11b	A 2.4GHz network.
value	Indicates the limit of SNR for the data packets received by a customer in the range from 1 to 30 in the unit of decibels.

Defaults In a 5 GHz network, the default is 16 decibels, and in a 2.4 GHz network, the default is 12 decibels.

Command Mode Global configuration mode

Usage Guide If the SNR of the data/voice packets transmitted by a mobile subscriber is lower than the specified threshold, the blind spot detection and repair algorithm considers the mobile subscriber to be a failed subscriber. In the running period of the blind spot detection and repair algorithm: If the subscriber failure count/rate reaches the specified limit, the blind spot detection and repair algorithm determines that there exists a blind spot in the current environment; if the transmit power does not reach the maximum level, the blind spot detection and repair algorithm increments the transmit power of the radio AP by one level.

Configuration Examples The following example configures the limit of SNR for a subscriber in the blind spot detection and repair algorithm in a 2.4GHz network to 20 decibels.

```
Ruijie(config)# advanced 802.11b coverage profile 20
```

Related Commands

Command	Description
advanced 802.11 coverage	Enables or disables the blind spot detection and repair algorithm.
advanced 802.11 coverage exception global	Sets the limit of subscriber failure rate in the blind spot detection algorithm.
advanced 802.11 coverage fail-rate	Sets the limit of packet failure rate in the blind spot detection algorithm.
advanced 802.11 coverage level global	Sets the limit of failed subscriber count in the blind spot detection algorithm.
advanced 802.11 coverage packet-count	Sets the limit of failed packet count in the blind spot detection algorithm.
advanced 802.11 coverage rssi-threshold	Sets the packet signal limit in the blind spot detection algorithm.

Platform Description N/A

1.21 advanced 802.11 coverage rssi-threshold

Use this command to specify the limit of RSSI for the data/voice packets in the blind spot detection

and repair algorithm. Use the **no** or **default** form of this command to restore the default setting.

advanced { 802.11a | 802.11b } coverage { data | voice } rssi-threshold *value*

no advanced { 802.11a | 802.11b } coverage { data | voice } rssi-threshold

default advanced { 802.11a | 802.11b } coverage { data | voice } rssi-threshold

Parameter Description

Parameter	Description
802.11a	A 5GHz network.
802.11b	A 2.4GHz network.
data	Specifies the limit of RSSI for data packets.
voice	Specifies the limit of RSSI for voice packets.
value	Specifies the limit of RSSI in the range from -90 to -60 in the unit of dBm.

Defaults

The default for data packets is -80 dBm.

The default for voice packets is -75 dBm.

Command Mode

Global configuration mode

Usage Guide

If the strength of signals transmitted by a mobile subscriber is lower than the limit or if the count/rate of voice/data packets reaches the specified limit, the blind spot detection and repair algorithm considers the mobile subscriber to be a failed subscriber. In the running period of the blind spot detection and repair algorithm: If the subscriber failure count/rate reaches the specified limit, the blind spot detection and repair algorithm determines that there exists a blind spot in the current environment; if the transmit power does not reach the maximum level, the blind spot detection and repair algorithm increments the transmit power of the radio AP by one level.

The specified limit of RSSI is used to analyze whether there exists a blind spot. When the RSSI value for the received data/voice packets is lower than the specified limit, there may exist a potential blind spot.

Configuration Examples

The following example configures the limit of RSSI for data packets in the blind spot detection and repair algorithm in a 2.4GHz network to -75 dBm.

```
Ruijie(config)# advanced 802.11b coverage data rssi-threshold -75
```

Related Commands

Command	Description
advanced 802.11 coverage	Enables or disables the blind spot detection and repair algorithm.
advanced 802.11 coverage exception global	Sets the limit of subscriber failure rate in the blind spot detection algorithm.
advanced 802.11 coverage fail-rate	Sets the limit of packet failure rate in the blind spot detection algorithm.

advanced 802.11 coverage level global	Sets the limit of failed subscriber count in the blind spot detection algorithm.
advanced 802.11 coverage packet-count	Sets the limit of failed packet count in the blind spot detection algorithm.
show advanced 802.11 coverage	Displays the related information of the blind detection algorithm.

Platform Description N/A

1.22 advanced 802.11 factory

Use this command to restore all RRM configurations to the default settings.

advanced { 802.11a | 802.11b } factory

Parameter Description

Parameter	Description
802.11a	Restores the configurations of a 5GHz network.
802.11b	Restores the configurations of a 2.4GHz network.

Defaults N/A

Command Mode Global configuration mode

Usage Guide N/A

Configuration Examples The following example restores all RRM configurations of a 2.4GHz network to the default values.

```
Ruijie(config)# advanced 802.11b factory
```

Related Commands

Command	Description
show advanced 802.11 channel	Displays the related information of the DCA algorithm.
show advanced 802.11 coverage	Displays the related information of the blind spot detection and repair algorithm.
show advanced 802.11 logging	Displays the related information of the RRM log.
show advanced 802.11 monitor	Displays the related information of RRM monitoring.
show advanced 802.11 profile global	Displays the related information of the RRM limit.
show advanced 802.11 txpower	Displays the related information of the TPC

	algorithm.

Platform Description N/A

1.23 advanced 802.11 group-leader

Use this command to configure the group leader of RRM, which is to manually specify the leader of the RF group for the current device. Use the **no** or **default** form of this command to restore the default setting.

advanced { 802.11a | 802.11b } group-leader *ip-address*

no advanced { 802.11a | 802.11b } group-leader

default advanced { 802.11a | 802.11b } group-leader

Parameter Description

Parameter	Description
802.11a	A 5 GHz network.
802.11b	A 2.4 GHz network.
ip-address	Configures the IP address of the RF group leader, which must be the IP address of loopback 0 interface on the group leader device.

Defaults The device itself is configured as the group leader by default.

Command Mode Global configuration mode

Usage Guide Use this command to configure the RF group leader. If the group leader is not configured, ACs will consider themselves as the group leader. The running of the RRM algorithm is managed by the group leader after it is configured.

Note that if another AC is configured as the group leader of the frequency range where the current device locates, you cannot add other ACs as members of the RF group on the device.

Configuration Examples The following example configures the RF group leader of a 2.4 GHz network as 1.1.1.1.

```
Ruijie(config)# advanced 802.11b group-leader 1.1.1.1
```

Related Commands

Command	Description
show advanced 802.11 group	Displays RF group information.
advanced 802.11 group-member	Configures RF group members.

Platform Description N/A

1.24 advanced 802.11 group-member

Use this command to configure RF group members of RRM, which is to manually add group member devices of the current AC. Use the **no** or **default** form of this command to restore the default setting.

advanced { 802.11a | 802.11b } group-member *ip-address*

no advanced { 802.11a | 802.11b } group-member

default advanced { 802.11a | 802.11b } group-member

Parameter Description

Parameter	Description
802.11a	A 5 GHz network.
802.11b	A 2.4 GHz network.
ip-address	IP address of the RF group member device, which must be the IP address of loopback 0 interface on the device.

Defaults No RF group member of RRM is configured by default.

Command Mode Global configuration mode

Usage Guide Use this command to configure the RF group member list. The AC member devices need to configure the device as the group leader and then form the same RF group after reaching a consensus.
Note that when an AC adds group member devices, which means the AC will perform the RRM group computing as the group leader. Therefore, it cannot configure other ACs as the group leader of itself.
Different group leaders and group members can be configured for 802.11a and 802.11b networks.

Configuration Examples The following example configures the RF group members of a 2.4 GHz network as 1.1.1.2 and 1.1.1.3 and the RF group leader of a 5 GHz network as 1.1.1.2.

```
Ruijie(config)# advanced 802.11b group-member 1.1.1.2
Ruijie(config)# advanced 802.11b group-member 1.1.1.3
```

Related Commands

Command	Description
show advanced 802.11 group	Displays RF group information.
advanced 802.11 group-leader	Configures the RF group leader.

Platform Description N/A

1.25 advanced 802.11 logging channel

Use this command to open/close the log about channel allocation. Use the **no** or **default** form of this command to restore the default setting.

advanced { 802.11a | 802.11b } logging channel { on | off }
no advanced { 802.11a | 802.11b } logging channel
default advanced { 802.11a | 802.11b } logging channel

Parameter Description

Parameter	Description
802.11a	A 5GHz network.
802.11b	A 2.4GHz network.
on	Indicates the log about channel allocation is opened.
off	Indicates the log about channel allocation is closed.

Defaults The log about channel allocation is closed by default.

Command Mode Global configuration mode

Usage Guide N/A

Configuration Examples The following example opens the log about channel allocation in a 2.4GHz network.

```
Ruijie(config)# advanced 802.11b logging channel on
```

Related Commands

Command	Description
advanced 802.11 channel global	Configures the running mode of the DCA algorithm.
show advanced 802.11 logging	Displays the on/off information of the log.

Platform Description N/A

1.26 advanced 802.11 logging coverage

Use this command to open/close the log about the limit of subscriber quantity. Use the **no** or **default** form of this command to restore the default setting.
advanced { 802.11a | 802.11b } logging coverage { on | off }
no advanced { 802.11a | 802.11b } logging coverage
default advanced { 802.11a | 802.11b } logging coverage

Parameter Description

Parameter	Description
802.11a	A 5GHz network.
802.11b	A 2.4GHz network.
on	Indicates the log about the limit of subscriber quantity is opened.

off	Indicates the log about the limit of subscriber quantity is closed.

Defaults The log about the limit of subscriber quantity is closed by default.

Command Mode Global configuration mode

Usage Guide N/A

Configuration Examples The following example opens the log about the limit of subscriber quantity in a 2.4GHz network.

```
Ruijie(config)# advanced 802.11b logging coverage on
```

Related Commands

Command	Description
advanced 802.11 profile clients	Configures the limit of subscriber quantity.
show advanced 802.11 logging	Displays the on/off information of the log.

Platform Description N/A

1.27 advanced 802.11 logging foreign

Use this command to open/close the log about the AP interference threshold-crossing report. Use the **no** or **default** form of this command to restore the default setting.

advanced { 802.11a | 802.11b } logging foreign { on | off }

no advanced { 802.11a | 802.11b } logging foreign

default advanced { 802.11a | 802.11b } logging foreign

Parameter Description

Parameter	Description
802.11a	A 5GHz network.
802.11b	A 2.4GHz network.
on	Indicates the log about the AP interference threshold-crossing report is opened.
off	Indicates the log about the AP interference threshold-crossing report is closed.

Defaults The log about the AP interference threshold-crossing report is closed by default.

Command Mode Global configuration mode

Usage Guide N/A

Configuration Examples The following example opens the log about the AP interference threshold-crossing report in a 2.4GHz network.

```
Ruijie(config)# advanced 802.11b logging foreign on
```

Related Commands

Command	Description
advanced 802.11 profile foreign	Configures the AP interference limit.
show advanced 802.11 logging	Displays the on/off information of the log.

Platform Description N/A

1.28 advanced 802.11 logging load

Use this command to open/close the log about the load threshold-crossing report. Use the **no** or **default** form of this command to restore the default setting.

advanced { 802.11a | 802.11b } logging load { on | off }

no advanced { 802.11a | 802.11b } logging load

default advanced { 802.11a | 802.11b } logging load

Parameter Description

Parameter	Description
802.11a	A 5GHz network.
802.11b	A 2.4GHz network.
on	Indicates the log about the load threshold-crossing report is opened.
off	Indicates the log about the load threshold-crossing report is closed.

Defaults The log about the load threshold-crossing report is closed by default.

Command Mode Global configuration mode

Usage Guide N/A

Configuration Examples The following example opens the log about the load threshold-crossing report in a 2.4GHz network.

```
Ruijie(config)# advanced 802.11b logging foreign on
```

Related Commands

Command	Description
advanced 802.11 profile utilization	Configures the load limit.
show advanced 802.11 logging	Displays the on/off information of the log.

Platform Description N/A

1.29 advanced 802.11 logging noise

Use this command to open/close the log about the channel noise threshold-crossing report. Use the **no** or **default** form of this command to restore the default setting.

advanced { 802.11a | 802.11b } logging noise { on | off }

no advanced { 802.11a | 802.11b } logging noise

default advanced { 802.11a | 802.11b } logging noise

Parameter Description

Parameter	Description
802.11a	A 5GHz network.
802.11b	A 2.4GHz network.
on	Indicates the log about the channel noise threshold-crossing report is opened.
off	Indicates the log about the channel noise threshold-crossing report is closed.

Defaults The log about the channel noise threshold-crossing report is closed by default.

Command Mode Global configuration mode

Usage Guide N/A

Configuration Examples The following example opens the log about the channel noise threshold-crossing report in a 2.4GHz network.

```
Ruijie(config)# advanced 802.11b logging foreign on
```

Related Commands

Command	Description
advanced 802.11 profile noise	Configures the channel noise limit.
show advanced 802.11 logging	Displays the on/off information of the log.

Platform Description N/A

1.30 advanced 802.11 logging performance

Use this command to open/close the log about the performance threshold-crossing report. Use the **no** or **default** form of this command to restore the default setting.

advanced { 802.11a | 802.11b } logging performance { on | off }
no advanced { 802.11a | 802.11b } logging performance
default advanced { 802.11a | 802.11b } logging performance

Parameter Description

Parameter	Description
802.11a	A 5GHz network.
802.11b	A 2.4GHz network.
on	Indicates the log about the performance threshold-crossing report is opened.
off	Indicates the log about the performance threshold-crossing report is closed.

Defaults The log about the performance threshold-crossing report is closed by default.

Command Mode Global configuration mode

Usage Guide N/A

Configuration Examples The following example opens the log about the performance threshold-crossing report in a 2.4GHz network.

```
Ruijie(config)# advanced 802.11b logging performance on
```

Related Commands

Command	Description
advanced 802.11 profile performance	Configures the performance limit.
show advanced 802.11 logging	Displays the on/off information of the log.

Platform Description N/A

1.31 advanced 802.11 logging txpower

Use this command to open/close the log about power allocation. Use the **no** or **default** form of this command to restore the default setting.
advanced { **802.11a** | **802.11b** } **logging txpower** { **on** | **off** }
no advanced { **802.11a** | **802.11b** } **logging txpower**
default advanced { **802.11a** | **802.11b** } **logging txpower**

Parameter Description

Parameter	Description
802.11a	A 5GHz network.

802.11b	A 2.4GHz network.
on	Indicates the log about power allocation is opened.
off	Indicates the log about power allocation is closed.

Defaults The log about power allocation is closed by default.

Command Mode Global configuration mode

Usage Guide N/A

Configuration Examples The following example opens the log about the power allocation event in a 2.4GHz network.

```
Ruijie(config)# advanced 802.11b logging txpower on
```

Related Commands

Command	Description
advanced 802.11 txpower global	Configures the running mode of the TPC algorithm.
show advanced 802.11 logging	Displays the on/off information of the log.

Platform Description N/A

1.32 advanced 802.11 monitor channel-list

Use this command to set the scope of monitored channels. Use the **no** or **default** form of this command to restore the default setting.

advanced { **802.11a** | **802.11b** } **monitor channel-list** { **all** | **country** | **dca** }

no advanced { **802.11a** | **802.11b** } **monitor channel-list**

default advanced { **802.11a** | **802.11b** } **monitor channel-list**

Parameter Description

Parameter	Description
802.11a	A 5GHz network.
802.11b	A 2.4GHz network.
all	Indicates all channels are monitored.
country	Indicates the channels with the specified country code are monitored.
dca	Indicates the channels used by the DCA algorithm are monitored.

Defaults The channels with the specified country code are monitored by default.

Command Mode Global configuration mode

Usage Guide The command can be used to set the list of channels to be monitored by the AP.
When you select **all**, the RRM monitors all channels including:
802.11a: 36, 40, 44, 48, 52, 56, 60, 64, 100, 104, 108, 112, 116, 120, 124, 128, 132, 136, 140, 149, 153, 157, 161, and 165.
802.11b/g: 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, and 13.

Configuration Examples The following example only monitors the channels used by the DCA algorithm in a 2.4GHz network.

```
Ruijie(config)# advanced 802.11b monitor channel-list dca
```

Related Commands

Command	Description
show advanced 802.11 monitor	Displays the monitoring-related information.

Platform Description N/A

1.33 advanced 802.11 monitor coverage

Use this command to set the interval of monitoring the subscriber information. Use the **no** or **default** form of this command to restore the interval to the default value.
advanced { **802.11a** | **802.11b** } **monitor coverage** *seconds*
no advanced { **802.11a** | **802.11b** } **monitor coverage**
default advanced { **802.11a** | **802.11b** } **monitor coverage**

Parameter Description

Parameter	Description
802.11a	A 5GHz network.
802.11b	A 2.4GHz network.
seconds	Indicates the monitoring interval in the range from 60 to 3,600 in the unit of seconds.

Defaults The default is 180 seconds.

Command Mode Global configuration mode

Usage Guide

The interval here is also the running period of the blind spot detection and repair algorithm.

Configuration Examples The following example configures the interval of monitoring the subscriber information in a 2.4GHz network to 300 seconds.

```
Ruijie(config)# advanced 802.11b monitor coverage 300
```

Related Commands

Command	Description
show advanced 802.11 monitor	Displays the monitoring-related information.

Platform Description N/A

1.34 advanced 802.11 monitor load

Use this command to set the interval of monitoring the load information. Use the **no** or **default** form of this command to restore the default setting.

advanced { **802.11a** | **802.11b** } **monitor load** *seconds*

no advanced { **802.11a** | **802.11b** } **monitor load**

default advanced { **802.11a** | **802.11b** } **monitor load**

Parameter Description

Parameter	Description
802.11a	A 5GHz network.
802.11b	A 2.4GHz network.
seconds	Indicates the monitoring interval in the range from 60 to 3,600 in the unit of seconds.

Defaults The default is 60 seconds.

Command Mode Global configuration mode

Usage Guide N/A

Configuration Examples The following example configures the interval of monitoring the load information in a 2.4GHz network to 180 seconds.

```
Ruijie(config)# advanced 802.11b monitor load 180
```

Related Commands

Command	Description
show advanced 802.11 monitor	Displays the monitoring-related information.

Platform Description N/A

1.35 advanced 802.11 monitor mode

Use this command to enable/disable the monitoring function of the radio AP. Use the **no** or **default**

form of this command to restore the default setting.

advanced { 802.11a | 802.11b } monitor mode { enable | disable }

no advanced { 802.11a | 802.11b } monitor mode

default advanced { 802.11a | 802.11b } monitor mode

Parameter Description

Parameter	Description
802.11a	A 5GHz network.
802.11b	A 2.4GHz network.
enable	Indicates the monitoring function of the AP is enabled.
disable	Indicates the monitoring function of the AP is disabled.

Defaults The monitoring function of the AP is disabled by default.

Command Mode Global configuration mode

Usage Guide N/A

Configuration Examples The following example enables the monitoring function of the AP in a 2.4GHz network.

```
Ruijie(config)# advanced 802.11b monitor mode enable
```

Related Commands

Command	Description
show advanced 802.11 monitor	Displays the monitoring-related information.

Platform Description N/A

1.36 advanced 802.11 monitor noise

Use this command to set the interval of monitoring the noise information. Use the **no** or **default** form of this command to restore the interval to the default value.

advanced { 802.11a | 802.11b } monitor noise *seconds*

no advanced { 802.11a | 802.11b } monitor noise

default advanced { 802.11a | 802.11b } monitor noise

Parameter Description

Parameter	Description
802.11a	A 5GHz network.
802.11b	A 2.4GHz network.
seconds	Indicates the monitoring interval in the range from 60 to 3,600 in the unit of seconds.

Defaults The default is 180 seconds.

Command Mode Global configuration mode

Usage Guide None

Configuration Examples The following example configures the interval of monitoring the noise information in a 2.4GHz network to 300 seconds.

```
Ruijie(config)# advanced 802.11b monitor noise 300
```

Related Commands

Command	Description
show advanced 802.11 monitor	Displays the monitoring-related information.

Platform Description N/A

1.37 advanced 802.11 monitor signal

Use this command to set the interval at which the AP monitors the environmental signals. Use the **no** or **default** form of this command to restore the interval to the default value.

advanced { 802.11a | 802.11b } monitor signal *seconds*

no advanced { 802.11a | 802.11b } monitor signal

default advanced { 802.11a | 802.11b } monitor signal

Parameter Description

Parameter	Description
802.11a	A 5GHz network.
802.11b	A 2.4GHz network.
seconds	Indicates the monitoring interval in the range from 60 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 configures the interval of monitoring the environmental signals in a 2.4GHz network to 120 seconds.

```
Ruijie(config)# advanced 802.11b monitor signal 120
```

Related Commands

Command	Description
show advanced 802.11 monitor	Displays the monitoring-related information.

Platform Description N/A

1.38 advanced 802.11 profile clients

Use this command to configure the maximum number of subscribers associated with the radio AP in the global configuration mode. Use the **no** or **default** form of this command to restore the default setting.
advanced { **802.11a** | **802.11b** } **profile clients** { **global** | *ap-name* } *clients-num*
no advanced { **802.11a | 802.11b** } **profile clients** { **global |** *ap-name* }
default advanced { **802.11a** | **802.11b** } **profile clients** { **global** | *ap-name* }

Use this command to configure the maximum number of subscribers associated with the radio AP in the AP configuration mode. Use the **no** or **default** form of this command to restore the default setting.
advanced { **802.11a** | **802.11b** } **profile clients** *clients-num*
no advanced { 802.11a | 802.11b } profile clients
default advanced { **802.11a** | **802.11b** } **profile clients**

Parameter Description

Parameter	Description
global	Specifies the limit of subscriber quantity for all APs.
ap-name	Specifies the limit of subscriber quantity for a specific AP, and this parameter is not necessary in the AP configuration mode.
802.11a	A 5GHz network.
802.11b	A 2.4GHz network.
clients-num	Specifies the limit of subscriber quantity in the range from 1 to 128.

Defaults The default is 32.

Command Mode Global configuration mode/AP configuration mode

Usage Guide When configuring the limit of subscriber quantity for a specific AP, the configured parameters will be saved in the template file of AP configuration. You can view the parameters configured during the AP is running by the how ap-config running command.

Configuration Examples The following example configures the limit of subscriber quantity for all APs in a 2.4GHz network to 20.

```
Ruijie(config)# advanced 802.11b profile clients global 20
```

The following example configures the limit of subscriber quantity for an AP named ap2 in a 2.4GHz network to 25.

```
Ruijie(config)#ap-config ap2
Ruijie(config-ap)# advanced 802.11b profile clients 25
```

Related Commands

Command	Description
show advanced 802.11 profile	Displays the limit-related information.

Platform Description N/A

1.39 advanced 802.11 profile foreign

Use this command to configure the AP interference limit in the global configuration mode. Use the **no** or **default** form of this command to restore the default setting.
advanced { **802.11a** | **802.11b** } **profile foreign** { **global** | *ap-name* } *percent*
no advanced { **802.11a** | **802.11b** } **profile foreign** { **global** | *ap-name* }
default advanced { **802.11a** | **802.11b** } **profile foreign** { **global** | *ap-name* }

Use this command to configure the AP interference limit in the AP configuration mode. Use the **no** or **default** form of this command to restore the default setting.
advanced { **802.11a** | **802.11b** } **profile foreign** *percent*
no advanced { **802.11a** | **802.11b** } **profile foreign**
default advanced { **802.11a** | **802.11b** } **profile foreign**

Parameter Description

Parameter	Description
802.11a	A 5GHz network.
802.11b	A 2.4GHz network.
global	Specifies the interference limit for all APs in the global configuration mode.
ap-name	Specifies the interference limit for a specific AP in the global configuration mode, and this parameter is optional in the AP configuration mode.
percent	Indicates the percentage of interference in the range from 1% to 100%.

Defaults The default is 60%.

Command Mode Global configuration mode/AP configuration mode

Usage Guide When configuring the interference limit for a specific AP, the configured parameters will be saved in the template file of AP configuration.

Configuration Examples The following example sets the interference limit for all APs in a 2.4GHz network to 30%.

```
Ruijie(config)# advanced 802.11b profile foreign global 30
```

The following example sets the interference limit for an AP named **ap2** in a 2.4GHz network to 50%.

```
Ruijie(config)# ap-config ap2
Ruijie(config-ap)# advanced 802.11b profile interference 50
```

Related Commands

Command	Description
show advanced 802.11 profile	Displays the limit-related information.

Platform Description N/A

1.40 advanced 802.11 profile noise

Use this command to configure the channel noise limit in the global configuration mode. Use the **no** or **default** form of this command to restore the default setting.
advanced { **802.11a** | **802.11b** } **profile noise** { **global** | *ap-name* } *value*
no advanced { **802.11a** | **802.11b** } **profile noise** { **global** | *ap-name* }
default advanced { **802.11a** | **802.11b** } **profile noise** { **global** | *ap-name* }

Use this command to configure the channel noise limit in the AP configuration mode. Use the **no** or **default** form of this command to restore the default setting.
advanced { **802.11a** | **802.11b** } **profile noise** *value*
no advanced { **802.11a** | **802.11b** } **profile noise**
default advanced { 802.11a | 802.11b } profile noise

Parameter Description

Parameter	Description
802.11a	A 5GHz network.
802.11b	A 2.4GHz network.
global	Specifies the limit of channel noise for all APs in the global configuration mode.
ap-name	Specifies the limit of channel noise for a specific AP in the global configuration mode, and this parameter is not necessary in the AP configuration mode.
value	Indicates the limit of channel noise in the range from -127 to 0 in the unit of dBm.

Defaults The default is -70 dBm.

Command Mode Global configuration mode/AP configuration mode

Usage Guide When configuring the limit of channel noise for a specific AP, the configured parameters will be saved in the template file of AP configuration. You can view the parameters when AP is running by running the **show ap-config running** command.

Configuration Examples The following example configures the limit of channel noise for all APs in a 2.4GHz network to -80 dBm.

```
Ruijie(config)# advanced 802.11b profile noise global -80
```

The following example configures the limit of channel noise for an AP named ap2 in a 2.4GHz network to -65 dBm.

```
Ruijie(config)# ap-config ap2
Ruijie(config-ap)# advanced 802.11b profile noise -65
```

Related Commands

Command	Description
show advanced 802.11 profile	Displays the limit-related information.

Platform Description

1.41 advanced 802.11 profile throughput

Use this command to configure the limit of data throughput on the AP in the global configuration mode. Use the **no** or **default** form of this command to restore the default setting.
advanced { **802.11a** | **802.11b** } **profile throughput** { **global** | *ap-name* } *value*
no advanced { **802.11a** | **802.11b** } **profile throughput** { **global** | *ap-name* }
default advanced { **802.11a** | **802.11b** } **profile throughput** { **global** | *ap-name* }

Use this command to configure the limit of data throughput on the AP in the AP configuration mode. Use the **no** or **default** form of this command to restore the default setting.
advanced { **802.11a** | **802.11b** } **profile throughput** *value*
no advanced { **802.11a** | **802.11b** } **profile throughput**
default advanced { **802.11a** | **802.11b** } **profile throughput**

Parameter Description

Parameter	Description
802.11a	A 5GHz network.
802.11b	A 2.4GHz network.
global	Specifies the throughput limit for all APs in the global configuration mode.
ap-name	Specifies the throughput limit for a specific AP in the global

	configuration mode and this parameter is not necessary in the AP configuration mode.
value	Specifies the throughput limit in the range from 1,000 to 1,000,000,000 in the unit of bps.

Defaults The default is 150,000,000 Bps.

Command Mode Global configuration mode/AP configuration mode

Usage Guide When configuring the throughout limit for a specific AP, the configured parameters will be saved in the template file of AP configuration. You can view the parameters when AP is running by running the **show ap-config running** command.

Configuration Examples The following example configures the throughput limit for all APs in a 2.4GHz network to 10,000.

```
Ruijie(config)# advanced 802.11b profile throughput global 10000
```

The following example configures the throughput limit for an AP named **ap2** in a 2.4GHz network to 20,000,000.

```
Ruijie(config)# ap-config ap2
Ruijie(config-ap)# advanced 802.11b profile throughput 20000000
```

Related Commands

Command	Description
show advanced 802.11 profile	Displays the limit-related information.

Platform Description

1.42 advanced 802.11 profile utilization

Use this command to configure the limit of AP utilization rate in the global configuration mode. Use the **no** or **default** form of this command to restore the default setting.
advanced { **802.11a** | **802.11b** } **profile utilization** { **global** | *ap-name* } *percent*
no advanced { **802.11a** | **802.11b** } **profile utilization** { **global** | *ap-name* }
default advanced { **802.11a** | **802.11b** } **profile utilization** { **global** | ap-name }

Use this command to configure the limit of AP utilization rate in the AP configuration mode. Use the **no** or **default** form of this command to restore the default setting.
advanced { **802.11a** | **802.11b** } **profile utilization** *percent*
no advanced { **802.11a** | **802.11b** } **profile utilization**
default advanced { **802.11a** | **802.11b** } **profile utilization**

Parameter

Parameter	Description

Description

802.11a	A 5GHz network.
802.11b	A 2.4GHz network.
global	Specifies the limit of utilization rate for all APs in the global configuration mode.
ap-name	Specifies the limit of utilization rate for a certain AP in the global configuration mode and this parameter is not necessary in the AP configuration mode.
percent	Indicates the utilization percentage in the range from 1% to 100%.

Defaults The default is 80%.

Command Mode Global configuration mode/AP configuration mode

Usage Guide When configuring the limit of utilization rate for a specific AP, the configured parameters will be saved in the template file of AP configuration. You can view the parameters when AP is running by running the **show ap-config running** command.

Configuration Examples The following example configures the utilization rate limit for all APs in a 2.4GHz network to 50%.

```
Ruijie(config)# advanced 802.11b profile utilization global 50
```

The following example configures the utilization rate limit for an AP named **ap2** in a 2.4GHz network to 30%.

```
Ruijie(config)#ap-config ap2
Ruijie(config-ap)# advanced 802.11b profile utilization 30
```

Related Commands

Command	Description
show advanced 802.11 profile	Displays the limit-related information.

Platform Description N/A

1.43 advanced 802.11 txpower co-channel

Use this command to configure the TPC algorithm to consider only the neighbor AP in the same channel. Use the **no** or **default** form of this command to restore the default setting.

advanced { **802.11a** | **802.11b** } **txpower co-channel** { **enable** | **disable** }

no advanced { **802.11a** | **802.11b** } **txpower co-channel**

default advanced { **802.11a** | **802.11b** } **txpower co-channel**

Parameter

Parameter	Description

Description

802.11a	A 5GHz network.
802.11b	A 2.4GHz network.
enable	Indicates that only the neighbor AP in the same channel is considered.
disable	Indicates that all neighbor APs are considered.

Defaults All neighbor APs are considered by default.

Command Mode Global configuration mode

Usage Guide N/A

Configuration Examples The following example configures the TPC algorithm in a 2.4GHz network to consider only the neighbor AP in the same channel.

```
Ruijie(config)#advanced 802.11b txpower co-channel enable
```

Platform Description N/A

1.44 advanced 802.11 txpower dtpc

Use this command to enable/disable the dynamic TPC algorithm. Use the **no** or **default** form of this command to restore the default setting.

advanced { **802.11a** | **802.11b** } **txpower dtpc** { **enable** | **disable** }

no advanced { 802.11a | 802.11b } txpower dtpc

default advanced { 802.11a | 802.11b } txpower dtpc

Parameter Description

Parameter	Description
802.11a	A 5GHz network.
802.11b	A 2.4GHz network.
enable	Indicates the dynamic TPC algorithm is enabled.
disable	Indicates the dynamic TPC algorithm is disabled.

Defaults The dynamic TPC algorithm is disabled by default.

Command Mode Global configuration mode

Usage Guide N/A

Configuration The following example enables the TPC algorithm in a 2.4GHz network.

Examples

```
Ruijie(config)# advanced 802.11b txpower dtpc enable
```

Related Commands

Command	Description
advanced 802.11 txpower global	Configures the running mode of the TPC algorithm.
show advanced 802.11 txpower	Displays the related information of the TPC algorithm.

Platform Description N/A

1.45 advanced 802.11 txpower global

Use this command to specify the running mode of the TPC algorithm. Use the **no** or **default** form of this command to restore the default setting.

advanced { **802.11a** | **802.11b** } **txpower global** { **auto** | **once** | *power-level* }

no advanced { 802.11a | 802.11b } txpower global

default advanced { 802.11a | 802.11b } txpower global

Parameter Description

Parameter	Description
802.11a	A 5GHz network.
802.11b	A 2.4GHz network.
auto	Specifies the running mode of the TPC algorithm as periodical running.
once	Specifies the running mode of the TPC algorithm as triggered running.
power-value	Disables the TPC algorithm and specify the power level (valid value: 1 to 8). The command takes effect only when the TPC algorithm is enabled.

Defaults The running mode of the TPC algorithm is specified as periodical running by default.

Command Mode Global configuration mode

Usage Guide The TPC algorithm can be run in three modes: periodical, triggered, and disabled. If the running mode of the TPC algorithm is set to **auto** or **on-demand**, the TPC algorithm has the opportunity to run only when the TPC algorithm is enabled by running the **advanced 802.11 txpower dtpc** command. If the running mode of the TPC algorithm is set to **triggered**, you can enable the TPC algorithm once by running the **advanced 802.11 txpower update** command. If the TPC algorithm is disabled, you can specify the power level for all APs by entering the power-value.

The following table lists the conversions between power levels and power values.

Power Level	Power Value (dBm)	Power Value (mW)
1	20	100
2	17	50
3	14	25
4	11	12.5
5	8	6.5
6	5	3.2
7	2	1.6
8	-1	0.8

Configuration Examples

The following example configures the running mode of the TPC algorithm in a 2.4GHz network to **trigger** and enables the TPC algorithm once.

```
Ruijie(config)# advanced 802.11b txpower global once
Ruijie(config)# advanced 802.11b txpower update
```

The following example disables the TPC algorithm in a 2.4GHz network, and specifies the power level for all APs as 1.

```
Ruijie(config)# advanced 802.11b txpower global 1
```

Related Commands

Command	Description
advanced 802.11 txpower dtpc	Enables the TPC algorithm.
advanced 802.11 txpower update	Enables the TPC algorithm once.
show advanced 802.11 txpower	Displays the related information of the TPC algorithm.

Platform Description

N/A

1.46 advanced 802.11 txpower threshold

Use this command to specify the RSSI limit for the third largest neighbor used by the TPC algorithm. Use the **no** or **default** form of this command to restore the default setting.

advanced { **802.11a** | **802.11b** } **txpower threshold** *value*

no advanced { 802.11a | 802.11b } txpower threshold

default advanced { 802.11a | 802.11b } txpower threshold

Parameter Description

Parameter	Description
802.11a	A 5GHz network.
802.11b	A 2.4GHz network.
value	Specifies the RSSI limit in the range from -90 to -50 in the unit of dBm.

Defaults The default is -60 dBm.

Command Mode Global configuration mode

Usage Guide When the RSSI value of the third largest neighbor of the AP exceeds the specified limit, the TPC algorithm adjusts the power level for the AP. Otherwise, the TPC algorithm restores the power level to the highest level. When the environmental interference is very high, you can specify the RSSI limit to a little smaller value so that the AP is more sensitive to the environmental interference.

Configuration Examples The following example configures the RSSI limit of the third largest neighbor used by the TPC algorithm in a 2.4GHz network to -65 dBm.

```
Ruijie(config)# advanced 802.11b txpower threshold -65
```

Related Commands

Command	Description
advanced 802.11 txpower dtpc	Enables the TPC algorithm.
advanced 802.11 txpower global	Configures the running mode of the TPC algorithm.
show advanced 802.11 txpower	Displays the related information of the TPC algorithm.

Platform Description N/A

1.47 advanced 802.11 txpower update

Use this command to enable the TPC algorithm once manually.

advanced { **802.11a** | **802.11b** } **txpower update**

Parameter Description

Parameter	Description
802.11a	A 5GHz network.
802.11b	A 2.4GHz network.

Defaults N/A

Command Mode Global configuration mode

Usage Guide When the running mode of the TPC algorithm is configured to **once**, you can run this command to enable the TPC algorithm once and the running time of the TPC algorithm is the next running period. The command takes effect only when the running mode of the TPC algorithm is configured to **once**.

Configuration Examples The following example configures the running mode of the TPC algorithm in a 2.4GHz network to **once** and enables the TPC algorithm once.

```
Ruijie(config)# advanced 802.11b txpower global once
Ruijie(config)# advanced 802.11b txpower update
```

Related Commands

Command	Description
advanced 802.11 txpower dtpc	Enables the TPC algorithm.
advanced 802.11 txpower global	Configures the running mode of the TPC algorithm.
show advanced 802.11 txpower	Displays the related information of the TPC algorithm.

Platform Description N/A

1.48 network rf-network-name

Use this command to configure the RF group name for an AC. Use the **no** or **default** form of this command to restore the default setting.

network rf-network-name *group-name*

no network rf-network-name

default network rf-network-name

Parameter Description

Parameter	Description
group-name	Indicates the RF group name for an AC.

Defaults The default is rf-network.

Command Mode Global configuration mode

Usage Guide The command can be used to add a radio AC to a RF group. The ACs configured with the same RF group name composes a global RF group, and implement the operations of the DCA and TPC algorithms cooperatively.

Configuration Examples The following example adds a radio AC to the RF group named rf-group.

```
Ruijie(config)# network rf-network-name rf-group
```

Related Commands

Command	Description
show advanced 802.11 channel	Displays the related information of the DCA algorithm.

Platform Description N/A

1.49 show advanced 802.11 channel

Use this command to display the related information of the DCA algorithm.

show advanced { **802.11a** | **802.11b** } **channel**

Parameter Description

Parameter	Description
802.11a	A 5GHz network.
802.11b	A 2.4GHz network.

Command Mode Privileged EXEC mode/Global configuration mode

Usage Guide N/A

Configuration Examples The following example displays the information on the DCA algorithm in a 2.4GHz network.

```
Ruijie# show advanced 802.11b channel
Automatic Channel Assignment
  Radio Type..................................... 802.11b
  Channel Assignment Mode........................ AUTO
  Channel Update Interval........................ 120 seconds
  Periodic Motion (Day of A Week)................ All days
  Anchor Time (Hour of The Day).................. 20
  The Duration of DCA (By Hour).................. 24
  Consider Foreign Factor........................ yes
  Consider Load Factor........................... no
  Consider Noise Factor.......................... no
  Switch Channel When Countered.................. disable
  Packet Loss Rate Threshold.....................100%
  Clients Threshold.............................. 0 client
  Channel Assignment Leader...................... 192.168.1.2
  Last Run....................................... 11 seconds ago
  DCA Sensitivity Level.......................... MEDIUM (15 dB)
  DCA 802.11n Channel Width...................... 20 MHz
  Auto-RF Allowed Channel List................... 1,6,11
  Auto-RF Unused Channel List.................... 2,3,4,5,7,8,9,10,12,13
```

The **show advanced 802.11 channel** command is used to display the information description table.

Field	Description

Channel Assignment Mode	Indicates the running mode of the DCA algorithm.
Channel Update Interval	Indicates the running interval of the DCA algorithm.
Anchor time (Hour of the day)	Indicates the time at which the DCA algorithm begins to run in a day.
Consider Foreign Factor	Specifies whether the AP interference factor is considered by the DCA algorithm.
Consider Load Factor	Specifies whether the load factor is considered by the DCA algorithm.
Consider Noise Factor	Specifies whether the channel noise factor is considered by the DCA algorithm.
Channel Assignment Leader	Indicates the MAC address of the leader of the RF group that implements the DCA algorithm.
Last Run	Indicates the last-running time of the DCA algorithm.
DCA Sensitivity Level	Indicates the sensitivity to the environment when the DCA algorithm considers channel allocation.
DCA 802.11n Channel Width	Indicates the bandwidth used by the DCA algorithm in a 5GHz network.
Auto-RF Allowed Channel List	Indicates the channel number allowed by the DCA algorithm.
Auto-RF Unused Channel List	Indicates the channel number barred by the DCA algorithm.

Related Commands

Command	Description
advanced 802.11 channel	Configures the DCA algorithm.
show advanced 802.11 group	Displays the RF group information.

Platform Description N/A

1.50 show advanced 802.11 coverage

Use this command to display the related information of the blind spot detection and repair algorithm.

show advanced { 802.11a | 802.11b } coverage

Parameter Description

Parameter	Description
802.11a	A 5GHz network.
802.11b	A 2.4GHz network.

Command Mode Privileged EXEC mode/Global configuration mode

Usage Guide N/A

Configuration Examples The following example displays the information on the blind spot detection and repair algorithm in a 2.4GHz network.

```
Ruijie# show advanced 802.11b coverage
Coverage Hole Detection
  Radio Type..................................... 802.11b
  802.11b Coverage Hole Detection Mode........... Enable
  802.11b Coverage Voice Packet Count............ 10 packets
  802.11b Coverage Voice Packet Percentage....... 20%
  802.11b Coverage Voice RSSI Threshold.......... -75  dBm
  802.11b Coverage Data Packet Count............. 10 packets
  802.11b Coverage Data Packet Percentage........ 20%
  802.11b Coverage Data RSSI Threshold........... -80  dBm
  802.11b Global Coverage Exception Level........ 25%
  802.11b Global Client Minimum Exception Level.. 3 clients
  802.11b Global Coverage Profile Value.......... 12  dB
```

The **show advanced 802.11 coverage** command is used to display the information description table.

Field	Description
Coverage Hole Detection Mode	Specifies whether the blind spot detection and repair algorithm is enabled.
Coverage Voice Packet Count	Specifies the limit of failed voice packet count in the blind spot detection and repair algorithm.
Coverage Voice Packet Percentage	Specifies the limit of failed voice packet percentage in the blind spot detection and repair algorithm.
Coverage Voice RSSI Threshold	Specifies the minimum RSSI value for the voice packets in the blind spot detection and repair algorithm.
Coverage Data Packet Count	Specifies the limit of failed data packet count in the blind spot detection and repair algorithm.
Coverage Data Packet Percentage	Specifies the limit of failed data packet percentage in the blind spot detection and repair algorithm.
Coverage Data RSSI Threshold	Specifies the minimum RSSI value for the data packets in the blind spot detection and repair algorithm.
Global Coverage Exception Level	Specifies the minimum failed subscriber percentage in the blind spot detection and repair algorithm.
Global Client Minimum Exception Level	Specifies the minimum failed subscriber count in the blind spot detection and repair algorithm.
Global Coverage Profile Value	Specifies the SNR threshold in the blind spot detection and repair algorithm, which is used to judge whether a subscriber is at a blind spot.

Related Commands

Command	Description
advanced 802.11 coverage	Configures the blind spot detection and repair

	algorithm.

Platform Description N/A

1.51 show advanced 802.11 group

Use this command to the display the RF group information of the RRM function.

show advanced { **802.11a** | **802.11b** } **group**

Parameter Description

Parameter	Description
802.11a	A 5GHz network.
802.11b	A 2.4GHz network.

Command Mode Privileged EXEC mode/Global configuration mode

Usage Guide N/A

Configuration Examples The following example displays the RF group information in a 2.4GHz network.

```
Ruijie# show advanced 802.11b group
RF Group Information
  Radio Type ..................................... 802.11b
  RF Group Name .................................. rf-network
  I'm leader ..................................... yes
  Group member ................................... 192.168.1.3 (disconnected)
  Last Run ....................................... 602 seconds ago
```

The **show advanced 802.11 group** command is used to display the information description table.

Field	Description
RF Group Name	Specifies the RF group name.
Group member	The current RF group member. Connect indicates that the group member is connected, while disconnect indicates that the group member is not connected.
I'm leader	Specifies whether the AC is the group leader.
Last Run	Specifies the last-running time of the RF group.

Related Commands

Command	Description
advanced 802.11 leader	Configures the RF group leader.
advanced 802.11 member	Configures the RF group member.
show advanced 802.11 channel	Displays information related to the DCA

	algorithm.
show advanced 802.11 txpower	Use this command to display the related information of the TPC algorithm.

Platform Description N/A

1.52 show advanced 802.11 logging

Use this command to display the on/off information of the RRM log.

show advanced { **802.11a** | **802.11b** } **logging**

Parameter Description

Parameter	Description
802.11a	A 5GHz network.
802.11b	A 2.4GHz network.

Command Mode Privileged EXEC mode/Global configuration mode

Usage Guide N/A

Configuration Examples The following example Display the on/off status of the RRM log in a 2.4GHz network.

```
Ruijie# show advanced 802.11b logging
RF Event and Performance Logging
  Radio Type..................................... 802.11b
  Channel Update Logging......................... Off
  TxPower Update Logging......................... Off
  Coverage Profile Logging....................... Off
  Foreign Profile Logging........................ Off
  Load Profile Logging........................... Off
  Noise Profile Logging.......................... Off
  Performance Profile Logging.................... Off
```

The **show advanced 802.11 logging** command is used to display the information description table.

Field	Description
Channel Update Logging	Indicates the switch of the log about channel modification performed by the DCA algorithm.
TxPower Update Logging	Indicates the switch of the log about power modification performed by the TPC algorithm.
Coverage Profile Logging	Indicates the switch of the log about the subscriber quantity threshold-crossing report.

Foreign Profile Logging	Indicates the switch of the log about the AP interference threshold-crossing report.
Load Profile Logging	Indicates the switch of the log about the load threshold-crossing report.
Noise Profile Logging	Indicates the switch of the log about the channel noise threshold-crossing report.
Performance Profile Logging	Indicates the switch of the log about the AP throughput threshold-crossing report.

Related Commands

Command	Description
advanced 802.11 logging	Use this command to modify the on/off status of the RRM log.

Platform Description N/A

1.53 show advanced 802.11 monitor

Use this command to display the monitoring-related information.

show advanced { **802.11a** | **802.11b** } **monitor**

Parameter Description

Parameter	Description
802.11a	A 5GHz network.
802.11b	A 2.4GHz network.

Command Mode Privileged EXEC mode/Global configuration mode

Usage Guide N/A

Configuration Examples The following example Display the monitoring information in a 2.4GHz network.

```
Ruijie# show advanced 802.11b monitor
Radio Resources Monitoring
  Radio Type..................................... 802.11b
  Monitor Mode................................... disable
  Monitor Channels............................... country channels
  AP Load Interval............................... 60 seconds
  AP Noise Interval.............................. 180 seconds
  AP Signal Strength Interval.................... 180 seconds
```

The **show advanced 802.11 monitor** command is used to display the information description table.

Field	Description
Monitor Mode	Specifies whether RRM monitoring is enabled.
Monitor Channels	Indicates the scope of monitored channels.
AP Monitor Interval	Indicates the monitoring interval (unit: second).
AP Coverage Interval	Indicates the interval of monitoring the subscriber information (unit: second).
AP Load Interval	Indicates the interval of monitoring the load (unit: second).
AP Noise Interval	Indicates the interval of monitoring the channel noise (unit: second).
AP Signal Strength Interval	Indicates the interval of monitoring the environmental signals of the AP (unit: second).
AP Neighbor Message Interval	Indicates the interval at which the AP sends a neighbor message (unit: second).

Related Commands

Command	Description
advanced 802.11 monitor	Configures RRM monitoring.

Platform Description N/A

1.54 show advanced 802.11 profile

Use this command to display the monitoring limit of the RRM.

show advanced { **802.11a** | **802.11b** } **profile** { **global** | *ap-name* }

Parameter Description

Parameter	Description
ap-name	Indicates the monitoring limit for a single AP is displayed.
global	Indicates the monitoring limit for all APs is displayed.
802.11a	A 5GHz network.
802.11b	A 2.4GHz network.

Command Mode Privileged EXEC mode/Global configuration mode

Usage Guide N/A

Configuration Examples The following example Display the global monitoring limits used by RRM in a 2.4GHz network.

```
Ruijie# show advanced 802.11b profile global
AP Global Performance Profiles
  Radio Type..................................... 802.11b
  Interference Threshold......................... 60%
```

```
Noise Threshold.............................. -70 dBm
RF Utilization Threshold..................... 80%
Throughput Threshold......................... 150000000 bps
Clients Threshold............................ 32 clients
```

Related Commands

Command	Description
advanced 802.11 profile	Configures the limits for RRM monitoring.

Platform Description N/A

1.55 show advanced 802.11 summary

Use this command to display the channels and power level used by the current AP.

show advanced { 802.11a | 802.11b } summary

Parameter Description

Parameter	Description
802.11a	A 5GHz network.
802.11b	A 2.4GHz network.

Command Mode Privileged EXEC mode/Global configuration mode

Usage Guide N/A

Configuration Examples The following example displays the channels and power level used by the current AP in a 2.4GHz network.

```
Ruijie# show advanced 802.11b summary
AP Name            MAC Address    Slot ID Channel TxPower Level
------------------ -------------- ------- ------- -------------
ap1                001a.a94e.de47   1     11*     1*(100%)
ap2                00d0.f822.33aa   1     11*     2*(50%)
ap3                001a.a9c5.8951   1      6*     2*(50%)
```

The **show advanced 802.11 summary** command is used to display the information description table.

Field	Description
AP Name	Indicates the AP name.
MAC Address	Indicates the MAC address of the current AP.
Slot ID	Indicates the radio id value of the current AP.

Channel	Indicates the current working channel number.
TxPower Level	Indicates the current transmit power level.

***** indicates whether the channel number or power level can be modified by the RRM algorithm.

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

1.56 show advanced 802.11 txpower

Use this command to display the related information of the TPC algorithm.

show advanced { 802.11a | 802.11b } txpower

Parameter Description

Parameter	Description
802.11a	A 5GHz network.
802.11b	A 2.4GHz network.

Command Mode Privileged EXEC mode/Global configuration mode

Usage Guide N/A

Configuration Examples The following example displays the related information of the TPC algorithm in a 2.4GHz network.

```
Ruijie# show advanced 802.11b txpower
Automatic Transmit Power Assignment
  Radio Type..................................... 802.11b
  Dynamic Transmit Power Control Support......... disable
  Transmit Power Assignment Mode................. AUTO
  Transmit Power Update Interval................. 120 seconds
  Consider The Same Channel Neighbor Only........ No
  Transmit Power Threshold....................... -60 dBm
  Transmit Power Assignment Leader............... 192.169.33.2
  Last Run....................................... 806 seconds ago
```

The **show advanced 802.11 txpower** command is used to display the information description table.

Field	Description
Dynamic Transmit Power Control Support	Specifies whether the TPC algorithm is enabled.

Transmit Power Assignment Mode	Indicates the running mode of the TPC algorithm.
Transmit Power Level	Indicates the power level used by the AP when the TPC algorithm is disabled.
Transmit Power Update Interval	Indicates the running interval of the TPC algorithm.
Transmit Power Threshold	Indicates the limit of environmental signals used by the TPC algorithm.
Transmit Power Assignment Leader	Indicates the MAC address of the leader of the group that implements the TPC algorithm.
Last Run	Specifies the last-running time of the TPC algorithm.

Related Commands

Command	Description
advanced 802.11 txpower	Configures the TPC algorithm.
show advanced 802.11 group	Display thes current RF group information.

Platform Description N/A

1.57 show ap auto-rf radio

Use this command to display the RF resource information of the AP.

show ap auto-rf radio *radio-id ap-name*

Parameter Description

Parameter	Description
radio-id	Indicates the ID of the RF to be displayed.
ap-name	Indicates the name of the AP to be displayed.
802.11a	A 5GHz network.
802.11b	A 2.4GHz network.

Defaults N/A

Command Mode Privileged EXEC mode/Global configuration mode

Usage Guide N/A

Configuration Examples The following example displays the information about the RF with the ID of 1 on the AP named **ap1**.

```
Ruijie#show ap auto-rf radio 1 ap1
Number Of Slots ................................ 2
AP Name ........................................ ap1
Mac Address .................................... 00d0.f822.33aa
  Radio Type ................................... 802.11b
```

```
Radio Slot ID ................................ 1
Monotior Mode ................................ ENABLED
Noise Information
  Noise Profile .............................. PASSED
  (Information Updated 83 Seconds Ago)
  Channel   1 ................................ -98 dBm
  Channel   2 ................................ -98 dBm
  Channel   3 ................................ -98 dBm
  Channel   4 ................................ -98 dBm
  Channel   5 ................................ -98 dBm
  Channel   6 ................................ -98 dBm
  Channel   7 ................................ -98 dBm
  Channel   8 ................................ -98 dBm
  Channel   9 ................................ -98 dBm
  Channel  10 ................................ -98 dBm
  Channel  11 ................................ -98 dBm
  Channel  12 ................................ -98 dBm
  Channel  13 ................................ -98 dBm
Interfere Information
  Interfere Profile .......................... PASSED
  (Information Updated 83 Seconds Ago)
  Channel   1 ................................  1%
  Channel   2 ................................  1%
  Channel   3 ................................  1%
  Channel   4 ................................  1%
  Channel   5 ................................  1%
  Channel   6 ................................  1%
  Channel   7 ................................  1%
  Channel   8 ................................  1%
  Channel   9 ................................  1%
  Channel  10 ................................  1%
  Channel  11 ................................  1%
  Channel  12 ................................  1%
  Channel  13 ................................  1%
Load Information
  Load Profile ............................... PASSED
  (Information Updated 16 Seconds Ago)
  Receive Utilization ........................ 0%
  Transmit Utilization ....................... 0%
  Channel Utilization ........................ 0%
  Channel Throughput ......................... 164160 bps
Coverage Information
  Coverage Profile ........................... PASSED
  (Information Updated 72 Seconds Ago)
```

```
  Load Clients ............................... 11 clients
  Pool SNR Clients ........................... 2 clients
Client Signal Strengths
  RSSI -100 dBm .............................. 0 clients
  RSSI  -92 dBm .............................. 0 clients
  RSSI  -84 dBm .............................. 0 clients
  RSSI  -76 dBm .............................. 2 clients
  RSSI  -68 dBm .............................. 3 clients
  RSSI  -60 dBm .............................. 3 clients
  RSSI  -52 dBm .............................. 1 clients
  RSSI  -44 dBm .............................. 2 clients
Client Signal To Noise Ratios
  SNR   0 dB ................................. 0 clients
  SNR   5 dB ................................. 2 clients
  SNR  10 dB ................................. 0 clients
  SNR  15 dB ................................. 0 clients
  SNR  20 dB ................................. 3 clients
  SNR  25 dB ................................. 2 clients
  SNR  30 dB ................................. 1 clients
  SNR  35 dB ................................. 1 clients
  SNR  40 dB ................................. 1 clients
  SNR  45 dB ................................. 0 clients
  SNR  50 dB ................................. 1 clients
  SNR  55 dB ................................. 0 clients
Nearby RADs
  (Information Updated 83 Seconds Ago)
  RAD fc8b.973f.d863 802.11b ................. -61 dBm on channel 1
  RAD d614.4b13.9cde 802.11b ................. -48 dBm on channel 1
  RAD c8d3.a32a.c8e4 802.11b ................. -53 dBm on channel 10
  RAD c83a.351a.9d18 802.11b ................. -60 dBm on channel 6
  RAD c83a.3517.1e70 802.11b ................. -60 dBm on channel 10
  RAD bcf6.853e.bdc0 802.11b ................. -61 dBm on channel 4
  RAD ace8.7b91.7c53 802.11b ................. -55 dBm on channel 6
  RAD a815.4d2e.6ef8 802.11b ................. -60 dBm on channel 1
  RAD 940c.6d61.7e82 802.11b ................. -54 dBm on channel 6
  RAD 940c.6d61.7d24 802.11b ................. -61 dBm on channel 6
  RAD 940c.6d61.7c8a 802.11b ................. -55 dBm on channel 13
  RAD 221a.a9c5.89f3 802.11b ................. -34 dBm on channel 1
  RAD 1cfa.68dd.b042 802.11b ................. -55 dBm on channel 1
  RAD 1cfa.68c7.9056 802.11b ................. -59 dBm on channel 1
  RAD 14e6.e4bc.1460 802.11b ................. -61 dBm on channel 6
  RAD 1414.4b5c.5f58 802.11b ................. -60 dBm on channel 13
  RAD 0c72.2cec.1be8 802.11b ................. -56 dBm on channel 1
  RAD 00ff.ffff.ff0c 802.11b ................. -56 dBm on channel 6
```

```
RAD 00aa.aaaa.aaae 802.11b .................. -47 dBm on channel 1
RAD 0087.3298.c11c 802.11b .................. -57 dBm on channel 1
RAD 001a.a9c5.892d 802.11b .................. -58 dBm on channel 11
RAD 001a.a94a.82b9 802.11b .................. -49 dBm on channel 6
RAD 001a.a916.967a 802.11b .................. -60 dBm on channel 9
RAD 001a.a916.95a2 802.11b .................. -52 dBm on channel 9
```

The **show ap auto-rf radio** command is used to display the information description table.

Field	Description
Number Of Slots	Indicates the number of RFs on the AP.
AP Name	Indicates the AP name.
Mac Address	Indicates the MAC address of the current AP.
Radio Type	Indicates the type of the displayed RF.
Radio Slot ID	Indicates the ID of the current RF.
Noise Information	Indicates that the system begins to display the information about channel noise.
Noise Profile	Indicates the threshold-crossing status of the noise.
Interfere Information	Indicates that the system begins to display the information about the AP interference factor.
Interfere Profile	Indicates the threshold-crossing status of AP interference.
Load Information	Indicates that the system begins to display the load information.
Load Profile	Indicates the threshold-crossing status of the load.
Receive Utilization	Indicates that the load is received.
Transmit Utilization	Indicates that the load is sent.
Channel Utilization	Indicates the total load of the current channel.
Channel Throughput	Indicates the current throughput.
Coverage Information	Indicates that the system begins to display the information about subscriber quantity.
Coverage Profile	Indicates the threshold-crossing status of subscriber quantity.
Client Signal To Noise Ratios	Indicates that the system begins to display the information about the subscriber SNR level.

Related Commands

Command	Description
show advanced 802.11 monitor	Displays the related information of RRM monitoring.

Platform Description

2 RF Resource Scheduling Commands

2.1 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*

Use this command to apply a scheduling session to an AP or an AP group. Use the **no** form of this command to remove the configuration.

schedule session *sid* [**radio** *radio-id*]

no schedule session *sid* [**radio** *radio-id*]

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
radio-id	Specifies the radio ID of the scheduling session to be applied or deleted, in the range from 1 to the total number of radios on the 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/AP configuration mode/AP group configuration

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. You can specify radio ID or slot ID for the scheduling session. By default, it is applied to all radios instead of slot IDs.

⚠ If you delete the scheduling session in the global configuration mode, the scheduling session on WLAN, AP and AP group 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 on fit AP networking topology.

```
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 Description N/A

2.2 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** { **everyday** | *day1* [**to** *day2*] } **time { all-day |** *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 64 for an AC.
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.
everyday	The session occurs every day, which is the simplified form of **period** *sun* **to** *sat*.
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.
all-day	The session time range is a whole day, which is the simplified form of **time** *00:00* **to** *23:59*.

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

2.3 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.

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 scheduling session 1.

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

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

3 Band Select Commands

3.1 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

3.2 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 Description

Parameter	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

3.3 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

3.4 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

3.5 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 N/A

Description

3.6 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

3.7 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

Command Privileged EXEC mode

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
  Acceptable Client RSSI (dBm)............................ -80
  Access Denial Count..................................... 0
  Age Out Dual Band (seconds)............................. 60
  Age Out Suppression (seconds)........................... 20
  Probe Cycle Count....................................... 2
  Scan Cycle Period Threshold (milliseconds).............. 200
```

Related Commands

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

Platform Description N/A

3.8 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

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

4 CorrectLink Commands

4.1 clink bandsel-5g-client-threshold

Use this command to configure the 5 GHz preferred load threshold of correctLink. Use the **no** form of this command to restore the default settings.

clink bandsel-5g-client-threshold *thrd*

no clink bandsel-5g-client-threshold

Parameter Description	**Parameter**	**Description**
	thrd	5 GHz preferred load threshold

Defaults 100

Command Mode Global configuration mode

Default Level 15

Usage Guide After the 5 GHz preferred load threshold is configured, if a WLAN supports both the 2.4 GHz and 5 GHz frequency bands and load of 5 GHz signals is less than the threshold in the WLAN, the client cannot be associated with the WLAN in the 2.4 GHz frequency band.

Configuration Examples The following example configures the 5 GHz preferred load threshold of correctLink to **30**.

```
Ruijie(config)# clink bandsel-5g-client-threshold 30
```

Verification Run the **show run** command to display the configurations.

Prompts N/A

Common Errors N/A

Platform Description This command is supported only on the AC.

4.2 clink bandsel-5g-rssi-threshold

Use this command to configure the 5 GHz preferred RSSI threshold of correctLink. Use the **no** form of this command to restore the default settings.

clink bandsel-5g-rssi-threshold *thrd*

no clink bandsel-5g-rssi-threshold

Parameter Description	Parameter	Description
	thrd	5 GHz preferred RSSI threshold

Defaults 20

Command Mode Global configuration mode

Default Level 15

Usage Guide After the 5 GHz preferred RSSI threshold is configured, if a WLAN supports both the 2.4 GHz and 5 GHz frequency bands and the RSSI of 5 GHz signals is greater than the threshold in the WLAN, the client cannot be associated with the WLAN in the 2.4 GHz frequency band.

Configuration Examples The following example configures the 5 GHz preferred RSSI threshold of correctLink to **30**.

```
Ruijie(config)# clink bandsel-5g-rssi-threshold 30
```

Verification Run the **show run** command to display the configurations.

Prompts N/A

Common Errors N/A

Platform Description This command is supported only on the AC.

4.3 clink enable

Use this command to enable correctLink. Use the **no** form of this command to restore the default settings.

clink enable

no clink enable

Parameter Description	Parameter	Description
	N/A	N/A

Defaults correctLink is disabled by default.

Command Mode Global configuration mode

Default Level 15

Usage Guide This command is used to enable correctLink.

Configuration Examples The following example enables correctLink.

```
Ruijie(config)# clink enable
```

Verification Run the **show run** command to display the configurations.

Prompts N/A

Common Errors N/A

Platform Description This command is supported only on the AC.

4.4 clink lb-client-delta-threshold

Use this command to configure the load balancing difference threshold of correctLink. Use the **no** form of this command to restore the default settings.

clink lb-client-delta-threshold *thrd*

no clink lb-client-delta-threshold

Parameter Description

Parameter	Description
thrd	Load balancing difference threshold

Defaults 5

Command Mode Global configuration mode

Default Level 15

Usage Guide When a client detects APs, if the difference between an AP's RSSI and the detected highest RSSI is less than the remote association RSSI threshold, the set of these APs is called an APset.

After the load balancing difference threshold is configured, it is determined that load imbalance exists and a current client cannot access AP X when all of the following conditions are met:

1. The number of clients associated with AP X is greater than the load balancing enabling threshold.
2. An APset exists and AP Y unassociated with the current client exists in the APset.
3. The number of clients associated with AP Y is less than the number of clients associated with AP X by a value higher than the load balancing difference threshold.

Configuration The following example configures the load balancing difference threshold to **10**.

Examples	`Ruijie(config)# clink lb-client-delta-threshold 10`
Verification	Run the **show run** command to display the configurations.
Prompts	N/A
Common Errors	N/A
Platform Description	This command is supported only on the AC.

4.5 clink lb-client-threshold

Use this command to configure the load balancing judgment threshold of correctLink. Use the **no** form of this command to restore the default settings.

clink lb-client-threshold *thrd*

no clink lb-client-threshold

Parameter

Parameter	Description

thrd	Load balancing judgment threshold

Defaults 30

Command Mode Global configuration mode

Default Level 15

Usage Guide With load balancing enabled, when the load of clients associated with the AP exceeds the load balancing judgment threshold, load balancing judgment is performed.

Configuration Examples The following example configures the load balancing judgment threshold to **25**.

```
Ruijie(config)# clink lb-client-threshold 25
```

Verification Run the **show run** command to display the configurations.

Prompts N/A

Common Errors N/A

Platform Description This command is supported only on the AC.

4.6 clink max-fails

Use this command to configure the rate-limiting attempt threshold of correctLink. Use the **no** form of this command to restore the default settings.

clink max-fails *thrd*

no clink max-fails

Parameter Description

Parameter	Description
thrd	Rate-limiting attempt threshold

Defaults 2

Command Mode Global configuration mode

Default Level 15

Usage Guide After a client is rate-limited for a certain number of times equal to the rate-limiting

attempt threshold, stop rate limiting to guarantee access experience of the client.

Configuration Examples The following example configures the rate-limiting attempt threshold to **3**.

```
Ruijie(config)# clink max-fails 3
```

Verification Run the **show run** command to display the configurations.

Prompts N/A

Common Errors N/A

Platform Description This command is supported only on the AC.

4.7 clink rssi-delta-threshold

Use this command to configure the remote association RSSI difference threshold of correctLink. Use the **no** form of this command to restore the default settings.

clink rssi-delta-threshold *thrd*

no clink rssi-delta-threshold

Parameter Description

Parameter	Description
thrd	Remote association RSSI difference threshold

Defaults 10

Command Mode Global configuration mode

Default Level 15

Usage Guide After the remote association RSSI difference threshold is configured, when the difference between the uplink associated RSSI of the client and the detected highest RSSI is greater than the threshold, it is determined that the client is a remote client and cannot access the AP.

Configuration Examples The following example configures the remote association RSSI difference threshold to **5**.

```
Ruijie(config)# clink rssi-delta-threshold 5
```

Verification Run the **show run** command to display the configurations.

Prompts N/A

Common Errors	N/A
Platform Description	This command is supported only on the AC.

5 Smart Antenna Commands

5.1 smartant enable radio

Use this command to enable the smart antenna (Smartant) function of the specified radio on the specified AP. Use the **no** form of this command to disable the smart antenna function.

smartant enable radio *radio-id*

no smartant enable radio *radio-id*

Parameter Description

Parameter	Description
radio-id	Configures the radio ID.

Defaults The smart antenna function is enabled by default.

Command Mode AP configuration mode

Usage Guide This command is supported only on Smartant-capable devices.

Configuration Examples The following example enables the smart antenna function of radio 1 on a specified AP.

```
Ruijie(config-ap)# smartant enable radio  1
```

The following example disables the smart antenna function of radio 1 on a specified AP.

```
Ruijie(config-ap)# no smartant enable radio  1
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

6 Frequency Spectrum Scanning Commands

6.1 spectral enable

Use this command to enable the frequency spectrum scanning (FSS) function on the AP.

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

spectral enable

no spectral enable

Parameter Description

Parameter	Description
N/A	N/A

Defaults This function is disabled by default.

Command Mode AP configuration mode

Usage Guide This command is only supported on the APs supporting FSS.

This command does not support bath configuration.

Configuration Examples The following example enables the FSS function.

```
Ruijie(config)# ap-config AP0001
Ruijie(config-ap)# spectral enable
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

6.2 spectral period

Use this command to configure the AP scanning cycle.

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

spectral period *num*

no spectral period

Parameter Description

Parameter	Description

num	Configures the scanning cycle within the range from 1 to 100 in the unit of microseconds.

Defaults The default is 5 microseconds.

Command Mode AP configuration mode

Usage Guide This command is only supported on the APs supporting FSS.
This command does not support bath configuration.

Configuration Examples The following example configures the scanning cycle of the specified AP.

```
Ruijie(config)# ap-config AP0001
Ruijie(config-ap)# spectral period 10
```

The following example restores the scanning cycle of the specified AP to the default setting.

```
Ruijie(config-ap)# no spectral period
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

6.3 spectral stability

Use this command to configure with the interference recognition accuracy for the specified AP.
Use the **no** form of this command to restore the default setting.
spectral stability vbr | **bth** | **bts** | **cph** | **mwo** | **cwa** *num*
no spectral stability vbr | **bth** | **bts** | **cph** | **mwo** | **cwa**

Parameter Description

Parameter	Description
vbr *num*	Configures recognition accuracy of the video bridge, in the range from 1 to 5.
bth *num*	Configures recognition accuracy of the Bluetooth headset, in the range from 1 to 4.
bts *num*	Configures recognition accuracy of the Bluetooth voice, in the range from 1 to 2.
cph *num*	Configures recognition accuracy of the cordless phone, in n the range from 3 to 5.
mwo *num*	Configures recognition accuracy of the microwave, in the range from 1 to 5.

cwa *num*	Configures recognition accuracy of the continuous wave, in the range from 4 to 10.

Defaults See the Limitation and Specifications manual.

Command Mode AP configuration mode

Usage Guide This command is only supported on the APs supporting FSS.
This command does not support bath configuration.

Configuration Examples The following example configures recognition accuracy of the FSS video bridge on the specified AP.

```
Ruijie(config)# ap-config AP0001
Ruijie(config-ap)# spectral stability vbr 2
```

The following example restores recognition accuracy of the video bridge to the default setting on the specified AP.

```
Ruijie(config-ap)# no spectral stability vbr
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

7 WLAN Location Commands

7.1 wlocation ae-ip

Use this command to configure the IP address of the AE server connected with the specified AP.
Use the **no** form of this command to restore the default setting.
wlocation ae-ip *ip-address*
no wlocation ae-ip

Parameter Description

Parameter	Description
ip-address	The IP address of the AE server

Defaults The IP address of the AE server is not configured by default.

Command Mode AP configuration mode

Usage Guide N/A

Configuration Examples The following example configures the IP address of the AE server on the specified AP.

```
Ruijie(config-ap)# wlocation ae-ip 1.1.1.1
```

The following example restores the IP address of the AE to the default setting.

```
Ruijie(config-ap)# no wlocation ae-ip
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

7.2 wlocation ae-port

Use this command to set the port number of the AE server connected with the specified AP.
Use the **no** form of this command to restore the default setting.
wlocation ae-port *port*
no wlocation ae-port

Parameter Description

Parameter	Description

port	The port number of the AE server

Defaults The default port number is 12092.

Command Mode AP configuration mode

Usage Guide N/A

Configuration Examples The following example sets the port number of the AE server connected with the specified AP.

```
Ruijie(config-ap)# wlocation ae-port 12093
```

The following example restores the port number of the AE server connected with the specified AP to the default configuration.

```
Ruijie(config-ap)# no wlocation ae-port
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

7.3 wlocation compound enable

Use this command to enable the function of transmitting aggregate data of wireless location.
Use the **no** form of this command to disable this function.
wlocation compound enable
no wlocation compound enable

Parameter Description

Parameter	Description
N/A	N/A

Defaults This function is enabled by default.

Command Mode AP configuration mode

Usage Guide N/A

Configuration Examples The following example enables the function of transmitting aggregate data of wireless location on the specified AP.

```
Ruijie(config-ap)# wlocation compound enable
```

The following example disables the function of transmitting aggregate data of wireless location on the specified AP.

```
Ruijie(config-ap)# no wlocation compound enable
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

7.4 wlocation enable

Use this command to enable the WLAN Location (WL) function on the specified AP.

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

wlocation enable

no wlocation enable

Parameter Description

Parameter	Description
N/A	N/A

Defaults This function is disabled by default.

Command Mode AP configuration mode

Usage Guide N/A

Configuration Examples The following example enables WLAN location on the AP.

```
Ruijie(config-ap)# wlocation enable
```

The following example disables WLAN location on the AP.

```
Ruijie(config-ap)# wlocation enable
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

7.5 wlocation ignore beacon enable

Use this command to enable the AP to ignore beacon packets.

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

wlocation ignore beacon enable

no wlocation ignore beacon enable

Parameter Description

Parameter	Description
N/A	N/A

Defaults This function is disabled by default.

Command Mode AP configuration mode

Usage Guide Use this command to ignore beacon packets to save bandwidth.

Configuration Examples The following example enables the AP to ignore beacon packets.

```
Ruijie(config-ap)# wlocation ignore beacon enable
```

The following example disables the AP from ignoring beacon packets.

```
Ruijie(config-ap)# no wlocation ignore beacon enable
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

7.6 wlocation mu enable

Use this command to enable Mobile Unit (MU) wireless location on the specified AP.

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

wlocation mu enable

no wlocation mu enable

Parameter Description

Parameter	Description
N/A	N/A

Defaults This function is disabled by default.

Command Mode AP configuration mode

Usage Guide MU wireless location locates Wi-Fi connected mobile devices like laptops and mobiles.

Configuration Examples The following example enables MU wireless location on the specified AP.

```
Ruijie(config-ap)# wlocation mu enable
```

The following example disables MU wireless location on the specified AP.

```
Ruijie(config-ap)# no wlocation mu enable
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

7.7 wlocation mu report enable

Use this command to enable the AP to send MU location packets directly.

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

wlocation mu report enable

no wlocation mu report enable

Parameter Description

Parameter	Description
N/A	N/A

Defaults This function is disabled by default.

Command Mode AP configuration mode

Usage Guide Use this command to send MU location packets directly and travel through NAT network without the three-way handshake.

Configuration Examples The following example enables the AP to send MU location packets directly.

```
Ruijie(config-ap)# wlocation mu report enable
```

The following example disables the AP from sending MU location packets directly.

```
Ruijie(config-ap)# no wlocation mu report enable
```

Related

Command	Description

Commands

N/A	N/A

Platform Description N/A

7.8 wlocation mu report reduce enable

Use this command to enable the AP to send reduced MU location packets.
Use the **no** form of this command to restore the default setting.
wlocation mu report reduce enable
no wlocation mu report reduce enable

Parameter Description

Parameter	Description
N/A	N/A

Defaults This function is disabled by default.

Command Mode AP configuration mode

Usage Guide Use this command to reduce bandwidth for the network featuring wireless location, which is deployed with Ruijie location servers.

Configuration Examples The following example enables the AP to send reduced MU location packets.

```
Ruijie(config-ap)# wlocation mu report reduce enable
```

The following example disables the AP from sending reduced MU location packets.

```
Ruijie(config-ap)# no wlocation mu report reduce enable
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

7.9 wlocation send-mu-time

Use this command to set frequency of sending MU location packets on the specified AP.
Use the **no** form of this command to restore the default setting.
wlocation send-mu-time *interval*

no wlocation send-mu-time

Parameter Description

Parameter	Description
interval	Packets sending interval in the range from 100 to 600,000 in the unit of milliseconds.

Defaults The default is 300 milliseconds.

Command Mode AP configuration mode

Usage Guide N/A

Configuration Examples The following example sets frequency to send MU location packets on the specified AP.

```
Ruijie(config-ap)# wlocation send-mu-time 400
```

The following example restores the frequency of sending MU location packets to the default setting.

```
Ruijie(config-ap)# no wlocation send-mu-time
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

7.10 wlocation send-tag-time

Use this command to set frequency to send tag location packets on the specified AP.
Use the **no** form of this command to restore the default setting.
wlocation send-tag-time *interval*
no wlocation send-tag-time

Parameter Description

Parameter	Description
interval	Packets sending interval within the range from 100 to 5,000 in the unit of milliseconds.

Defaults The default is 300 milliseconds.

Command Mode AP configuration mode

Usage Guide N/A

Configuration Examples The following example sets frequency to send tag location packets on the specified AP.

```
Ruijie(config-ap)# wlocation send-tag-time 400
```

The following example restores frequency of sending tag location packets to the default setting.

```
Ruijie(config-ap)# no wlocation send-tag-time
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

7.11 wlocation tag enable

Use this command to enable tag wireless location on the specified AP.

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

wlocation tag enable

no wlocation tag enable

Parameter Description

Parameter	Description
N/A	N/A

Defaults This function is disabled by default.

Command Mode AP configuration mode

Usage Guide N/A

Configuration Examples The following example enables tag wireless location on the specified AP.

```
Ruijie(config-ap)# wlocation tag enable
```

The following example disables tag wireless location on the specified AP.

```
Ruijie(config-ap)# no wlocation tag enable
```

Related Commands

Command	Description
N/A	N/A

Platform N/A

Description

7.12 wlocation tag report enable

Use this command to enable the function to send TAG location packets directly.

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

wlocation tag report enable

no wlocation tag report enable

Parameter Description

Parameter	Description
N/A	N/A

Defaults This function is disabled by default.

Command Mode AP configuration mode

Usage Guide Use this command to send TAG location packets directly and travel through NAT network without the three-way handshake.

Configuration Examples The following example enables the AP to send TAG location packets directly.

```
Ruijie(config-ap)# wlocation tag report enable
```

The following example disables the AP from sending TAG location packets directly.

```
Ruijie(config-ap)# no wlocation tag report enable
```

Related Commands

Command	Description
N/A	N/A

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 Description

Parameter	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 The following example set the retransmission count for the multicast key negotiation packet to 5.

Examples

```
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 N/A

Description

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
```

The following example disables the RSN authentication mode of WLAN1.

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

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 N/A

Description

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

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 rsn dot11r

Use this command to enable the 802.11r function.
security rsn dot11r enable
Use this command to disable the 802.11r function.
security rsn dot11r disable

Parameter Description

Parameter	Description
enable	Enables the 802.11r function.
disable	Disables the 802.11r function.

Defaults The 802.11r function is disabled by default.

Command Mode	WLAN security configuration mode
Default Level	14
Usage Guide	The 802.11r function can be enabled only when the following conditions are met: 1. RSN authentication is enabled. 2. WPA authentication is disabled, that is, WPA and RSN cannot be enabled simultaneously. 3. The access authentication mode (AKM) is configured as PSK or 802.1x. 4. AES encryption is enabled. 5. TKIP encryption is disabled, that is, AES and TKIP cannot be enabled simultaneously.

Configuration Example	1. The following example enables the 802.11r function for WLAN 1.
	`Ruijie(config-wlansec)#security rsn dot11r enable`
	
	2. The following example disables the 802.11r function for WLAN 2.
	`Ruijie(config-wlansec)#security rsn dot11r disable`

Verification	Run the **show running-config** command to check whether the configuration takes effect.

Prompt	`Ruijie(config)#wlansec 1`
	`Ruijie(config-wlansec)#security rsn dot11r enable`
	`%ERROR% 802.11R requires RSN to be enabled, run command 'security rsn enable' first.`
	
	`Ruijie(config-wlansec)#security rsn ciphers tkip enable`
	`Ruijie(config-wlansec)#security rsn dot11r enable`
	`%ERROR% 802.11R requires ciphers aes to be enabled, run command 'security rsn ciphers aes enable' first.`

Common Error	1: In WLAN security configuration mode, the 802.11r function is enabled when RSN authentication is not enabled. 2: In WLAN security configuration mode, the 802.11r function is enabled when AES encryption is disabled. 3. The 802.11r function is enabled when WPA or TKIP is enabled.
Platform Description	N/A

1.13 security rsn dot11r reassoc-timeout

Use this command to configure the re-association timeout duration of the 802.11r function in WLAN security configuration mode, that is, the maximum interval for a client to send an association request after the client authentication is completed. This command takes effect only after the 802.11r function is enabled.

security rsn dot11r reassoc-timeout *timeout-seconds*

Parameter Description

Parameter	Description
timeout-seconds	Timeout duration in seconds. The value is an integer ranging from 1 to 120.

Defaults The timeout duration is 20 seconds by default.

Command Mode WLAN security configuration mode

Default Level 14

Usage Guide This command is used to configure the re-association timeout duration of the 802.11r function in the unit of seconds.

Configuration Example The following example sets the re-association timeout duration of the 802.11r function on WLAN 1 to 30s.

```
Ruijie(config)#wlansec 1
Ruijie(config-wlansec)#security dot11r reassoc-timeout 30
```

Verification Run the **show running-config** command to check whether the configuration takes effect.

Common Error N/A

Platform Description N/A

1.14 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

1.15 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

1.16 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 mode WLAN security configuration 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** |	Configures an authentication method in the

disable }	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

1.17 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. There are two authentication methods: PSK and 802.1x.

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

1.18 security wpa akm psk set-key

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

1.19 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. There are two encryption methods: AES and TKIP.

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

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

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

1.20 show wclient security

Use this command to display security configuration of STAs.

show wclient security *mac-address*

Parameter

Parameter	Description

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

1.21 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

1.22 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 N/A

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

1.23 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 WIDS Commands

2.1 attack-detection enable

Use this command to enable the IDS attack detection. Use the **no** form of this command to restore the default setting.

attack-detection enable { **all** | **flood** | **ddos** | **spoof** | **weak-iv** }

no attack-detection enable { **all** | **flood** | **ddos** | **spoof** | **weak-iv** }

Parameter Description

Parameter	Description
all	Enables all types of IDS attack detection.
flood	Enables the Flooding IDS attack detection.
weak-iv	Enables the Weak-IV IDS attack detection.
spoof	Enables the Spoofing IDS attack detection.
ddos	Enables the DDOS IDS attack detection.

Defaults This function is disabled by default.

Command Mode WIDS configuration mode

Usage Guide N/A

Configuration Examples The following example enables the Flooding IDS attack detection.

```
Ruijie(config-wids)# attack-detection enable flood
```

The following example disables the Flooding IDS attack detection.

```
Ruijie(config-wids)#no attack-detection enable flood
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

2.2 attack-detection ddos

Use this command to specify the packet threshold and interval for DDOS attack detection. Use the **no** form of this command to restore the default setting.

attack-detection ddos { **arp-threshold** *num* | **icmp-threshold** *num* | **syn-threshold** *num* | **interval**

time }

no attack-detection ddos { **arp-threshold** | **icmp-threshold** | **syn-threshold** | **interval** }

Parameter Description

Parameter	Description
interval *time*	DDOS detection interval in the range from 10 to 60 in the unit of seconds.
arp-threshold *num*	ARP packet threshold in the range from 1 to 10000 in the unit of pps.
icmp-threshold *num*	ICMP packet threshold in the range from 1 to 10000 in the unit of pps.
syn-threshold *num*	SYN packet threshold in the range from 1 to 10000 in the unit of pps.

Defaults The **arp-threshold** is 50pps, **icmp-threshold** is 100pps, **syn-threshold** is 50pps, and **interval** is 30 seconds by default.

Command Mode WIDS configuration mode

Usage Guide N/A

Configuration Examples The following example sets ARP packet threshold to 200pps for DDOS attack detection.

```
Ruijie(config-wids)# attack-detection ddos arp-threshold 200
```

The following example restores ARP packet threshold to the default setting.

```
Ruijie(config-wids)#no attack-detection ddos arp-threshold
```

Platform Description N/A

2.3 attack-detection flood multi-mac

Use this command to specify the packet threshold and interval for Flooding attack detection in a multi-user system. Use the **no** form of this command to restore the default setting.

attack-detection flood multi-mac { **assoc** | **reassoc** | **disassoc** | **probe** | **action** | **auth** | **deauth | null-data** } **threshold** *num* **interval** *time*

no attack-detection flood multi-mac { **assoc** | **reassoc** | **disassoc** | **probe** | **action** | **auth** | **deauth | null-data** }

Parameter Description

Parameter	Description
assoc	Specifies the association packet.
reassoc	Specifies the reassocation packet.
disassoc	Specifies the disassociation packet.
probe	Specifies the probe request packet.

action	Specifies the action packet.
auth	Specifies the authentication packet.
deauth	Specifies the deauthentication packet.
null-data	Specifies the null data packet.
threshold *num*	Packet threshold in the range from 1 to 10,000.
interval *time*	Statistics interval threshold in the range from 10 to 60 in the unit of seconds.

Defaults The **threshold** is 4,800 and the **interval** is 10 seconds by default.

Command Mode WIDS configuration mode

Usage Guide N/A

Configuration Examples The following example sets **assoc** to 200 and **interval** to 20s for Flooding attack detection in a multi-user system.

```
Ruijie(config-wids)# attack-detection flood multi-mac assoc threshold 200
interval 20
```

The following example restores **assoc** and **interval** to the default setting.

```
Ruijie(config-wids)#no attack-detection flood multi-mac assoc
```

Platform Description N/A

2.4 attack-detection flood single-mac

Use this command to set the packet threshold and statistics interval for Flooding attack detection in a single-user system. Use the **no** form of this command to restore the default setting.

attack-detection flood single-mac { **total** | **assoc** | **reassoc** | **disassoc** | **probe** | **action** | **auth** | **deauth | null-data** } **threshold** *num* **interval** *time*

no attack-detection flood single-mac { **tota** | **assoc** | **reassoc** | **disassoc** | **probe** | **action** | **auth** | **deauth | null-data** }

Parameter Description

Parameter	Description
total	Specifies all types of packets.
assoc	Specifies the association packet.
reassoc	Specifies the reassocation packet.
disassoc	Specifies the disassociation packet.
probe	Specifies the probe request packet.

action	Specifies the action packet.
auth	Specifies the authentication packet.
deauth	Specifies the deauthentication packet.
null-data	Specifies the null data packet
threshold *num*	Packet threshold in the range from 1 to 5000.
interval *time*	Statistics interval threshold in the range from 10 to 60 in the unit of seconds.

Defaults The **threshold** is 300 and the **interval** is 10 seconds by default.

Command Mode WIDS configuration mode

Usage Guide N/A

Configuration Examples The following example sets **assoc** to 200 and **interval** to 20000 milliseconds for Flooding attack detection in a single-user system.

```
Ruijie(config-wids)# attack-detection flood single-mac assoc threshold 200 interval 20000
```

The following example restores **assoc** and **interval** to the default setting.

```
Ruijie(config-wids)#no attack-detection flood single-mac assoc
```

Platform Description N/A

2.5 attack-detection spoof

Use this command to set the packet threshold and statistics interval for Spoofing attack detection.
Use the **no** form of this command to restore the default setting.
attack-detection spoof { **threshold** *num* **| interval** *time* }
no attack-detection spoof { **threshold** | **interval** }

Parameter Description

Parameter	Description
threshold *num*	Packet threshold in the range from 1 to 1000.
interval *time*	Detection interval in the range from 10 to 60 in the unit of seconds.

Defaults The **threshold** is 1 second and the **interval** is 50 seconds by default.

Command Mode WIDS configuration mode

Usage Guide N/A

Configuration Examples The following example sets the packet threshold for Spoofing attack detection to 20.

```
Ruijie(config-wids)# attack-detection spoof threshold 20
```

The following example restores the ARP packet threshold for Spoofing attack detection to the default setting.

```
Ruijie(config-wids)#no attack-detection spoof threshold
```

Platform Description N/A

2.6 attack-detection weak-iv

Use this command to set the packet thresMhold and interval for Weak IV attack. Use the **no** form of this command to restore the default setting.

attack-detection weak-iv { **threshold** *num* **| interval** *time* }

no attack-detection weak-iv { **threshold** | **interval** }

Parameter Description

Parameter	Description
threshold *num*	Packet threshold in the range from 1 to 10000.
interval *time*	Detection interval in the range from 1 to 60 in the unit of seconds.

Defaults The **threshold** is 10 seconds and the **interval** is 15 seconds by default.

Command Mode WIDS configuration mode

Usage Guide N/A

Configuration Examples The following example sets the packet threshold for Weak IV attack detection to 200.

```
Ruijie(config-wids)# attack-detection weak-iv threshold 200
```

The following example restores the packet threshold for Weak IV attack to the default setting.

```
Ruijie(config-wids)#no attack-detection weak-iv threshold
```

Platform Description N/A

2.7 attack-detection statistics ac-max

Use this command to configure the maximum number of IDS attack detection lists on the AC. Use the **no** form of this command to restore the default setting.

attack-detection statistics ac-max *num*
no attack-detection statistics ac-max

Parameter Description

Parameter	Description
num	The maximum number of IDS attack detection lists on the AC in the range from 1 to 4096.

Defaults The default is 2048.

Command Mode WIDS configuration mode

Usage Guide N/A

Configuration Examples The following example configures the maximum number of the IDS attack detection list to 2000.

```
Ruijie(config-wids)# attack-detection statistics ac-max 2000
```

The following example restores the maximum number of the IDS attack detection list to the default setting.

```
Ruijie(config-wids)#no attack-detection statistics ac-max
```

Platform Description N/A

2.8 attack-detection statistics ap-max

Use this command to configure the maximum number of IDS attack detection lists on the AP. Use the **no** form of this command to restore the default setting.
attack-detection statistics ap-max *num*
no attack-detection statistics ap-max

Parameter Description

Parameter	Description
num	The maximum number of IDS attack detection lists on the AP in the range from 1 to 1024.

Defaults The default is 512.

Command Mode WIDS configuration mode

Usage Guide N/A

Configuration Examples The following example sets the maximum number of IDS attack detection lists on the AC to 1000.

```
Ruijie(config-wids)# attack-detection statistics ap-max 1000
```

The following example restores the maximum number of IDS attack detection lists to the default setting.

```
Ruijie(config-wids)#no attack-detection statistics ap-max
```

Platform Description N/A

2.9 countermeasures ap-max

Use this command to configure the maximum number of APs for the countermeasures.
Use the **no** form of this command to restore the default setting.
countermeasures ap-max *ap-num*
no countermeasures ap-max

Parameter Description

Parameter	Description
ap-num	Specifies the maximum number of APs for the countermeasures in the range from 1 to 256.

Defaults The default is 30.

Command Mode WIDS configuration mode

Usage Guide The countermeasure function must be enabled before you configure this command.

Configuration Examples The following example sets the maximum number of APs for the countermeasures to 22.

```
Ruijie(config-wids)# countermeasures ap-max 22
```

The following example restores the maximum number of APs for the countermeasures to the default setting.

```
Ruijie(config-wids)#no countermeasures ap-max
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

2.10 countermeasures enable

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

countermeasures enable

no countermeasure enable

Parameter Description

Parameter	Description
N/A	N/A

Defaults This function is disabled by default.

Command Mode WIDS configuration mode

Usage Guide This command does not take effect in AP normal working mode.

Configuration Examples The following example enables the device countermeasures.

```
Ruijie(config-wids)#countermeasures enable
```

The following example disables the device countermeasures.

```
Ruijie(config-wids)#no countermeasures enable
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

2.11 countermeasures channel-match

Use this command to enable the channel-based countermeasures. Use the **no** form of this command to restore the default setting.

countermeasures channel-match

no countermeasures channel-match

Parameter Description

Parameter	Description
N/A	N/A

Defaults This function is disabled by default.

Command Mode WIDS configuration mode

Usage Guide Use this command after the device countermeasures are enabled.

Configuration Examples The following example enables the channel-based countermeasures.

```
Ruijie(config-wids)# countermeasures channel-match
```

The following example disables the channel-based countermeasures.

```
Ruijie(config-wids)#no countermeasures channel-match
```

Platform Description N/A

2.12 countermeasures interval

Use this command to set the device countermeasures interval. Use the **no** form of this command to restore the default setting.

countermeasures interval *time*

no countermeasures interval

Parameter Description

Parameter	Description
time	Device countermeasures interval in the range from 100 to 10000 in the unit of milliseconds.

Defaults The default is 1000 milliseconds.

Command Mode WIDS configuration mode

Usage Guide N/A

Configuration Examples The following example sets the countermeasures interval to 2000 milliseconds.

```
Ruijie(config-wids)# countermeasures interval 2000
```

The following example restores the countermeasures interval to the default setting.

```
Ruijie(config-wids)#no countermeasures interval
```

Platform Description N/A

2.13 countermeasures mode

Use this command to configure the device countermeasures mode. Use the **no** form of this command to restore the default setting.

countermeasures mode { **all** | **adhoc** | **config** | **rogue** | **ssid** }

no countermeasures mode { **all** | **adhoc** | **config** | **rogue** | **ssid** }

Parameter Description

Parameter	Description
all	Indicates all countermeasures are enabled.
ssid	Indicates the devices with the same SSID on the AP are subjected to the countermeasures.
rogue	Indicates only detected rogue devices are subjected to the countermeasures.
adhoc	Indicates only detected adhoc devices are subjected to the countermeasures.
config	Indicates only the devices configured in the static attack list are subjected to the countermeasures.

Defaults This function is disabled by default.

Command Mode WIDS configuration mode

Usage Guide The countermeasure function must be enabled before you configure this command.

Configuration Examples The following example sets the device countermeasures mode to **adhoc**.

```
Ruijie(config-wids)# countermeasure mode adhoc
```

The following example disables the **adhoc** mode.

```
Ruijie(config-wids)#no countermeasures mode adhoc
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

2.14 countermeasures rssi-min

Use this command to configure the lower limit of the signal for the countermeasures.

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

countermeasures rssi-min *num*
no countermeasures rssi-min

Parameter Description

Parameter	Description
num	Specifies the lower limit of the signal strength for the countermeasures in the range from 0 to 75 (-95 to -20).

Defaults The default is 25 (-70).

Command Mode WIDS configuration mode

Usage Guide The countermeasure function must be enabled before you configure this command.

Configuration Examples The following example sets the lower limit of the signal strength for the countermeasures to 40.

```
Ruijie(config-wids)# countermeasures rssi-min 40
```

The following example restores the default setting.

```
Ruijie(config-wids)#no countermeasures rssi-min
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

2.15 countermeasures fuzzy-enable

Use this command to enable the fuzzy containment function.
Use the **no** form of this command to disable this function.
countermeasures fuzzy-enable
no countermeasures fuzzy-enable

Parameter Description

Parameter	Description
N/A	N/A

Defaults By default, fuzzy containment is disabled.

Command Mode WIDS configuration mode

Usage Guide If containment modes include the configuration containment mode, rogue APs whose SSID are similar to those in the SSID blacklist are contained. If containment modes include the SSID containment mode, rogue APs whose SSIDs are similar to the SSID of the local host are contained. Fuzzy containment takes effect only in configuration containment mode and SSID containment mode.

Configuration Examples The following example enables the fuzzy containment function.

```
Ruijie(config-wids)# countermeasures fuzzy-enable
```

The following example disables the fuzzy containment function.

```
Ruijie(config-wids)# no countermeasures fuzzy-enable
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

2.16 device aging duration

Use this command to configure device aging duration. Use the **no** form of this command to restore the default setting.

device aging duration *time*

no device aging duration

Parameter Description

Parameter	Description
time	Indicates device aging duration in the range from 500 to 5000 in the unit of seconds.

Defaults The default is 1200 seconds.

Command Mode WIDS configuration mode

Usage Guide N/A

Configuration Examples The following example sets the device aging duration to 1000 seconds.

```
Ruijie(config-wids)# device aging duration 1000
```

The following example restores the device aging duration to the default setting.

```
Ruijie(config-wids)#no device aging duration
```

Related

Command	Description

Commands

N/A	N/A

Platform Description N/A

2.17 device attack mac-address

Use this command to configure an entry for static attack list. Use the **no** form of this command to delete a configured entry of the static attack list.

device attack mac-address *H.H.H*

no device attack mac-address *H.H.H*

Parameter Description

Parameter	Description
H.H.H	Indicates the device with this source MAC address is subjected to the countermeasures.

Defaults N/A

Command Mode WIDS configuration mode

Usage Guide This configuration is one of the policies for detecting Rogue devices.

Configuration Examples The following example configures the device with the static attack source MAC address of 0000.0000.0001.

```
Ruijie(config-wids)# device attack mac-address 0000.0000.0001
```

The following example deletes the static attack list with its source MAC address of 0000.0000.0001.

```
Ruijie(config-wids)#no device attack mac-address 0000.0000.0001
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

2.18 device attack max

Use this command to configure the maximum number of the static attack list.

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

device attack max *num*
no device attack max

Parameter Description

Parameter	Description
num	Specifies the maximum number of the static attack list in the range from 1 to 1024.

Defaults The default is 512.

Command Mode WIDS configuration mode

Usage Guide N/A

Configuration Examples The following example sets the maximum number of the static attack list to 900.

```
Ruijie(config-wids)# device attack max 900
```

The following example restores the default setting.

```
Ruijie(config-wids)#no device attack max
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

2.19 device black-ssid

Use this command to configure an entry for the SSID blacklist. Use the **no** form of this command to remove an entry from the SSID blacklist.
device black-ssid *ssid*
no device black-ssid *ssid*

Parameter Description

Parameter	Description
ssid	The SSID configured to the blacklist. The detection device detects this SSID for countermeasures in WIDS config mode,

Defaults N/A

Command Mode WIDS configuration mode

Usage Guide N/A

Configuration Examples The following example configures SSID: my-vlan to the SSID blacklist.

```
Ruijie(config-wids)# device black-ssid my-wlan
```

The following example removes SSID: my-vlan from the SSID blacklist.

```
Ruijie(config-wids)#no device black-ssid my-wlan
```

Platform Description N/A

2.20 device channel-bind

Use this command to configure channel scan for a specified radio. Use the **no** form of this command to restore the default setting.

device channel-bind radio *radio-id* { **channel** *num* | **max-cycles** *value* }

no device channel-bind radio *radio-id*

Parameter Description

Parameter	Description
radio *radio-id*	Radio ID.
channel *num*	Channel number in the range from 1 to 255.
max-cycles *value*	Scan cycle in the range from 0 to 255.

Defaults The **channel** is CCnet and the **max-cycles** is 10 by default.

Command Mode AP configuration mode

Usage Guide N/A

Configuration Examples The following example configures the scan cycle to 20.

```
Ruijie#configure
Ruijie(config)#ap-config ap1
Ruijie(config-ap)#device channel-bind radio 1 max-cycles 20
```

Platform Description N/A

2.21 device detected-ap-max

Use this command to configure the maximum number of detected AP list members. Use the **no** form

of this command to restore the default setting.

device detected-ap-max *num*

no device detected-ap-max *num*

Parameter Description

Parameter	Description
detected-ap-max *num*	The maximum number of detected AP list members.

Defaults The default is 2048.

Command Mode WIDS configuration mode

Usage Guide N/A

Configuration Examples The following example configures the maximum number of detected AP list members to 1000.

```
Ruijie#configure
Ruijie(config)#wids
Ruijie(config-wids)#device detected-ap-max 1000
```

Platform Description N/A

2.22 device friendly-flags

Use this command to configure the friendly flag on a device. Use the **no** form of this command to restore the default setting.

device friendly-flags *value*

no device friendly-flags

Parameter Description

Parameter	Description
value	Friendly flag value in the range from 1 to 4294967295.

Defaults The default is 0.

Command Mode WIDS configuration mode

Usage Guide By configuring the friendly flag, AC/AP is able to recognize a friendly AP. The default is random configuration.

Configuration Examples The following example configures the friendly flag to 4294967295.

```
Ruijie(config-wids)# device friendly-flags 4294967295
```

The following example restores the friendly flag to the default setting.

```
Ruijie(config-wids)#no device friendly-flags
```

Platform Description N/A

2.23 device max-black-ssid

Use this command to configure the maximum number of the SSID blacklist. Use the **no** form of this command to restore the default setting.

device max-black-ssid *num*

no device max-black-ssid

Parameter Description

Parameter	Description
num	The maximum number of the SSID blacklist in the range from 1 to 1024.

Defaults The default is 512.

Command Mode WIDS configuration mode

Usage Guide N/A

Configuration Examples The following example configures the maximum number of the SSID blacklist to 900.

```
Ruijie(config-wids)# device max-black-ssid 900
```

The following example restores the default setting.

```
Ruijie(config-wids)#no device max-black-ssid
```

Platform Description N/A

2.24 device mode

Use this command to configure the working mode of the AP. Use the **no** form of this command to restore the default setting.

device mode { **monitor** | **normal** | **hybrid** } [**radio** *radio-id*]

no device mode

Parameter

Parameter	Description

Description

monitor	Indicates AP works in the monitor mode.
normal	Indicates AP works in the normal mode.
hybrid	Indicates AP works in the hybrid mode.
radio	Specifies a radio to work in the monitor mode, while other radios to work in normal mode.

Defaults The AP works in the normal mode by default.

Command Mode AP configuration mode

Usage Guide N/A

Configuration Examples The following example sets the working mode of the AP to **hybrid**.

```
Ruijie#configure
Enter configuration commands, one per line.  End with CNTL/Z.
Ruijie(config)#ap-config ap1
Ruijie(config-ap)#device mode hybrid
```

The following example sets the working mode of the radio3 to **monitor**.

```
Ruijie#configure ter
Enter configuration commands, one per line.  End with CNTL/Z.
Ruijie(config)#ap-config ap1
Ruijie(config-ap)#device mode monitor radio 3
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

2.25 device permit mac-address

Use this command to configure an entry for the permissible MAC address list. Use the **no** form of this command to delete an entry from the permissible MAC address list.

device permit mac-address *H.H.H*

no device permit mac-address *H.H.H*

Parameter Description

Parameter	Description
H.H.H	Indicates the device with this source MAC address is legal.

Defaults N/A

Command Mode WIDS configuration mode

Usage Guide This configuration is one of the policies for detecting rogue devices.

Configuration Examples The following example configures the device with the permissible source MAC address of 0000.0000.0001.

```
Ruijie(config-wids)# device permit mac-address 0000.0000.0001
```

The following example deletes the device with the permissible source MAC address of 0000.0000.0001.

```
Ruijie(config-wids)#no device permit mac-address 0000.0000.0001
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

2.26 device permit mac-address max

Use this command to configure the maximum number of the permissible MAC address list.
Use the **no** form of this command to restore the default setting.
device permit mac-address max *num*
no device permit mac-address max

Parameter Description

Parameter	Description
num	Specifies the maximum number of the permissible MAC address list in the range from 1 to 2048.

Defaults The default is 1024.

Command Mode WIDS configuration mode

Usage Guide N/A

Configuration Examples The following example sets the maximum number of the permissible MAC address list to 1000.

```
Ruijie(config-wids)# device permit mac-address max 1000
```

The following example restores the default setting.

```
Ruijie(config-wids)#no device permit mac-address max
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

2.27 device permit ssid

Use this command to configure an entry for the permissible SSID list. Use the **no** form of this command to delete an entry for the permissible SSID list.

device permit ssid *ssid*

no device permit ssid *ssid*

Parameter Description

Parameter	Description
ssid	Configures this SSID to the permissible SSID list.

Defaults N/A

Command Mode WIDS configuration mode

Usage Guide This configuration is one of the policies for detecting rogue devices.

Configuration Examples The following example configures SSID: my-wlan to the permissible SSID list.

```
Ruijie(config-wids)# device permit ssid my-wlan
```

The following example removes SSID: my-wlan from the permissible SSID list.

```
Ruijie(config-wids)#no device permit ssid my-wlan
```

Platform Description N/A

2.28 device permit max-ssid

Use this command to configure the maximum number of the permissible SSID list members. Use the **no** form of this command to restore the default setting.

device permit max-ssid *num*

no device permit max-ssid

Parameter Description

Parameter	Description
num	Specifies the maximum number of permissible SSID list members in the range from 1 to 1024.

Defaults The default is 512.

Command Mode WIDS configuration mode

Usage Guide N/A

Configuration Examples The following example sets the maximum number of the permissible SSID list members to 900.

```
Ruijie(config-wids)# device permit max-ssid 900
```

The following example restores the default setting.

```
Ruijie(config-wids)#no device permit max-ssid
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

2.29 device permit vendor bssid

Use this command to configure an entry for the permissible vendor list. Use the **no** form of this command to delete an entry for the permissible vendor list.

device permit vendor bssid *H.H.H*

no device permit vendor bssid *H.H.H*

Parameter Description

Parameter	Description
H.H.H	Indicates this vendor's address is a permissible address.

Defaults N/A

Command Mode WIDS configuration mode

Usage Guide The vendor number is used to configure the first three bytes of a MAC address. Do not configure

multiple MAC addresses with the same vendor number. This configuration is one of the policies for detecting Rogue devices.

Configuration Examples The following example configures the MAC address 0000.0000.0001 into the permissible vendor list.

```
Ruijie(config-wids)# device permit vendor bssid 0000.0000.0001
```

The following example deletes the MAC address 0000.0000.0001 from the permissible vendor list.

```
Ruijie(config-wids)#no device permit vendor bssid 0000.0000.0001
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

2.30 device permit vendor bssid max

Use this command to configure the maximum number of the permissible vendor list members.
Use the **no** form of this command to restore the default setting.
device permit vendor bssid max *num*
no device permit vendor bssid max

Parameter Description

Parameter	Description
num	Specifies the maximum number of the permissible vendor list members in the range from 1 to 1024.

Defaults The default is 512.

Command Mode WIDS configuration mode

Usage Guide N/A

Configuration Examples The following example sets the maximum number of the permissible vendor list members to 1000.

```
Ruijie(config-wids)# device permit vendor bssid max 1000
```

The following example restores the default setting.

```
Ruijie(config-wids)#no device permit vendor bssid max
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

2.31 device scan-para

Use this command to configure Rogue AP detection parameters according to *CMCC WLAN AC-AP Interoperability Specification*.

device scan-para { **radio** *radio-id* **scan-type** { **active** | **passive** } **device-detect** { **enable** | **disable** } | **ap-mode** { **normal** | **monitor** } | **detect-rpt-time** *time* }

no device scan-para { **radio** *radio-id* | **ap-mode** | **detect-rpt-time** }

Parameter Description

Parameter	Description
radio *radio-id*	Radio ID.
scan-type active	Scan type: active.
scan-type passive	Scan type: passive.
device-detect enable	Enables detection.
device-detect disable	Disables detection.
ap-mode normal	AP operation mode: normal mode.
ap-mode monitor	AP operation mode: monitor mode.
detect-rpt-time *time*	Detection report interval in the range from 60 to 120 in the unit of seconds.

Defaults The scan type is passive, detection is disabled and detection report interval is 60 seconds by default.

Command Mode AP configuration mode

Usage Guide N/A

Configuration Examples The following example restores for Rogue AP detection type and status to the default setting according to *CMCC WLAN AC-AP Interoperability Specification*.

```
Ruijie#configure
Enter configuration commands, one per line.  End with CNTL/Z.
Ruijie(config)#ap-config ap1
Ruijie(config-ap)#no device scan-para radio 1
```

Platform Description N/A

2.32 device unknown-sta dynamic-enable

Use this command to enable dynamic unknown STA detection. Use the **no** form of this command to restore the default setting.

device unknown-sta dynamic-enable

no device unknown-sta dynamic-enable

Parameter Description

Parameter	Description
N/A	N/A

Defaults The function is disabled by default.

Command Mode WIDS configuration mode

Usage Guide This command takes effect only when the AP works in the normal mode,

Configuration Examples The following example enables dynamic unknown STA detection.

```
Ruijie(config-wids)# device unknown-sta dynamic-enable
```

The following example disables dynamic unknown STA detection.

```
Ruijie(config-wids)#no device unknown-sta dynamic-enable
```

Platform Description N/A

2.33 device unknown-sta mac-address

Use this command to configure an entry for the static unknown STA list. Use the **no** form of this command to delete an entry for the static unknown STA list.

device unknown-sta mac-address *H.H.H*

no device unknown-sta mac-address *H.H.H*

Parameter Description

Parameter	Description
H.H.H	Indicates that the user of this MAC address is unknown STA.

Defaults N/A

Command Mode WIDS configuration mode

Usage Guide This command is one of the policies for detecting Rogue devices.

Configuration Examples The following example configures the MAC address 0000.0000.0001 to the unknown STA list.

```
Ruijie(config-wids)# device unknown-sta mac-address 0000.0000.0001
```

The following example removes the MAC address 0000.0000.0001 from the unknown STA list.

```
Ruijie(config-wids)#no device unknown-sta mac-address 0000.0000.0001
```

Platform Description N/A

2.34 device unknown-sta mac-address max

Use this command to configure the maximum number of the unknown STA list members. Use the **no** form of this command to restore the default setting,

device unknown-sta mac-address max *num*

no device unknown-sta mac-address max

Parameter Description

Parameter	Description
num	The maximum number of the unknown STA list members in the range from 1 to 256.

Defaults The default is 128.

Command Mode WIDS configuration mode

Usage Guide N/A

Configuration Examples The following example configures the maximum number of the unknown STA list members to 200.

```
Ruijie(config-wids)# device unknown-sta mac-address max 200
```

The following example restores the maximum number of the unknown STA list members to the default setting.

```
Ruijie(config-wids)#no device unknown-sta mac-address max
```

Platform Description N/A

2.35 device unknown-sta report enable

Use this command to report detected unknown STAs to the AC. Use the **no** form of this command to

disable this function,
device unknown-sta report enable
no device unknown-sta report enable

Parameter Description

Parameter	Description
N/A	N/A

Defaults By default, this function is disabled.

Command Mode WIDS configuration mode

Usage Guide This function takes effect only when the AP does not operate in Normal mode. The scanning result can be reported to the AC.

Configuration Examples The following example enables reporting detected unknown STAs to the AC.

```
Ruijie(config-wids)# device unknown-sta report enable
```

The following example disables reporting detected unknown STAs to the AC.

```
Ruijie(config-wids)# no device unknown-sta report enable
```

Platform Description N/A

2.36 dos-detection

Use this command to enable DOS attack detection and its threshold according to *CMCC WLAN AC-AP Interoperability Specification*. Use the **no** form of this command to restore the default setting.
dos-detection { **enable** | **threshold** *num* | **interval** *time* }
no dos-detection { **enable** | **threshold** | **interval** }

Parameter Description

Parameter	Description
enable	Enables DOS attack detection.
threshold *num*	Packet threshold in the range from 1 to 5000.
Interval *time*	Detection interval in the range from 1 to 60000 in the unit of milliseconds.

Defaults This function is disabled, **threshold** is 30, and **interval** is 1000 milliseconds by default.

Command Mode WIDS configuration mode

Usage Guide N/A

Configuration Examples The following example enable DOS attack detection according to *CMCC WLAN AC-AP Interoperability Specification*.

```
Ruijie(config-wids)#dos-detection enable
```

Platform Description N/A

2.37 dynamic-blacklist enable

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

dynamic-blacklist enable

no dynamic-blacklist enable

Parameter Description

Parameter	Description
N/A	N/A

Defaults This function is disabled by default.

Command Mode WIDS configuration mode

Usage Guide N/A

Configuration Examples The following example enables the dynamic blacklist.

```
Ruijie(config-wids)# dynamic-blacklist enable
```

The following example disables the dynamic blacklist.

```
Ruijie(config-wids)#no dynamic-blacklist enable
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

2.38 dynamic-blacklist lifetime

Use this command to configure the dynamic blacklist entry lifetime. Use the **no** form of this command

to restore the default setting.

dynamic-blacklist lifetime *time*

no dynamic-blacklist lifetime

Parameter Description

Parameter	Description
time	Indicates the dynamic blacklist entry lifetime in the range from 60 to 1200 in the unit of seconds.

Defaults The default is 300 seconds.

Command Mode WIDS configuration mode

Usage Guide N/A

Configuration Examples The following example sets the dynamic blacklist entry lifetime to 600 seconds.

```
Ruijie(config-wids)# dynamic-blacklist lifetime 600
```

The following example restores the default setting.

```
Ruijie(config-wids)#no dynamic-blacklist lifetime
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

2.39 dynamic-blacklist ac-max

Use this command to configure the maximum number of the dynamic blacklist members on the AC. Use the **no** form of this command to restore the default setting.

dynamic-blacklist ac-max *num*

no dynamic-blacklist ac-max

Parameter Description

Parameter	Description
num	The maximum number of the dynamic blacklist members on the AC in the range from 1 to 4096.

Defaults The default is 2048.

Command WIDS configuration mode

Mode

Usage Guide N/A

Configuration Examples The following example configures the maximum number of the dynamic blacklist members on the AC to 2000.

```
Ruijie(config-wids)# dynamic-blacklist ac-max 2000
```

The following example restores the default setting.

```
Ruijie(config-wids)#no dynamic-blacklist ac-max
```

Platform Description N/A

2.40 dynamic-blacklist ap-max

Use this command to configure the maximum number of dynamic blacklist members on the AP. Use the **no** form of this command to restore the default setting.
dynamic-blacklist ap-max *num*
no dynamic-blacklist ap-max

Parameter Description

Parameter	Description
num	The maximum number of the dynamic blacklist on the AP in the range from 1 to 4096.

Defaults The default is 2048.

Command Mode WIDS configuration mode

Usage Guide N/A

Configuration Examples The following example configures the maximum number of dynamic blacklist members on the AP to 1000.

```
Ruijie(config-wids)# dynamic-blacklist ap-max 1000
```

The following example restores the default setting.

```
Ruijie(config-wids)#no dynamic-blacklist ap-max
```

Platform Description N/A

2.41 hybrid-scan radio

Use this command to enable the radio scan. Use the **no** form of this command to disable the radio scan.

hybrid-scan radio *num* **enable**

hybrid-scan radio *num* **disable**

Parameter Description

Parameter	Description
radio *num*	Radio number.

Defaults This function is enabled by default.

Command Mode AP configuration mode

Usage Guide N/A

Configuration Examples The following example disables the scan for radio 1.

```
Ruijie#configure
Ruijie(config)#ap-config ap1
Ruijie(config-ap)#hybrid-scan radio 1 disable
```

Platform Description N/A

2.42 kickout client

Use this command to kick out associate users.

kickout client *H.H.H*

Parameter Description

Parameter	Description
H.H.H	The MAC address of the user to kick out.

Defaults N/A

Command Mode WIDS configuration mode

Usage Guide Use this command to disconnect a specified STA association.

Configuration The following example kicks out the MAC address 0000.0000.0001.

Examples

```
Ruijie(config-wids)# kickout client 0000.0000.0001
```

Platform Description N/A

2.43 kickout threshold

Use this command to kick out the low-rate STA. Use the **no** form of this command to restore the default setting.

kickout threshold *rate*

no kickout threshold

Parameter Description

Parameter	Description
rate	Packet sending-receiving rate in the range from 0 to 130 in the unit of Mbps.

Defaults The default is 0, indicating not filtering low-rate STA.

Command Mode WIDS configuration mode

Usage Guide This command is used to filter the low-rate STA. When the wireless access end detects that the sending-receiving rate of STA is less than the configured threshold, it disconnects the association.

Configuration Examples The following example filters the STA with sending-receiving rate less than 20 Mbps.

```
Ruijie(config-ac)# kickout threshold 20
```

The following example disables the filtering.

```
Ruijie(config-wids)#no kickout threshold
```

Related Commands

Command	Description
wids	Enters the WIDS configuration mode.

Platform Description N/A

2.44 reset attack-list all

Use this command to clear the entries of all attack lists.

reset attack-list all

Parameter Description

Parameter	Description
N/A	N/A

Defaults N/A

Command Mode WIDS configuration mode

Usage Guide N/A

Configuration Examples The following example clears the entries of all attack lists.

```
Ruijie(config-wids)# reset attack-list all
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

2.45 reset black-ssid all

Use this command to clear the entries of the SSID blacklist.

reset black-ssid all

Parameter Description

Parameter	Description
N/A	N/A

Defaults N/A

Command Mode WIDS configuration mode

Usage Guide N/A

Configuration Examples The following example clears the entries of the SSID blacklist.

```
Ruijie(config-wids)#reset black-ssid all
```

Platform Description N/A

2.46 reset detected

Use this command to reset the device list detected in a WLAN.

reset detected { **all** | **adhoc** | **rogue** { **ap** | **client** } | **mac-address** *H.H.H* }

Parameter Description

Parameter	Description
all	Indicates you reset all devices detected in a WLAN.
adhoc	Indicates you reset the detected adhoc client.
rogue ap	Indicates you reset the detected Rogue AP.
rogue client	Indicates you reset the detected Rogue client.
mac-address *H.H.H*	Indicates you reset the device with the source MAC address H.H.H.

Defaults N/A

Command Mode WIDS configuration mode

Usage Guide N/A

Configuration Examples The following example resets the information of detected Rogue APs.

```
Ruijie(config-wids)#reset detected rogue ap
```

The following example resets the information of detected device with MAC address 0000.0000.0001.

```
Ruijie(config-wids)#reset detected mac-address 0000.0000.0001
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

2.47 reset dos-detected

Use this command to clear the information from DOS attack detection according to *CMCC WLAN AC-AP Interoperability Specification*.

reset dos-detected

Parameter Description

Parameter	Description
N/A	N/A

Defaults N/A

Command Mode WIDS configuration mode

Usage Guide N/A

Configuration Examples The following example clears the information from DOS attack detection according to *CMCC WLAN AC-AP Interoperability Specification*.

```
Ruijie(config-wids)#reset dos-detected
```

Platform Description N/A

2.48 reset dynamic-blacklist

Use this command to reset dynamic blacklist entries.

reset dynamic-blacklist { **all** | **mac-address** *H.H.H* }

Parameter Description

Parameter	Description
all	Indicates you reset all dynamic blacklist entries.
mac-address *H.H.H*	Indicates you reset the dynamic blacklist entry with the source MAC address H.H.H.

Defaults N/A

Command Mode WIDS configuration mode

Usage Guide N/A

Configuration Examples The following example resets the dynamic blacklist entry with the source MAC address 0000.0000.0001.

```
Ruijie(config)# wids
Ruijie(config-wids)# reset dynamic-blacklist mac-address 0000.0000.0001
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

2.49 reset permit-mac all

Use this command to clear the entries of all permissible MAC address lists.

reset permit-mac all

Parameter Description

Parameter	Description
N/A	N/A

Defaults N/A

Command Mode WIDS configuration mode

Usage Guide N/A

Configuration Examples The following example clears the entries of all permissible MAC address lists.

```
Ruijie(config-wids)# reset permit-mac all
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

2.50 reset permit-ssid all

Use this command to clear the entries of all permissible SSID lists.

reset permit-ssid all

Parameter Description

Parameter	Description
N/A	N/A

Defaults N/A

Command Mode WIDS configuration mode

Usage Guide N/A

Configuration Examples The following example clears the entries of all permissible SSID lists.

```
Ruijie(config-wids)# reset permit-ssid all
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

2.51 reset permit-vendor all

Use this command to clear the entries of all permissible vendor lists.

reset permit-vendor all

Parameter Description

Parameter	Description
N/A	N/A

Defaults N/A

Command Mode WIDS configuration mode

Usage Guide N/A

Configuration Examples The following example clears the entries of all permissible vendor lists.

```
Ruijie(config-wids)# reset permit-vendor all
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

2.52 reset rogue-ap detected

Use this command to clear the information from Rogue AP detection according to *CMCC WLAN AC-AP Interoperability Specification*.

reset rogue-ap detected

Parameter Description

Parameter	Description
N/A	N/A

Defaults N/A

Command Mode WIDS configuration mode

Usage Guide N/A

Configuration Examples The following example clears the information from Rogue AP detection.

```
Ruijie(config-wids)#reset rogue-ap detected
```

Platform Description N/A

2.53 reset ssid-filter

Use this command to remove all SSIDs or a specified SSID from blacklists and whitelists.

reset ssid-filter { **ssid all** | **in-ssid** *ssid* }

Parameter Description

Parameter	Description
ssid all	All SSIDs.
in-ssid *ssid*	The specified SSID.

Defaults N/A

Command Mode WIDS configuration mode

Usage Guide N/A

Configuration Examples The following example removes all SSIDs from blacklists and whitelists.

```
Ruijie(config-wids)#reset ssid-filter ssid all
```

Platform Description N/A

2.54 reset ssid-filter blacklist all

Use this command to remove all SSIDs from blacklists.

reset ssid-filter blacklist all

Parameter Description

Parameter	Description
N/A	N/A

Defaults N/A

Command Mode WIDS configuration mode

Usage Guide N/A

Configuration Examples The following example clears all the SSIDs from blacklists,

```
Ruijie(config-wids)#reset ssid-filter blacklist all
```

Platform Description N/A

2.55 reset ssid-filter blacklist all in-ssid

Use this command to remove a specified SSID from blacklists.

reset ssid-filter blacklist all in-ssid *string*

Parameter Description

Parameter	Description
string	Removes specified SSIDs from the blacklist.

Defaults N/A

Command Mode WIDS configuration mode

Usage Guide N/A

Configuration Examples The following example removes SSID: my-vlan from blacklists.

```
Ruijie(config-wids)#reset ssid-filter blacklist all in-ssid my-wlan
```

Platform N/A

Description

2.56 reset ssid-filter whitelist all

Use this command to remove all SSIDs from whitelists.

reset ssid-filter whitelist all

Parameter Description

Parameter	Description
N/A	N/A

Defaults N/A

Command Mode WIDS configuration mode

Usage Guide N/A

Configuration Examples The following example removes all SSIDs from whitelists.

```
Ruijie(config-wids)#reset ssid-filter whitelist all
```

Platform Description N/A

2.57 reset ssid-filter whitelist all in-ssid

Use this command to remove a specified SSID from whitelists.

reset ssid-filter whitelist all in-ssid *string*

Parameter Description

Parameter	Description
string	Removes all the whitelists from a specified SSID.

Defaults N/A

Command Mode WIDS configuration mode

Usage Guide N/A

Configuration Examples The following example removes SSID: my-wlan from whitelists.

```
Ruijie(config-wids)#reset ssid-filter whitelist all in-ssid my-wlan
```

Platform Description N/A

2.58 reset static-blacklist all

Use this command to clear the entries of all static blacklists.

reset static-blacklist all

Parameter Description

Parameter	Description
N/A	N/A

Defaults N/A

Command Mode WIDS configuration mode

Usage Guide N/A

Configuration Examples The following example clears the entries of all static blacklists.

```
Ruijie(config-wids)# reset static-blacklist all
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

2.59 reset statistic all

Use this command to clear attack detection statistics.

reset statistic all

Parameter Description

Parameter	Description
N/A	N/A

Defaults N/A

Command Mode WIDS configuration mode

Usage Guide N/A

Configuration Examples The following example clears attack detection statistics.

```
Ruijie(config-wids)# reset statistic all
```

Platform Description N/A

2.60 reset unknown-sta all

Use this command to clear the entries of unknown STA lists.

reset unknown-sta all

Parameter Description

Parameter	Description
N/A	N/A

Defaults N/A

Command Mode WIDS configuration mode

Usage Guide N/A

Configuration Examples The following example clears the entries of unknown STA lists.

```
Ruijie(config-wids)#reset unknown-sta all
```

Platform Description N/A

2.61 reset user-isolation-permit-list all

Use this command to clear the entries of all permissible lists for user isolation.

reset user-isolation-permit-list all

Parameter Description

Parameter	Description
N/A	N/A

Defaults N/A

Command Mode WIDS configuration mode

Usage Guide N/A

Configuration Examples The following example clears the entries of all permissible lists for user isolation.

```
Ruijie(config-wids)# reset user-isolation-permit-list all
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

2.62 reset whitelist all

Use this command to clear the entries of all whitelists.

reset whitelist all

Parameter Description

Parameter	Description
N/A	N/A

Defaults N/A

Command Mode WIDS configuration mode

Usage Guide N/A

Configuration Examples The following example clears the entries of all whitelists.

```
Ruijie(config-wids)# reset whitelist all
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

2.63 rogue-ap countermeasures enable

Use this command to enable Rogue AP countermeasures according to *CMCC WLAN AC-AP Interoperability Specification*. Use the **no** form of this command to restore the default setting.

rogue-ap countermeasures enable
no rogue-ap countermeasures enable

Parameter Description

Parameter	Description
N/A	N/A

Defaults The function is disabled by default.

Command Mode WIDS configuration mode

Usage Guide N/A

Configuration Examples The following example enables Rogue AP countermeasures.

```
Ruijie(config-wids)#rogue-ap countermeasures enable
```

The following example disables Rogue AP countermeasures.

```
Ruijie(config-wids)#no rogue-ap countermeasures enable
```

Platform Description N/A

2.64 scan-channels dual-band

Use this command to configure automatic channel scanning between two frequency bands. Use the no form of this command to restore the default setting.
scan-channels dual-band radio *radio-id*
no scan-channels dual-band radio *radio-id*

Parameter Description

Parameter	Description
radio-id	Indicates the radio ID.

Defaults By default, this function is disabled.

Command Mode AP configuration mode

Usage Guide The RF modules of partial APs support both the 2.4 GHz and 5 GHz frequency bands. When the RF modules are used for channel scanning, this command can be used for automatic channel scanning between the two frequency bands, to obtain the scanning results of these two frequency bands and perform containment. After the frequency bands are switched, channels configured by running the **scan-channels { 802.11a | 802.11b } channels** command are scanned. In addition, for some APs

that have channel restrictions, the restricted channels will be automatically skipped during channel scanning.

Configuration Examples The following example enables dual-band scanning on the Radio3 of AP1.

```
Ruijie#configure
Ruijie(config)#ap-config ap1
Ruijie(config-ap)# scan-channels dual-band radio 3
```

Platform Description N/A

2.65 scan-channels { 802.11a | 802.11b } channels

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

scan-channels { **802.11a** | **802.11b** } **channels** *nuim1 num2…num13*

no scan-channels { **802.11a** | **802.11b** }

Parameter Description

Parameter	Description
802.11a	5GHz channel.
802.11b	2.4GHz channel.
channels *num*	Channel value.

Defaults No scan channel is configured by default.

Command Mode AP configuration mode

Usage Guide N/A

Configuration Examples The following example configures the 5GHz scan channel as 149 153 157.

```
Ruijie#configure
Ruijie(config)#ap-config ap1
Ruijie(config-ap)#scan-channels 802.11a channels 149 153 157
```

Platform Description N/A

2.66 show wids attacklist

Use this command to display the WIDS static attack list.

show wids attack-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 the WIDS static attack list.

```
Ruijie# show wids attack-list
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

2.67 show wids blacklist

Use this command to display the static or dynamic blacklist.

show wids blacklist { **static** | **dynamic** }

Parameter Description

Parameter	Description
static	Displays the static blacklist.
dynamic	Displays the dynamic blacklist.

Defaults N/A

Command Mode Privileged EXEC mode.

Usage Guide N/A

Configuration Examples The following example displays the static blacklist.

```
Ruijie# show wids blacklist static
```

The following example displays the dynamic blacklist.

```
Ruijie# show wids blacklist dynamic
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

2.68 show wids black-ssid

Use this command to display the SSID blacklist.

show wids black-ssid

Parameter Description

Parameter	Description
N/A	N/A

Command Mode Privileged EXEC mode

Usage Guide N/A

Configuration Examples The following example displays the SSID blacklist.

```
Ruijie# show wids black-ssid
```

Platform Description N/A

2.69 show wids detected

Use this command to display the devices detected in a WLAN.

show wids detected { **adhoc** | **all** | **friendly ap** | **interfering ap** | **rogue** { **adhoc-ap** | **ap** | **client** | **config-ap** | **ssid-ap** } | **mac-address** *H.H.H* }

Parameter Description

Parameter	Description
adhoc	Displays the detected ad-hoc network.
all	Displays all devices detected in a WLAN.
friendly ap	Displays the detected friendly AP.
interfering ap	Displays the detected interference AP.
rogue adhoc-ap	Displays the detected Rogue ad-hoc AP.
rogue ap	Displays the detected Rogue AP.
rogue client	Displays the detected Rogue Client.

rogue config-ap	Displays the detected Rogue config AP.
rogue ssid -ap	Displays the detected Rogue SSID AP.
mac-address *H.H.H*	Displays the detected device with the source MAC address H.H.H.

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide N/A

Configuration Examples The following example displays the Rogue AP detected in a WLAN.

```
Ruijie# show wids detected rogue ap
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

2.70 show wids dos-detected

Use this command to display the information from DOS detection according to *CMCC WLAN AC-AP Interoperability Specification*.

show wids dos-detected

Parameter Description

Parameter	Description
N/A	N/A

Command Mode Privileged EXEC mode

Usage Guide N/A

Configuration Examples The following example displays the information from DOS detection according to *CMCC WLAN AC-AP Interoperability Specification*.

```
Ruijie# show wids dos-detected
```

Platform Description N/A

2.71 show wids ssid-filter

Use this command to display the blacklists and whitelists for all SSIDs or a specified SSID.

show wids ssid-filter { **blacklist all** [**in-ssid** *string*] | **ssid all** | **whitelist all** [**in-ssid** *string*] }

Parameter Description

Parameter	Description
blacklist all	Displays the blacklists for all SSIDs.
blacklist all in-ssid *string*	Displays the blacklists for a specified SSID.
ssid all	Displays the blacklists and whitelists for all SSIDs.
white all	Displays the whitelists for all SSIDs.
whitelist all in-ssid *string*	Displays the whitelists for a specified SSID.

Defaults N/A

Command Mode Privileged EXEC mode.

Usage Guide N/A

Configuration Examples The following example displays the blacklists for all SSIDs.

```
Ruijie# show wids ssid-filter blacklist all
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

2.72 show wids permitted

Use this command to display the MAC address, SSID, and vendor lists trusted in a WLAN.

show wids permitted { **mac-address** | **ssid** | **vendor** }

Parameter Description

Parameter	Description
mac-address	Displays the trusted MAC address list.
ssid	Displays the trusted SSID list.
vendor	Displays the trusted vendor list.

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide N/A

Configuration Examples The following example displays the SSID list trusted in WLAN.

```
Ruijie# show wids permitted ssid
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

2.73 show wids rogue-ap detected

Use this command to display the information from Rogue AP detection according to *CMCC WLAN AC-AP Interoperability Specification*.

show wids rogue-ap detected

Parameter Description

Parameter	Description
N/A	N/A

Command Mode Privileged EXEC mode

Usage Guide N/A

Configuration Examples The following example displays the information from Rogue AP detection according to *CMCC WLAN AC-AP Interoperability Specification.*

```
Ruijie# show wids rogue-ap detected
```

Platform Description N/A

2.74 show wids statistics

Use this command to display the IDS attack detection statistics.

show wids statistics

Parameter

Parameter	Description

Description

N/A	N/A

Defaults N/A

Command Mode Privileged EXEC mode.

Usage Guide N/A

Configuration Examples The following example displays the IDS attack detection statistics.

```
Ruijie# show wids statistics
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

2.75 show wids unknown-sta

Use this command to display the entries of unknown STA lists.

show wids unknown-sta

Parameter Description

Parameter	Description
N/A	N/A

Command Mode Privileged EXEC mode

Usage Guide N/A

Configuration Examples The following example displays the entries of unknown STA lists.

```
Ruijie# show wids unknown-sta
```

Platform Description N/A

2.76 show wids user-isolation permit-mac

Use this command to display the information of the permissible MAC address list for user isolation.

show wids user-isolation permit-mac

Parameter Description

Parameter	Description
N/A	N/A

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide N/A

Configuration Examples The following example displays the information of the permissible MAC address list for user isolation.

```
Ruijie# show wids user-isolation permit-mac
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

2.77 show wids whitelist

Use this command to display the whitelist.

show wids whitelist

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 whitelist.

```
Ruijie# show wids whitelist
```

Related Commands

Command	Description

N/A	N/A

Platform Description N/A

2.78 ssid-filter max

Use this command to configure the maximum number of the blacklist and whitelist members for SSIDs. Use the **no** form of this command to restore the default setting.

ssid-filter max *num*

no ssid-filter max

Parameter Description

Parameter	Description
num	The maximum number of the blacklist and whitelist members in the range from 1 to 128.

Defaults The default is 64.

Command Mode WIDS configuration mode

Usage Guide N/A

Configuration Examples The following example configures the maximum number of the blacklist and whitelist members for SSIDs as 40.

```
Ruijie(config-wids)# ssid-filter max 40
```

The following example restores the default setting.

```
Ruijie(config-wids)#no ssid-filter max
```

Platform Description N/A

2.79 ssid-filter blacklist mac-address in-ssid

Use this command to configure an entry for a specified SSID blacklist. Use the **no** form of this command to restore the default setting.

ssid-filter blacklist mac-address *H.H.H* **in-ssid** *string*

no ssid-filter blacklist mac-address *H.H.H* **in-ssid** *string*

Parameter Description

Parameter	Description

H.H.H	The MAC address of an entry to configure.
string	SSID.

Defaults N/A

Command Mode WIDS configuration mode

Usage Guide This command is not allowed to use when there is the same entry in the SSID whitelist,

Configuration Examples The following example configures MAC 0000.0000.0001 for the blacklist of SSID: my-wlan.

```
Ruijie(config-wids)# ssid-filter blacklist mac-address 0000.0000.0001 in-ssid my-wlan
```

The following example restores the default setting.

```
Ruijie(config-wids)# no ssid-filter blacklist mac-address 0000.0000.0001 in-ssid my-wlan
```

Platform Description N/A

2.80 ssid-filter blacklist max

Use this command to set the maximum number of the SSID blacklist members. Use the **no** form of this command to restore the default setting.

ssid-filter blacklist max *num*

no ssid-filter blacklist max

Parameter Description

Parameter	Description
num	The maximum number of SSID blacklist members in the range from 1 to 2,048.

Defaults The default is 256.

Command Mode WIDS configuration mode

Usage Guide N/A

Configuration Examples The following example sets the maximum number of the blacklist members as 50.

```
Ruijie(config-wids)#ssid-filter blacklist max 50
```

The following example restores the default setting.

```
Ruijie(config-wids)#no sid-filter blacklist max
```

Platform Description N/A

2.81 ssid-filter whitelist mac-address in-ssid

Use this command to configure an entry for a specified SSID whitelist. Use the **no** form of this command to restore the default setting.
ssid-filter whitelist mac-address *H.H.H* **in-ssid** *string*
no ssid-filter whitelist mac-address *H.H.H* **in-ssid** *string*

Parameter Description

Parameter	Description
H.H.H	The MAC address of the entry configured for the specified SSID whitelist.
string	The specified SSID.

Defaults N/A

Command Mode WIDS configuration mode

Usage Guide This command is not allowed to use when there is the same entry in the SSID blacklist,

Configuration Examples The following example configures MAC 0000.0000.0001 to the whitelist of SSID: my-wlan.

```
Ruijie(config-wids)# ssid-filter whitelist mac-address 0000.0000.0001 in-ssid my-wlan
```

The following example restores the default setting.

```
Ruijie(config-wids)# no ssid-filter whitelist mac-address 0000.0000.0001 in-ssid my-wlan
```

Platform Description N/A

2.82 ssid-filter whitelist max

Use this command to set the maximum number of the SSID whitelist members. Use the **no** form of this command to restore the default setting.
ssid-filter whitelist max *num*
no ssid-filter whitelist max

Parameter Description

Parameter	Description
num	The maximum number of the SSID whitelist members in the range from 1 to 2,048.

Defaults The default is 256

Command Mode WIDS configuration mode

Usage Guide N/A

Configuration Examples The following example sets the maximum number of the whitelist members as 50.

```
Ruijie(config-wids)#ssid-filter whitelist max 50
```

The following example restores the default setting.

```
Ruijie(config-wids)#no sid-filter whitelist max
```

Platform Description N/A

2.83 static-blacklist mac-address

Use this command to configure an entry for the static blacklist. Use the **no** form of this command to delete the static blacklist

static-blacklist mac-address *H.H.H*

no static-blacklist mac-address *H.H.H*

Parameter Description

Parameter	Description
H.H.H	Indicates you set the device with the source MAC address H.H.H as a static blacklist entry.

Defaults N/A

Command Mode WIDS configuration mode

Usage Guide If the MAC address is configured in the whitelist, the blacklist configuration is not permitted.

Configuration Examples The following example configures the device with the source MAC address 0000.0000.0001 to the static blacklist.

```
Ruijie(config-wids)# static-blacklist mac-address 0000.0000.0001
```

The following example restores the default setting.

```
Ruijie(config-wids)# no static-blacklist mac-address 0000.0000.0001
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

2.84 static-blacklist max

Use this command to configure the maximum number of static blacklist members.

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

static-blacklist max *number*

no static-blacklist max

Parameter Description

Parameter	Description
number	Specifies the maximum number of static blacklist members in the range from 1 to 2048.

Defaults The default is 1024.

Command Mode WIDS configuration mode

Usage Guide N/A

Configuration Examples The following example sets the maximum number of static blacklist members to 1000.

```
Ruijie(config-wids)# static-blacklist max 1000
```

The following example restores the default setting.

```
Ruijie(config-wids)#no static-blacklist max
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

2.85 user-isolation enable

Use this command to enable user isolation on the AP or AC. Use the **no** form of this command to disable this function.

user-isolation { **ac** | **ap** | **ssid-ac** | **ssid-ap** | **wlan-id** *num* } **enable**

no user-isolation { **ac** | **ap** | **ssid-ac** | **ssid-ap** | **wlan-id** *num* } **enable**

Parameter Description

Parameter	Description
ac	Enables user isolation on the AC.
ssid-ac	Enables SSID-based user isolation on the AC.
ap	Enables user isolation on the AP.
ssid-ap	Enables SSID-based user isolation on the AP.
wlan-id *num*	Enables WLAN based user isolation on the AP according to *CMCC WLAN AC-AP Interoperability Specification*.

Defaults This function is disabled by default.

Command Mode WIDS configuration mode

Usage Guide N/A

Configuration Examples The following example enables user isolation on an AC.

```
Ruijie(config-wids)# user-isolation ac enable
```

The following example restores the default setting.

```
Ruijie(config-wids)#no user-isolation ac enable
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

2.86 user-isolation permit-mac mac

Use this command to configure a permissible MAC address list for user isolation. Use the **no** form of this command to delete a permissible MAC address.

user-isolation permit-mac mac *H.H.H*

no user-isolation permit-mac mac *H.H.H*

Parameter Description

Parameter	Description
H.H.H	The permissible MAC address list for user isolation.

Defaults N/A

Command Mode WIDS configuration mode

Usage Guide N/A

Configuration Examples The following example sets MAC 0000.0000.0001 as a permissible MAC for user isolation.

```
Ruijie(config-wids)# user-isolation permit-mac mac-list 0000.0000.0001
```

The following example deletes MAC 0000.0000.0001 from the permissible MAC address list.

```
Ruijie(config-wids)#no user-isolation permit-mac 0000.0000.0001
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

2.87 user-isolation permit-mac max

Use this command to configure the maximum number of a permissible MAC address list for user isolation.

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

user-isolation permit-mac max *num*

no user-isolation permit-mac max

Parameter Description

Parameter	Description
num	The maximum number of a permissible MAC address list for user isolation in the range from 1 to 2048.

Defaults The default is 1024.

Command Mode WIDS configuration mode

Usage Guide N/A

Configuration Examples The following example sets the maximum number of a permissible MAC address list for user isolation to 100.

```
Ruijie(config-wids)# user-isolation permit-mac max 100
```

The following example restores the default setting.

```
Ruijie(config-wids)#no user-isolation permit-mac max
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

2.88 whitelist mac-address

Use this command to configure an entry for the whitelist. Use the **no** form of this command to delete the whitelist.

whitelist mac-address *H.H.H*

no whitelist mac-address *H.H.H*

Parameter Description

Parameter	Description
H.H.H	Indicates you set the device with the source MAC address H.H.H as a whitelist entry.

Defaults N/A

Command Mode WIDS configuration mode

Usage Guide N/A

Configuration Examples The following example configures the device with the source MAC address 0000.0000.0001 to the whitelist.

```
Ruijie(config-wids)# whitelist mac-address 0000.0000.0001
```

The following example deletes the device with the source MAC address 0000.0000.0001 from the whitelist.

```
Ruijie(config-wids)# no whitelistmac-address 0000.0000.0001
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

2.89 whitelist max

Use this command to configure the maximum number of whitelists.

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

whitelist max *num*

no whitelist max

Parameter Description

Parameter	Description
num	Specifies the maximum number of whitelists in the range from 1 to 2048.

Defaults The default is 1024.

Command Mode WIDS configuration mode

Usage Guide N/A

Configuration Examples The following example sets the maximum number of whitelists to 1000.

```
Ruijie(config-wids)# whitelist max 1000
```

The following example restores the default setting.

```
Ruijie(config-wids)#no whitelist max
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

2.90 wids

Use this command to enter the WIDS configuration mode.

wids

Parameter Description

Parameter	Description

N/A	N/A

Defaults N/A

Command Mode Global configuration mode

Usage Guide N/A

Configuration Examples The following example enters the WIDS configuration mode.

```
Ruijie(config)# wids
Ruijie(config-wids)#
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

3 CPU Protection Commands

3.1 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

3.2 mgmt-ratelimit

Use this command to perform rate limit on wireless management packets. Use the no form of this command to restore the default setting.

mgmt-ratelimit { **disable** | **per-cti pps** *value* | **total pps** *value* }

no mgmt-ratelimit { **disable** | **per-cti pps** | **total pps** }

Parameter Description

Parameter	Description
disable	Disables the rate limit function.
per-cti pps *value*	Rate limit on CTI-based wireless management packets.
total pps *value*	Rate limit on AC-based wireless management packets.

Defaults This function is only supported on the AC.
The default rate limit on CTI-based wireless management packets is 8 pps.
The default rate limit on AC-based wireless management packets varies the AC model.

Command Mode Global configuration mode

Usage Guide N/A

Configuration Examples The following example sets the rate limit on AC-based wireless management packets to 200pps.

```
Ruijie(config)#mgmt-ratelimit total pps 200
```

Related Command

Command	Description
N/A	N/A

Platform Description N/A

3.3 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

3.4 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 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.

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

3.5 show mgmt-ratelimit cti

Use this command to display statistics about CTI-based wireless management packets.

show mgmt-ratelimit cti *ifx*

Parameter Description

Parameter	Description
cti *ifx*	**I**nterface index of the specified CTI.

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide N/A

Configuration Examples The following example displays statistics about CTI-based wireless management packets whose interface index is 9.

```
Ruijie#show mgmt-ratelimit cti 9
```

Related Command

Command	Description
N/A	N/A

Platform Description N/A

3.6 show mgmt-ratelimit summary

Use this command to display statistics about AC-based wireless management packets.

show mgmt-ratelimit 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 statistics about AC-based wireless management packets.

```
Ruijie#show mgmt-ratelimit summary
```

Related Command

Command	Description
N/A	N/A

Platform Description N/A

4 NFPP Commands

4.1 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

4.2 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

4.3 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

4.4 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

4.5 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

4.6 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

4.7 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

4.8 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

4.9 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

4.10 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

4.11 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

4.12 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

4.13 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

4.14 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

4.15 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

4.16 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

4.17 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

4.18 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

4.19 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

4.20 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

4.21 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

4.22 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

4.23 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

4.24 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

4.25 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

4.26 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

4.27 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

4.28 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

4.29 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

4.30 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

4.31 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

4.32 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

4.33 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

4.34 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

4.35 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

4.36 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

4.37 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

4.38 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

4.39 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

4.40 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

4.41 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

4.42 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

4.43 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 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)# ip-guard monitored-host-limit 200
```

Related Commands

Command	Description
show nfpp ip-guard summary	Displays the configuration.

Platform Description N/A

4.44 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

4.45 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

4.46 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

4.47 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

4.48 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. 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). 0 indicates not to write the log to the buffer but generate the syslog immediately. With both the *number_of_message* and *length_in_seconds* values are 0, it indicates not to write the log to the buffer 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

4.49 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

4.50 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

4.51 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

4.52 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

4.53 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

4.54 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

4.55 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

4.56 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

4.57 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

4.58 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

4.59 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

4.60 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

4.61 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

4.62 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

4.63 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

4.64 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

4.65 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

4.66 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

4.67 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

4.68 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

4.69 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

4.70 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

4.71 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

4.72 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

4.73 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

4.74 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

4.75 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

4.76 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

4.77 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

4.78 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

4.79 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

4.80 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

4.81 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

4.82 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

4.83 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

4.84 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

4.85 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

4.86 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

4.87 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

4.88 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

4.89 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 2. ISOLATED 3. ISOLATE_FAILE 4. SCAN 5. PORT_ATTACKED

Related

Command	Description

Commands		
	clear nfpp log	Clears the NFPP log buffer.

Platform Description N/A

4.90 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

4.91 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

5 WAPI Commands

5.1 security wapi

Use this command to enable or disable WAPI security mode.

security wapi { **enable | disable** }

Parameter Description

Parameter	Description
enable	Enables WAPI security mode.
disable	Disables WAPI security mode.

Defaults This function is disabled by default.

Command mode WLAN security configuration mode

Usage Guide N/A

Configuration Examples The following example enables WAPI security mode.

```
Ruijie(wlansec)# security wapi enable
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

5.2 security wapi 2-cert

Use this command to enable or disable two-certificate authentication.

security wapi 2-cert { **enable** | **disable** }

Parameter Description

Parameter	Description
enable	Enables two-certificate authentication.
disable	Disables two-certificate authentication.

Defaults This function is disabled by default.

Command WLAN security configuration mode

mode

Usage Guide Before running this command, ensure that WAPI security mode has been enabled.
Two-certificate authentication mode and three-certificate authentication mode cannot be used synchronously.

Configuration Examples The following example enables two-certificate authentication.

```
Ruijie(wlansec)# security wapi 2-cert enable
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

5.3 security wapi 3-cert

Use this command to enable or disable three-certificate authentication.
security wapi 3-cert { **enable** | **disable** }

Parameter Description

Parameter	Description
enable	Enables three-certificate authentication.
disable	Disables three-certificate authentication.

Defaults This function is disabled by default.

Command mode WLAN security configuration mode

Usage Guide Before running this command, ensure that WAPI security mode has been enabled.
Two-certificate authentication mode and three-certificate authentication mode cannot be used synchronously.

Configuration Examples The following example enables three-certificate authentication.

```
Ruijie(wlansec)# security wapi 3-cert enable
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

5.4 security wapi ae cert

Use this command to configure a WAPI certificate for an AE.

security wapi ae cert *ae_certfile*

Parameter Description

Parameter	Description
ae_certfile	Specifies the certificate file of the AE.

Defaults N/A

Command mode WLAN security configuration mode

Usage Guide Before running this command, ensure that WAPI security mode has been enabled and the certificate file has been imported into the AE.

Configuration Examples The following example enables WAPI security mode for WLAN 1 and specifies AE certificate EccAE.cer.

```
Ruijie# configure terminal
Ruijie(config)# wlansec 1
Ruijie(wlansec)# security wapi enable
Ruijie(wlansec)# security wapi ae cert EccAE.cer
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

5.5 security wapi asu address

Use this command to set an IP address for an ASU in certificate authentication mode.

security wapi asu address *ip_address*

Parameter Description

Parameter	Description
ip_address	Specifies the IP address of the ASU.

Defaults N/A

Command WLAN security configuration mode

mode

Usage Guide Enable WAPI security mode before setting an IP address for the ASU.

Configuration Examples The following example enables WAPI security mode for WLAN 1 and sets IP address 192.168.1.123 for the ASU.

```
Ruijie# configure terminal
Ruijie(config)# wlansec 1
Ruijie(wlansec)# security wapi enable
Ruijie(wlansec)# security wapi asu address 192.168.1.123
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

5.6 security wapi asu cert

Use this command to configure an ASU certificate in three-certificate authentication mode.
security wapi asu cert *asu_certfile*

Parameter Description

Parameter	Description
asu_certfile	Specifies the name of the ASU certificate file.

Defaults N/A

Command mode WLAN security configuration mode

Usage Guide Before running this command, ensure that WAPI security mode has been enabled and the certificate file has been imported into the AE.
In three-certificate authentication mode, you need to configure an ASU certificate.
In two-certificate authentication mode, the ASU certificate is not needed.

Configuration Examples The following example enables WAPI security mode for WLAN 1 and specifies ASU certificate EccASU.cer.

```
Ruijie# configure terminal
Ruijie(config)# wlansec 1
Ruijie(wlansec)# security wapi enable
Ruijie(wlansec)# security wapi asu cert EccASU.cer
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

5.7 security wapi ca cert

Use this command to configure a CA certificate.

security wapi ca cert *ca_certfile*

Parameter Description

Parameter	Description
ca_certfile	Specifies the name of the CA certificate file.

Defaults N/A

Command mode WLAN security configuration mode

Usage Guide Before running this command, ensure that WAPI security mode has been enabled and the certificate file has been imported into the device.
In two-certificate authentication mode, the CA is also the ASU. Therefore, a CA certificate is an ASU certificate. You do not need to configure an ASU certificate separately.
In three-certificate authentication mode, the certificate issuing system is separated from the certificate authentication system. The certificate management system is responsible for issuing ASU certificates. Therefore, you need to configure an ASU certificate.

Configuration Examples The following example enables WAPI security mode for WLAN 1 and specifies CA certificate EccCA.cer.

```
Ruijie# configure terminal
Ruijie(config)# wlansec 1
Ruijie(wlansec)# security wapi enable
Ruijie(wlansec)# security wapi ca cert EccCA.cer
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

5.8 security wapi psk

Use this command to enable or disable pre-sharing key (PSK) authentication.

security wapi psk { **enable | disable** }

Parameter Description

Parameter	Description
enable	Enables PSK authentication.
disable	Disables PSK authentication.

Defaults This function is disabled by default.

Command mode WLAN security configuration mode

Usage Guide Before running this command, ensure that WAPI security mode has been enabled.

Configuration Examples The following example enables PSK authentication.

```
Ruijie(wlansec)# security wapi psk enable
```

Related Commands

Command	Description
security wapi psk set-key { **ascii** | **hex** }	Configures a WAPI PSK.

Platform Description N/A

5.9 security wapi psk set-key

Use this command to set a WAPI PSK.

security wapi 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 Before running this command, ensure that WAPI security mode has been enabled.
The length of the PSK is from 8 to 32 bits.
ascii: Specifies an ASCII PSK.
hex: Specifies a hexadecimal PSK. The length of the password must be an even number.

Configuration Examples The following example enables PSK authentication for WLAN 1 and sets the PSK to 12345678.

```
Ruijie# configure terminal
Ruijie(config)# wlansec 1
Ruijie(wlansec)# security wapi enable
Ruijie(wlansec)# security wapi psk enable
Ruijie(wlansec)# security wapi psk set-key ascii 12345678
```

Related Commands

Command	Description
security wapi psk enable	Enables the WAPI PSK.

Platform Description N/A

5.10 show wapi-sta summary

Use this command to display information about WAPI users in authenticated and authenticating lists.
show wapi-sta summary

Parameter Description

Parameter	Description
N/A	N/A

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 information about WAPI users that have been authenticated and are being authenticated.
Enter privileged EXEC mode and run the **show wapi-sta summary** command to display information about WAPI users in the authenticated and authenticating lists.

```
Ruijie#show wapi-sta summary
In the authenticated list:
authenticated sta number: 1
INDEX    STA-MAC-addr    AP-MAC-addr      WLAN ID    MODE      CUR-STATE
```

```
1        000b.c002.9cbe    021b.b120.687e    1      CERT      AUHIENTICATED
In the authenticating list:
authenticating sta number: 0
INDEX    STA-MAC-addr   AP-MAC-addr      WLAN ID    MODE      CUR-STATE
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

1 WLAN QoS Commands

1.1 ap-based

Use this command to configure the upstream and downstream traffic rate limit of the current AP.
Use the **no** form of this command to restore the default setting.
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 ap-based { **per-user-limit** | **total-user-limit** } { **down-streams** | **up-streams** }

Use this command to configure the intelligent total-user-limit of the current AP.
Use the **no** form of this command to restore the default setting.
ap-based total-user-limit { **down-streams** | **up-streams** } **intelligent**
no 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	Downstream traffic limit of the AP
up-streams	Upstream traffic limit of the AP
intelligent	Enables intelligent rate limit.
average-data-rate	Average rate limit, ranging from 8 to 261,120 in the unit of 8Kbps.
burst-data-rate	Burst rate limit, ranging from 8 to 261,120 in the unit of 8Kbps.

Defaults The traffic limit and intelligent total-user-limit are disabled by default.

Command mode AP configuration mode

Usage Guide N/A

Configuration Examples The following example configures the average downstream rate of the AP 1 to 800 Kbps and the burst rate to 1,600 Kbps.

```
Ruijie(config)# ap-config wlan-ap-001
Ruijie(config-ap)# ap-based down-streams average-data-rate 800
burst-data-rate 1600
```

Related Commands

Command	Description
netuser H.H.H { **inbound**	**outbound** } **average-data-rate** *average-data-rate*	Configures the client-based in-band and out-of-band traffic rate limit.

burst-data-rate *burst-data-rate*	
wlan-based { **down-streams** | **up-streams** } **average-data-rate** *average-data-rate* **burst-data-rate** *burst-data-rate*	Configures the WLAN-based upstream and downstream traffic rate limit.

Platform Description

1.2 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 AP configuration mode

Usage Guide When the AP works in fit AP mode, the fair scheduling can be configured only on the AC.

Configuration Examples The following example disables fair scheduling on the AP.

```
Ruijie(config)# ap-config ap-name
Ruijie(ap-config)# no fair-schedule
```

Related Commands

Command	Description
N/A	N/A

Platform Description

1.3 netuser

Use this command to configure the in-band and out-of-band traffic limit for a specified user in the current WLAN.
Use the **no** form of this command to restore the default setting.
netuser *mac-address* { **inbound** | **outbound** } **average-data-rate** *average-data-rate* **burst-data-rate**

burst-data-rate

no 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 261,120 in the unit of 8Kbps.
burst-data-rate	Burst rate limit, ranging from 8 to 261,120 in the unit of 8Kbps.

Defaults No traffic limit is set by default.

Command mode AC configuration mode.

Usage Guide N/A

Configuration Examples The following example sets the average in-band rate to 800Kbps and burst rate to 1,600 Kbps for the user 0000.0000.0001 in WLAN 1.

```
Ruijie(config)# wlan-config 1
Ruijie(ac-config)# netuser 0000.0000.0001 inbound average-data-rate 800
burst-data-rate 1600
```

Related Commands

Command	Description
wlan-based { **down-streams** | **up-streams** } **average-data-rate** *average-data-rate* **burst-data-rate** *burst-data-rate*	Configures the WLAN-based upstream and downstream traffic rate limit.
ap-based { **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 limit.

Platform Description

1.4 show dot11 ratelimit

Use this command to display WLAN rate limit information.

show dot11 ratelimit { **wlan** | **ap** | **user** }

show dot11 ratelimit wlan perap

Parameter

Parameter	Description

Description

wlan	Displays the rate limit information of all WLANs.
ap	Displays the rate limit information of all APs.
user	Displays the rate limit information of all users.
perap	Displays the total WLAN rate limit information of all APs.

Defaults N/A

Command mode Privileged EXEC mode

Usage Guide N/A

Configuration Examples The following example displays the rate limit information of all APs.

```
Ruijie# show dot11 ratelimit ap
```

Related Commands

Command	Description
N/A	N/A

Platform Description

1.5 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 AC configuration mode

Usage Guide N/A

Configuration The following example sets the fair scheduling priority for user 0000.0000.0001 on the AC to 3.

Example

```
Ruijie(config)# ac-controller
Ruijie(config-ac)# sta-fair 0000.0000.0001 priority 3
```

Platform Description

1.6 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-based { **per-user-limit** | **total-user-limit** | **per-ap-limit** } { **down-streams** | **up-streams** } **average-data-rate** *average-data-rate* **burst-data-rate** *burst-data-rate*
no wlan-based { **per-user-limit** | **total-user-limit** | **per-ap-limit** } { **down-streams** | **up-streams** }

Use this command to configure the intelligent per-ap-limit of the current WLAN.
Use the **no** form of this command to restore the default setting.
wlan-based per-ap-limit { **down-streams** | **up-streams** } **intelligent**
no wlan-based per-ap-limit { **down-streams** | **up-streams** } **intelligent**

Parameter Description

Parameter	Description
per-user-limit	Limit for each user on the WLAN.
total-user-limit	Limit for the entire WLAN.
per-ap-limit	Limit WLAN Total for each AP.
down-streams	Total downstream traffic limit of the WLAN.
up-streams	Total upstream traffic limit of the WLAN.
intelligent	Whether to enable intelligent per-ap-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 The function is disabled by default.

Command mode WLAN configuration mode

Usage Guide N/A

Configuration Examples The following example configures the average downstream rate of WLAN 1 to 800 Kbps and burst rate to 1,600 Kbps.

```
Ruijie(config)# wlan-config 1
Ruijie(wids-config)# wlan-based down-streams average-data-rate 800
burst-data-rate 1600
```

Related Commands

Command	Description
ap-based { **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 limit.
netuser *H.H.H* { **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 limit.

Platform Description

1.7 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 AC 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 The following example enables WQoS traffic statistics for all APs associated with the AC.

```
Ruijie(config-ac)#wqos fs enable
```

Platform Description

2 WMM Commands

2.1 wlan-qos map-table

Use this command to configure packet priority mapping for the current WLAN. Use the **no** form of this command to restore the default setting.

wlan-qos map-table { **dot11e-inner-dscp** | **dot11e-tunnel-dscp** | **dscp-dot11e** } **import** *import-tag-value* **export** *export-tag-value*

no wlan-qos map-table { **dot11e-inner-dscp** | **dot11e-tunnel-dscp** | **dscp-dot11e** } **import** *import-tag-value*

Parameter Description

Parameter	Description
dot11e-inner-dscp	Sets priority mapping from dot11e to internal DSCP.
dot11e-tunnel-dscp	Sets priority mapping from dot11e to CAPWAP DSCP.
dscp-dot11e	Sets priority mapping from DSCP to dot11e.
import *import-tag-value*	Sets priority of the incoming original packet. WMM (dot11e) is one of QoS fields of 802.11 wireless protocol headers. It refers to WLAN priority, in the range from 0 to 7. DSCP is the priority field of IP protocol headers, in the range from 0 to 63. The default is 0.
export *export-tag-value*	Sets priority of the outgoing packet. WMM (dot11e) is one of QoS fields of 802.11 wireless protocol headers. It refers to WLAN priority, in the range from 0 to 7. DSCP is the priority field of IP protocol headers, in the range from 0 to 63. The default is 0.

Defaults

DSCP-to-dot11e Mapping Table

DSCP	802.11e
0~7	0
16~23	1
24~31	2
8~15	3
32~39	4
40~47	5
48~55	6
56~63	7

dot11e-to-DSCP Mapping Table

802.11e	DSCP
0	0
3	8
1	16

2	24
4	32
5	40
6	48
7	56

Command Mode WLAN configuration mode

Usage Guide The configuration takes effect after the WMM service is enabled.

Configuration Examples The following example sets priority mapping from DSCP to dot11e. The priority of the incoming original packet is 1 and that of the outgoing packet is 10.

```
Ruijie# configure terminal
Ruijie(config)# wlan-config 1
Ruijie(config-wlan)# wlan-qos map-table dscp-dot11e import 1 export 10
```

Platform Description N/A

2.2 wmm dot1p enable

Use this command to enable 802.11p QoS mapping policy mechanism. Use the **no** form of this command to restore the default setting.

wmm dot1p enable radio *radio-id*

no wmm dot1p enable radio *radio-id*

Parameter Description

Parameter	Description
radio *radio-id*	Specifies the radio on which 802.11p QoS mapping policy mechanism is enabled/disabled, in the range from 1 to 96.

Defaults This function is disabled by default.

Command Mode AP configuration mode

Usage Guide The configuration takes effect after the WMM service is enabled.

Configuration Examples The following example enables 802.11p QoS mapping policy mechanism for radio 1 on VOICE-AP.

```
Ruijie# configure terminal
Ruijie(config)# ap-config VOICE-AP
Ruijie(config-ap)# wmm dot1p enable radio 1
```

Platform Description N/A

2.3 wmm dot1p policy

Use this command to configure how to apply the 802.11p QoS mapping policy mechanism for the AP. Use the **no** form of this command to restore the default setting.

wmm dot1p policy 1q [*1q-policy-value*] **radio** *radio-id*

no wmm dot1p policy radio [*radio-id*]

Parameter Description

Parameter	Description
1q *1q-policy-value*	Applies the 802.11p QoS mapping policy mechanism, in the range from 0 to 1. The default is 0. Q=1: AP tags the priority domain of 802.1Q according to 802.1p. Q=0: AP tags the priority domain of 802.1Q according to the user priority in the **Qos Control** field of IEEE 802.11 headers. Apply "Q=1" method when there is no **QoS Control** field.
radio *radio-id*	Specifies the radio on which 802.11p QoS mapping policy mechanism is applied, in the range from 1 to 96.

Defaults The default is 0.

Command Mode AP configuration mode

Usage Guide The configuration takes effect after the WMM service is enabled.
The configuration is valid only when the 802.11p QoS mechanism is enabled.

Configuration Examples The following example tags the priority domain of 802.1Q for radio 1 on VOICE-AP.

```
Ruijie# configure terminal
Ruijie(config)# ap-config VOICE-AP
Ruijie(config-ap)# wmm dot1p 1q 1 radio 1
```

Platform Description N/A

2.4 wmm dot1p tag

Use this command to configure 802.1p priority. Use the **no** form of this command to restore the default setting.

wmm dot1p tag [*tag-value*] { **back-ground** | **best-effort** | **video** | **voice** } **radio** *radio-id*

no wmm dot1p tag { **back-ground** | **best-effort** | **video** | **voice** } **radio** *radio-id*

Parameter Description

Parameter	Description
tag *tag-value*	Sets the 802.1p priority, in the range from 0 to 7.
back-ground	Sets the back-ground queue.
best-effort	Sets the best-effort queue.
video	Sets the video queue.
voice	Sets the voice queue.
radio *radio-id*	Specifies the radio on which 802.11p priority is configured, in the range from 1 to 96.

Defaults The default **best-effort** is 0; the default **back-ground** is 2; the default **video** is 4; the default **voice** is 6.

Command Mode AP configuration mode

Usage Guide The configuration takes effect after the WMM service is enabled.
The configuration is valid only when the 802.11p QoS mechanism is enabled.

Configuration Examples The following example sets 802.1p priority to 5 for radio 1 on VOICE-AP.

```
Ruijie# configure terminal
Ruijie(config)# ap-config VOICE-AP
Ruijie(config-ap)# wmm dot1p tag 5 voice radio 1
```

Platform Description N/A

2.5 wmm dscp enable

Use this command to enable DSCP QoS mapping policy mechanism. Use the **no** form of this command to restore the default setting.
wmm dscp enable radio *radio-id*
no wmm dscp enable radio *radio-id*

Parameter Description

Parameter	Description
radio *radio-id*	Specifies the radio on which DSCP QoS mapping policy mechanism is enabled/disabled, in the range from 1 to 96.

Defaults This function is disabled by default.

Command Mode AP configuration mode

Usage Guide The configuration takes effect after the WMM service is enabled.

Configuration Examples The following example enables DSCP QoS mapping policy mechanism for radio 1 on VOICE-AP.

```
Ruijie# configure terminal
Ruijie(config)# ap-config VOICE-AP
Ruijie(config-ap)# wmm dscp enable radio 1
```

Platform Description N/A

2.6 wmm dscp policy

Use this command to configure how to apply the DSCP QoS mapping policy mechanism for the AP. Use the **no** form of this command to restore the default setting.

wmm dscp policy outer-tunnel [*outer-tunnel-value*] **inner-tunnel** [*inner-tunnel-value*] **radio** *radio-id*

no wmm dscp policy radio *radio-id*

Parameter Description

Parameter	Description
outer-tunnel *outer-tunnel-value*	Configures how to apply the DSCP QoS mapping policy mechanism for the outer tunnel header, in the range from 0 to 1. The default is 0. In the centralized forwarding mode: O=1: AP sets DSCP domain for the tunnel header according to pushed configuration policy; O=0: AP sets DSCP domain for the tunnel header according to inner tunnel packets. If inner tunnel packets are encrypted or non-IPv4/ IPv6, the "O=1" method will be applied. In the local forwarding mode: O=1: invalid value; O=0: invalid value.
inner-tunnel *inner-tunnel-value*	Configures how to apply the DSCP QoS mapping policy mechanism for the inner tunnel header, in the range from 0 to1. The default is 0. In the centralized forwarding mode: AP sets DSCP domain for the tunnel header according to inner tunnel packets; If inner tunnel packets are encrypted or non-IPv4/IPv6, the "I=1" method will be applied. I=0: AP cannot modify the DSCP domain of user packets. In the local forwarding mode: I=1: AP configures the DSCP domain for user packets according to the pushed configuration policy. I=0: AP cannot modify the DSCP domain of user packets.
radio *radio-id*	Specifies the radio on which DSCP QoS mapping policy mechanism is applied, in the range from 1 to 96.

Defaults The default is 0.

Command Mode AP configuration mode

Usage Guide The configuration takes effect after the WMM service is enabled.
The configuration is valid only when the DSCP QoS mechanism is enabled.

Configuration Examples The following example sets both outer and inner tunnel headers to 0 for DSCP mapping mechanism of radio 1 on VOICE-AP.

```
Ruijie# configure terminal
Ruijie(config)# ap-config VOICE-AP
Ruijie(config-ap)# wmm dscp outer-tunnel 0 inner-tunnel 0 radio 1
```

Platform Description N/A

2.7 wmm dscp tag

Use this command to configure the DSCP identification. Use the **no** form of this command to restore the default setting.
wmm dscp tag [*tag-value*] { **back-ground** | **best-effort** | **video** | **voice** } **radio** *radio-id*
no wmm dscp tag { **back-ground** | **best-effort** | **video** | **voice** } **radio** *radio-id*

Parameter Description

Parameter	Description
tag *tag-value*	Sets the DSCP priority, in the range from 0 to 63.
back-ground	Sets the back-ground queue.
best-effort	Sets the best-effort queue.
video	Sets the video queue.
voice	Sets the voice queue.
radio *radio-id*	Specifies the radio on which the DSCP identification is configured, in the range from 1 to 96.

Defaults The default **best-effort** is 0; the default **back-ground** is 16; the default **video** is 32; the default **voice** is 48.

Command Mode AP configuration mode

Usage Guide

The configuration takes effect after the WMM service is enabled.
DSCP identification is valid only when the DSCP mechanism is enabled.

Configuration Examples The following example sets the DSCP identification to 5 for voice queue of radio 1 on VOICE-AP.

```
Ruijie# configure terminal
Ruijie(config)# ap-config VOICE-AP
Ruijie(config-ap)# wmm dscp tag 5 voice radio 1
```

Platform Description N/A

2.8 wmm edca-client

Use this command to configure the EDCA parameters for the client. Use the **no** form of this command to restore the default setting.

wmm edca-client { **back-ground** | **best-effort** | **video** | **voice** } { **aifsn** [*aifsn-value*] **cwmin** [*cwmin-value*] **cwmax** [*cwmax-value*] **txop** [*txop-value*] | **length** [*queue-length*] } **radio** *radio-id*

no wmm edca-client { **back-ground** | **best-effort** | **video** | **voice** } [**length**] **radio** *radio-id*

Parameter Description

Parameter	Description
back-ground	Sets the back-ground queue.
best-effort	Sets the best-effort queue.
video	Sets the video queue.
voice	Sets the voice queue.
aifsn *aifsn-value*	Sets the **aifsn** value, in the range from 1 to15.
cwmin *cwmin-value*	Sets the **cwmin** value, in the range from 0 to 15.
cwmax *cwmax-value*	Sets the **cwmax** value, in the range from 0 to 15.
txop *txop-value*	Sets the **txop** value, in the range from 0 to 255 in the unit of 32 μs.
length *queue-length*	Sets the AC queue length in the range from 1 to 255. The default is 255.
radio *radio-id*	Specifies the radio on which the client EDCA parameters are configured, in the range from 1 to 96.

Defaults

AC	aifs	cwmin	cwmax	txop
back-ground	7	4	10	0
best-effort	3	4	10	0
video	2	3	4	94
voice	2	2	3	47

Command Mode AP configuration mode

Usage Guide The configuration takes effect after the WMM service is enabled.

⚠ The **cwmax** value must be greater than the **cwmin** value. Otherwise, a configuration error message is displayed.

Configuration Examples The following example configures **asfsn** to 2, **cwmin** to 2, **cwmax** to 3 and **txop** to 50 for the voice queue of radio 1 on VOICE-AP.

```
Ruijie# configure terminal
Ruijie(config)# ap-config VOICE-AP
Ruijie(config-ap)# wmm edca-client voice aifsn 2 cwmin 2 cwmax 3 txop 50 radio
1
```

Platform Description N/A

2.9 wmm edca-radio

Use this command to configure the EDCA parameters for the AP. Use the **no** form of this command to restore the default setting.

wmm edca-radio { **back-ground** | **best-effort** | **video** | **voice** } { **aifsn** [*aifsn-value*] **cwmin** [*cwmin-value*] **cwmax** [*cwmax-value*] **txop** [*txop-value*] | **noack** } **radio** *radio-id*

no wmm edca-radio { **back-groud** | **best-effort** | **video** | **voice** } [**noack**] **radio** *radio-id*

Parameter Description

Parameter	Description
back-ground	Sets the back-ground queue.
best-effort	Sets the best-effort queue.
video	Sets the video queue.
voice	Sets the voice queue.
aifsn *aifsn-value*	Sets the **aifsn** value, in the range from 1 to 15.
cwmin *cwmin-value*	Sets the **cwmin** value, in the range from 0 to 15.
cwmax *cwmax-value*	Sets the **cwmax** value, in the range from 0 to 15.
txop *txop-value*	Sets the **txop** value, in the range from 0 to 255 in the unit of 32 μs.
noack	Indicates that the no ack policy is enabled. The no ack policy is disabled by default.
radio *radio-id*	Specifies the radio on which the client EDCA parameters are configured, in the range from 1 to 96.

Defaults

AC	aifs	cwmin	cwmax	txop
back-ground	7	4	10	0
best-effort	3	4	6	0
video	1	3	4	94
voice	1	2	3	47

Command Mode AP configuration mode

Usage Guide The configuration takes effect after the WMM service is enabled.

According to the IEEE 802.11 standard, no ACK is returned for multicast or broadcast frames.

The **cwmax** value must be greater than the **cwmin** value. Otherwise, a configuration error message is displayed.

Configuration Examples The following example sets **aifsn** to 1, **cwmin** to 1, **cwmax** to 3, **txop** to 50 for the voice queue of radio 1 on VOICE-AP.

```
Ruijie# configure terminal
Ruijie(config)# ap-config VOICE-AP
Ruijie(config-ap)# wmm edca-radio voice aifsn 1 cwmin 1 cwmax 3 txop 50 radio 1
```

Platform Description N/A

2.10 wmm enable

Use this command to enable the WMM service. Use **no** form of this command to disable the WMM service.

wmm enable radio *radio-id*

no wmm enable radio *radio-id*

Parameter Description

Parameter	Description
radio *radio-id*	Specifies the radio on which the WMM service is enabled/disabled, in the range from 1 to 96.
no	Disables the WMM service.

Defaults This function is enabled by default.

Command Mode AP configuration mode

Usage Guide When the WMM service is disabled, the default priority queue is used for reception and mapping.

Configuration Examples The following example enables the WMM service for radio 1 on VOICE-AP.

```
Ruijie# configure terminal
Ruijie(config)# ap-config VOICE-AP
Ruijie(config-ap)# wmm enable radio 1
```

Platform Description N/A

WLAN Networking Configuration Commands

1 WLAN Hot-Backup Commands

1.1 context

Use this command to configure a hot-backup context and enter hot-backup context configuration mode. Use the **no** form of this command to remove the hot-backup context.

context *context-id*

no context *context-id*

Parameter Description

Parameter	Description
context-id	hot-backup context ID. For the same peer device, the context ID on the access controller must be unique.

Defaults N/A

Command Mode Hot-backup configuration mode

Usage Guide For the same peer device, the context ID on the access controller must be unique.

Configuration Examples The following example adds **Context 10**:

```
Ruijie# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Ruijie(config)# wlan hot-backup 1.1.1.1
Ruijie(config-hotbackup)# context 10
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

1.2 dhcp-pool

Use this command to associate a DHCP address pool with a hot-backup context. Use the **no** form of this command to remove the association.

dhcp-pool *pool-name*

no dhcp-pool *pool-name*

Parameter Description

Parameter	Description
pool-name	DHCP address pool name

Defaults N/A

Command Mode Hot-backup context configuration mode

Usage Guide The same DHCP address pool must be associated with the hot-backup context on the master and slave AC devices. Different DHCP address pools must be associated with the different hot-backup contexts on an AC device.

Configuration Examples The following example associates **Context 10** with the DHCP address pool **dhcp-pool1**:

```
Ruijie(config-hotbackup)# context 10
Ruijie(config-hotbackup-ctx)# dhcp-pool dhcp-pool1
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

1.3 dhcpv6-pool

Use this command to associate a DHCPv6 address pool with a hot-backup context. Use the **no** form of this command to remove the association.

dhcpv6-pool *pool-name*

no dhcpv6-pool *pool-name*

Parameter Description

Parameter	Description
pool-name	DHCPv6 address pool name

Defaults N/A

Command Mode Hot-backup context configuration mode

Usage Guide The same DHCPv6 address pool must be associated with the hot-backup context on the master and slave AC devices. Different DHCPv6 address pools must be associated with the different hot-backup

contexts on an AC device.

Configuration Examples The following example associates **Context 10** with the DHCP address pool **dhcp-pool1**:

```
Ruijie# configure terminal

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

Ruijie(config)# wlan hot-backup 1.1.1.1

Ruijie(config-hotbackup)# context 10

Ruijie(config-hotbackup-ctx)# dhcpv6-pool dhcpv6-pool1
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

1.4 hello-interval

Use this command to set the keep-alive interval for AC hot backup. Use the **no** form or **default** form of this command to restore the default keep-alive interval.
hello-interval *hello-interval*
no hello-interval
default hello-interval

Parameter Description

Parameter	Description
hello-interval	Specifies the keep-alive interval for AC hot backup. The range is from 10 to 600,000. The unit is millisecond. After the hierarchical AC function is configured, the range is from 30,000 to 600,000.

Defaults The default value relates to the current operation mode: If the operation mode is normal, the default is 2 seconds (2,000 milliseconds). If the operation mode is quick-switch, the default is 10 milliseconds.

Command Mode Hot-backup configuration mode

Usage Guide Set a keep-alive interval based on the current load on ACs and the required interruption time.

Configuration The following example sets the keep-alive interval for AC hot backup to 100 milliseconds:

Examples

```
Ruijie# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Ruijie(config)# wlan hot-backup 1.1.1.1
Ruijie(config-hotbackup)# hello-interval 100
```

Related Commands

Command	Description
work-mode	Configures the operation mode.

Platform Description N/A

1.5 kplv-pkt

Use this command to set the format of hot-backup keep-alive packets. Use the **no** form or **default** form of this command to restore the default format of hot-backup keep-alive packets.

kplv-pkt [**ip** | **udp**]

no kplv-pkt

default kplv-pkt

Parameter Description

Parameter	Description
ip	Sets the format of hot-backup keep-alive packets to IP packets.
udp	Sets the format of hot-backup keep-alive packets to UDP packets. The UDP port number is 7435.

Defaults By default, the hot-backup keep-alive packets are sent in the format of IP packets.

Command Mode Hot-backup configuration mode

Usage Guide You can set the format of keep-alive packets of hot-backup based on the current network environment between two AC devices.

It is necessary to use send hot-backup keep-alive packets in the format of UDP packets when NAT is applied between two AC devices.

Configuration Examples The following example sets the format of hot-backup keep-alive packets to UDP packets.

```
Ruijie# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Ruijie(config)# wlan hot-backup 1.1.1.1
Ruijie(config-hotbackup)# kplv-pkt udp
```

Related Commands

Command	Description

N/A	N/A

Platform Description N/A

1.6 local-ip

Use this command to configure the local IP address. Use the **no** form of this command to remove the local IP address.

local-ip *ip-address*

no local-ip

Parameter Description

Parameter	Description
ip-address	IP address of the local end.

Defaults By default, the IP address of interface Loopback0 is used as the local IP address.

Command Mode Hot-backup configuration mode

Usage Guide You can use this command to configure the IP address of a Layer3 interface on the local device for hot backup.

When the local IP address changes, hot backup disconnects. Then the new local IP address will be used for hot backup connection.

Configuration Examples The following example configures the IP address of SVI ports for AC hot backup connection.

```
Ruijie# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Ruijie(config)# vlan 10
Ruijie(config-vlan)# exit
Ruijie(config)# interface vlan 10
Ruijie(config-if-VLAN 10)# ip address 10.10.10.10 255.255.255.0
Ruijie(config)# wlan hot-backup 1.1.1.1
Ruijie(config-hotbackup)# local-ip 10.10.10.10
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

1.7 priority level

Use this command to set the priority of the local AC in a hot-backup context. Use the **no** form or **default** form of this command to restore the default priority.

priority level *priority*

no priority level *priority*

default priority level *priority*

Parameter Description

Parameter	Description
priority	Sets the AC priority. The range is from 0 to 7. 7 indicates the highest priority.

Defaults The default priority is 4.
In hierarchical AC scenarios, the default priority of a branch AC is 7.

Command Mode Hot-backup context configuration mode

Usage Guide In an AC hot-backup context, the AC with a higher priority is the master AC. If the two ACs have the same priority, the AC with a smaller MAC address is the master AC. When an AC is set with the highest priority, it becomes the master AC.

Configuration Examples The following example sets the priority of an AC to 6:

```
Ruijie# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Ruijie(config)# wlan hot-backup 1.1.1.1
Ruijie(config-hotbackup)# context 10
Ruijie(config-hotbackup-ctx)# priority level 6
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

1.8 show wlan hot-backup

Use this command to display the configurations of a peer AC.

show wlan hot-backup [*ip-address*]

Parameter

Parameter	Description

Description

ip-address	Specifies the IP address of a peer AC.

Defaults N/A

Command Mode Privileged EXEC mode, global configuration mode

Usage Guide N/A

Configuration Examples The following example displays the current hot-backup configuration:

```
Ruijie# show wlan hot-backup
wlan hot-backup peer list:
  ip address          hot-backup state          description
  -------------------- ---------- ---------------- -----------
  6.6.6.6            Enable    CHANNEL_UP      Office
```

The following example displays the hot-backup configuration of the peer AC with the IP address 6.6.6.6:

```
Ruijie# show wlan hot-backup 6.6.6.6
wlan hot-backup 6.6.6.6
  hot-backup    : Enable
  connect state  : CHANNEL_UP
  hello-interval : 100
  kplv-pkt      : ip
  work-mode     : QUICK-SWITCH
  !
  context 10
    hot-backup role       : PAIR-STANDBY
    hot-backup rdnd state  : REALTIME-SYN
    hot-backup priority   : 4
    ap-group             : apg-10
    dhcp-pool            : sta_2
    vrrp interface - group : VLAN 10 - 1
    vrrp interface - group : VLAN 3 - 3
  !
  context 20
    hot-backup role       : PAIR-ACTIVE
    hot-backup rdnd state  : REALTIME-SYN
    hot-backup priority   : 4
    ap-group             : default
    ap-group             : apg-20
    ap-group             : apg-30
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

1.9 show wlan hot-backup dhcp-pool config

Use this command to display the binding configuration between hot-backup context and DHCP address pool.

show wlan hot-backup dhcp-pool config *ip-address*

Parameter Description

Parameter	Description
ip-address	Specifies the IP address of a peer AC.

Defaults N/A

Command Mode Privileged EXEC mode, global configuration mode

Usage Guide N/A

Configuration Examples The following example displays binding configuration between the hot-backup context and DHCP address pool on the device of 192.168.120.100.

```
Ruijie#show wlan hot-backup dhcp-pool config 192.168.120.100
wlan hot-backup 192.168.120.100
  context 10
    dhcp-pool: hb-itc2
dhcp-pool: hb-itc3
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

1.10 show wlan hot-backup dhcpv6-pool config

Use this command to display the binding configuration between hot-backup context and DHCPv6

address pool.

show wlan hot-backup dhcpv6-pool config *ip-address*

Parameter Description

Parameter	Description
ip-address	Specifies the IP address of a peer AC.

Defaults N/A

Command Mode Privileged EXEC mode, global configuration mode

Usage Guide N/A

Configuration Examples The following example displays binding configuration between the hot-backup context and DHCPv6 address pool on the device of 192.168.120.100.

```
Ruijie#show wlan hot-backup dhcpv6-pool config 192.168.120.100
wlan hot-backup 192.168.120.100
  context 10
    dhcpv6-pool: hb-itc1
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

1.11 show wlan hot-backup vrrp config

Use this command to display the binding configuration between hot-backup context and VRRP group.

show wlan hot-backup vrrp config *ip-address*

Parameter Description

Parameter	Description
ip-address	Specifies the IP address of a peer AC.

Defaults N/A

Command Mode Privileged EXEC mode, global configuration mode

Usage Guide N/A

Configuration Examples The following example displays binding configuration between the hot-backup context and VRRP group on the device of 192.168.120.100.

```
Ruijie#show wlan hot-backup vrrp config 192.168.120.100
wlan hot-backup 192.168.120.100
  context 10
    vrrp interface VLAN 104 group 10
vrrp interface VLAN 105 group 20
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

1.12 vrrp interface group

Use this command to associate the VRRP group with an AC hot-backup context. Use the **no** form of this command to remove the association.

vrrp interface *interface-name* **group** *vrrp-group*

no vrrp interface *interface-name* **group** *vrrp-group*

Parameter Description

Parameter	Description
interface-name	Interface name of the VRRP group.
vrrp-group	VRRP group number

Defaults N/A

Command Mode Hot-backup context configuration mode

Usage Guide The same VRRP group should be configured on the two hot-backup associated ACs in a hot-backup context.

Different VRRP groups should be configured accordingly in different hot-backup contexts on an AC.

Configuration Examples The following example associates **Context 10** with VRRP backup group 1 on the interface **vlan2**:

```
Ruijie# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Ruijie(config)# wlan hot-backup 1.1.1.1
Ruijie(config-hotbackup)# context 10
Ruijie(config-hotbackup-ctx)# vrrp interface vlan2 group 1
```

Related

Command	Description

Commands		
	N/A	N/A

Platform Description N/A

1.13 wlan hot-backup

Use this command to configure an IP address for the peer AC and enter hot-backup configuration mode, or to configure the hierarchical AC role.

Use the **no** form of this command to remove the IP address or the hierarchical AC role.

wlan hot-backup [*ip-address* **| center | branch**]

no wlan hot-backup [*ip-address* **| center | branch**]

Parameter Description

Parameter	Description
ip-address	IP address of the peer AC. Multiple peer IP addresses can be configured.
center	Indicates the center AC
branch	Indicates the branch AC

Defaults N/A

Command Mode Hot-backup configuration mode

Usage Guide You can configure multiple IP addresses for peer ACs.

The following restrictions are added after the hierarchical AC is configured:

1. The quick-switch mode configured in work-mode must not be used;
2. The lower limit for the hello-interval is changed to 30s;
3. The UDP configuration in kplv-pkt must not be used;
4. The hierarchical AC role cannot be configured if AC hot-back is enabled.

Configuration Examples The following example sets the IP address 192.168.1.100 for a peer AC in a hot-backup context:

```
Ruijie# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Ruijie(config)# wlan hot-backup 192.168.1.100
Ruijie(config-hotbackup)#
```

The following example sets the center AC role:

```
Ruijie# configure terminal

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

Ruijie(config)# wlan hot-backup center
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

1.14 wlan hot-backup enable

Use this command to enable AC hot-backup. Use the **no** form of this command to disable hot-backup.

wlan hot-backup enable

no wlan hot-backup enable

Parameter Description

Parameter	Description
N/A	N/A

Defaults By default, the AC hot-backup function is disabled.

Command Mode Hot-backup configuration mode

Usage Guide An AC hot-backup context takes effect only after hot-backup is enabled.

Configuration Examples The following example enables AC hot backup:

```
Ruijie# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Ruijie(config)# wlan hot-backup 1.1.1.1
Ruijie(config-hotbackup)# wlan hot-backup enable
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

1.15 work-mode

Use this command to configure the working mode of hot-backup. Use the **no** form or **default** form of this command to restore the default working mode.

work-mode [**normal** | **quick-switch | cold**]

no work-mode

Parameter Description

Parameter	Description
normal	Indicates normal switchover mode.
quick-switch	Indicates quick switchover mode.
cold	Indicates the lightweight backup mode in hierarchical AC scenarios.

Defaults By default, the normal switchover mode is used.

Command Mode Hot-backup configuration mode

Usage Guide The command for hot-backup working mode is introduced in consideration of the following three application scenarios.

- Practical application scenario: requires stable operation to avoid hot-backup vibration. This scenario can works in normal switchover mode and the default heartbeat detection period is 2 second.
- Performance test scenario: requires sensitive test and fast switchover in scenarios such as system demonstration and performance test. This scenario works in quick switchover mode and the default heartbeat detection period is 10 milliseconds.
- In hierarchical AC scenarios, a new work mode, cold is added, which indicates lightweight data backup. In cold mode, most data backup with the peer is forbidden and only little data transmission is reserved. When traffic of the center AC is heavy, configure the work mode as cold to reduce the load of the center AC. In cold mode, when a branch AC is faulty, STAs need to be re-associated and STAs' IP addresses need to be obtained again for authentication. In cold mode, the unified upgrade, unified management, and license sharing functions are reserved.

The normal switchover mode is the default working mode. The quick switchover mode is required only in performance test scenarios.

Configuration Examples The following example configures AC hot-backup working in quick switchover mode.

```
Ruijie# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Ruijie(config)# wlan hot-backup 1.1.1.1
Ruijie(config-hotbackup)# work-mode quick-switch
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

1.16 description

Use this command to configure the name of the hot backup peer. Use the **no** form of this command to remove the setting.

description *name*

no description

Parameter Description

Parameter	Description
name	Indicates the name of the hot backup peer.

Defaults By default, the description is not configured.

Command Mode Hot-backup configuration mode

Usage Guide The later configuration will overwrite the former name.

Configuration Examples The following example configures the name of the hot backup peer to Office.

```
Ruijie# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Ruijie(config)#wlan hot-backup 10.1.1.2
Ruijie(config-hotbackup)#description Office
```

Related Commands

Command	Description
N/A	N/A

Platform Description This command is supported on WLAN AC device.

2 WDS Commands

2.1 autowds

Use this command to enable automatic bridging for APs.
Use the no form of this command to disable this function.
autowds
no autowds

Parameter Description

Parameter	Description
N/A	N/A

Defaults Automatic bridging is disabled by default.

Command Mode AP configuration mode/AP group configuration mode

Usage Guide Generally, this function is only available to non-root bridge for APs. It can be configured in AP configuration mode for all or single and AP group configuration mode. The order of precedence is: AP configuration mode (single) > AP group configuration mode > AP configuration mode (all).

Configuration Examples The following example enables automatic bridging for APs.

```
Ruijie(config-ap)# autowds
```

Platform Description N/A

2.2 bridge security

Use this command to enable bridge encryption (only in the non-root bridge mode). Use the **no** form of this command to restore the default settings.
bridge security [**radio** *num*] { **wpa** | **rsn** } **ciphers** { **aes** } **akm psk key** { **ascii** | **hex** } *key*
no bridge security

Parameter Description

Parameter	Description

radio *num*	Configured the RF port on ACs.
wpa	Configures WPA authentication.
rsn	Configures RSN authentication.
aes	Configures AES encryption.
psk	Specifies pre-shared key authentication as the access authentication mode.
ascii	Specifies ASCCI password.
hex	Specifies hex password.
key	**ascii**: 8 to 63 characters; **hex**: 64 characters.

Defaults No encryption parameter is configured by default.

Command Mode AP: Interface configuration mode
AC: AP configuration mode

Usage Guide This command is only applicable to non-root ends.
It is configured directly on fat APs while on ACs when APs are fit.

⚠ Make sure that the bridge encryption parameters are completely the same to network encryption parameters.

⚠ In the non-root bridge mode, only after being committed will the **bridge security** command take effect on ACs.

Configuration Examples The following example enables bridge encryption on APs: Once this configuration takes effect, non-root APs start scanning and bridging if the network nearby shares the same encryption parameters.

```
Ruijie(config-if-Dot11radio 1/0)# station-role non-root-bridge
Ruijie(config-if-Dot11radio 1/0)# parent ssid ruijie-root
Ruijie(config-if-Dot11radio 1/0)# bridge security wpa ciphers aes akm psk key ascii
12345678
```

The following example removes bridge encryption configuration on APs.

```
Ruijie(config-if-Dot11radio 1/0)# no bridge security
```

The following example enables bridge encryption on ACs: Once this configuration takes effect and is pushed, non-root APs start scanning and bridging if the network nearby shares the same encryption parameters.

```
Ruijie(config-ap)# bridge security radio 1 wpa ciphers aes akm psk key ascii 12345678
Ruijie(config-ap)# wds config commit radio 1
```

Related

Command	Description

Commands		
	show running-config	Displays bridge security on APs.
	show ap-config wds-config	Displays bridge security on ACs.

Platform Description N/A

2.3 bridge vlan

Use this command to create a VLAN for the fit AP.

Use the **no** form of this command to remove the configuration.

bridge vlan *vid*

no bridge vlan *vid*

Parameter Description

Parameter	Description
vid	VLAN ID

Defaults N/A

Command Mode AP configuration mode

Usage Guide This command is used to create or delete a VLAN on ACs.

⚠ Create VLANs on the actual demand. Too many VLANs influence AP performance.

Configuration Examples The following example creates VLAN 2 / 3 / 5. (If this VLAN is not on the AP, it will be created.)

```
Ruijie(config-ap)# bridge vlan 2
Ruijie(config-ap)# bridge vlan 3
Ruijie(config-ap)# bridge vlan 5
```

The following example deletes VLAN 5. (If the VLAN is created by others, it will be deleted.)

```
Ruijie(config-ap)# no bridge vlan 5
```

Related Command

Command	Description
N/A	N/A

Platform Description N/A

2.4 bridge with-client

Use this command to enable bridge coverage (only in WDS bridging mode).

bridge with-client { **enable** | **disable** } [**radio** *radio-id*]

Parameter Description

Parameter	Description
enable	Enables bridge coverage.
disable	Disables bridge coverage.
radio *radio-id*	ID of the radio to be configured on ACs.

Defaults This function is disabled by default.

Command Mode AP configuration mode

Usage Guide Only after this function is enabled will bridge coverage take effect in a WDS network.

It is recommended to disable this function.

In the non-root bridge working mode, only after being committed will the modified **bridge with-client** command take effect.

Configuration Examples The following example enables WDS bridge coverage in the root bridge mode for Radio 2 on ACs.

```
Ruijie(config-ap)#bridge with-client enable radio 2
```

The following example enables WDS bridge coverage in the non-root bridge mode for Radio 2 on ACs.

```
Ruijie(config-ap)#bridge with-client enable radio 2
Ruijie(config-ap)#wds config commit radio 2
```

Related Commands

Command	Description
show running-config	Displays bridge coverage on APs.
show ap-config wds-config	Displays bridge coverage on ACs.

Platform Description N/A

2.5 parent

Use this command to configure the root end to connect in the non-root bridge mode.

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

parent { **mac-address** *HHHH.HHHH.HHHH* | **ssid** *ssid* } [**radio** *radio-id*]
no parent { **mac-address** | **ssid** } [**radio** *radio-id*]

Parameter Description

Parameter	Description
mac-address *HHHH.HHHH.HHHH*	BSSID of a specified root end as a fixed access point.
ssid *ssid*	SSID of a specified root end eligible for roaming.
radio *radio-id*	ID of the radio to be configured on ACs.

Defaults N/A

Command Mode AP configuration mode

Usage Guide Use this command to enable the non-root end to search for the root end and enables WDS bridge. In non-root fit mode, they are usually configured by pre-configuration on APs instead of ACs.

It is recommended to use the **parent mac-address** command for fixed peer-to-peer structure. You can use the **parent ssid** command to enable non-root roaming.

Only a professional is qualified to modify the configuration on ACs after fully understanding the application scenario. Any modification mistake will disconnect ACs from a non-root interface.

Only after being committed will the modified **parent** command take effect on ACs.

Configuration Examples The following example configures non-root-bridge on the AC to access a root end according to its BSSID.

```
Ruijie(config-ap)#no parent ssid radio 2
Ruijie(config-ap)#parent mac-address 00d0.f822.3301 radio 2
Ruijie(config-ap)#wds config commit radio 2
```

The following example configures non-root-bridge on the AC to access a root end according to its SSID.

```
Ruijie(config-ap)#no parent mac-address radio 2
Ruijie(config-ap)#parent ssid ruijie-root radio 2
Ruijie(config-ap)#wds config commit radio 2
```

Platform Description N/A

2.6 show ap-config wds-bridge-info

Use this command to display WDS bridge information on an interface.
show ap-config wds-bridge-info { **summary** | *ap-name* **radio** *radio-id* }

Parameter Description

Parameter	Description
summary	Displays the AP list configured with WDS.
ap-name	AP name
radio-id	Radio ID

Command Mode Privileged EXEC mode

Usage Guide This command is used to display WDS bridge information on APs.

Configuration Examples The following example displays the WDS bridge information information.

```
Ruijie#show ap-config wds-bridge-info summary
Ap Name      Mac Address    Radio  Station Role
-----------  -------------  -----  ----------------
Ap-001       00d0.f822.3301   2    ROOT-BRIDGE
Ap-002       00d0.f822.3304   2    NONROOT-BRIDGE
```

The following example displays the WDS bridge.

```
Ruijie# show ap-config wds-bridge-info Ap-001 radio 2
WDS-MODE: ROOT-BRIDGE
BRIDGE-WLAN:
  Status OK
Wlanid 1, SSID ruijie_root, BSSID 32d0.f822.3303

WBI 1/0
  NONROOT 00d0.f822.3304

WBI 1/1
  NONROOT 00d0.f822.3307
```

Field Description

Field	Description
WDS-MODE	WDS bridge mode.
BRIDGE-WLAN	WLAN used for bridge.
WBI	WDS bridge link.

The following example displays the WDS bridge information.

```
Ruijie# show ap-config wds-bridge-info Ap-002 radio 2
```

```
WDS-MODE: NONROOT-BRIDGE
MAC: 00d0.f822.3304

WBI 1/0
  ROOT 32d0.f822.3303
```

Platform Description N/A

2.7 show ap-config wds-config

Use this command to display WDS configuration.

show ap-config wds-config [*ap-name*]

Parameter Description

Parameter	Description
ap-name	AP name.

Command Mode Privileged EXEC mode

Usage Guide This command is used to display WDS configuration on APs.

Configuration Examples The following example displays WDS configuration.

```
Ruijie#show ap-config wds-config
ap-config 001a.1a03.027b
 station-role root-bridge bridge-wlan 1 radio 1
 station-role root-ap radio 2
 [Uncommit] station-role non-root-bridge radio 1
 bridge with-client enable radio 1
 bridge vlan 2
 bridge vlan 3
!
!!!!!
ap-config 00d0.f822.33b4
 station-role root-ap radio 1
 station-role root-ap radio 2
!
```

The following example displays WDS configuration.

```
Ruijie# show ap-config wds-config 001a.1a03.027b
ap-config 001a.1a03.027b
 station-role root-bridge bridge-wlan 1 radio 1
 station-role root-ap radio 2
 [Uncommit] station-role non-root-bridge radio 1
 bridge with-client enable radio 1
 bridge vlan 2
 bridge vlan 3
!
```

Platform Description N/A

2.8 station-role

Use this command to specify AP bridge mode.

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

station-role { **root-ap** | **root-bridge bridge-wlan** *wlan-id* | **non-root-bridge** } [**radio** *radio-id*]

no station-role [**radio** *radio-id*]

Parameter Description

Parameter	Description
root-ap	Sets the AP working mode as non-bridge mode.
non-root-bridge	Sets the AP working mode as non-root bridge.
root-bridge	Sets the AP working mode as root bridge.
bridge-wlan *wlan-id*	WLAN ID used for root bridge.
radio radio-id	ID of the radio to configure on ACs.

Defaults The default is non-bridge mode.

Command Mode AP configuration mode

Usage Guide To apply WDS, you must first specify an AP bridge mode. The non-root fit bridge mode is enabled not on ACs but APs.

For APs in the root bridge mode, the WLAN ID used for root bridge must be specified. If not, WDS cannot start. Furthermore, the WLAN SSID should not be hidden, or the bridge may fail.

It is better to have professional technicians conduct non-root configuration on ACs. If the configuration is incorrect, the non-root bridge will lose connection with the AC.

Configuration Examples

The following example specifies the root bridge mode on the AC.

```
Ruijie(config-ap)# station-role root-bridge bridge-wlan 1 radio 2
```

The following example specifies the non-root bridge mode on the AC.

```
Ruijie(config-ap)# station-role non-root-bridge radio 1
Ruijie(config-ap)# parent mac-address 0001.0002.0003 radio 1
Ruijie(config-ap)# wds config commit radio 1
```

Related Commands

Command	Description
parent mac-address *HHHH.HHHH.HHHH*	Configures the MAC address of the parent node.

Platform Description

N/A

2.9 wds config

Use this command to commit or clear inactive non-root commands after they are configured on ACs.

wds config [**clear** | **commit**] **radio** *radio-id*

Parameter Description

Parameter	Description
clear	Clears inactive WDS configuration.
commit	Commits inactive WDS configuration.
radio-id	ID of the radio to be configured.

Defaults

N/A

Command Mode

AP configuration mode

Usage Guide

The AC enters the WDS edit mode after configured or synchronized with non-root. In this case, most WDS commands do not take effect until the **wds cofig commi**t command is executed.

Modify non-root configuration on the AC cautiously. Make sure the configuration is correct before committed.

The bridge is disconnected and re-created after the **wds config commit** command is executed.

Configuration Examples

The following example modifies the non-root parent on the AC from parent ssid ruijie-root to parent mac 0001.0002.0003 (it is recommended to perform the configuration during pre-configuration on the AP instead of modifying non-root configuration on the AC).

```
Ruijie(config-ap)# no parent ssid radio 2
Ruijie(config-ap)# parent mac-address 0001.0002.0003 radio 2
Ruijie(config-ap)# wds config commit radio 2
```

The following example discards all inactive WDS configuration on the AC (For instance, the **parent** configuration is discarded in the above example).

```
Ruijie(config-ap)# no parent ssid radio 2
Ruijie(config-ap)# parent mac-address 0001.0002.0003 radio 2
Ruijie(config-ap)# wds config clear radio 2
```

Related Commands

Command	Description
show ap-config wds-config	Display WDS configuration.

Platform Description

N/A

2.10 wds ctrl eth

Use this command to enable Ethernet port control (only for non-root bridge mode).

wds ctrl eth

no wds ctrl eth

Parameter Description

Parameter	Description
N/A	N/A

Defaults

This function is disabled by default.

Command Mode

AP: Global configuration mode

AC: AP configuration mode

Usage Guide

This function is configured on APs for non-root fat bridge and on ACs for non-root fit bridge.

⚠ Use this command carefully. Once it is configured, Ethernet ports will be disconnected if the bridging fails. Thereby, ACs will lose control of APs.

Configuration Examples

The following configuration enables Ethernet port control on the AP.

```
Ruijie(config)#wds ctrl eth
```

The following configuration enables Ethernet port control on the AC.

```
Ruijie(config-ap)#wds ctrl eth
```

Related Commands

Command	Description
show running-config	Displays the running configuration.
show ap-config running	Displays the running configuration on APs.

Platform Description N/A

2.11 wds head-chan

Use this command to set the channels for APs in the front or rear of vehicles.

wds head-chan *num1* **tail-chan** *num2* [**radio** *radio-id*]

no wds head-chan [**radio** *radio-id*]

Parameter Description

Parameter	Description
num1	Front AP channel
num2	Rear AP channel
radio *radio-id*	(Optional on ACs) Radio ID

Defaults This function is disabled by default.

Command Mode AP: Interface configuration mode

AC: AP configuration mode

Usage Guide This function is configured on APs for non-root fat bridge and on ACs for non-root fit bridge.

⚠ This command is used for non-root bridge (in the front or rear of vehicles) to change channels, so as to balance loads.

⚠ If the channel is changed on ACs, use the **commit** command to activate the change.

Configuration Examples The following configuration sets the channel for the APs in the front and rear of the vehicle.

```
Ruijie(config-if-Dot11radio 1/0)# wds head-chan 36 tail-chan 52
```

The following configuration restores the channel for AP in the front of the vehicle.

```
Ruijie(config-if-Dot11radio 1/0)# no wds head-chan
```

The following configuration sets the channels for the AP in the front and rear of the vehicle on the AC.

```
Ruijie(config-ap)# wds head-chan 36 tail-chan 52 radio 2
Ruijie(config-ap)#wds config commit radio 2
```

Related Commands

Command	Description
show running-config	Displays the running configuration.
show ap-config running	Displays the running configuration on APs.

Platform Description N/A

2.12 wds pre-config

Use this command to create or delete non-root pre-configuration.

wds pre-config [**delete**] [**radio** *radio-id*]

Parameter Description

Parameter	Description
delete	Deletes pre-configuration.
radio *radio-id*	ID of the radio to be configured on ACs.

Defaults N/A

Command Mode AP configuration mode

Usage Guide

Before the noon-root fit AP works in the non-root fit mode, it must get pre-configured.

When the WDS bridge mode is disabled, use the **wds pre-config delete** command to delete configuration files on the non-root end.

Configuration Examples The following example removes WDS non-root pre-configuration for radio 1 on the AC.

```
Ruijie(config-ap)# wds pre-config delete radio 1
```

Related Commands N/A

Platform N/A

Description

2.13 wds security enable

Use this command to enable WDS encryption (only for WDS bridge).

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

wds security enable [**radio** *radio-id*]

no wds security enable [**radio** *radio-id*]

Parameter Description

Parameter	Description
radio *radio-id*	(Optional on ACs) Radio ID

Defaults N/A

Command Mode AP: Interface configuration mode

AC: AP configuration mode

Usage Guide This command is used to enable WDS encryption for security.

The non-root bridge and connected root bridge must have the same configuration, or the bridging will fail.

In the non-root bridge mode, use the **commit** command to activate the configuration.

Configuration Examples The following example enables WDS encryption on the AP.

```
Ruijie(config-if-Dot11radio 1/0)#wds security enable
```

The following example enables WDS encryption in the root bridge mode on the AC.

```
Ruijie(config-ap)#wds security enable radio 2
```

The following example enables WDS encryption in the non-root bridge mode on the AC.

```
Ruijie(config-ap)#wds security enable radio 2
Ruijie(config-ap)#wds config commit radio 2
```

Related Commands N/A

Platform Description N/A

2.14 wds-mode enable

Use this command to enable WDS bridge mode (only for WDS bridge-capable AP).

wds-mode enable

Use this command to disable WDS bridge mode.

wds-mode disable

Parameter Description

Parameter	Description
N/A	N/A

Defaults N/A

Command Mode AP: Global configuration mode

AC: AP configuration mode

Usage Guide This command is for the AP630 series outdoor products.

AP will restart after this command is executed.

Configuration Examples The following example enables WDS bridge mode on the AP.

```
Ruijie(config)#wds-mode enable
```

The following example enables WDS bridge mode on the AC.

```
Ruijie(config-ap)#wds-mode enable
```

Related Commands N/A

Platform Description N/A

2.15 show wds-mode

Use this command to display the WDS bridge mode configuration on APs.

show wds-mode

Parameter Description

Parameter	Description
N/A	N/A

Command Mode Privileged EXEC mode

Usage Guide This command is used to display the WDS bridge mode configuration on APs.

Configuration Examples The following example displays the WDS bridge mode configuration.

```
Ruijie#show wds-mode
wds-mode disable.
```

Platform Description This command is supported only on AP devices.

2.16 show ap-config wds-mode summary

Use this command to display the WDS bridge mode configuration on ACs.

show ap-config wds-mode summary

Parameter Description

Parameter	Description
N/A	N/A

Command Mode Privileged EXEC mode

Usage Guide This command is used to display the WDS bridge mode configuration on ACs.

Configuration Examples The following example displays the WDS bridge mode configuration.

```
show ap-config wds-mode summary
AP Name                                  AP MAC          WDS MODE
---------------------------------------- --------------- ---------------
```

Platform Description N/A

3 RIPT Commands

3.1 enable-ssid at-capwap-down

Use this command to enable SSID after the CAPWAP connection between the AC and AP is interrupted.
Use the **no** form of this command to disable this function.
Use the **default** form of this command to restore the default setting.
enable-ssid at-capwap-down
no enable-ssid at-capwap-down
default enable-ssid at-capwap-down

Parameter Description

Parameter	Description
N/A	N/A

Defaults This function is disabled by default.

Command Modes WLAN configuration mode

Usage Guide If the function of SSID enabling after connection interruption is enabled STAs can access the network after the AP is disconnected. After the AP connection is recovered, if the function of SSID enabling after connection interruption is enabled for the WLAN, the WLAN stops working, STAs are not allowed to access the network and online STAs become offline.

Configuration Examples The following example enables the function of SSID enabling after connection interruption on WLAN10.

```
Ruijie(config)# wlan-config 10 ssid-1x-esc
Ruijie(config-wlan)# enable-ssid at-capwap-down
```

Related Commands

Command	Description
show ap-config summary ript-enable	Displays the RIPT state of APs.

Platform Description N/A

3.2 free-webauth at-capwap-down

Use this command to enable free Web authentication after connection interruption.
Use the **no** form of this command to disable this function.

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

free-webauth at-capwap-down

no free-webauth at-capwap-down

default free-webauth at-capwap-down

Parameter Description

Parameter	Description
N/A	N/A

Defaults This function is disabled by default.

Command Modes WLAN configuration mode

Usage Guide When the AP connects to the AC, STAs can access the network only after Web or MAB authentication. When the connection between the AP and AC is interrupted, STAs can access the network without Web or MAB authentication. After the connection between the AP and AC is recovered, STAs can access the network after Web or MAB authentication.

Configuration Examples The following example enables free Web authentication after connection interruption on WLAN10.

```
Ruijie(config)# wlan-config 10 ssid-web
Ruijie(config-wlan)# free-webauth at-capwap-down
```

Related Commands

Command	Description
show ap-config summary ript-enable	Displays the RIPT state of APs.

Platform Description N/A

3.3 ript enable

Use this command to enable the RIPT function for a specified AP. Use the **no** or **default** form of this command to restore the default setting.

ript enable

no ript enable

default ript enable

Parameter Description

Parameter	Description
N/A	N/A

Defaults This function is disabled by default.

Command Modes AP configuration mode/ AP group configuration mode

Usage Guide Use this command to enable the RIPT function for a single AP.

The moment that the RIPT function is enabled or disabled, the AP terminates its CAPWAP connection to the AC and then establishes a new connection.

Configuration Examples The following example enables the RIPT function for AP 007.

```
Ruijie(config)# ap-config AP007
Ruijie(config-ap)# ript enable
```

Related Commands

Command	Description
show ap-config summary ript-enable	Displays the RIPT state of APs.

Platform Description N/A

3.4 ript-monitor

Use this command to enable or disable the monitoring function for AC configuration changes.

ript-monitor { **enable** | **disable** }

Parameter Description

Parameter	Description
enable	Enables the monitoring function for AC configuration changes.
disable	Disables the monitoring function for AC configuration changes.

Defaults This function is enabled by default.

Command Modes Privileged EXEC mode/Global configuration mode

Usage Guide Use this command to enable or disable the monitoring function for AC configuration changes without influence on the AP. When this function is disabled, AC configuration changes will be neglected by the RIPT AP.

This monitoring function should not be disabled unless you make sure related configuration on the AC

will not affect AP's configuration. After the configuration is complete in the global configuration mode, re-enable this function in the privileged EXEC mode.

⚠ The moment that the RIPT function is enabled or disabled, the AP terminates its CAPWAP connection to the AC and then establishes a new connection.

⚠ This configuration takes effect instantly both in the privileged EXEC mode and the global configuration while is not saved in the former mode.

Configuration Examples

The following example enables the monitoring function for AC configuration changes and performs the configuration without influence on the AP.

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

The following example enables the monitoring function for AC configuration changes.

```
Ruijie(config)# end
Ruijie# ript-monitor enable
```

The following example disables the monitoring function for AC configuration changes and saves this configuration.

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

Platform Description

N/A

3.5 show ap-config summary ript-enable

Use this command to display the RIPT state of APs.

show ap-config summary ript-enable

Parameter Description

Parameter	Description
N/A	N/A

Command Modes

Privileged EXEC mode

Usage Guide Use this command to display the information about the APs enabled with the RIPT function.

Configuration Examples The following example displays the RIPT state of APs.

```
Ruijie# show ap-config summary ript-enable
AP Name                              IP Address      Mac Address    ript-enable State
-------------------------------------- --------------- --------------
----------- -----
AP_0001                               172.18.18.11    001a.0000.de47 Y          Run
AP_0002                               172.18.18.12    001a.0000.33aa Y          Run
```

Field Description:

Field	Description
AP Name	Name of an AP.
IP Address	IP address of an AP.
Mac Address	MAC address of an AP.
ript-enable	RIPT state of an AP.
State	Link state of an AP.

Platform Description N/A

3.6 show ript-monitor

Use this command to display the monitoring information about AC configuration changes.

show ript-monitor

Parameter Description

Parameter	Description
N/A	N/A

Command Modes Privileged EXEC mode

Usage Guide Use this command to display the configuration about the RIPT group and the backup RADIUS.

Configuration Examples The following example displays the monitoring information about AC configuration changes.

```
Ruijie# show ript-monitor
Ript-monitor                    : Enable
Global Configuration ID         : 10
```

Field Description:

Field	Description

Ript-monitor	Whether the monitoring function is enabled.
Global Configuration ID	The ID is generated automatically based on AC configuration changes and increments progressively.

Platform Description N/A

4 VAC Commands

4.1 device

In standalone mode, use this command to set the device ID in VAC system.

device *device_id*

Restore the default setting.

no device

Parameter Description

Parameter	Description
device_id	Device ID in VAC system. ☑ ID range depends on the model in use.

Default The default device ID is 1.

Command Mode Config-vac-domainmode

Usage Guide The device with a smaller device ID is elected as the master device if two devices are both master devices or if the two devices share the same priority and are just started with their roles not determined.
The device with a higher priority is elected as the master device.

Configuration Example 1: Set 2 as the device ID.

```
Ruijie(config)# virtual-ac domain 1
Ruijie(config-vac-domain)# device 2
Ruijie(config-vac-domain)# exit
```

Verification Run the **show virtual-ac config** command to display the configuration.

Common Errors -

4.2 device convert mode

Use this command to convert between standalone mode and VAC mode.

device convert mode { **virtual** | **standalone** } [*device_id*]

Parameter Description

Parameter	Description
virtual	Conversion to VAC mode.
standalone	Conversion to standalone mode.
device_id	Device ID.

Default Standalone mode is the default mode.

Command Mode Privileged EXEC mode

Usage Guide After the **device convert mode virtual** command is run, the software automatically backs up the global configuration file in standalone mode as “standalone.text”, deletes global configuration file “config.text”, and then asks the user if “config_vac.text” is allowed to replace “config.text”. If the user chooses “yes”, “config_vac.text” replaces “config.text”. Otherwise, the global configuration file “config.text” is not restored, and the related configuration of the VAC system is written to the configuration file “config_vac.dat” before the device is reloaded.

After the **device convert mode standalone** command is run, the software automatically backs up the global configuration file in standalone mode as “virtuac-ac.text”, deletes global configuration file “config.text”, and then asks the user if “standalone.text” is allowed to replace “config.text”. If the user chooses “yes”, “standalone.text” replaces “config.text”. Otherwise, the global configuration file “config.text” is not restored, and the related configuration of the VAC system is written to the configuration file “config_vac.dat” before the device is reloaded.

This command can be run in both standalone and VAC modes. In standalone mode, the current device carries out the conversion. In VAC mode, when the parameter of device_id is added, then the specified standby device operates the conversion; when this parameter is not added, the master device performs the conversion. It is suggested to converse standby devices before the master device.

Configuration Example 1 : The following example converts to VAC mode.

```
Ruijie# device convert mode virtual
```

2 : In VAC mode, convert the device whose ID is 2 to standalone mode and then convert the device whose ID is 1 to standalone mode.

```
Ruijie# device convert mode standalone  2
Ruijie# device convert mode standalone 1
```

Verification -

Prompts

1. Conversion from VAC mode to standalone mode.

The system asks whether the user would like to switch the device to standalone mode. If the user chooses “yes”, the software backs up config.text as standalone.text, deletes config.text, and reloads the device.

```
Convert mode will backup and delete config file, and reload the device. Are you sure
to continue[yes/no]
```

The system asks whether the user wants to recover the config.text file from the backup file.

```
Do you want to recover config file from back file in standalong mode  (press ’ctrl
+ c’ to cancel) [yes/no]:n
```

2. Conversion from standalone mode to VAC mode.

The system asks whether the user would like to switch the device to VAC mode. If the user chooses “yes”, the software backs up config.text as virtual-ac.text, deletes config.text, and reloads the device.

```
Convert mode will backup and delete config file, and reload the device. Are you sure
to continue[yes/no]
```

The system asks whether the user wants to recover the config.text file from the backup file.

```
Do you want to recover config file from back file in virtual-ac mode (press ’ctrl
+ c’ to cancel) [yes/no]:
```

Common Errors

-

4.3 device priority

Use this command to configure device priority in the VAC system.

device *device_id* **priority** *priority_num*

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

no device *device_id* **priority**

Parameter Description

Parameter	Description
device_id	ID of the device to be configured with priority. ☑ Range depends on the model in use. Please refer to configuration manuals for details.
priority_num	Priority number, range: 1 – 255.

Default

priority_num: the default value is 100.

Command Mode config-vac-domain configuration mode

Usage Guide A larger value indicates a higher priority. The device with a higher priority is elected as the master device. This command is available in both the standalone mode and VAC mode. The changed priority takes effect only after the device restart.
In VAC mode, *device_id* indicates the ID of the currently running device. If the device ID does not exist, the priority configuration does not take effect.

Configuration Example 1: In standalone mode, the following example sets the priority of Device 1 to 200.

```
Ruijie(config)# virtual-ac domain 1
Ruijie(config-vac-domain)# device 1 priority 200
Ruijie(config-vac-domain)# exit
```

2: In VAC mode, the following example sets the priority of Device 1 to 200 and restores the default setting of Device2.

```
Ruijie(config)# virtual-ac domain 1
Ruijie(config-vac-domain)# device 1 priority 200
Ruijie(config-vac-domain)# no device 2 priority
Ruijie(config-vac-domain)# exit
```

Verification Run the **show virtual-ac** command to display the configuration.

Common Errors -

4.4 dual-active bfd interface

Use this command to configure the BFD detection port.
dual-active bfd interface *interface-name*

Use the no form of this command to delete the BFD detection port.
no dual-active bfd interface *interface-name*

Parameter Description

Parameter	Description
interface-name	Type and number of the detection port.

Default -

Command Mode config-vac-domain configuration mode

Usage Guide BFD detection ports must be routed ports residing in different devices.

Configuration Example The following example configures Gi1/0/1 as the BFD-based dual-master detection port.

```
Ruijie(config)# interface GigabitEthernet 1/0/1
Ruijie(config-if- GigabitEthernet 1/0/1)# no switchport
Ruijie(config)# interface GigabitEthernet 2/0/1
Ruijie(config-if- GigabitEthernet 2/0/1)# no switchport
Ruijie(config)# virtual-ac domain 1
Ruijie(config-vac-domain)# dual-active bfd interface GigabitEthernet 1/0/1
Ruijie(config-vac-domain)# dual-active bfd interface GigabitEthernet 2/0/1
```

Verification Run the **show virtual-ac dual-active bfd** command to display the configuration.

Common Errors Detection ports are not routed ports.

4.5 dual-active detection

Use this command to configure dual-master detection.
dual-active detection { **aggregateport | bfd** }

Use the **no** form of this command to restore the default setting.
no dual-active detection { **aggregateport | bfd** }

Parameter Description

Parameter	Description
aggregateport	Specifies the aggregate port-based detection.
bfd	Indicates BFD detection.

Default The dual-master detection is disabled.

Command Mode config-vac-domain configuration mode

Usage Guide This command can be configured only in VAC mode.

Configuration 1. The following example enables BFD-based dual-master detection.

Example

```
Ruijie(config)# virtual-ac domain 1
Ruijie(config-vac-domain)# dual-active detection bfd
```

2. The following example disables BFD-based dual-master detection.

```
Ruijie(config)# virtual-ac domain 1
Ruijie(config-vac-domain)# no dual-active detection bfd
```

3. The following example enables aggregate port-based dual-master detection.

```
Ruijie(config)# virtual-ac domain 1
Ruijie(config-vac-domain)# dual-active detection aggregateport
```

4. The following example disables aggregate port-based dual-master detection.

```
Ruijie(config)# virtual-ac domain 1
Ruijie(config-vac-domain)# no dual-active detection aggregateport
```

Verification Run the **show virtual-ac dual-active summary** command to display the congifuration.

Common Errors -

4.6 dual-active exclude interface

Use this command to specify excluded ports that do not need to be disabled in recovery mode.
dual-active exclude interface *interface-name*

Use the **no** form of this command to remove the excluded ports.
no dual-active exclude interface *interface-name*

Parameter Description

Parameter	Description
interface-name	Type and ID of a port.

Command Mode config-vac-domainconfiguration mode

Usage Guide This command can be configured only in VAC mode.
Excluded ports must be routing ports and cannot be heartbeat ports.
You can configure multiple excluded ports.

Configuration Example The following example configures Gi0/3 as the excluded port of dual-master detection.

```
Ruijie(config)# interface GigabitEthernet 0/3
```

```
Ruijie(config-if- GigabitEthernet 0/3)# no switchport
Ruijie(config)# virtual-ac domain 1
Ruijie(config-vac-domain)# dual-active exclude interface GigabitEthernet 0/3
```

Verification Run the **show virtual-ac dual-active summary** command to display the configuration.

Common Errors Excluded ports are not routed ports.

4.7 dual-active interface

Use this command to configure the dual-master detection port.
dual-active interface *interface-name*

Use the **no** form of this command to delete the dual-master detection port.
no dual-active interface

Parameter Description

Parameter	Description
interface-name	Type and ID of the detection port. The port has to be an AP port.

Default -

Command Mode config-vac-domain configuration mode

Usage Guide There is only one aggregate port-based dual-master detection port. You need to create the detection port before configuring an AP port as the detection port. The subsequently configured detection port replaces the previously configured one.

Configuration Example The following example configures aggregateport1 as the detection port.

```
Ruijie(config)# virtual-ac domain 1
Ruijie(config-vac-domain)# dual-active interface aggregateport 1
```

Verification Run the **show virtual-ac dual-active summary** command to display the configuration.

Common Errors The detection port is not an AP port.

4.8 slave preemptive enable

Use this command to configure slave device preemption.
slave preemptive enable

Use the no form of this command to restore the default setting.
no slave preemptive enable

Parameter Description

Parameter	Description
-	-

Default Slave device preemption is disabled by default.

Command Mode config-vac-domain configuration mode

Usage Guide This command is configurable only in VAC mode.

Configuration Example The following example enables slave device preemption.

```
Ruijie(config)# virtual-ac domain 1
Ruijie(config-vac-domain)# slave preemptive enable
```

Verification Run the show running-config command to display the configuration.

Common Errors -

4.9 virtual-ac domain

Use this command to configure the domain ID.
virtual-ac domain *domain_id*

Use the **no** form of this command to restore the default setting.
no virtual-ac domain

Parameter Description

Parameter	Description
domain_id	Virtual domain ID of a VAC system. Range: 1 - 255.

Default The default domain ID is100.

Command Mode config-vac-domain configuration mode.

Usage Guide Only devices with the same domain ID can compose a VAC system. The domain ID must be unique in the LAN.

Configuration Example The following example set the domain ID to 1.

```
Ruijie(config)# virtual-ac domain 1
Ruijie(config-vac-domain)#
```

Verification -

Common Errors -

4.10 vac-port

Use this command to enter the heartbeat configuration mode.

vac-port

Parameter Description

Parameter	Parameter
-	-

Default -

Command Mode Configuration mode

Usage Guide This command is available in both the standalone mode and VAC mode.

Configuration Example 1. The following example enters the heartbeat configuration mode in standalone mode.

```
Ruijie(config)# vac-port
Ruijie(config-vac-port)#
```

2. The following example enters the heartbeat configuration mode in VAC mode.

```
Ruijie(config)# vac-port
Ruijie(config-vac-port)#
```

Verification -

Common Errors -

4.11 port-member interface

Use this command to configure a heartbeat port.

port-member interface *interface-name* [**copper | fiber**]

Use this command o delete a heartbeat port.

no port-member interface *interface-name*

Parameter Description

Parameter	Description
interface-name	Port name, such as GigabitEthernet 0/1.
copper	Electrical port attribute.
fiber	SFP port attribute.

Default -

Command Mode config-vac-port configuration mode

Usage Guide This command is available in both VAC mode and standalone mode. The command configuration needs to be saved.

interface-name: A heartbeat port can be either a 10G or a Gigabit port. A Gigabit port can be an optical/electrical port. If media type is not specified, a default Gigabit port is an optical port. In terms of an optical/electrical port, its attribute should be specified.

Configuration Example The following example adds/deletes a heartbeat port in standalone mode.

```
Ruijie(config)# vac-port
Ruijie(config-vac-port)# port-member interface GigabitEthernet 0/1
Ruijie(config-vac-port)# no port-member interface GigabitEthernet 0/2
```

Verification Run the **show virtual-ac link port** command to display the configuration.

Common Errors -

4.12 session

Use this command to redirect to the console of the master device or any device.

session { **device** *device_id* | **master** }

Parameter Description

Parameter	Description
device	Redirection to the console of a member device.
device_id	Member device ID, whose range depends on the model in use.
master	Redirection to the console of a master device.

Default -

Command Mode Privileged EXEC mode

Usage Guide This command is configurable in VAC mode.

Configuration Example 1. The following example redirects from the console of Device 2 to the console of the master device, and then exits.

```
Ruijie-STANDBY#session master
Ruijie#exit
Ruijie-STANDBY#
```

2. The following example redirects from console of the master device to the console of Device 2, and the exits.

```
Ruijie#session device 2
Ruijie-STANDBY#exit
Ruijie#
```

Verification -

Common Errors -

4.13 show device id

Use this command to display the device ID.

show device id

Parameter Description

Parameter	Description
-	-

Command Mode Privileged EXEC mode

Usage Guide -

Configuration Example 1. The following example displays the device ID in standalone mode.

```
Ruijie #show device id
Device ID is 2
```

2. The following example displays the device ID in VAC mode.

```
Ruijie#show device id
Device ID is 1
```

Common Errors -

4.14 show virtual-ac

Use this command to display information about the currently running VAC system, topology structure, or current VAC system parameters.

show virtual-ac

Parameter Description

Parameter	Description
-	-

Command Mode Privileged EXEC mode

Usage Guide -

Configuration Example 1. The following example displays information in standalone mode.

```
Ruijie# show virtual-ac
Current system is running in “STANDALONE” mode.
```

2. The following example displays information about two member switching devices in VAC mode.

```
Ruijie#show virtual-ac
```

```
Device_id    Domain_id    Priority    Status    Role
-------------------------------------------------------------
1(1)         1(1)         100(100)    OK        ACTIVE
2(2)         1(1)         100(100)    OK        STANDBY
```

Parameter meaning:

Parameter	Meaning
Device_id	Device ID. The configured values are shown in brackets, which take effect after the system reboot.
Domain_id	Domain ID. The configured values are shown in brackets, which take effect after the system reboot.
Priority	Priority. The configured values are shown in brackets, which take effect after the system reboot.
Status	Device status: OK- the device is normal; Recovery- recovery status; Leave-leave status; Isolate- isolation status.
Role	Role: ACTIVE- master device; STANDBY- member device.

4.15 show virtual-ac config

Use this command to display the VAC system configuration in standalone or VAC mode.

show virtual-ac config [*device_id*]

Parameter Description

Parameter	Description
device_id	Device ID. If this parameter is specified, only the VAC system configuration of the specific device is displayed.

Command Mode Privileged EXEC mode

Usage Guide -

Configuration Example 1. The following example displays the VAC system configuration on the current device in standalone mode.

```
Ruijie#show virtual-ac config
device_id: 1 (mac: 00d0.f810.3323)
!
virtual-ac domain 1
!
device 1
device 1 priority 200
!
```

```
port-member interface GigabitEthernet 0/1
port-member interface GigabitEthernet 0/2
!
device convert mode standalone
!
```

2. The following example displays the VAC system configuration on the current device in VAC mode.

```
Ruijie#show virtual-ac config
device_id: 1 (mac: 00d0.f810.1111)
!
virtual-ac domain 1
!
device 1
device 1 priority 200
!
port-member interface GigabitEthernet 0/1
port-member interface GigabitEthernet 0/2
!
device convert mode virtual
!

device_id: 2 (mac: 00d0.f810.2222)
!
virtual-ac domain 1
!
device 2
device 2 priority 100
!
port-member interface GigabitEthernet 0/1
port-member interface GigabitEthernet 0/2
!
device convert mode virtual
!
```

3. The following example displays the Device1 configuration of the VAC system in VAC mode.

```
Ruijie#show virtual-ac config 1
device_id: 1 (mac: 00d0.f810.1111)
!
virtual-ac domain 1
!
device 1
```

```
device 1 priority 200
!
port-member interface GigabitEthernet 0/1
port-member interface GigabitEthernet 0/2
!
```

Parameters:

Parameter	Meaning
device_id	Device ID.
Virtual-ac domain	Domain where the device belongs.
priority	Priority of the device.
vac-port	Configuration information of the heartbeat port.

4.16 show virtual-ac dual-active

Use this command to display the current dual-master detection configuration.

show virtual-ac dual-active summary

Parameter Description

Parameter	Description
-	

Command Mode Privileged EXEC mode

Usage Guide -

Configuration Example The following example displays the current dual-master detection configuration.

```
Ruijie# show virtual-ac dual-active summary
Interfaces excluded from shutdown in recovery mode:
GigabitEthernet 0/3
GigabitEthernet 0/4
In dual-active recovery mode: No
Dual-active interface configured:
    GigabitEthernet 0/1
```

Parameters:

Parameter	Meaning
Interfaces excluded from shutdown in recovery mode	Configuration of excluded ports.
Dual-active interface configured	Detection port.

4.17 show virtual-ac link

Use this command to display configuration of the heartbeat port.

show virtual-ac link [**port**]

Parameter Description

Parameter	Description
port	Physical heartbeat port.

Command Mode Privileged EXEC mode

Usage Guide There are three statuses for a heartbeat port:

1. DOWN: the physical port is linked down;
2. UP: the physical port is linked up, but no an available peer heartbeat port is detected;
3. OK: the physical port is linked up, and an available peer heartbeat port is detected.

Configuration Example 1. The following example displays the heartbeat link running status.

```
Ruijie# show virtual-ac link
VAC-PORT    State   Peer-PORT       Rx      Tx      Uptime
------------------------------------------------------------------------------
----
1/1     UP      2/1         100000  100000  1d,4h,29m
2/1     UP      1/1         100000  100000  1d,4h,29m
```

Parameters:

Parameter	Meaning
VAC-PORT	Heartbeat port list.
State	Heartbeat port status, which is either DOWN or UP.
Peer-PORT	Peer heart beat port.
Rx	Received packets.
Tx	Sent packets.
Uptime	Uptime of the port.

2. The following example displays information of the physical heartbeat ports.

```
Ruijie# show virtual-ac link port

Device 1:
Port                      State  Peer-port           Rx    Tx  Uptime
------------------------------------------------------------------------------
-----
```

```
GigabitEthernet 0/1   OK     GigabitEthernet 0/1     9000  9000    0d,0h,20m

Device 2:
Port                      State  Peer-port           Rx    Tx  Uptime

------------------------------------------------------------------------------
-----
GigabitEthernet 0/1   OK     GigabitEthernet 0/1     9000  9000    0d,0h,20m
```

Parameters:

Parameter	Meaning
Port	Port list.
State	Port status.
Peer-port	Peer port.
Rx	Received packets.
Tx	Sent packets.
Uptime	Uptime of the port.

4.18 show virtual-ac role

Use this command to display the number, role and priority of each device.

show virtual-ac role

Parameter Description

Parameter	Description
-	-

Command Mode Privileged EXEC mode

Usage Guide N/A

Configuration Example 1. The following runs the command in standalone mode.

```
Ruijie# show virtual-ac
Current system is running in “STANDALONE” mode.
```

2. The following example runs the command in VAC mode and displays information of 2 standby devices.

```
Ruijie#show virtual-ac
Device_id    Domain_id    Priority    Status    Role
------------------------------------------------------------------------------
1(1)        1(1)         100(100)    OK        ACTIVE
2(2)        1(1)         100(100)    OK        STANDBY
```

Parameters:

Parameter	Meanign
Device_id	Device ID. The configured values are shown in brackets, which take effect after the system reboot.
Domain_id	Domain ID. The configured values are shown in brackets, which take effect after the system reboot.
Priority	Priority. The configured values are shown in brackets, which take effect after the system reboot.
Status	Device status: OK- the device is normal; Recovery- recovery status; Leave-leave status; Isolate- isolation status.
Role	Role: ACTIVE- master device; STANDBY- member device.

4.19 show virtual-ac topology

Use this command to display the topology status of the VAC system.

show virtual-ac topology

Parameter Description

Parameter	Description
-	-

Command Mode Privileged EXEC mode

Usage Guide -

Configuration Example The following example displays topology status.

```
Ruijie# show virtual-ac topology
Introduction: '[num]' means switch num, '(num/num)' means VAC-port num.

Chain Topology:
[1](1/2)---(2/1)[2]

Device[1]: ACTIVE, MAC: 00d0.f822.33d6
Device[2]: STANDBY, MAC: 1234.5678.9003
```

Parameters:

Parameter	Meaning
Ring Topology	Topology structure.

Device[-]	Device description

5 Bonjour Gateway Commands

5.1 bonjour-gateway airplay-preemption

Use this command to disable preemption prohibition. Use the **no** form of this command to enable preemption prohibition.

bonjour-gateway airplay-preemption disable

no bonjour-gateway airplay-preemption disable

Parameter Description

Parameter	Description
N/A	N/A

Defaults This function is disabled by default.

Command Mode Global configuration mode

Default Level 14

Usage Guide The **bonjour-gateway airplay-preemption disable** command is used to disable preemption prohibition. By default, preemption prohibition of the Bonjour gateway is enabled.

Configuration Examples The following example disables preemption prohibition in global configuration mode.

```
Ruijie(config)#
Ruijie(config)#bonjour-gateway airplay-preemption disable
```

Verification Run the **show running-config** command to display the configurations.

Prompts N/A

Common Errors N/A

Platform Description N/A

5.2 bonjour-gateway airplay-rename

Use this command to disable automatic renaming of the Bonjour gateway. Use the **no** form of this command to enable automatic renaming of the Bonjour gateway.

bonjour-gateway airplay-rename disable

no bonjour-gateway airplay-rename disable

Parameter Description

Parameter	Description
N/A	N/A

Defaults This function is disabled by default.

Command Mode Global configuration mode

Default Level 14

Usage Guide The **bonjour-gateway airplay-rename disable** command is used to disable automatic renaming. The **no bonjour-gateway airplay-rename disable** command is used to enable automatic renaming. By default, automatic renaming of the Bonjour gateway is enabled.

Configuration Examples The following example disables automatic renaming in global configuration mode.

```
Ruijie(config)#
Ruijie(config)#bonjour-gateway airplay-rename disable
```

Verification Run the **show running-config** command to display the configurations.

Prompts N/A

Common Errors N/A

Platform Description N/A

5.3 bonjour-gateway enable

Use this command to enable the Bonjour gateway. Use the **no** form of this command to disable the Bonjour gateway.

bonjour-gateway enable

no bonjour-gateway enable

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

Defaults This function is disabled by default.

Command Mode Interface configuration mode

Default Level 14

Usage Guide The **bonjour-gateway enable** command is used to enable the Bonjour gateway in interface configuration mode. The **no bonjour-gateway enable** command is used to disable the Bonjour gateway. By default, the Bonjour gateway is disabled.

Configuration Examples The following example enables the Bonjour gateway.

```
Ruijie(config)#
Ruijie(config)#interface vlan 1
Ruijie(config-if-vlan 1)#bonjour-gateway enable
```

Verification Run the **show running-config** command to display the configurations.

Prompts N/A

Common Errors N/A

Platform Description N/A

5.4 bonjour-gateway global-strategy

Use this command to apply a specified Bonjour policy globally. Use the **no** form of this command to cancel

the applied Bonjour policy.

bonjour-gateway global-strategy *name*

no bonjour-gateway strategy

Parameter Description

Parameter	Description
name	Name of a Bonjour policy.

Defaults No Bonjour policy is applied globally by default.

Command Mode Configuration mode

Default Level 14

Usage Guide The **bonjour-gateway global-strategy** command is used to apply a specified Bonjour policy globally. The **no bonjour-gateway global-strategy** command is used to cancel the applied Bonjour policy. By default, no Bonjour policy is applied globally.

Configuration Examples The following example applies a Bonjour policy globally.

```
Ruijie(config)#
Ruijie(config)# bonjour-gateway global-strategy teacher
```

Verification Run the **show running-config** command to display the configurations.

Prompts N/A

Common Errors N/A

Platform Description N/A

5.5 bonjour-gateway query enable

Use this command to enable the active query of Bonjour services. Use the **no** form of this command to disable the active query of Bonjour services.

bonjour-gateway query enable

no bonjour-gateway query enable

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

Defaults This function is disabled by default.

Command Mode Global configuration mode

Default Level 14

Usage Guide The **bonjour-gateway query enable** command is used to enable the active query of Bonjour services. The **no bonjour-gateway query enable** command is used to disable the active query of Bonjour services. By default, the active query of Bonjour services is disabled.

Configuration Examples The following example enables the active query of Bonjour services.

```
Ruijie(config)#bonjour-gateway query enable
```

Verification Run the **show running-config** command to display the configurations.

Prompts N/A

Common Errors N/A

Platform Description N/A

5.6 bonjour-gateway query interval

Use this command to configure the interval for sending query packets to a discovered service. Use the **no** form of this command to restore the default settings.

bonjour-gateway query interval *number*

no bonjour-gateway query interval

Parameter Description

Parameter	Description
number	Interval for sending query packets to a discovered service in seconds. The value ranges from **5** to **600**.

Defaults The interval is 15 seconds by default.

Command Mode Global configuration mode

Default Level 14

Usage Guide The **bonjour-gateway query interval** command is used to configure the interval for sending query packets to a discovered service. The **no bonjour-gateway query interval** command is used to restore the default settings. By default, the interval for sending query packets to a discovered service is 15 seconds.

Configuration Examples The following example sets the interval for sending query packets to a discovered service to 60 seconds.

```
Ruijie(config)#bonjour-gateway query interval 60
```

Verification Run the **show running-config** command to display the configurations.

Prompts N/A

Common Errors N/A

Platform Description N/A

5.7 bonjour-gateway strategy

Use this command to apply a specified Bonjour policy. Use the **no** form of this command to cancel the applied Bonjour policy.

bonjour-gateway strategy *name*

no bonjour-gateway strategy *name*

Parameter Description

Parameter	Description
name	Name of a Bonjour policy.

Defaults No Bonjour policy is applied on Layer-3 interfaces by default.

Command Mode	Interface configuration mode
Default Level	14
Usage Guide	The **bonjour-gateway strategy** command is used to apply a specified Bonjour policy on Layer-3 interfaces. The **no bonjour-gateway strategy** command is used to cancel the applied Bonjour policy. By default, no Bonjour policy is applied on Layer-3 interfaces.

Configuration Examples	The following example applies a Bonjour policy in VLAN 1.
	`Ruijie(config)#`
	`Ruijie(config)#interface vlan 1`
	`Ruijie(config-if-vlan 1)#bonjour-gateway strategy teacher`

Verification	Run the **show running-config** command to display the configurations.
Prompts	N/A
Common Errors	N/A
Platform Description	N/A

5.8 bonjour-gateway strategy-mode

Use this command to create a Bonjour policy. Use the **no** form of this command to delete a Bonjour policy.
bonjour-gateway strategy-mode *name*
no bonjour-gateway strategy-mode *name*

Parameter Description

Parameter	Description
name	Name of a Bonjour policy.

Defaults	No Bonjour policy is created by default.
Command Mode	Global configuration mode
Default Level	14

Usage Guide The **bonjour-gateway strategy-mode** command is used to create a Bonjour policy. The **no bonjour-gateway strategy-mode** command is used to delete a Bonjour policy. By default, no Bonjour policy is created. A maximum of 1000 Bonjour policies can be created on the device.

Configuration Examples The following example creates a Bonjour policy named **teacher**.

```
Ruijie(config)# bonjour-gateway strategy-mode teacher
```

Verification Run the **show running-config** command to display the configurations.

Prompts N/A

Common Errors N/A

Platform Description N/A

5.9 service

Use this command to enable prohibition of service discovery in wired or wireless mode. Use the **no** form of this command to disable prohibition of service discovery in wired or wireless mode.

service [wired | wireless] disable

no service [wired | wireless] disable

Parameter Description

Parameter	Description
N/A	N/A

Defaults Service discovery is allowed in both wired and wireless modes by default.

Command Mode Configuration mode

Default Level 14

Usage Guide The **service [wired | wireless] disable** command is used to enable prohibition of service discovery in wired or wireless mode. The **no service [wired | wireless] disable** command is used to restore service discovery in wired or wireless mode. By default, service discovery is allowed in both wired and wireless modes.

Configuration Examples The following example enables prohibition of service discovery in wired mode.

```
Ruijie(config)#bonjour-gateway strategy-mode teacher
```

```
Ruijie(config-bonjour-gateway)#service wired disable
```

Verification Run the **show running-config** command to display the configurations.

Prompts N/A

Common Errors N/A

Platform Description N/A

5.10 service type

Use this command to configure a service rule. Use the **no** form of this command to delete a service rule.

service type *type* **[instance** *name* **| disable]**

no service type *type* **[instance** *name* | **disable]**

Parameter Description

Parameter	Description
type	Type of a service that can be found by the client.
name	Instance name of a service that needs to be searched for by the client.

Defaults The client can find all services by default.

Command Mode Configuration mode

Default Level 14

Usage Guide The **service type** command is used to configure a service rule. The **no service type** command is used to delete a service rule. By default, the client can find all services.

Table: Mapping Between the Service Type and Protocol

Parameter	Description
amazontv	Amazon TV
airplay	Airplay
airprint	Airprint
chat	Chat
googlecast	Google cast
itunes	ITunes

raop	Remote Audio Output Protocol
remotemgmt	Remote management
sharing	Sharing
xmind	Xmind

Configuration Examples The following example sets the type of the service that can be found by the client to **ftp**, and the IP address of the service to **10.0.0.5**.

```
Ruijie(config)#bonjour-gateway strategy-mode teacher
Ruijie(config-bonjour-gateway)#service type ftp ip 10.0.0.5
```

Verification Run the **show running-config** command to display the configurations.

Prompts N/A

Common Errors N/A

Platform Description N/A

5.11 service vlan

Use this command to configure a VLAN that allows forwarding query and response packets. Use the **no** form of this command to delete a VLAN that allows forwarding query and response packets.

service vlan range *vlan-id-list* **[access-vlan]**

no service vlan

Parameter Description

Parameter	Description
vlan-id-list	Sets a VLAN list.
access-vlan	Allows to forward query and response packets in the client-accessed VLAN.

Defaults Packets can be forwarded in all VLANs by default.

Command Mode Interface configuration mode

Default Level 14

Usage Guide The **service vlan range** command is used to configure a VLAN that allows forwarding query and response packets. The **no service vlan** command is used to delete the settings. By default, packets can be

forwarded in all VLANs.

Configuration Examples The following example allows forwarding query and response packets in VLAN 5.

```
Ruijie(config)#bonjour-gateway strategy-mode teacher
Ruijie(config-bonjour-gateway)#service vlan range 5
Ruijie(config-bonjour-gateway)#service vlan access-vlan
```

Verification Run the **show running-config** command to display the configurations.

Prompts N/A

Common Errors N/A

Platform Description N/A

5.12 show bonjour-gateway service-database

Use this command to display information about the discovered Bonjour service.

show bonjour-gateway service-database

Parameter Description

Parameter	Description
N/A	N/A

Command Mode Privileged EXEC mode, global configuration mode, and interface configuration mode

Default Level 14

Usage Guide This command is used to display information about the discovered Bonjour service.

Configuration Examples The following example displays information about the discovered Bonjour service in privileged EXEC mode.

```
Ruijie# show bonjour-gateway service-database
Total number of discarded query packets    : 0
Total number of discarded response packets : 20
Total number of bonjour services          : 3

------------------------------------------------------------------------------
Name                   Type           VLAN     TTL     IP
```

```
------------------------------------------------------------------------------
-
Apple TV                airplay       1        4500    192.168.10.2
B8782E5101E7@Apple TV     raop          2        4500    192.168.10.2
70-35-60-63.1 Apple TV    sleep-proxy    3        4500    192.168.10.2
```

Prompts N/A

Platform Description N/A

5.13 show bonjour-gateway service-database ip

Use this command to display information about the specified IP Bonjour service discovered by the device.

show bonjour-gateway service-database ip *address*

Parameter Description

Parameter	Description
address	Indicates the IP address for the Bonjour service.

Command Mode Privileged EXEC mode, global configuration mode, and interface configuration mode

Default Level 14

Usage Guide This command is used to display information about the specified IP Bonjour service discovered by the device.

Configuration Examples The following example displays information about the discovered Bonjour service in privileged EXEC mode.

```
RUIJIE(config)#show bonjour-gateway service-database ip 192.168.197.178
Service name ..................... R08833.local
Service type ..................... airplay,raop,
VLAN ............................. 1
Interface name ................... Gi0/8
IP Address ....................... 192.168.197.178
MAC Address ...................... 509a.4c4e.2149
Wired/Wireless ................... wired
TTL(sec) ......................... 118
```

Prompts N/A

Platform Description	N/A

5.14 show bonjour-gateway strategy-mode

Use this command to display the Bonjour policy information.

show bonjour-gateway strategy-mode

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

Command Mode	Privileged EXEC mode, global configuration mode, and interface configuration mode
Default Level	14
Usage Guide	This command is used to display the Bonjour policy information.
Configuration Examples	The following example displays the Bonjour policy information in privileged EXEC mode.

```
Ruijie# show bonjour-gateway strategy-mode
Total number of configured bonjour strategy: 1

                        bonjour gateway strategy
-------------------------------------------------------------------------------
--
bonjour gateway strategy name : teacher
VLAN         : 1
Access-VLAN   : Enabled
Service vlan   : 5

Service type      IP address/Instance name
ftp             10.0.0.5

bonjour gateway strategy name : student
VLAN         : 2
Access-VLAN   : Enabled
Service vlan   : 6

Service type      IP address/Instance name
ftp             10.0.0.5
```

Prompts	N/A
Platform Description	N/A

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-number*]

Parameter Description

Parameter	Description
interface-type interface-number	Interface type and interface ID

Defaults N/A

Command Mode Privileged EXEC mode.

Usage Guide In the privileged EXEC mode, use the **show interfaces** command to display the counters or the **clear counters** command to clear the counters. If the interface is not specified, the counters on all interfaces will be cleared.

Configuration Examples The following example clears the counters on interface gigabitethernet 1/1.

```
Ruijie# clear counters gigabitethernet 1/1
```

Related Commands

Command	Description
show interfaces	Displays the interface information.

Platform Description N/A

1.4 clear interface

Use this command to reset the interface.

clear interface *interface-type interface-number*

Parameter Description

Parameter	Description
interface-type interface-number	Interface type and interface ID

Defaults N/A

Command Mode Privileged EXEC mode.

Usage Guide This command is only used on the switch port, member port of the L2 Aggregate port, routing port, and member port of the L3 aggregate port. This command is equal to the **shutdown** and **no shutdown** commands.

Configuration Examples The following example resets the interface gigabitethernet 1/1.

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

Related Commands

Command	Description
shutdown	Disables the interface.

Platform Description N/A

1.5 description

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

description *string*

no description

Parameter Description

Parameter	Description
string	Interface alias

Defaults No alias is configured by default.

Command Mode Interface configuration mode.

Usage Guide Use **show interfaces** to display the interface information, including the alias.

Configuration Examples The following example configures the alias of interface.

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

Related Commands

Command	Description
show interfaces	Displays the interface information.

Platform Description N/A

1.6 duplex

Use this command to specify the duplex mode for the interface. Use the **no** form of this command to restore the default setting.

duplex { **auto** | **full** | **half** }

no duplex

Parameter Description

Parameter	Description
auto	Self-adaptive full duplex and half duplex
full	Full duplex
half	Half duplex

Defaults The default is **auto**,

Command Mode Interface configuration mode.

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

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

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

Related Commands

Command	Description
show interfaces	Displays the interface information.

Platform Description N/A

1.7 errdisable recovery

Use this command to recover the interface in violation.

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

Parameter Description

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

Defaults It is disabled by default.

Command Mode Global configuration mode.

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

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

```
Ruijie(config)# interface gigabitethernet 1/1
Ruijie(config-if)# errdisable recovery
```

Related Commands

Command	Description
switchport port-security violation shutdown	Configures the port security violation to shutdown.

Platform Description N/A.

1.8 interface

Use this command to enter the interface configuration mode.

interface *interface-type interface-number*

Parameter Description

Parameter	Description
interface-type	The interface type.
interface-number	The interface ID.

Defaults N/A

Command Mode Interface configuration mode

Usage Guide This command is used to enter interface configuration mode. The user can modify the interface configuration next,

Configuration Examples The following example enters configuration mode on Aggregateport 1.

```
Ruijie(config)# interface Aggregateport 1
Ruijie(config-if-Aggregateport 1)#
```

The following example enters configuration mode on GigabitEthernet 1/2.

```
Ruijie(config)# interface GigabitEthernet 1/2
Ruijie(config-if-GigabitEthernet 1/2)#
```

The following example configuration mode on VLAN 1.

```
Ruijie(config)# interface vlan 1
Ruijie(config-if-VLAN 1)#
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

1.9 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
Ruijie(config-if-range)# bandwidth 100
```

The following example enters interface configuration mode on multiple interfaces by defining the macro name.

```
Ruijie(config)# define interface-range route1 gigabitEthernet 0/0-2
Ruijie(config)# interface range macro route1
Ruijie(config-if-range)# bandwidth 100
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

1.10 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

Parameter	Description

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 medium-type

Use this command to specify the medium type for an interface. Use the **no** form of this command to restore the default setting.

medium-type { **auto-select** [**prefer** [**fiber | copper**]] **| fiber** | **copper** }

no medium-type

Parameter Description

Parameter	Description
fiber	Optical interface.
prefer [**fiber**	**copper**]	The preferred medium type for the interface is selected.
auto-select	Auto-selects the medium type for the interface.
copper	Copper interface.

Defaults The default is **copper**.

Command Mode Interface configuration (physical interface, except for AP and SVI)

Usage Guide If a port can be selected as an optical port or electrical port, you can only select one of them. Once the media type is selected, the attributes of the port, for example, status, duplex, flow control, and rate, all mean those of the currently selected media type. After the port type is changed, the attributes of the new port type take the default values, which can be modified as needed.

Configuration Examples The following example specifies the medium type for interface gigabitethernet 1/1.

```
Ruijie(config)# interface gigabitethernet 1/1
Ruijie(config-if)# medium-type copeer
```

Related Commands

Command	Description
show interfaces	Displays the interface information.

Platform Description

1.12 mtu

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

mtu *num*

Parameter Description

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

Defaults The default is 1500.

Command Mode Interface configuration mode.

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

Configuration Examples The following example sets the MTU supported on interface gigabitethernet 1/1 to 9000.

```
Ruijie(config)# interface GigabitEthernet 1/1
Ruijie(config-if-GigabitEthernet)# mtu 9000
```

Related Commands

Command	Description
show interfaces	Displays the interface information.

Platform Description N/A

1.13 shutdown

Use this command to disable an interface. Use the **no** form of this command to enable a disabled port.

shutdown

no shutdown

Parameter Description

Parameter	Description
N/A	N/A

Defaults By default, the administrative status of an interface is Up.

Command Mode Interface configuration mode

Usage Guide Use this command to stop the forwarding on the interface (Gigabit Ethernet interface, Aggregate port or SVI). You can enable the port with the **no shutdown** command. If you shut down the interface, the configuration of the interface exists, but does not take effect. You can view the interface status by using the **show interfaces** command.

If you use the script to run no shutdown frequently and rapidly, the system may prompt the interface status reversal.

Configuration Examples The following example disables an interface.

```
Ruijie(config)# interface aggregateport 1
Ruijie(config-if)# shutdown
```

The following example enables an interface.

```
Ruijie(config)# interface aggregateport 1
Ruijie(config-if)# no shutdown
```

Related Commands

Command	Description
clear interface	Resets the hardware.
show interfaces	Displays the interface information.

Platform Description N/A

1.14 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

1.15 snmp-server if-index persist

Use this command to set the interface index persistence. The interface index remains the same after the device is restarted.

snmp-server if-index persist

Parameter Description

Parameter	Description
N/A	N/A

Defaults This function is disabled by default.

Command Mode Global configuration mode

Usage Guide After this command is configured, all interface indexes are saved in the configuration file. After the device is restarted, interface indexes remain the same as before.

Configuration Examples The following example enables the interface index persistence.

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

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

1.16 speed

Use this command to configure the speed on the port. Use the **no** form of this command to restore the default setting.

speed [**10 | 100 | 1000 | auto**]

Parameter Description

Parameter	Description
10	The transmission rate of the interface is 10Mbps.
100	The transmission rate of the interface is 100Mbps.
1000	The transmission rate of the interface is 1000Mbps.
auto	Self-adaptive

Defaults The default is **auto**.

Command Mode Interface configuration mode.

Usage Guide If an interface is the member of an aggregate port, the rate of the interface depends on the rate of the aggregate port. You can set the rate of the interface, but it does not take effect until the interface exits the aggregate port. Use **show interfaces** to display configuration. The rate varies by interface types.

For example, you cannot set the rate of a SFP interface to 10M.

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

1.17 switchport

Use this command to configure a Layer 3 interface. Use the **no** form of this command to restore the default setting.

switchport

no switchport

Parameter Description

Parameter	Description
N/A	N/A

Defaults All the interfaces are in Layer 2 mode by default.

Command Mode Interface configuration mode.

Usage Guide This command is valid only for physical interfaces. The **switchport** command is used to disable the interface and re-enable it. In this status, the device will send the information to indicate the connect status. If the interface is changed to Layer 3 mode from Layer 2, all the attributes in Layer 2 mode will be cleared.

Configuration Examples The following example configures a Layer 3 interface.

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

Related Commands

Command	Description
show interfaces	Displays the interface information.

Platform Description N/A

1.18 switchport access

Use this command to configure an interface as a statics access port and add it to a VLAN. Use the **no** form of this command to restore the default setting.

switchport access vlan *vlan-id*

no switchport access vlan

Parameter Description

Parameter	Description
vlan-id	The VLAN ID at which the port to be added.

Defaults By default, the switch port is an access port and the VLAN is VLAN 1.

Command Mode Interface configuration mode.

Usage Guide Enter one VLAN ID. The system will create a new one and add the interface to the VLAN if you enter a new VLAN ID. If the VLAN ID already exists, the command adds the interface to the VLAN.
If the port is a trunk port, the operation does not take effect.

Configuration Examples The following example configures interface gigabitethernet 1/1 as a statistic access port and adds it to VLAN 2.

```
Ruijie(config)# interface gigabitethernet 1/1
Ruijie(config-if)# switchport access vlan 2
```

Related Commands

Command	Description
switchport mode	Configures the interface as Layer 2 mode (switch port mode).
switchport trunk	Configures a native VLAN and the allowed-VLAN list for the trunkport.

Platform Description N/A

1.19 switchport mode

Use this command to specify a L2 interface (switch port) mode. You can specify this interface to be an access port or a trunk port or an 802.1Q tunnel. Use the **no** form of this command to restore the default setting.

switchport mode { **access** | **trunk** }

no switchport mode

Parameter Description

Parameter	Description
access	Configures the switch port as an access port.
trunk	Configures the switch port as a trunk port.

Defaults The default is **access**.

Command Mode Interface configuration mode.

Usage Guide If a switch port mode is access port, it can be the member port of only one VLAN. Use **switchport access vlan** to specify the member of the VLAN.
A trunk port can be the member port of various VLANs defined by the allowed-VLAN list. The allowed VLAN list of the interface determines the VLANs to which the interface may belong. The trunk port is the member of all the VLANs in the allowed VLAN list. Use **switchport trunk** to define the allowed-VLANs list.

Configuration Examples The following example specifies a L2 interface (switch port) mode.

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

Related Commands

Command	Description
switchport access	Configures an interface as a statics access port and assigns it to a VLAN.
switchport trunk	Configures a native VLAN and the allowed-VLAN list for the trunk port.

Platform Description N/A

1.20 switchport trunk

Use this command to specify a native VLAN and the allowed-VLAN list for the trunk port. Use the **no** form of this command to restore the default setting.
switchport trunk { **allowed vlan** { **all |** [**add** | **remove** | **except**] *vlan-list* } | **native vlan** *vlan-id* }
no switchport trunk { **allowed vlan** | **native vlan** }

Parameter Description

Parameter	Description
allowed vlan *vlan-list*	Configures the list of VLANs allowed on the trunk port. *vlan-list* can be a VLAN or a range of VLANs starting with the smaller VLAN ID and ending with the larger VLAN ID and being separated by hyphen, for example, 10 to 20. The segments can be separated with a comma

	(,), for example, 1 to 10, 20 to 25, 30, 33. all means that the allowed VLAN list contains all the supported VLANs; add means to add the specified VLAN list to the allowed VLAN list; remove means to remove the specified VLAN list from the allowed VLAN list; except means to add all the VLANs other than those in the specified VLAN list to the allowed VLAN list;
native vlan *vlan-id*	Configures the native VLAN.

Defaults The allowed VLAN list is all, the Native VLAN is VLAN1.

Command Mode Interface configuration mode.

Usage Guide Native VLAN:
A trunk port belongs to one native VLAN. A native VLAN means that the untagged packets received/sent on the trunk port belong to the VLAN. Obviously, the default VLAN ID of the interface (that is, the PVID in the IEEE 802.1Q) is the VLAN ID of the native VLAN. In addition, when frames belonging to the native VLAN are sent over the trunk port, they are untagged.
Allowed-VLAN List:
By default, a trunk port sends traffic to and received traffic from all VLANs (ID 1 to 4094). However, you can prevent the traffic from passing over the trunk by configuring allowed VLAN lists on a trunk.
Use show interfaces switchport to display configuration.

Configuration Examples The following example configures Native VLAN of Trunk port GigabitEthernet 1/1 to VLAN 2.

```
Ruijie(config)# interface GigabitEthernet 1/1
Ruijie(config-if-GigabitEthernet 1/1)# switchport trunk native vlan 2
```

Related Commands

Command	Description
show interfaces	Displays the interface information.
switchport access	Configures an interface as a statics access port and assigns it to a VLAN.

Platform Description N/A

1.21 show interfaces

Use this command to display the interface information and optical module information.
show interfaces [*interface-type interface-number*] [**description | switchport | trunk**]

Parameter Description

Parameter	Description
interface-id interface-number	Interface (including Ethernet interface, aggregate port, SVI or loopback interface).
description	The description of the interface, including the link status.
switchport	Layer 2 interface information.
trunk	Trunk port, applicable for physical port and aggregate port.

Defaults

Command Mode Privileged EXEC mode.

Usage Guide This command is used to show all basic information if no parameter is specified.

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

```
SwitchA#show interfaces gigabitEthernet 0/1
Index(dec):1 (hex):1
GigabitEthernet 0/1 is DOWN  , line protocol is DOWN
Hardware is Broadcom 5464 GigabitEthernet
Interface address is: no ip address
  MTU 1500 bytes, BW 1000000 Kbit
  Encapsulation protocol is Bridge, loopback not set
  Keepalive interval is 10 sec , set
  Carrier delay is 2 sec
  RXload is 1 ,Txload is 1
  Queueing strategy: FIFO
    Output queue 0/0, 0 drops;
    Input queue 0/75, 0 drops
  Switchport attributes:
    interface's description:""
    medium-type is copper
    lastchange time:0 Day: 0 Hour: 0 Minute:13 Second
    Priority is 0
    admin duplex mode is AUTO, oper duplex is Unknown
    admin speed is AUTO, oper speed is Unknown
flow receive control admin status is OFF,flow send control admin status is OFF,flow
receive control oper status is Unknown,flow send control oper status is Unknown
broadcast Storm Control is OFF,multicast Storm Control is OFF,unicast Storm Control
is OFF
 Port-type: trunk
   Native vlan:1
Allowed vlan lists:1-4094
```

```
Active vlan lists:1, 3-4
  5 minutes input rate 0 bits/sec, 0 packets/sec
  5 minutes output rate 0 bits/sec, 0 packets/sec
    0 packets input, 0 bytes, 0 no buffer, 0 dropped
    Received 0 broadcasts, 0 runts, 0 giants
    0 input errors, 0 CRC, 0 frame, 0 overrun, 0 abort
    0 packets output, 0 bytes, 0 underruns , 0 dropped
0 output errors, 0 collisions, 0 interface resets
```

The following example displays the interface information when the Gi0/1 is an Access port.

```
SwitchA#show interfaces gigabitEthernet 0/1
Index(dec):1 (hex):1
GigabitEthernet 0/1 is DOWN  , line protocol is DOWN
Hardware is Broadcom 5464 GigabitEthernet
Interface address is: no ip address
  MTU 1500 bytes, BW 1000000 Kbit
  Encapsulation protocol is Bridge, loopback not set
  Keepalive interval is 10 sec , set
  Carrier delay is 2 sec
  RXload is 1 ,Txload is 1
  Queueing strategy: FIFO
    Output queue 0/0, 0 drops;
    Input queue 0/75, 0 drops
  Switchport attributes:
    interface's description:""
    medium-type is copper
    lastchange time:0 Day: 0 Hour: 0 Minute:13 Second
    Priority is 0
    admin duplex mode is AUTO, oper duplex is Unknown
    admin speed is AUTO, oper speed is Unknown
    flow receive control admin status is OFF,flow send control admin status is
OFF,flow receive control oper status is Unknown,flow send control oper status is
Unknown
broadcast Storm Control is OFF,multicast Storm Control is OFF,unicast Storm Control
is OFF
Port-type: access
Vlan id : 2
  5 minutes input rate 0 bits/sec, 0 packets/sec
  5 minutes output rate 0 bits/sec, 0 packets/sec
    0 packets input, 0 bytes, 0 no buffer, 0 dropped
    Received 0 broadcasts, 0 runts, 0 giants
    0 input errors, 0 CRC, 0 frame, 0 overrun, 0 abort
    0 packets output, 0 bytes, 0 underruns , 0 dropped
0 output errors, 0 collisions, 0 interface resets
```

The following example displays the layer-2 interface information when the Gi0/1 is a Hybrid port.

```
SwitchA#show interfaces gigabitEthernet 0/1
Index(dec):1 (hex):1
GigabitEthernet 0/1 is DOWN  , line protocol is DOWN
Hardware is Broadcom 5464 GigabitEthernet
Interface address is: no ip address
  MTU 1500 bytes, BW 1000000 Kbit
  Encapsulation protocol is Bridge, loopback not set
  Keepalive interval is 10 sec , set
  Carrier delay is 2 sec
  RXload is 1 ,Txload is 1
  Queueing strategy: FIFO
    Output queue 0/0, 0 drops;
    Input queue 0/75, 0 drops
  Switchport attributes:
    interface's description:""
    medium-type is copper
    lastchange time:0 Day: 0 Hour: 0 Minute:13 Second
    Priority is 0
    admin duplex mode is AUTO, oper duplex is Unknown
    admin speed is AUTO, oper speed is Unknown
    flow receive control admin status is OFF,flow send control admin status is
OFF,flow receive control oper status is Unknown,flow send control oper status is
Unknown
broadcast Storm Control is OFF,multicast Storm Control is OFF,unicast Storm Control
is OFF
Port-type: hybrid
Tagged vlan id:2
Untagged vlan id:none
  5 minutes input rate 0 bits/sec, 0 packets/sec
  5 minutes output rate 0 bits/sec, 0 packets/sec
    0 packets input, 0 bytes, 0 no buffer, 0 dropped
    Received 0 broadcasts, 0 runts, 0 giants
    0 input errors, 0 CRC, 0 frame, 0 overrun, 0 abort
    0 packets output, 0 bytes, 0 underruns , 0 dropped
0 output errors, 0 collisions, 0 interface resets
```

The following example displays the layer-2 information of the Gi0/1.

```
Ruijie# show interfacesgigabitEthernet 0/1 switchport
Interface Switchport ModeAccess Native Protected VLAN lists
--------- ---------- --------- ------ ------ ---------
GigabitEthernet 0/1 enabled Access 11  Disabled  ALL
```

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

1.22 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

1.23 show interfaces link-state-change statistics

Use this command to display the link state change statistics, including the time and count.

show interfaces [*interface-type interface-number*] **link-state-change statistics**

Parameter Description

Parameter	Description
interface-type interface-number	The interface type and ID.

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide If you do not specify an interface, the link state statistics of all interfaces are displayed.

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

```
Ruijie# show interfaces GigabitEthernet 0/1 link-state-change statistics
Interface    Link state    Link state change times     Last change time
-----------  ---------     ----------------------
-------------------
Gi 0/1       down          100                         2012-12-24
15:00:00
```

Interface	Description
Link state	Current link state.
Link state change times	The count of link state change.
Last change time	The time when the last link state change occurs.

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

1.24 show interfaces status

Use this command to display interface status information.

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

Parameter Description

Parameter	Description
interface-type interface-number	The interface type and ID.
status	Displays interface status information, including speed and duplex.

Defaults N/A

Command Mode Privileged EXEC mode

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

Configuration Examples The following example displays the status information of interface GigabitEthernet 0/1.

```
Ruijie#show interfaces GigabitEthernet 0/1 status
Interface            Status      Vlan    Duplex  Speed   Type
-------------------  ----------  ------  ------  ------  ------
GigabitEthernet 0/1    up          1       Full    1000M   copper
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

1.25 show interfaces status err-disable

Use this command to display the interface violation status.

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

Parameter Description

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

Defaults

Command Mode Any CLI mode

Usage Guide If you do not specify an interface, violation status of all interfaces is displayed.

Configuration Examples The following example displays the violation status of interface GigabitEthernet 0/1.

```
Ruijie#show interface gigabitEthernet 0/1 status err-disabled
Interface                    Status         Reason
-------------------------------- ---------------- ----------------
GigabitEthernet 0/1           err-disabled    BPDU Guard
```

The violation status is displayed as **err-disabled**.

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

1.26 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    Average Usage     Output Usage
Input Usage
-------------------------- ------------ ------------------
----------------- -----------------
GigabitEthernet 0/0        1000 Mbit    0.002822759%      0.001183280%
0.004462237%
```

Bandwidth refers to the interface link bandwidth, the maximum speed of link. Average Usage refers to the current usage.

Related Commands

Command	Description
N/A	N/A

Platform 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-learning

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

mac-address-learning

no mac-address-learning

default mac-address-learning

Parameter Description

Parameter	Description
N/A	N/A

Defaults The address learning function is enabled.

Command Mode Interface configuration mode.

Usage Guide MAC address learning cannot be disabled on the port where the security function is enabled. The security function cannot be configured on the port where address learning is disabled.

Configuration Examples The following example disables the port address learning function.

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

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

2.3 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 Description

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

Defaults The default is 300.

Command Mode Global configuration mode.

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

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

Command	Description

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

Platform Description N/A

2.4 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

2.5 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

2.6 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

2.7 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

2.8 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

2.9 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

2.10 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

2.11 show mac-address-table dynamic

Use this command to display the dynamic MAC address.

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

Parameter Description

Parameter	Description
mac-addr	Destination MAC address of the entry

vlan-id	VLAN of the entry, in the range from 1 to 4094.
interface-id	Interface that the packet is forwarded to. It may be a physical port or an aggregate port

Defaults

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

2.12 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

2.13 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

2.14 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 information.

```
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

2.15 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

2.16 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

2.17 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 Aggregate Port Commands

3.1 aggregateport load-balance

Use this command to configure a global load-balance algorithm for aggregate ports or a load-balance algorithm for an aggregate port . Use the **no** form of this command to return the default setting.

aggregateport load-balance { **dst-mac** | **src-mac** | **src-dst-mac** | **dst-ip** | **src-ip** | **src-dst ip** | s **src-dst-ip-l4port** | **src- l4port** | **dst-l4port** | **src-dst-l4port** | **src-ip-src-l4port** | **src-ip-dst-l4port** | **dst-ip-src-l4port** | **dst-ip-dst-l4port** | **src-ip-src-dst-l4port** | **dst-ip-src-dst-l4port** | **src-dst-ip-src-l4port** | **src-dst-ip-dst-l4port }**

no aggregateport load-balance

Parameter Description

Parameter	Description
dst-mac	Load balance based on the destination MAC addresses of the incoming packets. For all the links of an aggregate port, the messages with the same destination MAC addresses are sent to the same port, and those with different destination MAC addresses are sent to different ports.
src-mac	Load balance based on the source MAC addresses of the incoming packets. For all the links of an aggregate port, the messages from different addresses are distributed to different ports, and those from the same addresses are distributed to the same port.
src-dst-ip	Load balance based on the source IP address and destination IP address. Packets with different source and destination IP address pairs are forwarded through different ports. The packets with the same source and destination IP address pairs are forwarded through the same links. At layer 3, this load balancing style is recommended.
dst-ip	Load balance based on the destination IP addresses of the incoming packets. For all the links of an aggregate port, the messages with the same destination IP addresses are sent to the same port, and those with different destination IP addresses are sent to different ports.
src-ip	Load balance based on the source IP addresses of the incoming packets. For all the links of an aggregate port, the messages from different addresses are distributed to different ports, and those from the same addresses are distributed to the same port.
src-dst-mac	Load balance based on the source and destination MAC addresses. Packets with different source and destination MAC address pairs are forwarded through different ports. The packets with the same source and destination MAC address pairs are forwarded through the same port.
src-dst-ip-l4port	Load balance based on the source IP address, destination IP address, L4 source port number and L4 destination port number.
src- l4port	Load balance based on the L4 source port number.
dst- l4port	Load balance based on the L4 destination port number.

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

Defaults The default load balance mode is **src-dst-mac** for the L2 AP port and **src-dst-ip** for the L3 AP port .

Command Mode Global configuration mode/Interface configuration mode

Usage Guide You can run aggregateport load-balance in interface configuration mode of an AP port on devices that support load balancing configuration on a specific AP port. The configuration in interface configuration mode prevails. To disable the load balancing algorithm, run no aggregateport load-balance in interface configuration mode of the AP port. After that, the load balancing algorithm configured in global configuration mode takes effect.

Configuration Examples The following example configures a load-balance algorithm globally based on the destination MAC address.

```
Ruijie(config)# aggregateport load-balance dst-mac
```

Related Commands

Command	Description
show aggregateport load-balance	Displays aggregate port configuration.

Platform Description N/A

3.2 aggregateport member linktrap

Use this command to send LinkTrap to aggregate port members. Use the **no** form of this command to restore the default setting.

aggregateport member linktrap
no aggregateport member linktrap

Parameter Description

Parameter	Description
N/A	N/A

Defaults This function is disabled by default.

Command Mode Global configuration mode

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

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

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

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

3.3 ap-interface wireport port-group

Use this command to configure member ports of the AP port via an access controller. Use the **no** form of this command to restore the default setting.
ap-interface wireport *port-number* **port-group** *ap-number*
no ap-interface wireport *port-number* **port-group**

Parameter Description

Parameter	Description
port-number	Wired port ofan access point
ap-number	AP port

Defaults This function is disabled by default.

Command Mode AP configuration mode/ AP group configuration mode

Usage Guide You can configure this command on an access controller to add a wired port of an access point to an AP port. If this port is a member port of another AP port, the configuration does not take effect.

Configuration Examples The following example adds port GigabitEthernet 0/1 of the access point to AggregatePort 1.

```
Ruijie(config)#
Ruijie(config)#ap-config 00d8.aabb.cc02
You are going to config AP(00d8.aabb.cc02), which is online now.
Ruijie(config-ap)#ap-interface wireport 1 port-group 1
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

3.4 interfaces aggregateport

Use this command to create the aggregate port or enter interface configuration mode of the aggregate port. Use the **no** form of this command to restore the default setting.

interfaces aggregateport *ap-number*

no interfaces aggregateport *ap-number*

Parameter Description

Parameter	Description
ap-number	Aggregate port number.

Defaults The aggregate port is not created by default.

Command Mode Global configuration mode

Usage Guide If the aggregate port is created, this command is used to enter the interface configuration mode. Otherwise, this command is used to create the aggregate port and then enter its interface configuration mode.

Configuration Examples The following example creates AP 5 and enters its interface configuration mode.

```
Ruijie# configure terminal
Ruijie(config)# interfaces aggregateport 5
Ruijie(config-if-Aggregateport 5)# end
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

3.5 port-group

Use this command to assign a physical interface to be a member port of a static aggregate port or an LACP aggregate port. Use the **no** form of this command to restore the default setting.

port-group *port-group-number*

port-group *key-number* **mode** { **active** | **passive** }

no port-group

Parameter Description

Parameter	Description
port-group-number	Member group ID of an aggregate port, the interface number of the aggregate port.
key-number	Member group ID of an LACP aggregate port, the interface number of the LACP aggregate port.
active	Places a port into an active negotiating state, in which the port initiates negotiations with remote ports by sending LACP packets.
passive	Places a port into a passive negotiating state, in which the port responds to LACP packets it receives but does not initiate LACP negotiation.

Defaults By default, the physical port does not belong to any aggregate port.

Command Mode Interface configuration mode.

Usage Guide All the members of an aggregate port belong to a VLAN or configured to be trunk ports. The ports belonging to different native VLANs cannot form an aggregate port.

Configuration Examples The following example specifies the Ethernet interface 1/3 as a member of the static AP 3.

```
Ruijie(config)# interface gigabitethernet 1/3
Ruijie(config-if-GigabitEthernet 1/3)# port-group 3
```

The following example specifies the Ethernet interface 2/3 as a member of the LACP AP4 and set the aggregation mode to active.

```
Ruijie(config)# interface gigabitethernet 2/3
Ruijie(config-if-GigabitEthernet 2/3)# port-group 4 mode active
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

3.6 show aggregateport

Use this command to display the aggregate port configuration.

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

Parameter Description

Parameter	Description
aggregate-port-number	Number of the aggregate port.
load-balance	Displays the load-balance algorithm on the aggregate port.
summary	Displays the summary of the aggregate port.

Defaults N/A

Command Mode Any mode

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

Configuration Examples The following example displays the aggregate port configuration.

```
Ruijie# show aggregateport 1 summary
AggregatePort  MaxPorts        SwitchPort Mode                    Ports
-------------  --------------- ---------- ------  ----------------------------
------------------------
Ag1            8               Enabled    ACCESS                   Gi0/2
```

Related Commands

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

Platform Description N/A

4 VLAN Commands

4.1 add

Use this command to add one or a group Access interface into current VLAN. Use the **no** or **default** form of the command to remove the Access interface.

add interface { *interface-id* | **range** *interface-range* }

no add interface { *interface-id* | **range** *interface-range* }

default add interface { *interface-id* | **range** *interface-range* }

Parameter Description

Parameter	Description
interface-id	Layer-2 Ethernet interface or layer-2 AP port.
range *interface-range*	Range of the Layer-2 Ethernet interface or layer-2 AP port.

Defaults All layer-2 Ethernet interfaces are in the VLAN1.

Command mode VLAN configuration mode.

Usage Guide This command is only valid for the access port.

The configuration of this command is the same as specifying the VLAN to which interface belongs in the interface configuration mode (that is the **switchport access vlan** *vlan-id* command). For the two commands of adding the interface to the VLAN, the command configured later will overwrite the one configured before and take effect.

The configuration of adding the layer-2 AP into current VLAN through this command will only take effect for the layer-2 AP port, but not for the member port of the layer-2 AP port.

Configuration Examples The following example adds the interface GigabitEthernet 0/10 to VLAN20.

```
Ruijie# configure terminal
SwitchA(config)#vlan 20
SwitchA(config-vlan)#add interface GigabitEthernet 0/10
Ruijie# show interface GigabitEthernet 0/10 switchport
Interface  Switchport   Mode  Access  Native Protected  VLAN lists
----------  --------      -----  -----  ---- ---------- -------
GigabitEthernet 0/10 enabled  ACCESS  20   1   Disabled  ALL
```

The following example adds the interface range GigabitEthernet 0/1-10 to VLAN200.

```
Ruijie# configure terminal
SwitchA(config)#vlan 200
SwitchA(config-vlan)#add interface range GigabitEthernet 0/1-10
Ruijie# show vlan
```

```
SwitchA#show vlan
VLAN Name        Status                    Ports
---- -------    ------------    ----------------------------
1 VLAN0001    STATIC   Gi0/11,Gi0/12,Gi0/13,Gi0/14,Gi0/15,
Gi0/16,Gi0/17,Gi0/18,Gi0/19,Gi0/20,Gi0/21, Gi0/22, Gi0/23, Gi0/24
200 VLAN0200 STATIC  Gi0/1,Gi0/2,Gi0/3,Gi0/4,Gi0/5,
Gi0/6,Gi0/7,Gi0/8,Gi0/9,Gi0/10
```

The following example adds the AggregatePort10 to VLAN20.

```
Ruijie# configure terminal
SwitchA(config)#vlan 20
SwitchA(config-vlan)#add interface aggregateport 10
Ruijie# show interface aggregateport 10 switchport
Interface  Switchport   Mode  Access  Native Protected  VLAN lists
----------  --------      -----  -----  ---- ---------- -------
AggregatePort 10 enabled  ACCESS  20   1   Disabled  ALL
```

Related Commands

Command	Description
show interface *interface-id* **switchport**	Displays the layer-2 interfaces.

Platform Description N/A

4.2 name

Use this command to specify the name of a VLAN. Use the **no** or **default** form of this command to restore the default setting.

name *vlan-name*

no name

default name

Parameter Description

Parameter	Description
vlan-name	VLAN name

Defaults The default name of a VLAN is the combination of “VLAN” and VLAN ID, for example, the default name of the VLAN 2 is “VLAN0002”.

Command mode VLAN configuration Mode.

Usage Guide N/A

Configuration Examples 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

4.3 show vlan

Use this command to display member ports of the VLAN.

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

Parameter Description

Parameter	Description
vlan-id	VLAN ID

Defaults N/A

Command mode All modes

Usage Guide 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
```

Related Commands

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

Platform Description N/A

4.4 switchport access

Use this command to configure an interface as a static access port and assign it to a VLAN. Use the **no** or **default** form of the command to assign the port to the default VLAN.

switchport access vlan *vlan-id*

no switchport access vlan

default switchport access vlan

Parameter Description

Parameter	Description
vlan-id	The VLAN ID at which the port to be added.

Defaults By default, the switch port is an access port and the VLAN is VLAN 1.

Command mode Interface configuration mode.

Usage Guide Enter one VLAN ID. The system will create a new one and add the interface to the VLAN if you enter a new VLAN ID. If the VLAN ID already exists, the command adds the port to the VLAN.
If the port is a trunk port, the operation does not take effect.

Configuration Examples

```
Ruijie(config)# interface gigabitethernet 1/1
Ruijie(config-if)# switchport access vlan 2
```

Related Commands

Command	Description
switchport mode	Specifies the interface as Layer 2 mode (switch port mode).
switchport trunk	Specifies a native VLAN and the allowed-VLAN list for the trunkport.

Platform Description N/A

4.5 switchport mode

Use this command to specify a L2 interface (switch port) mode. You can specify this interface to be an access port or a trunk port or a servicechain port. Use the **no** or **default** form of this command to restore the default setting.

switchport mode { **access** | **trunk** | **hybrid** | **uplink**}

no switchport mode

default switchport mode

Parameter Description

Parameter	Description
access	Configures the switch port as an access port.
trunk	Configures the switch port as a trunk port.
hybrid	Configures the switch port as a hybrid port.
uplink	Configures the switch port as an uplink port.

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

Command mode Interface configuration mode.

Usage Guide If a switch port is an access port, the port can be added only to one VLAN. You can run the **switchport access vlan** command to specify the VLAN to which the port belongs.
If a switch port is a trunk port, the port is added to all VLANs by default. You can also run the **switchport trunk allowed** command to add the port to or remove the port from a specified VLAN.
If a switch port is an uplink port, the port is added to all VLANs by default. Different from the trunk port, the uplink port sends packets with a tag carried, that is, the tag of packets from default VLANs will not be deleted. You can run the **switchport trunk allowed** command to add the port to or remove the port from a specified VLAN.
If a switch port is a hybrid port, the port is added to all VLANs by default. Different from a trunk port, a hybrid port can be added to a VLAN in tag or untag mode by running the **switchport hybrid allowed** command.

Configuration Examples The following example configures port 1 as an access port.

```
Ruijie(config)#int g 0/1
Ruijie(config-if-GigabitEthernet 0/1)#switchport mode access
```

The following example configures port 1 as a trunk port.

```
Ruijie(config)#int g 0/1
Ruijie(config-if-GigabitEthernet 0/1)# switchport mode trunk
```

The following example configures port 1 as an uplink port.

```
Ruijie(config)#int g 0/1
Ruijie(config-if-GigabitEthernet 0/1)# switchport mode uplink
```

The following example configures port 1 as a hybrid port.

```
Ruijie(config)#int g 0/1
Ruijie(config-if-GigabitEthernet 0/1)# switchport mode hybrid
```

Related Commands

Command	Description
switchport access	Configures an interface as a statics access port and assigns it to a VLAN.

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

Platform Description N/A

4.6 switchport hybrid allowed

Use this command to add the port to the VLAN or remove the port from the VLAN, Use the **no** or **default** form of this command to restore the default setting.

switchport hybrid allowed vlan { { [**add** | **only**] **tagged** *vlist* | [**add**] **untagged** *vlist* } | **remove** *vlist* }

no switchport hybrid allowed vlan

default switchport hybrid allowed vlan

Parameter Description

Parameter	Description
add	Adds the port to the VLAN.
only	Adds the port to the VLAN and removes the port from the VLANs not on the VLAN list.
tagged	Adds the port to the VLAN and the VLAN packets going out on the port are tagged with VLAN ID.
untagged	Adds the port to the VLAN and the VLAN packets going out on the port are not tagged with VLAN ID.
remove	Removes the port from the VLAN.
vlist	Specifies the VLAN.

Defaults By default, the hybrid port is in all VLANs. All VLAN packets (except native VLAN packets) going out on the port are tagged with VLAN ID. Native VLAN packets are not tagged with VLAN ID.

Command mode Interface configuration mode

Usage Guide N/A

Configuration Examples The following example adds the hybrid port to VLAN 20 and VLAN 30 and the VLAN packets going out on the port are not tagged with VLAN ID.

```
Ruijie(config)# interface gigabitEthernet 0/1
Ruijie(config-if-GigabitEthernet 0/1)# switchport mode hybrid
Ruijie(config-if-GigabitEthernet 0/1)#switchport hybrid allowed vlan untagged
20
Ruijie(config-if-GigabitEthernet 0/1)#switchport hybrid allowed vlan add
untagged 30
```

The following example adds the hybrid port to VLAN 40 and VLAN 50 and the VLAN packets going out on the port are tagged with VLAN ID,

```
Ruijie(config)# interface gigabitEthernet 0/1
Ruijie(config-if-GigabitEthernet 0/1)#switchport mode hybrid
Ruijie(config-if-GigabitEthernet 0/1)#switchport hybrid allowed vlan tagged
40
Ruijie(config-if-GigabitEthernet 0/1)#switchport hybrid allowed vlan tagged
50
```

The following example removes the hybrid port from VLAN 20.

```
Ruijie(config)# interface gigabitEthernet 0/1
Ruijie(config-if-GigabitEthernet 0/1)#switchport mode hybrid
Ruijie(config-if-GigabitEthernet 0/1)#switchport hybrid allowed
vlan remove 20
```

The following example adds the hybrid port to VLAN 20 and deletes all the other VLANs. The VLAN packets going out on the port are tagged with VLAN ID.

```
Ruijie(config)# interface gigabitEthernet 0/1
Ruijie(config-if-GigabitEthernet 0/1)#switchport mode hybrid
Ruijie(config-if-GigabitEthernet 0/1)#switchport hybrid allowed
vlan only tagged 20
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

4.7 switchport hybrid native

Use this command to configure the native VLAN for the hybrid port. Use the **no** or **default** form of this command to restore the default setting.

switchport hybrid native vlan *vlan-id*

no switchport hybrid native vlan

default switchport hybrid native vlan

Parameter Description

Parameter	Description
vlan-id	Configures the native VLAN for the hybrid port.

Defaults The default is VLAN 1.

Command Interface configuration mode

mode

Usage Guide Native VLAN packets going out on the hybrid port are not tagged with VLAN ID. Packets not tagged with VLAN ID coming in on the hybrid port are taken as native VLAN packets.

Configuration Examples The following example configures VLAN 20 as the native VLAN for hybrid port GigabitEthernet 0/1.

```
Ruijie(config-if-GigabitEthernet 0/1)#interface gigabitEthernet 0/1
Ruijie(config-if-GigabitEthernet 0/1)#switchport mode hybrid
Ruijie(config-if-GigabitEthernet 0/1)#switchport hybrid native vlan 20
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

4.8 switchport trunk allowed vlan

Use this command to add the trunk/uplink port to the VLAN or remove a trunk/uplink port from the VLAN. Use the **no** or **default** form of the command to restore the default setting.

switchport trunk allowed vlan { **all** | { **add** *vlan-list* | **remove** *vlan-list* | **except** *vlan-list* | **only** *vlan-list* } }

no switchport trunk allowed vlan

default switchport trunk allowed vlan

Parameter Description

Parameter	Description
all	Adds the trunk/uplink port to all VLANs.
add	Adds the trunk/uplink port to the VLAN.
remove	Removes the trunk/uplink port from the VLAN port.
except	Removes the trunk/uplink port from the VLAN and adds the port to all the other VLANs.
only	Adds the trunk/uplink port to the specified VLAN and removes the port from the VLANs not on the VLAN list.
vlan-list	Specifies the VLAN.

Defaults The trunk/unlink port is in all VLANs by default.

Command mode Interface configuration mode.

Usage Guide A trunk/uplink port transmits all VLAN (1-4094) data by default. You can block some VLAN data by configuring this command. Use the **show interfaces** command to display configuration.

Configuration Examples The following example removes trunk port GigabitEthernet 0/10 from VLAN 2.

```
Ruijie(config)# interface gigabitEthernet 0/10
Ruijie(config-if-GigabitEthernet 0/10)# switchport mode trunk
Ruijie(config-if-GigabitEthernet 0/10)# switchport trunk allowed vlan remove
2
```

The following example removes trunk port GigabitEthernet 0/10 from VLAN 2.

```
Ruijie(config)# interface gigabitEthernet 0/10
Ruijie(config-if-GigabitEthernet 0/10)# switchport trunk allowed vlan except
10
```

The following example removes uplink port GigabitEthernet 0/10 from VLAN 10.

```
Ruijie(config)# interface gigabitEthernet 0/10
Ruijie(config-if-GigabitEthernet 0/10)# switchport mode uplink
Ruijie(config-if-GigabitEthernet 0/10)# switchport trunk allowed vlan remove
10
```

The following example adds uplink port GigabitEthernet 0/10 to all VLANs except VLAN10.

```
Ruijie(config)# interface gigabitEthernet 0/10
Ruijie(config-if-GigabitEthernet 0/10)# switchport trunk allowed
vlan except 10
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

4.9 switchport trunk native vlan

Use this command to configure the native VLAN for the trunk/uplink port. Use the **no** or **default** form of this command to restore the default setting.

switchport trunk native vlan *vlan-id*
no switchport trunk native vlan
default switchport trunk native vlan

Parameter Description

Parameter	Description
vlan-id	Native VLAN ID.

Defaults By default, the native VLAN for the trunk/uplink port is VLAN 1.

Command mode Interface configuration mode

Usage Guide After this function is enabled, packets not tagged with VLAN ID are taken as native VLAN packets. Tags are removed from native VLAN packets going out on the trunk port.

Configuration Examples The following example configures VLAN 10 as the native VLAN for trunk port GigabitEthernet 0/10.

```
Ruijie(config)#interface gigabitEthernet 0/10
Ruijie(config-if-GigabitEthernet 0/10)# switchport mode trunk
Ruijie(config-if-GigabitEthernet 0/10)# switch trunk native vlan 10
```

The following example configures VLAN 10 as the native VLAN for unlink port GigabitEthernet 0/10.

```
Ruijie(config)#interface gigabitEthernet 0/10
Ruijie(config-if-GigabitEthernet 0/10)# switchport mode uplink
Ruijie(config-if-GigabitEthernet 0/10)# switch trunk native vlan 10
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

4.10 vlan

Use this command to enter the VLAN configuration mode. Use the **no** or **default** form of this command to restore the default setting.

vlan { *vlan-id* | **range** *vlan-range* }

no vlan { *vlan-id* | **range** *vlan-range* }

default vlan { *vlan-id* | **range** *vlan-range* }

Parameter Description

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

Defaults The default is static VLAN.

Command mode Global configuration mode.

Usage Guide 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

5 Super-VLAN Commands

5.1 proxy-arp

Use this command to enable the proxy ARP function for a VLAN. Use the **no** form of this command to disable this function. Use the **default** form of this command torestore the default setting.

proxy-arp

no proxy-arp

default proxy-arp

Parameter Description

Parameter	Description
N/A	N/A

Defaults This function is enabled by default.

Command mode VLAN configuration Mode.

Usage Guide Super VLAN and sub VLAN must be both enabled with proxy ARP.

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

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

The following example disables the proxy ARP function for VLAN 3.

```
Ruijie(config)# vlan 3
Ruijie(config-vlan)# no proxy-arp
```

Related Commands

Command	Description
show supervlan	Displays the super VLAN information.

Platform Description N/A

5.2 show supervlan

Use this command to display the configuration of the super VLAN and its sub VLANs.

show supervlan

show supervlan id *vlan-id*

Parameter Description

Parameter	Description
vlan-id	VLAN ID

Defaults N/A

Command mode Any mode

Usage Guide N/A

Configuration Examples The following example displays the configuration of super VLAN 2.

```
SwitchA(config-if-range)# show supervlan 2
supervlan id  supervlan arp-proxy  subvlan id  subvlan arp-proxy  subvlan ip
range
------------  -------------------  ----------  -----------------  ---------
          2         ON          10            ON         192.168.196.10 -
192.168.196.50
                              20            ON         192.168.196.60 -
192.168.196.100
                              30            ON         192.168.196.110 -
192.168.196.150
```

The following example displays the configuration of all super VLANs.

```
SwitchA(config-if-range)# show supervlan
supervlan id  supervlan arp-proxy  subvlan id  subvlan arp-proxy  subvlan ip
range
------------  -------------------  ----------  -----------------  ---------
          2         ON          10            ON         192.168.196.10 -
192.168.196.50
                              20            ON         192.168.196.60 -
192.168.196.100
                              30            ON         192.168.196.110 -
192.168.196.150
          6         ON          7             ON
                              8             ON
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

5.3 subvlan

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

subvlan *vlan-id-list*

no subvlan [*vlan-id-list*]

default subvlan [*vlan-id-list*]

Parameter Description

Parameter	Description
vlan-id-list	Sub VLAN ID of the VLAN. Multiple VLANs are supported.

Defaults No super VLAN is set by default.

Command mode VLAN configuration Mode.

Usage Guide Use the **no subvlan** command to delete all sub VLANs of this super VLAN.

Configuration Examples The following example sets the sub VLAN.

```
SwitchA(config)#vlan 2
SwitchA(config-vlan)#supervlan
SwitchA(config-vlan)#subvlan 10,20,30
```

Related Commands

Command	Description
show supervlan	Displays the super VLAN information.

Platform Description N/A

5.4 subvlan-address-range

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

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

no subvlan-address-range

default subvlan-address-range

Parameter Description

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

Defaults No IP address range is set by default.

Command mode VLAN configuration Mode.

Usage Guide N/A

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

```
Ruijie(config)# vlan 2
Ruijie(config-vlan)#subvlan-address-range 192.168.23.1 192.168.23.5
```

Related Commands

Command	Description
show supervlan	Displays the super VLAN information.

Platform Description N/A

5.5 supervlan

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

supervlan

no supervlan

default supervlan

Parameter Description

Parameter	Description
N/A	N/A

Defaults No super VLAN is set by default.

Command mode VLAN configuration Mode.

Usage Guide By default, the super VLAN function is disabled.

No physical port can be added to a super VLAN.

Once a VLAN is not a super VLAN, all its sub VLANs become common static VLANs.

Configuration Examples The following example configures a Sub VLAN.

```
Ruijie(config)# vlan 2
Ruijie(config-vlan)#supervlan
```

Related Commands

Command	Description
show supervlan	Displays the super VLAN information.

Platform Description N/A

6 MSTP Commands

6.1 bpdu src-mac-check

Use this command to enable the BPDU source MAC address check function on the interface. Use the **no** form of this command to restore the default setting.

bpdu src-mac-check *H.H.H*

no bpdu src-mac-check

Parameter Description

Parameter	Description
H.H.H	Indicates that only the BPDU messages from this MAC address are received.

Defaults This function is disabled by default.

Command Mode Interface configuration mode.

Usage Guide BPDU source MAC address check prevents BPDU packets from maliciously attacking switches and causing MSTP abnormal. When the switch connected to a port on a point-to-point link is determined, you can enable BPDU source MAC address check to receive BPDU packets sent only by the peer switch and discard all other BPDU packets, thereby preventing malicious attacks. You can enable the BPDU source MAC address check in interface configuration mode for a specific port. One port can only filter one MAC address.

Configuration Examples The following example indicates only the BPDU with 00d0.f800.1e2f as the source MAC address will be received by interface Gi 1/1 .

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

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

6.2 bridge-frame forwarding protocol bpdu

Use this command to enable BPDU transparent transmission. Use the **no** form of this command to restore the default setting.

bridge-frame forwarding protocol bpdu
no bridge-frame forwarding protocol bpdu

Parameter Description

Parameter	Description
N/A	N/A

Defaults This function is disabled by default.

Command Mode Global configuration mode

Usage Guide In the IEEE 802.1Q standard, 01-80-C2-00-00-00, the destination MAC address of BPDU frames, is reserved. Devices following the IEEE 802.1Q standard don't forward BPDU frames. In real network deployment, devices may be required to support BPDU transparent transmission. For example, when a device is not enabled with STP, BPDU transparent transmission can help implement STP calculation.
BPDU transparent transmission works only when STP is disabled.

Configuration Examples The following example enables BPDU transparent transmission.

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

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

6.3 clear spanning-tree counters

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

Parameter Description

Parameter	Description
interface-id	ID of the interface

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide It is used to clear the statistics of the sent and received STP packets.

Configuration Examples The following example clears the statistics of the sent and received STP packets.

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

The following example clears the statistics of the sent and received packets on interface Gi 0/1.

```
Ruijie# clear spanning-tree counters interface gigabitethernet 0/1
```

Related Commands

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

Platform Description N/A

6.4 clear spanning-tree detected-protocols

Use this command to force the interface to send the RSTP BPDU message and check the BPDU messages.

clear spanning-tree detected-protocols [**interface** *interface-id*]

Parameter Description

Parameter	Description
interface-id	ID of the interface

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide Use this command to force the interface to send the RSTP BPDU message.

Configuration Examples Forces to check the version of all interfaces.

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

Related Commands

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

	interface.

Platform Description N/A

6.5 clear spanning-tree mst topochange record

Use this command to clear STP topology change record.

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

Parameter Description

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

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide N/A

Configuration Examples The following example clears STP topology change record.

```
Ruijie# show spanning-tree mst 0 topochange record
Topology change information on mst 0:
 Time              Interface          Old status   New status   Type
 ------------------ ------------------- ------------ ------------
----------------
 2013.5.1 4:18:46   GI0/6              Learning    Forwarding   Normal
Ruijie# clear spanning-tree mst 0 topochange record
Ruijie# show spanning-tree mst 0 topochange record
%There's no topology change information has been record on mst 0.
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

6.6 show spanning-tree

Use this command to display the global spanning-tree configuration.

show spanning-tree [summary | forward-time | hello-time | max-age | inconsistentports|

tx-hold-count | pathcost method | max_hops | counters]

Parameter Description

Parameter	Description
summary	Displays the information of MSTP instances and forwarding status of the interfaces.
inconsistentports	Displays the block port due to root guard or loop guard.
forward-time	Displays BridgeForwardDelay.
hello-time	Displays BridgeHelloTime.
max-age	Displays BridgeMaxAge.
max-hops	Displays the maximum hops of an instance.
tx-hold-count	Displays TxHoldCount.
pathcost method	Displays the method used for calculating path cost.
counters	Displays the statistics of STP transceived packets.

Defaults N/A

Command Mode Privileged EXEC mode, global configuration mode and interface configuration mode.

Usage Guide N/A

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

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

The following example displays the sent and received STP packets.

```
Ruijie# show spanning-tree counters
---------------------- STP BPDU count ----------------------
 Port                            Receive      Send
 GigabitEthernet 0/3             0            122594

------------------------- STP TC or TCN count -------------------------
 MSTID      Port                            Receive      Send
 0          GigabitEthernet 0/3             0            0
```

Related Commands

Command	Description
spanning-tree pathcost method	Sets the pathcost method.
spanning-tree forward-time	Sets BridgeForwardDelay.
spanning-tree hello-time	Sets BridgeHelloTime.
spanning-tree max-age	Sets BridgeMaxAge.
spanning-tree max-hops	Sets the maximum hops of an instance.
spanning-tree tx-hold-count	Displays TxHoldCount.

Platform Description N/A

6.7 show spanning-tree interface

Use this command to display the STP configuration of the interface, including the optional spanning tree.

show spanning-tree interface *interface-id* [{ **bpdufilter** | **portfast** | **bpduguard** | **link-type** }]

Parameter Description

Parameter	Description
interface-id	Interface ID
bpdufilter	Displays the status of BPDU filter.
portfast	Displays the status of portfast.
bpduguard	Displays the status of BPDU guard.
link-type	Displays the link type of an interface.

Defaults N/A

Command Mode Privileged EXEC mode, global configuration mode and interface configuration mode.

Usage Guide N/A

Configuration Examples The following example displays the STP configuration on interface Gi 0/1.

```
Ruijie# show spanning-tree int gi 0/1

PortAdminPortFast : Disabled
PortOperPortFast : Disabled
PortAdminAutoEdge : Enabled
PortOperAutoEdge : Disabled
PortAdminLinkType : auto
PortOperLinkType : point-to-point
PortBPDUGuard : Disabled
PortBPDUFilter : Disabled
PortGuardmode  : None

###### MST 0 vlans mapped :ALL
PortState : forwarding
PortPriority : 128
PortDesignatedRoot : 32768.001a.a979.00ea
PortDesignatedCost : 0
PortDesignatedBridge :32768.001a.a979.00ea
PortDesignatedPortPriority : 128
```

```
PortDesignatedPort : 1
PortForwardTransitions : 1
PortAdminPathCost : 200000
PortOperPathCost : 200000
Inconsistent states : normal
PortRole : rootPort
```

Related Commands

Command	Description
spanning-tree bpdufilter	Enables the BPDU filter feature someone the interface.
spanning-tree portfast	Enables the portfast on the interface.
spanning-tree bpduguard	Enables the BPDU guard on the interface.
spanning-tree link-type	Sets the link type of the interface to point-to-point.

Platform Description N/A

6.8 show spanning-tree mst

Use this command to display the information of MST and instances.

show spanning-tree mst { **configuration** | *instance-id* [**interface** *interface-id*] }

Parameter Description

Parameter	Description
configuration	The MST configuration of the equipment.
instance-id	Instance number
interface-id	Interface number

Defaults

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

Usage Guide N/A

Configuration Examples The following example displays the information of MST and instances.

```
Ruijie# show spanning-tree mst configuration
Multi spanning tree protocol : Enable
Name    : test
Revision : 0
Instance  Vlans Mapped
-------- ---------------------------------------------
```

```
0       : 2-4094
1       : 1
```

Field Description

Field	Description
Multi spanning tree protocol	Enables MSTP protocol.
Name	Name of the MST region
Revision	Revision of the MST region
Instance Vlans Mapped	Mapping relation between the instance and VLAN

Related Commands

Command	Description
spanning-tree mst configuration	Configures the MST region.
spanning-tree mst cost	Displays the path cost of the instance.
spanning-tree mst max-hops	Displays the maximum hops of the instance.
spanning-tree mst priority	Displays the equipment priority of the instance.
spanning-tree mst port-priority	Displays the port priority of the instance.

Platform Description N/A

6.9 show spanning-tree mst topochange record

Use this command to display the STP topology change record.

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

Parameter Description

Parameter	Description
instance-id	Instance ID.

Defaults N/A

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

Usage Guide N/A

Configuration Examples The following example displays the STP topology change record of instance 0.

```
Ruijie# show spanning-tree mst 0 topochange record
Topology change information on mst 0:
 Time             Interface          Old status   New status   Type
 ------------------- -------------------- ------------ ------------
----------------
```

```
2013.5.1 4:18:46    GI0/6              Learning     Forwarding   Normal
```

Field	Description
Time	The time when the topology changes.
Interface	The interface whose topology changes.
Old status	Old STP status on the interface.
New status	New STP status on the interface.
Type	Topology change may be caused by the following causes: Normal: UP/DOWN state change on the interface, LoopGuard Block: Loop-inconsistence causes the interface to be blocked. RootGuard Block: Root-inconsistence causes the interface to be blocked. Inferior Block: Receiving inferior BPDU frames causes the interface to be blocked. LoopGuard Unblock: The interface returns to Forward status from loop-inconsistence. RootGuard Unblock: The interface returns to Forward status from root-inconsistence. Inferior Unblock-The interface returns to Forward status after not receiving inferior BPDU frames.

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

6.10 spanning-tree

Use this command to enable MSTP and configure its basic settings globally. The **no** form of the command disables the spanning-tree function. The **no** form of the command with parameters only restores the corresponding parameters to the default values, but does not disable the spanning-tree function.

spanning-tree [**forward-time** *seconds* | **hello-time** *seconds* | **max-age** *seconds*]

no spanning-tree [**forward-time** | **hello-time** | **max-age**]

Parameter Description

Parameter	Description
forward-time *seconds*	Interval at which the port status changes, in the range from 4 to 30 in

	the unit of seconds. The default is 15.
hello-time *seconds*	Interval at which the switch sends the BPDU message, in the range from 1 to 10 in the unit of seconds. The default is 2.
max-age *seconds*	Maximum aging time of the BPDU message, in the range from 6 to 40 in the unit of seconds. The default is 20.

Defaults This function is disabled by default.

Command Mode Global configuration mode.

Usage Guide The values of **forward-time, hello time** and **max-age** are interrelated. Modifying one of these three parameters will affect the others. There is a restricted relationship among the above three values.
2*(Hello Time+1.0snd) <= Max-Age Time <= 2*(Forward-Delay–1.0snd)
If the values do not according with the condition, the topology may be unstable.

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

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

The following example configures the BridgeForwardDelay.

```
Ruijie(config)# spanning-tree  forward-time 10
```

Related Commands

Command	Description
show spanning-tree	Displays the global STP configuration.
spanning-tree mst cost	Sets the PathCost of an STP interface.
spanning-tree tx-hold-count	Sets the global TxHoldCount of STP.

Platform Description N/A

6.11 spanning-tree autoedge

Use this command to enable Autoedge on the interface. Use the **disabled** form of this command to disable this function.
spanning-tree autoedge [**disabled**]

Parameter Description

Parameter	Description
disabled	Disabled Autoedge on the interface.

Defaults This function is enabled by default.

Command Interface configuration mode.

Mode

Usage Guide If the designated port of a device does not receive a BPDU from the downlink port within a specific period (3 seconds), the device regards a network device connected to the designated port, configures the port as an edge port, and switches the port directly into the forwarding state. The edge port will be automatically identified as a non-edge port after receiving a BPDU.
You can run the spanning-tree autoedge disabled command to disable Auto Edge.

Configuration Examples The following example disables Autoedge on the interface.

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

Related Commands

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

Platform Description N/A

6.12 spanning-tree bpdufilter

Use this command to enable BPDU filter on the interface. You can use the **enabled** or **disabled** option of the command to enable or disable the BPDU filter function on the interface.
spanning-tree bpdufilter [**enabled** | **disabled**]

Parameter Description

Parameter	Description
enabled	Enables BPDU filter on the interface.
disabled	Disables BPDU filter on the interface.

Defaults This function is disabled by default,

Command Mode Interface configuration mode.

Usage Guide If BPDU filter is enabled on a port, the port neither sends nor receives BPDUs.

Configuration Examples The following example enables BPDU filter on interface Gi 1/1.

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

Related Commands

Command	Description

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

Platform Description N/A

6.13 spanning-tree bpduguard

Use this command to enable the BPDU guard function on the interface. You can use the **enabled** or **disabled** option of the command to enable or disable the BPDU guard function on the interface.
spanning-tree bpduguard [**enabled** | **disabled**]

Parameter Description

Parameter	Description
enabled	Enables BPDU guard on the interface.
disabled	Disables BPDU guard on the interface.

Defaults This function is disabled by default.

Command Mode Interface configuration mode.

Usage Guide
1. If BPDU guard is enabled on a port, the port enters the error-disabled state after receiving a BPDU.
2. Run command **errdisable recovery** [**interval** *seconds*] to recover the interface in Error-disabled state.

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

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

Related Commands

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

Platform Description N/A

6.14 spanning-tree compatible enable

Use this command to send the message selectively carried with MSTI according to the interface attribute of current port to realize interconnection with other vendors. Use the **no** form of this command to restore the default setting.
spanning-tree compatible enable

no spanning-tree compatible enable

Parameter Description

Parameter	Description
N/A	N/A

Defaults This function is disabled by default. .

Command Mode Interface configuration mode.

Usage Guide If the compatibility mode is enabled on a port, this port will add different MSTI information into the to-be-sent BPDU based on the current port to realize interconnection between Ruijie devices and other SPs' devices.

Configuration Examples The following example enables the compatibility mode on interface Gi 0/1.

```
Ruijie(config)# interface gigabitethernet 0/1
Ruijie(config-if-interface-id-interface-id)#spanning-tree compatible enable
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

6.15 spanning-tree guard loop

Use this command to enable **loop guard** on the interface to prevent the root port or backup port from generating loop since they cannot receive bpdu. Use the **no** form of this command to disable **loop guard**.

spanning-tree guard loop

no spanning-tree guard loop

Parameter Description

Parameter	Description
N/A	N/A

Defaults This function is disabled by default.

Command Mode Interface configuration mode.

Usage Guide

1. Enabling loop guard on a root port or backup port will prevent possible loops caused by BPDU receipt failure.
2. The loop guard function and root guard function cannot be enabled at the same time.

Configuration Examples

The following example enables **loop guard** on interface Gi 0/1.

```
Ruijie(config)# interface gigabitethernet 0/1
Ruijie(config-if-interface-id)# spanning-tree guard loop
```

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

6.16 spanning-tree guard none

Use this command to disable **guard** on the interface. Use the **no** form of this command to enable this function

spanning-tree guard none

no spanning-tree guard none

Parameter Description

Parameter	Description
N/A	N/A

Defaults

This function is enabled by default.

Command Mode

Interface configuration mode.

Usage Guide

N/A

Configuration Examples

The following example disables **guard** on interface Gi 0/1.

```
Ruijie(config)# interface gigabitethernet 0/1
Ruijie(config-if-interface-id)# spanning-tree guard none
```

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

6.17 spanning-tree guard root

Use this command to enable **root guard** on the interface to prevent the change of current root bridge position because of error configuration and illegal packet attack. Use the **no** form of this command to restore the default setting.

spanning-tree guard root

no spanning-tree guard root

Parameter Description

Parameter	Description
N/A	N/A

Defaults This function is disabled by default.

Command Mode Interface configuration mode.

Usage Guide

1. If root guard is enabled, the current root bridge will not change due to incorrect configuration or illegal packet attacks.
2. The loop guard function and root guard function cannot be enabled at the same time.

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

```
Ruijie(config)# interface gigabitethernet 0/1
Ruijie(config-if-interface-id)# spanning-tree guard root
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

6.18 spanning-tree ignore tc

Use this command to enable the tc filtering on the interface. Use the **no** form of this command to restore the default setting. With tc filtering enabled, the TC packets received on the interface will not be processed.

spanning-tree ignore tc

no spanning-tree ignore tc

Parameter Description

Parameter	Description

N/A	N/A

Defaults This function is disabled by default.

Command Mode Interface configuration mode.

Usage Guide If TC filter is enabled on a port, the port does not process received TC packets.

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

```
Ruijie(config)# interface gigabitethernet 0/1
Ruijie(config-if-interface-id)# spanning-tree ignore tc
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

6.19 spanning-tree link-type

Use this command to configure the link type of the interface. Use the **no** form of this command to restore the default setting.

spanning-tree link-type [**point-to-point** | **shared**]

no spanning-tree link-type

Parameter Description

Parameter	Description
point-to-point	Sets the link type of the interface to point-to-point.
shared	Forcibly sets the link type of the interface to shared.

Defaults For a full-duplex interface, its link type is set to point-to-point link; for a half-duplex interface, its link type is set to shared.

Command Mode Interface configuration mode.

Usage Guide If the link type of a port is point-to-point connection, RSTP can rapidly converge. If the link type is not configured, the device automatically sets the link type based on the duplex mode of the port.

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

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

Related Commands

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

Platform Description N/A

6.20 spanning-tree loopguard default

Use this command to enable **loop guard** globally to prevent the root port or backup port from generating loop since they cannot receive bpdu. Use the **no** form of this command to restore the default setting.

spanning-tree loopguard default

no spanning-tree loopguard default

Parameter Description

Parameter	Description
N/A	N/A

Defaults This function is disabled by default.

Command Mode Global configuration mode.

Usage Guide Enabling loop guard on a root port or backup port will prevent possible loops caused by BPDU receipt failure.

Configuration Examples The following example enables **loop guard** globally to prevent the root port or backup port from generating loop since they cannot receive bpdu.

```
Ruijie(config)# spanning-tree loopguard default
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

6.21 spanning-tree max-hops

Use this command to set the maximum number of hops(Max-hopsCount) of the BPDU message in the global configuration mode, the number of hops in a region that the BPDU message passes before

being dropped. This parameter takes effect for all instances. Use the **no** form of this command to restore the default setting.

spanning-tree max-hops *hop-count*

no spanning-tree max-hops

Parameter Description

Parameter	Description
hop-count	Number of hops in a region that the BPDU message passes before being dropped. The range is 1 to 40 hops.

Defaults The default is 20 hops.

Command Mode Global configuration mode.

Usage Guide In the region, the BPDU message sent by the root bridge includes a Hot Count field. When the BPDU message passes a device, the Hop Count is decreased by 1 until it reaches 0, which indicates the BPDU message times out. The device will drop the BPDU message whose Hop Count is 0. Changing the max-hops command affects all instances.

Configuration Examples This example sets the max-hops of the spanning tree to 10 for all instances.

```
Ruijie(config)# spanning-tree  max-hops 10
```

Related Commands

Command	Description
show spanning-tree	Displays the MSTP information.

Platform Description N/A

6.22 spanning-tree mode

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

spanning-tree mode [**stp** | **rstp** | **mstp**]

no spanning-tree mode

Parameter Description

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

Defaults The default is **mstp**.

Command Mode Global configuration mode.

Usage Guide However, some vendors' devices do not work according to 802.1 protocol standards, possibly causing incompatibility. If other vendors' devices are incompatible with Ruijie devices, run this command to switch the STP mode to a lower version.

Configuration Examples The following example sets the STP version.

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

Related Commands

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

Platform Description N/A

6.23 spanning-tree mst configuration

Use this command to enter the MST configuration mode in the global configuration mode and configure the MSTP region. Use the **no** form of the command to restore the default setting.

spanning-tree mst configuration

no spanning-tree mst configuration

Parameter Description

Parameter	Description
N/A	N/A

Defaults

Command Mode Global configuration mode.

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

To return to the global configuration mode, enter exit.

After entering the MST configuration mode, you can configure MSTP Region parameters:

Configuration Examples This example enters the MST configuration mode.

```
Ruijie(config)# spanning-tree mst configuration
Ruijie(config-mst)# instance 1 vlan  3, 5-10
Ruijie(config-mst)# name region 1
```

```
Ruijie(config-mst)# revision  1
Ruijie(config-mst)# show spanning-tree mst configuration
Multi spanning tree protocol : Enable
Name    : region1
Revision : 1Instance  Vlans Mapped
----------  --------------------
0       1-2,4,11-4094
1       3,5-10
-----------------------------------
Ruijie(config-mst)# exit
Ruijie(config)#
```

Related Commands

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

Platform Description N/A

6.24 instance instance-id vlan vlan-range

Use this command to set instance and VLAN mapping relations. Use the **no** form of the command to restore the default setting.

instance *instance-id* **vlan** *vlan-range*

no instance *instance-id* { **vlan** *vlan-range* }

Parameter Description

Parameter	Description
instance-id	Instance ID, in the range from 0 to 64
vlan-range	VLAN range, in the range from 1 to 4094.

Defaults

The default is instance 0.

Command Mode MST configuration mode

Usage Guide **instance** *instance-id* **vlan** *vlan-range*：Add VLAN to MST instance. Instance-ID is in the range from 0 to 64 and VLAN is in the range from 1 to 4094. Use commas to separate VLAN IDs and use hyphen to indicate VLAN range, e.g., instance 10 vlan 2,3,6-9, which adds VLAN 2, 3, 4, 5, 6, 7, 8,

9 to instance 10. By default, all VLANs are in instance 0. Use the **no** form of this command to remove VLAN from instance 1-64.

If you create 64 instances by stacking on a Ruijie device with a small memory (e.g., 64M), the memory may be undersized. It is recommended to limit stacking instance number.

Configuration Examples

This example enters MST mode and maps VLAN 3 and 5-10 to MST instance1.

```
Ruijie(config)# spanning-tree mst configuration
Ruijie(config-mst)# instance 1 vlan 3, 5-10
Ruijie(config-mst)# show spanning-tree mst configuration
Multi spanning tree protocol : Enable
Name    :
Revision : 0
Instance  Vlans Mapped
----------  --------------------
0       1-2,4,11-4094
1       3,5-10
---------------------------------
Ruijie(config-mst)# exit
Ruijie(config)#
```

The following example removes VLAN3 from instance 1.

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

The following example removes instance 1.

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

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

6.25 revision

Use this command to set revision number of MSTP region. Use the **no** form of the command to restore the default setting.

revision *version*

no revision

Parameter Description

Parameter	Description
version	MST revision number, in the range from 0 to 65535.

Defaults

The default is 0.

Command Mode MST configuration mode

Usage Guide **revision** *version*: Sets the MST version, in the range from 0 to 65535.
show spanning-tree mst configuration: Displays MST region information.

Configuration Examples This example sets revision number to1.

```
Ruijie(config)# spanning-tree mst configuration
Ruijie(config-mst)# revision 1
Ruijie(config-mst)# show spanning-tree mst configuration
Multi spanning tree protocol : Enable
Name    :
Revision : 1
Instance  Vlans Mapped
-------- ---------------------------------------------
0       : ALL
Ruijie(config-mst)# exit
Ruijie(config)#
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

6.26 name

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

Parameter Description

Parameter	Description
name	MST name, up to 32 characters.

Defaults The default is NULL.

Command Mode MST configuration mode

Usage Guide **name** *name*: Sets the MST name, up to 32 characters.

show spanning-tree mst configuration: Displays MST region information.

Configuration Examples This example sets MST name to region1.

```
Ruijie(config)# spanning-tree mst configuration
Ruijie(config-mst)# name region1
Ruijie(config-mst)# show spanning-tree mst configuration
Multi spanning tree protocol : Enable
Name    : region1
Revision : 0
Instance  Vlans Mapped
-------- ---------------------------------------------
0       : ALL
Ruijie(config-mst)# exit
Ruijie(config)#
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

6.27 spanning-tree mst cost

Use this command to set the path cost of an instance in the interface configuration mode. Use the **no** form of the command to restore the default setting.

spanning-tree [**mst** *instance-id*] **cost** *cost*

no spanning-tree [**mst** *instance-id*] *cost*

Parameter Description

Parameter	Description
instance-id	Instance ID in the range from 0 to 64.
cost	Path cost in the range from 1 to 200,000,000.

Defaults The default instance-id is 0.

The default value is calculated by the link rate of the interface automatically.

1000 Mbps—20000

100 Mbps—200000

10 Mbps—2000000

Command Mode Interface configuration mode.

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

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

```
Ruijie(config)# interface gigabitethernet 1/1
Ruijie(config-if)# spanning-tree mst 3 cost 400
```

Related Commands

Command	Description
show spanning-tree mst	Displays the MSTP information of an interface.
spanning-tree mst port-priority	Configures the priority of an interface.
spanning-tree mst priority	Configures the priority of an instance.

Platform Description N/A

6.28 spanning-tree mst port-priority

Use this command to configure the interface priority for different instances in the interface configuration mode. It will determine which interface of a loop in a region is in charge of forwarding. Use the **no** form of this command to restore the default setting.

spanning-tree [**mst** *instance-id*] **port-priority** *priority*

no spanning-tree [**mst** *instance-id*] **port-priority**

Parameter Description

Parameter	Description
Instance-id	Instance ID, in the range of 0 to 64
priority	Interface priority. Sixteen integers are available: 0, 16, 32, 48, 64, 80, 96, 112, 128, 144, 160, 176, 192, 208, 224, 240, which are the multiples of 16.

Defaults The default instance-id is 0.
The default priority is 128.

Command Mode Interface configuration mode.

Usage Guide When a loop occurs in the region, the interface of the higher priority will be in charge of forwarding. If all interfaces have the same priority value, the interface of the smaller number will be in charge of the forwarding.
Run this command to determine which port in the loop of a region enters the forwarding state.

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

```
Ruijie(config)# interface gigabitethernet 1/1
Ruijie(config-if-interface-id)# spanning-tree mst 20 port-priority 0
```

Related Commands

Command	Description
show spanning-tree mst	Displays the MSTP information of an interface.
spanning-tree mst cost	Sets the path cost.
spanning-tree mst priority	Sets the device priority for different instances.

Platform Description N/A

6.29 spanning-tree mst priority

Use this command to set the device priority for different instances in the global configuration mode.
Use the **no** form of this command to restore the default setting.
spanning-tree [**mst** *instance-id*] **priority** *priority*
no spanning-tree [**mst** *instance-id*] **priority**

Parameter Description

Parameter	Description
instance-id	Instance ID, in the range of 0 to 64
priority	Device priority. Sixteen integers are available: 0, 4096, 8192, 12288, 16384, 20480, 24576, 28672, 32768, 36864, 40960, 45056, 49152,53248, 57344 and 61440, which are all multiples of 4096.

Defaults The default instance ID is 0.
The default device priority is 32768.

Command Mode Global configuration mode.

Usage Guide Configure the switch priority to determine a device as the root of the entire network and to determine the topology of the entire network.

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

```
Ruijie(config)# spanning-tree mst 20 priority 8192
```

Related Commands

Command	Description
show spanning-tree mst	Displays the MSTP information of an interface.
spanning-tree mst cost	Sets path cost.
spanning-tree mst port-priority	Sets the port priority of an instance.

Platform Description N/A

6.30 spanning-tree pathcost method

Use this command to configure the path cost of the port. Use the **no** form of this command to restore the default setting.

spanning-tree pathcost method { { **long** [**standard** } | **short** }

no spanning-tree pathcost method

Parameter Description

Parameter	Description
Long [**standard**]	Adopts the 802.1t standard to configure path cost. The standard indicates that use the expression recommended by the standard to calculate the cost value.
short	Adopts the 802.1d standard to configure path cost.

Defaults 802.1T standard is adopted to set path cost by default.

Command Mode Global configuration mode.

Usage Guide If the port path cost uses the default value, the device automatically calculates the port path cost based on the port rate.

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

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

Related Commands

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

Platform Description N/A

6.31 spanning-tree portfast

Use this command to enable the portfast on the interface. Use the disabled form of this command to restore the default setting,

spanning-tree portfast [**disabled**]

Parameter Description

Parameter	Description
disabled	Disables the portfast on the interface.

Defaults This function is disabled by default.

Command Mode Interface configuration mode.

Usage Guide After PortFast is enabled on a port, the port directly enters the forwarding state. However, since the Port Fast Operational State becomes disabled due to receipt of BPDUs, the port can properly run the STP algorithm and enter the forwarding state.

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

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

Related Commands

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

Platform Description N/A

6.32 spanning-tree portfast bpdufilter default

Use this command to enable the BPDU filter function globally. You can use the **no** form of the command to restore the default setting.
spanning-tree portfast bpdufilter default
no spanning-tree portfast bpdufilter default

Parameter Description

Parameter	Description
N/A	N/A

Defaults This function is disabled by default,

Command Mode Global configuration mode.

Usage Guide Once the BPDU filter is enabled, the BPDU message is neither received nor sent on the interface. Use the **show spanning-tree** command to display the configuration.

Configuration Examples The following example enables the BPDU filter function globally.

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

Related Commands

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

Platform Description N/A

6.33 spanning-tree portfast bpduguard default

Use this command to enable the BPDU guard globally. Use the **no** form of this command to restore the default setting,
spanning-tree portfast bpduguard default
no spanning-tree portfast bpduguard default

Parameter Description

Parameter	Description
N/A	N/A

Defaults This function is disabled by default.

Command Mode Global configuration mode.

Usage Guide Once the BPDU guard is enabled on the interface, it will enter the error-disabled status if the BPDU message arrives at the interface. Use the **show spanning-tree** command to display the configuration.


The global BPDU guard takes effect only when PortFast is enabled on a port.

Configuration Examples The following example enables the GPDU guard globally.

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

Related Commands

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

Platform Description N/A

6.34 spanning-tree portfast default

Use this command to enable the portfast feature on all interfaces globally. Use the **no** form of this command to restore the default setting.
spanning-tree portfast default
no spanning-tree portfast default

Parameter Description

Parameter	Description
N/A	N/A

Defaults This function is disabled by default.

Command Mode Global configuration mode.

Usage Guide N/A

Configuration Examples The following example enables the portfast feature on all interfaces globally.

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

Related Commands

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

Platform Description N/A

6.35 spanning-tree reset

Use this command to restore the **spanning-tree** configuration to the default setting.

spanning-tree reset

Parameter Description

Parameter	Description
N/A	N/A

Defaults N/A

Command Mode Global configuration mode.

Usage Guide The command do not have “**no**” command.

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

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

Related Commands

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

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

Platform Description N/A

6.36 spanning-tree tc-guard

Use this command to enable **tc-guard** on the interface to prevent the spread of TC messages. Use the **no** form of this command to disable this function on the interface.

spanning-tree tc-guard

no spanning-tree tc-guard

Parameter Description

Parameter	Description
N/A	N/A

Defaults This function is disabled by default.

Command Mode Global configuration mode.

Usage Guide Enable TC guard to prevent TC packets from spreading.

Configuration Examples The following example enables tc-guard on interface Gi 1/1.

```
Ruijie(config)# interface gigabitethernet 1/1
Ruijie(config-if-interface-id)# spanning-tree tc-guard
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

6.37 spanning-tree tc-protection

Use this command to enable **tc-protection** globally. Use The **no** form of this command to disable this function.

spanning-tree tc- protection

no spanning-tree tc- protection

Parameter Description

Parameter	Description

N/A	N/A

Defaults This function is disabled by default.

Command Mode Global configuration mode.

Usage Guide N/A

Configuration Examples The following example enables **tc-protection** globally.

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

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

6.38 spanning-tree tc-protection tc-guard

Use this command to enable tc-guard to prevent TC packets from being flooded. Use the **no** form of this command to restore the default setting.

spanning-tree tc-protection tc-guard

no spanning-tree tc-protection tc-guard

Parameter Description

Parameter	Description
N/A	N/A

Defaults This function is disabled by default.

Command Mode Global configuration mode.

Usage Guide Enable TC guard to prevent TC packets from spreading.

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

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

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

6.39 spanning-tree tx-hold-count

Use this command to configure the TxHoldCount of the STP, the maximum number of the BPDU messages sent in one second. Use the **no** form of this command to restore the default setting.

spanning-tree tx-hold-count *tx-hold-count*

no spanning-tree tx-hold-count

Parameter Description

Parameter	Description
tx-hold-count	Indicates the maximum number of BPDUs sent per second. The value ranges from 1 to 10. The default value is 3.

Defaults The default is 3.

Command Mode Global configuration mode.

Usage Guide N/A

Configuration Examples The following example sets the maximum number of the BPDU messages sent in one second.

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

Related Commands

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

Platform Description N/A

7 MAC VLAN Commands

7.1 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

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   00
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

8 VLAN Group Commands

8.1 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

8.2 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

8.3 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

8.4 vlan-list

Use this command to configure the VLAN list for a VLAN group on an AC device.

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

8.5 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 N/A

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

8.6 show vlan-group

Use this command to display the VLAN group configuration on an AP or AC device.
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 or AC device:

```
Ruijie# show vlan-group
VLAN-Group ID   Default VLAN  Assign-Mode       VLAN-List
---------  ------------  -----------------  ------------------------------
100           10          dhcp-server-state  1-10, 21-30, 51-70
128           NA          dot1x               110-130, 141-150
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

9 PPP Commands

9.1 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

9.2 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

9.3 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

9.4 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

9.5 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

9.6 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

9.7 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

9.8 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

9.9 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

9.10 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

10 PPPOE-CLIENT Commands

10.1 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

10.2 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

10.3 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

10.4 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

10.5 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

10.6 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.

10.7 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

10.8 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

10.9 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

10.10 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

10.11 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 interfaces only.

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

10.12 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

10.13 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

10.14 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

11 RLDP Commands

rldp detect-interval

Use this command to configure the interval at which the RLDP sends the detection message on the port. Use the **no** form of this command to restore the default value.

rldp detect-interval *interval*

no rldp detect-interval

Parameter Description

Parameter	Description
interval	Detection interval in the range 2 to 15 seconds

Defaults 3 seconds.

Command Mode Global configuration mode.

Usage Guide In the environment where STP is enabled, it is recommended that the product of interval multiplying the maximum number of detections is less than the topology convergence time of STP.

Configuration Examples The following example shows how to set the detection interval as 5s:

```
Ruijie(config)# rldp detect-interval 5
```

Related Commands

Command	Description
rldp detect-max	Sets the maximum number of detections.

Platform Description N/A.

rldp detect-max

Use this command to set the maximum number of sending detection packets on the port. If the neighboring port does not respond when this detection number is exceeded, the link is considered faulty. Use the **no** form of this command to restore it to the default value.

rldp detect-max *num*

no rldp detect-max

Parameter Description

Parameter	Description
num	Maximum number of detections in the range 2 to 10

Defaults 2.

Command Mode Global configuration mode.

Usage Guide Maximum detection time = (detection intervals * maximum number of detections) +1

Configuration Examples The following example shows how to set the maximum number of detections as 5:

```
Ruijie(config)# rldp detect-max 5
```

Related Commands

Command	Description
rldp detect-interval	Sets the detection interval.

Platform Description N/A.

rldp enable

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

rldp enable

no rldp enable

Parameter Description

Parameter	Description
N/A.	N/A.

Defaults Disabled.

Command Mode Global configuration mode.

Usage Guide You can enable RLDP on the interface only when the global RLDP is enabled.

Configuration Examples The following example shows how to enable RLDP:

```
Ruijie(config)# rldp enable
```

Related Commands

Command	Description
rldp port	Enables the RLDP function on the port.

Platform Description N/A.

rldp neighbor-negotiation

Use this command to enable RLDP neighbor negotiation. Use the **no** form or **default** form of this command to restore the default setting.

rldp neighbor-negotiation

no rldp neighbor-negotiation

default rldp neighbor-negotiation

Parameter Description

Parameter	Description
N/A.	N/A.

Defaults RLDP neighbor negotiation is disabled by default.

Command Mode Global configuration mode.

Usage Guide With neighbor negotiation enabled, RLDP unidirectional-/bidirectional-link detection starts only after the neighbor negotiation is successful. (Receiving the Prob message from the neighbor indicates the neighbor negotiation is successful.)

Configuration Examples The following example shows how to enable RLDP neighbor negotiation:

```
Ruijie#config
Ruijie(config)#rldp neighbor-negotiation
```

Related Commands

Command	Description
rldp port	Enables the RLDP function on the port.

Platform N/A.

Description

rldp port

Use this command to enable RLDP on the port and specify detection type and troubleshooting method. Use the **no** form of this command to disable the function.

rldp port { **unidirection-detect | bidirection-detect | loop-detect** } **shutdown-port**

no rldp port { **unidirection-detect | bidirection-detect | loop-detect** }

Parameter Description

Parameter	Description
unidirection-detect	Sets unidirectional link detection.
bidirection-detect	Sets bidirectional link detection.
loop-detect	Sets loop detection type.
shutdown-port	Shutdowns the port.

Defaults N/A

Command Mode Interface configuration mode.

Usage Guide The configuration takes effect on switch port, routed port, member ports of L2AP/L3AP, but does not take effect on L2AP/L3AP.

Configuration Examples The following example shows how to configure the troubleshooting method as shutdown-port.

```
Ruijie(config)# interface GigabitEthernet 2/0/9
Ruijie(config-if-GigabitEthernet 2/0/9)# rldp port loop-detect shutdown-port
```

Related Commands

Command	Description
rldp enable	Enables RLDP globally.

Platform Description N/A.

rldp reset

Use this command to make all the ports that have been handled using rldp shutdown or disable to perform RLDP detection again.

rldp reset

Parameter Description

Parameter	Description
N/A.	N/A.

Defaults N/A.

Command Mode Privileged EXEC mode.

Usage Guide N/A.

Configuration Examples The example below demonstrates how to use this command:

```
Ruijie# rldp reset
```

Related Commands

Command	Description
rldp enable	Enables RLDP globally.

Platform Description N/A.

show rldp

Use this command to display the RLDP information.

show rldp [**interface** *interface-id*]

Parameter Description

Parameter	Description
interface-id	Interface ID

Defaults N/A.

Command Mode Privileged EXEC mode.

Usage Guide N/A.

Configuration Examples The following example shows RLDP information:

```
Ruijie#show rldp
```

```
rldp state         : disable
rldp hello interval: 3
rldp max hello     : 2
rldp local bridge  : 00d0.f822.37da
-----------------------------------
GigabitEthernet 0/1
port state      : normal
neighbor bridge : 0000.0000.0000
neighbor port   :
unidirection detect information:
     action: shutdown-port
     state : normal
bidirection detect information:
     action: shutdown-port
     state : normal
loop detect information:
     action: shutdown-port
     state : normal
```

The following example shows the configuration information of all monitoring points on the interface GigabitEthernet 0/1:

```
Ruijie#show rldp interface GigabitEthernet 0/1
port state      : normal
local bridge    : 00d0.f822.37da
neighbor bridge : 00d0.f823.37db
neighbor port   : GigabitEthernet 0/1
unidirection detect information:
     action: shutdown-port
     state : normal
bidirection detect information:
     action: shutdown-port
     state : normal
loop detect information:
     action: shutdown-port
     state : normal
```

Related Commands

Command	Description
N/A.	N/A.

Platform N/A.

Description

12 LLDP Commands

12.1 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

12.2 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

12.3 clear lldp table

Use this command to clear LLDP neighbor information.

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

Parameter Description

Parameter	Description
interface-name	Interface name

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide If the **interface** parameter is specified, the LLDP neighbor information on the specified interface is cleared.

If the **interface** parameter is not specified, the LLDP neighbor information on all interfaces is cleared.

Configuration Examples The following example clears the LLDP neighbor information on interface 1.

```
Ruijie# show lldp neighbors interface GigabitEthernet 0/1
Lldp statistics information of port [GigabitEthernet 0/1]
------------------------------------------------------------
The number of lldp frames transmitted  : 0
The number of frames discarded   : 0
The number of error frames    : 0
The number of lldp frames received   : 0
The number of TLVs discarded   : 0
The number of TLVs unrecognized   : 0
The number of neighbor information aged out : 0
Ruijie# clear lldp table interface GigabitEthernet 0/1
Ruijie# show lldp neighbors interface GigabitEthernet 0/1
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

12.4 device-type

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

device-type *device-type*

no device-type

Parameter Description

Parameter	Description
device-type	Device type. The value ranges from 0 to 2. 0: The device type is DHCP Server. 1: The device type is switch. 2: The device type is LLDP MED terminal.

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

12.5 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 N/A

Description

12.6 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

12.7 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

12.8 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 value is 3.

Command Global configuration mode.

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

12.9 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 value is 4.

Command Mode Global configuration mode.

Usage Guide The value of Time To Live (TLV) in LLDP packet = TTL multiplier × LLDP packet transmit interval + 1. Therefore, the TTL of local device information on the neighbor device can be controlled by adjusting TTL multiplier.

Configuration Examples The following example sets TTL multiplier to 5.

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

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

Platform Description N/A

12.10 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 Description N/A

12.11 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

12.12 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

12.13 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

12.14 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

12.15 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

12.16 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

12.17 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 Global configuration mode.

Mode

Usage Guide To prevent LLDP from being initialized too frequently due to the frequent operating mode change, you can configure port initialization delay.

Configuration 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

12.18 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

12.19 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 1 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

12.20 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

network-policy	Network Policy TLV
profile-num	ID of network policy
power-over-ethernet	Extended Power-via-MDI TLV

Defaults By default, all TLVs other than Location Identification TLV can be advertised on the interface for products other than S12000. For the S12000 product series, only basic TLVs and IEEE 802.1 TLVs are advertised. To advertise IEEE 802.3 TLVs and LLDP-MED TLVs, run the **lldp tlv-enable** command.

Command Mode Interface configuration mode

Usage Guide During configuration of basic management TLVs, IEEE 802.1 TLVs, and IEEE 802.3 TLVs, if the **all** parameter is specified, all optional TLVs of the types are advertised.
During configuration of LLDP-MED TLVs, if the **all** parameter is specified, all LLDP-MED TLVs except Location Identification TLVs are advertised.
When configuring LLDP-MED Capability TLVs, configure LLDP-MED MAC/PHY TLVs first. When canceling LLDP-MED MAC/PHY TLVs, cancel LLDP-MED Capability TLVs first.
When configuring LLDP-MED TLVs, configure LLDP-MED Capability TLVs first so that LLDP-MED TLVs of other types can be configured.
To cancel LLDP-MED TLVs, cancel LLDP-MED TLVs of other types first so that LLDP-MED Capability TLVs can be canceled.

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

```
Ruijie# configure terminal
Ruijie(config)#interface gigabitethernet 0/1
Ruijie(config-if-GigabitEthernet 0/1)#lldp tlv-enable dot1-tlv all
```

The following example applies LLDP network policy 1 on the 0/1 interface.

```
Ruijie#config
Ruijie(config)#interface gigabitethernet 0/1
Ruijie(config-if-GigabitEthernet 0/1)#lldp tlv-enable med-tlv network-policy
   profile 1
```

The following example applies the LLDP Civic Address (ID: 1) configuration on the 0/1 interface.

```
Ruijie#config
Ruijie(config)#interface gigabitethernet 0/1
Ruijie(config-if-GigabitEthernet 0/1)#lldp tlv-enable med-tlv location
   civic-location identifier 1
```

The following example applies the emergency number (ID: 1) on the 0/1 interface.

```
Ruijie#config
Ruijie(config)#interface gigabitethernet 0/1
Ruijie(config-if-GigabitEthernet 0/1)#lldp location elin identifier 1
```

Related Commands	Command	Description
	show lldp tlv-config interface	Displays the attributes of advertisable TLVs

Platform Description N/A

12.21 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. Network connectivity device Class I: normal terminal device Class II: media terminal device; besides Class I capabilities, it also supports media streams. Class III: communication terminal device; it supports all the capabilities of Class I and Class II and IP communication.
HardwareRev	Hardware version
FirmwareRev	Firmware version
SoftwareRev	Software version
SerialNum	Serial number
Manufacturer name	Device manufacturer
Asset tracking identifier	Asset tracking ID
Port ID type	Port ID type
Port ID	Port ID
Port description	Port description
Management address subtype	Management address type

Management address	Management address
Interface numbering subtype	Type of the interface identified by the management address
Interface number	ID of the interface identified by the management address
Object identifier	ID of the object identified by the management address
Port VLAN ID	Port VLAN ID
Port and protocol VLAN ID	Port and Protocol VLAN ID
PPVID Supported	Indicates whether port and protocol VLAN is supported
PPVID Enabled	Indicates whether port and protocol VLAN is enabled
VLAN name of VLAN 1	Name of VLAN 1
Protocol Identity	Protocol identifier
Auto-negotiation supported	Indicates whether auto-negotiation is supported
Auto-negotiation enabled	Indicates whether auto-negotiation is enabled
PMD auto-negotiation advertised	Auto-negotiation advertising capability of the port
Operational MAU type	Speed and duplex state of the port
PoE support	Indicates whether POE is supported
Link aggregation supported	Indicates whether link aggregation is supported
Link aggregation enabled	Indicates whether link aggregation is enabled
Aggregation port ID	ID of the link aggregation port
Maximum frame Size	Maximum frame size supported by the port
Power-via-MDI device type	Device type, including: PSE (power sourcing equipment) PD (powered device)
Power-via-MDI power source	Power source type
Power-via-MDI power priority	Power supply priority
Power-via-MDI power value	Available power on port
Model name	Name of model

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

12.22 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

Parameter	Description

Description

civic-location	Encapsulates a common address of a network device.
elin	Encapsulates an emergency number.
identifier	Displays one address or emergency number configured.
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-location static
Elin location information
--------------------------
Identifier : t
Elin  : iiiiiiiiii
Ports     : Gi1/0/3
--------------------------
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

12.23 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 Network connectivity device: Class I: general terminal device Class II: media terminal device, including capabilities of Class I and supporting media stream Class III: communication terminal device, including capabilities of Class I and Class II and supporting IP communication
HardwareRev	Hardware version
FirmwareRev	Firmware version
SoftwareRev	Software version
SerialNum	Serial number
Manufacturer name	Manufacturer name
Asset tracking identifier	Asset ID
Port ID type	Port ID type
Port ID	Port ID
Port description	Port description
Port VLAN ID	VLAN ID of a port
Port and protocol VLAN ID	Port and protocol VLAN ID
PPVID Supported	Whether port and protocol VLAN is supported
PPVID Enabled	Whether port and protocol VLAN is enabled
VLAN name of VLAN 1	VLAN 1 name
Protocol Identity	Protocol ID
Auto-negotiation supported	Whether auto-negotiation is supported
Auto-negotiation enabled	Whether auto-negotiation is enabled
PMD auto-negotiation advertised	Port auto-negotiation advertisement capability
Operational MAU type	Rate and duplex status of port auto-negotiation
PoE support	Whether POE is supported
Link aggregation supported	Whether link aggregation is supported
Link aggregation enabled	Whether link aggregation is enabled
Aggregation port ID	ID of link aggregation port
Maximum frame Size	Maximum frame length supported by a port
Power-via-MDI device type	Device type, including: ● PSE ● PD
Power-via-MDI power source	Power type
Power-via-MDI power priority	Power supply priority
Power-via-MDI power value	Power value of a port where power is supplied

Related Commands	Command	Description
	N/A	N/A

Platform Description N/A

12.24 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	Interface name

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 information:
-------------------------
Network Policy Profile 1
   voice vlan 2 cos 4 dscp 6
   voice-signaling vlan 2000 cos 4 dscp 6
```

Related Commands	Command	Description
	N/A	N/A

Platform Description N/A

12.25 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

12.26 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

12.27 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 Mode Privileged EXEC mode

Usage Guide **Interface** parameter: display the LLDP TLV configuration of the specified interface.

Configuration Examples The following example displays TLV information of port 1.

```
Ruijie# show lldp tlv-config interface GigabitEthernet 0/1
LLDP tlv-config of port [GigabitEthernet 0/1]
-----------------------------------------------------
   NAME    STATUS DEFAULT
-------------------------------- ------ -----------
Basic optional TLV:
Port Description TLV   YES YES
System Name TLV    YES YES
System Description TLV   YES YES
System Capabilities TLV   YES YES
Management Address TLV   YES YES

IEEE 802.1 extend TLV:
Port VLAN ID TLV    YES YES
Port And Protocol VLAN ID TLV  YES YES
```

```
VLAN Name TLV     YES YES

IEEE 802.3 extend TLV:
MAC-Physic TLV    YES YES
Power via MDI TLV    YES YES
Link Aggregation TLV   YES YES
Maximum Frame Size TLV   YES YES

LLDP-MED extend TLV:
Capabilities TLV    YES YES
Network Policy TLV   YES YES
Location Identification TLV  NO  NO
Extended Power via MDI TLV  YES YES
Inventory TLV     YES YES
```

Related Commands	Command	Description
	N/A	N/A

Platform Description N/A

12.28 { 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.

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

13 DLDP Commands

13.1 clear dldp

Use this command to clear statistics about the times that DLDP is down or up at a specified monitoring point for renewing statistics.

clear dldp [**interface** *interface-name* [*ip-address*]]

Parameter Description

Parameter	Description
interface-name	Name of an Layer 3 interface
ip-address	IP address of a peer device

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide DLDP records statistics about the times that DLDP is down or up. You can use this command to clear statistics about the times that DLDP is down or up at a specified monitoring point and renew statistics. If an L3 interface or a device IP address is specified, statistics about the times that DLDP is down or up on the interface at one or all monitoring points will be cleared. If no L3 interface or IP address is specified, statistics about the times that DLDP is down or up at all monitoring points on all interfaces will be cleared.

Configuration Examples The following example clears statistics about the times that DLDP is down or up at all monitoring points on all interfaces.

```
Ruijie#clear dldp
```

The following example clears statistics about the times that DLDP is down or up at all monitoring points on the interface *vlan 1*.

```
Ruijie#clear dldp interface vlan 1
```

The following example clears statistics about the times that DLDP is down or up about the peer device 10.83.132.1 on the interface *vlan 1*.

```
Ruijie# clear dldp interface vlan 1 10.83.132.1
```

Related Commands	Command	Description
	N/A	N/A

Platform Description N/A

13.2 dldp

Use this command to configure DLDP detection.

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

dldp *ip-address* [*next-hop-ip*] [**mac-address** mac-addr] [**interval** *tick* | **retry** *retry-num* | **resume** *resume-num*]

no dldp *ip-address*

Parameter Description	Parameter	Description
	ip-address	IP address of the peer device to be detected
	next-hop-ip	Next-hop IP address specified when the device to be detected belongs to another different network
	mac-address *mac-addr*	The bound MAC address. If a next hop exists, its MAC address is configured.
	interval *tick*	Detection interval. The value range is from 1 to 6,000 in the unit of ticks, where 1 tick is equal to 10 milliseconds. The value must be an integral multiple of five.
	retry *retry-num*	Number of retry times. The value range is from 1 to 3,600.
	resume *resume-num*	Number of recovery times of the link to the peer device to be detected, indicating the number of consecutive packets received before a down link turns up. The value range is from 1 to 200.

Defaults By default, the interval tick is 10 (100ms). The *retry-num* is 3, and the *resume-num* is 3.

Command Mode Interface configuration mode

Usage Guide You can use this command to enable DLDP detection to quickly detect Ethernet link faults.
DLDP detection detects multiple IP addresses on Layer 3 ports. If they respond no ICMP packets, they are considered down; if one of them recovers response, they are considered up.

Configuration Examples The following example enables DLDP detection for the device 10.83.132.10.

```
Ruijie(config)#int gi0/0
```

```
Ruijie(config-if-GigabitEthernet 0/0)#ip address 10.83.132.1 24

Ruijie(config-if-GigabitEthernet 0/0)#dldp 10.83.132.10

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

The following example enables DLDP detection for the device 10.83.132.10 in another different network segment.

```
Ruijie#config

Ruijie(config)# int gi0/0

Ruijie(config-if-GigabitEthernet 0/0)#ip address 10.83.132.1 255.255.255.0

Ruijie(config-if-GigabitEthernet 0/0)#dldp 10.83.131.10 10.83.132.2
```

The following example disables DLDP detection for the device 10.83.132.10.

```
Ruijie#config

Ruijie(config)# int gi0/0

Ruijie(config-if-GigabitEthernet 0/0)#no dldp 10.83.132.10
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

13.3 dldp passive

Use this command to set DLDP to the passive mode.

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

dldp passive

no dldp passive

Parameter Description

Parameter	Description
N/A	N/A

Defaults The default is the active mode.

Command Mode Interface configuration mode

Usage Guide

If DLDP is enabled on devices at both ends of a link on a network and ICMP Echo packets are sent to each other for link detection, excessive packets exist between the two devices. If only one device sends ICMP Echo packets to the peer device on which the same detection parameters are configured, the peer device can detect whether the packets arrive in time and whether the link between them is normal. This method saves bandwidth and CPU resources.
You can set DLDP to the active mode for one device to initiate ICMP Echo packets, and set DLDP to the passive mode for the other device to passively receive the packets.

Configuration Examples

The following example sets DLDP to the passive mode.

```
Ruijie#config

Ruijie(config)# int gi0/0

Ruijie(config-if-GigabitEthernet 0/0)#ip address 10.83.132.1 255.255.255.0
//Set an IP address for vlan1.

Ruijie(config-if-GigabitEthernet 0/0)#dldp passive
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

13.4 dldp interval

Use this command to set the DLDP detection interval.
Use the **no** form of this command to restore the default setting.
dldp interval *tick*
no dldp interval

Parameter Description

Parameter	Description
tick	Detection interval (in ticks), in the range from 5 to 6,000. The value must be a multiple of 5. (1tick = 10 milliseconds)

Defaults The default interval is 10 (100ms).

Command Mode Global configuration mode

Usage Guide This command is used to set the DLDP detection interval.
If a device does not receive the reply packets from the peer device within the specific period (the time of this period is equal to that of the *detection packet retransmission interval* multiplied by the *retry count*), the device takes the L3 port as DOWN (though the physical link is up). Once the device receives the reply packets from the peer device, the device takes the L3 port as UP.

Configuration Examples The following example sets the DLDP detection interval to 20 ticks.

```
Ruijie#config

Ruijie(config)#dldp interval 20
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

13.5 dldp retry

Use this command to set the DLDP retry count.
Use the **no** form of this command to restore the default setting.
dldp retry *retry-num*
no dldp retry

Parameter Description

Parameter	Description
retry-num	Retry count, in the range from 1 to 3,600

Defaults The default is 3.

Command Mode Global configuration mode

Usage Guide This command is used to set the DLDP retry count.

Configuration Examples The following example sets the DLDP retry count to 4.

```
Ruijie#config

Ruijie(config)#dldp retry 4
```

Related Commands	Command	Description
	N/A	N/A

Platform Description N/A

13.6 dldp resume

Use this command to set the DLDP recovery count.

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

dldp resume *resume-num*

no dldp resume

Parameter Description	Parameter	Description
	resume-num	Recovery count of the peer device link, in the range from 1 to 200. The parameter indicates the number of DLDP detection packets received consecutively from the peer device before the link status goes from DOWN to UP.

Defaults The default is 3.

Command Mode Global configuration mode

Usage Guide This command is used to set the DLDP recovery count.

Configuration Examples The following example sets the DLDP recovery count to 4.

```
Ruijie#config

Ruijie(config)#dldp resume 4
```

Related Commands	Command	Description
	N/A	N/A

Platform N/A

Description

13.7 show dldp

Use this command to display DLDP configuration information or statistics at various monitoring points.

show dldp [**interface** *interface-name*] [**statistic**]

Parameter Description

Parameter	Description
interface-name	Name of an L3 interface
statistic	Statistics

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide You can use this command with the keyword **statistics** to display statistics at all monitoring points on all interfaces or a specific Layer 3 interface. If a Layer 3 interface is specified, this command displays DLDP configuration and statistics at all monitoring points on the Layer 3 interface.

Configuration Examples The following example displays DLDP configuration information at all monitoring points on all interfaces.

```
Ruijie#show dldp

Interface  Type        Ip       Next-hop    Interval  Retry  Resume  State

---------  -------  -----------  -----------  --------  -----  ------
------

Gi0/0       Passive  192.168.6.3  192.168.2.2  10       5     3      Up

Gi0/1       Passive  192.168.7.3             10       5     3      Up

Gi0/2       Passive  192.168.3.3  192.168.4.2  10       5     3      Up
```

The following example displays DLDP configuration information at all monitoring points on the Layer 3 interface GigabitEthernet 0/0.

```
Ruijie#show dldp intface gigabitEthernet 0/0

Interface  Type        Ip       Next-hop    Interval  Retry  Resume  State

---------  -------  -----------  -----------  --------  -----  ------
```

```
------

Gi0/0       Passive  192.168.6.3  192.168.2.2  10       5     3      Up


The following example displays DLDP statistics at all monitoring points on all
interfaces.

Ruijie#show dldp statistic

Interface  Type        Ip      record-time  Up-count  Down-count

---------  -------  -----------  -----------  --------  ----------

Gi0/0      Passive  192.168.6.3  2h34m5s     10       9

Gi0/1       Passive  192.168.3.3  1d2h3m52s    10       9
```

The following example displays DLDP statistics at all monitoring points on the Layer 3 interface GigabitEthernet 0/0.

```
Ruijie#show dldp statistic interface gigabitEthernet 0/0

Interface  Type        Ip      record-time  Up-count  Down-count

---------  -------  -----------  -----------  --------  ----------

Gi0/0       Passive  192.168.6.3  2h34m5s     10       9
```

Field	Description
record-time	Time length for recording the number of times that DLDP is up or down. The time is displayed in *y***d**h**m**s format: y: year d: day h: hour m: minute s: second Using the *Up-count* and *Down-count* parameters, you can check statistics about the number of times that DLDP is up or down within this time length.
Up-count	Number of times that DLDP is up at the specific monitoring point
Down-count	Number times that DLDP is down at the specific monitoring point

Related Commands

Command	Description
N/A	N/A

Platform Description	N/A

IP Address & Application Commands

1. IP Address/Service Commands
2. ARP Commands
3. IPv6 Commands
4. DHCP Commands
5. DHCPv6 Commands
6. DNS Commands
7. FTP Server Commands
8. FTP Client Commands
9. Tunnel Commands
10. Network Connectivity Test Tool Commands
11. TCP Commands
12. IPv4/IPv6 REF Commands
13. TFTP Server Commands
14. NAT Commands
15. Proxy ARP Commands

1 IP Address/Service Commands

1.1 ap-interface bvi num ip address

Use this command to configure an IP address and network mask for the bridge virtual interface (BVI) of the specified AP. Use the **no** form of this command to restore the setting.

ap-interface bvi *num* **ip address** { *ip-address network-mask* | **dynamic** }

no ap-interface bvi *num* **ip address**

Parameter Description

Parameter	Description
num	Configures the BVI interface number.
ip-address	Configures an IP addresses for the BVI interface.
network-mask	Configures a network mask for the BVI interface.
dynamic	Obtains an IP address and mask for the BVI interface dynamically.

Defaults This function is disabled by default.

Command Mode ap-config mode/ap-group mode

Usage Guide This command can be configured in either **ap-config** or **ap-group** mode. The **ap-config** mode can be further divided into **ap-config** all and **ap-config apname** modes. The modes are sorted by priority from high to low as follows: ap-config apname， ap-group and ap-config all. In whatever mode, each BVI interface can be configured with only one IP address. The AC pushes configuration to APs based on priority.

If the **ap-interface bv*i*** *num* **ip address** *ip-address network-mask* command is configured, you need to separate APs into different VLANs to avoid address collision.

Configuration Examples The following example configures IP address 192.168.2.1and network mask 255.255.255.0 for BVI 2 in ap-config ap120 mode.

```
Ruijie(config)#ap-config ap120
You are going to config AP(ap120), which is online now.
Ruijie(config-ap)#ap-interface bvi 2 ip address 192.168.2.1 255.255.255.0
```

The following example configures IP address 192.168.3.1 and network mask 255.255.255.0 for BVI 3 in ap-group mode.

```
Ruijie(config)#ap-group default
Ruijie(config-group)#ap-interface bvi 3 ip address 192.168.3.1 255.255.255.0
```

The following example configures IP address192.168.4.1 and network mask 255.255.255.0 for BVI 4 in ap-config all mode.

```
Ruijie(config)#ap-config all
Ruijie(config-ap)#ap-interface bvi 4 ip address 192.168.4.1 255.255.255.0
```

The following example obtains an IP address and network mask for BVI 4 dynamically in ap-config

all mode.

```
Ruijie(config)#ap-config all
Ruijie(config-ap)#ap-interface bvi 4 ip address dynamic
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

1.2 ip-address

Use this command to configure the IP address of an interface. Use the **no** form of this command to restore the default setting.

ip address *ip-address network-mask* [**secondary**]

no ip address [*ip-address network-mask* [**secondary**]]

Parameter Description

Parameter	Description
ip-address	32-bit IP address, with 8 bits in one group in decimal format. Groups are separated by dots.
network-mask	32-bit network mask. 1 stands for the mask bit, 0 stands for the host bit, with 8 bits in one group in decimal format. Groups are separated by dots.

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

1.3 ip address negotiate

Use this command to configure an IP address for the interface through PPP negotiation. Use the **no** form of this command to restore the setting.
ip address negotiate
no ip address negotiate

Parameter Description

Parameter	Description
N/A	N/A

Defaults This function is disabled by default.

Command Mode Interface configuration mode

Usage Guide 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 The following example obtains an IP address for the interface through PPP negotiation.

Examples

```
Ruijie(config)# interface dialer 1
Ruijie(onfig-if-dialer 1)# ip address negotiate
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

1.4 ip 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

1.5 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

1.6 ip icmp error-interval

Use this command to set the rate to send the ICMP destination unreachable packets triggered by DF in the IP header. Use the **no** form of this command to restore the default setting.

ip icmp error-interval DF milliseconds [*bucket-size*]

no ip icmp error-interval DF *milliseconds* [*bucket-size*]

Use this command to set the rate to send other ICMP error packets. Use the **no** form of this command to restore the default setting.

ip icmp error-interval milliseconds [bucket-size]

no ip icmp error-interval *milliseconds* [*bucket-siz*]

Parameter Description

Parameter	Description
milliseconds	The refresh period of the token bucket, in the range from 0 to 2147483647 in the unit of milliseconds. 0 indicates no limit on the rate to send ICMP error packets. The default is 100.
bucket-size	The number of tokens in the bucket, in the range is from 1 to 200. The default is 10.

Defaults The default rate is 10 packets per 100 millisecond.

Command Mode Global configuration mode.

Usage Guide To prevent DoS attack, the token bucket algorithm is adopted to limit the rate to send ICMP error packets.
If IP packets need to be fragmented while the DF is set to 1, the device sends ICMP destination unreachable packets numbered 4 to the source IP address for path MTU discovery. Rate limits on ICMP destination unreachable packets and other error packets are needed to prevent path MTU discovery failure.
It is recommended to set the refresh period to an integral multiple of 10 milliseconds. If the refresh period is not an integral multiple of 10 milliseconds, it is adjusted automatically. For example, 1 per 5 milliseconds is adjusted to 2 per 10 milliseconds; 3 per 15 milliseconds is adjusted to 2 per 10 milliseconds.

Configuration Examples The following example sets the rate to send the ICMP destination unreachable packets triggered by DF in the IP header to 100 per second.

```
Ruijie(config)# ip icmp error-interval DF 1000 100
```

The following example sets the rate to send other ICMP error packets to 10 per second.

```
Ruijie(config)# ip icmp error-interval 1000 10
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

1.7 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 The following example disables the device to return a Timestamp Reply.

Examples

```
Ruijie(config)# no ip icmp timestamp
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

1.8 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

1.9 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

1.10 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

1.11 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

1.12 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

1.13 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

1.14 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

1.15 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: Request packet: Reply packet: Unknown packet:	Show the total number of ARP packets received on the interface, including: ARP request packet ARP reply packet Unknown packet
TTL invalid packet number:	Show the TTL invalid packet number
ICMP packet input number: Echo request: Echo reply: Unreachable: Source quench: Routing redirect:	Show the total number of ICMP packets received on the interface, including: Echo request packet Echo reply packet Unreachable packet Source quench packet Routing redirection packet
Outgoing access list is	Show whether an outgoing access list has been configured for an interface.
Inbound access list is	Show whether an incoming access list has been configured for an interface.

Related Commands

Command	Description
N/A.	N/A.

Platform Description N/A.

1.19 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 The following example displays the output of this command.

Examples

```
Ruijie# show ip packet statistics
Total
 Received 1000 packets, 1000000 bytes
 Unicast:1000,Multicast:0,Broadcast:0
 Discards:0
 HdrErrors:0(BadChecksum:0,TTLExceeded:0,Others:0)
 NoRoutes:0
 Others:0
 Sent 100 packets, 6000 bytes
 Unicast:50,Multicast:50,Broadcast:0

VLAN 1
 Received 1000 packets, 1000000 bytes
 Unicast:1000,Multicast:0,Broadcast:0
 Discards:0
 HdrErrors:0(BadChecksum:0,TTLExceeded:0,Others:0)
 NoRoutes:0
 Others:0
 Sent 100 packets, 6000 bytes
 Unicast:50,Multicast:50,Broadcast:0
```

Related Commands

Command	Description
ip default-gateway	Configures the default gateway, which is only supported on the Layer 2 switch.

Platform Description N/A

1.20 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 The following example displays all IP address ranges.

Examples

```
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 Description N/A

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: RAW: raw sockets DGRAM: datagram type STREAM: stream type.
Protocol	Protocol.
LocalIP:Port	Local IP address and port.
ForeignIP:Port	Peer IP address and port.
State	State. This field is for only TCP sockets.
Total	The total number of sockets.

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

1.23 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 trusted

Use this command to set the maximum number of trusted ARP entries. Use the **no** form of this command to restore the default setting.

arp trusted *number*

no arp trusted

Parameter Description

Parameter	Description
number	Maximum number of trusted ARP entries. This value ranges from 10 to ARP table capacity minus 1,024.

Defaults The default value is half of the ARP table capacity.

Command Mode Global configuration mode.

Usage Guide To make this command valid, enable the trusted ARP function firstly. The trusted ARP entries and other entries share the memory. Too much trusted ARP entries may lead to insufficient ARP entry space. In general, you should set the maximum number of trusted ARP entries according to your

real requirements.

Configuration Examples The following example sets 1000 trusted ARPs.

```
Ruijie(config)# arp trusted 1000
```

Related Commands

Command	Description
service trustedarp	Enables the trusted ARP function.

Platform Description N/A

2.9 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

2.10 arp trusted aging

Use this command to set trusted ARP aging. Use the **no** form of this command to restore the default setting.

arp trusted aging

no arp trusted aging

Parameter Description

Parameter	Description
N/A	N/A

Defaults This function is disabled by default.

Command Mode Global configuration mode.

Usage Guide Use this command to set trusted ARP aging. Aging time is the same as dynamic ARP aging time. Use the **arp timeout** command to set aging time in interface mode.

Configuration Examples N/A

Related Commands

Command	Description
service trustedarp	Enables trusted ARP function.

Platform Description N/A

2.11 arp trusted user-vlan

Use this command to execute the VLAN transformation while setting the trusted ARP entries. Use the **no** form of this command to restore the default setting.

arp trusted user-vlan *vid1* **translated-vlan** *vid2*

no arp trusted user-vlan *vid1* **translated-vlan** *vid2*

Parameter Description

Parameter	Description
vid1	VID set by the server.
vid2	VID after the transformation.

Defaults This function is disabled by default.

Command Mode Global configuration mode.

Usage Guide In order to validate this command, enable the trusted ARP function first. This command is needed only when the VLAN sent by the server is different from the VLAN which takes effect in the trusted ARP entry.

Configuration Examples The following example sets the VLAN sent by the server to 3, but the VLAN which takes effect in the trusted ARP entry to 5.

```
Ruijie(config)# arp trusted user-vlan 3 translated-vlan 5
```

Related Commands

Command	Description
service trustedarp	Enables the trusted ARP function.

Platform Description N/A

2.12 arp unresolve

Use this command to set the maximum number of the unresolved ARP entries. Use **no** form of this command to restore the default setting.

arp unresolve *number*

no arp unresolve

Parameter Description

Parameter	Description
number	The maximum number of the unresolved ARP entries in the range from 1 to the ARP table size supported by the device.

Defaults The default is the ARP table size supported by the device.

Command Mode Global configuration mode.

Usage Guide If there are a large number of unresolved entries in the ARP cache table and they do not disappear after a period of time, this command can be used to limit the quantity of the unresolved entries.

Configuration Examples The following example sets the maximum number of the unresolved items to 500.

```
Ruijie(config)# arp unresolve 500
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

2.13 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 [**trusted**] [*ip* [*mask*]] | **interface** *interface-name*]

Parameter Description

Parameter	Description
trusted	Deletes trusted ARP entries. Dynamic ARP entries are deleted by default.
ip	Deletes ARP entries of the specified IP address. If *trusted* value is specified, trusted ARP entries are deleted; otherwise, all dynamic ARP entries are deleted which is the default.
mask	Deletes ARP entries in a subnet mask. If *trusted* value is specified, trusted ARP entries in the subnet mask are deleted; otherwise, all dynamic ARP entries are deleted. The dynamic ARP entry specified by the IP address is deleted by default.
interface *interface-name*	Deletes dynamic ARP entries on the specified interface. Dynamic ARP entries are deleted on all interfaces by default.

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide 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

2.14 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

2.15 local-proxy-arp

Use this command to enable local proxy ARP on the SVI interface. Use the **no** form of this command to restore the default setting.

local-proxy-arp

no local-proxy-arp

Parameter Description

Parameter	Description
N/A	N/A

Defaults N/A

Command Interface configuration mode

Mode

Usage Guide With local proxy ARP enabled, the device helps a host to obtain MAC addresses of other hosts on the subnet. If the device enables switchport protected, users on different ports are segregated on layer 2. After local proxy ARP is enabled, the device serves as a proxy to send a response after receiving an ARP request. The ARP response contains a MAC address which is the device's Ethernet MAC address, realizing communication between different hosts through L3 routes.

Configuration Examples The following example enables local proxy ARP on VLAN1.

```
Ruijie(config)# interface vlan 1
Ruijie(config-if-VLAN 1)# local-proxy-arp
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

2.16 show arp

Use this command to display the Address Resolution Protocol (ARP) cache table

show arp [*interface-type interface-number* | **trusted** [*ip* [*mask*]] | [*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. If **trusted** is configured, only trusted ARP entries are displayed. Otherwise, untrusted ARP entries are displayed.
mask	Displays the ARP entries of the network segment included within the mask. If **trusted** is configured, only trusted ARP entries are displayed. Otherwise, untrusted ARP entries are displayed.
static	Displays all the static ARP entries.
complete	Displays all the resolved dynamic ARP entries.
incomplete	Displays all the unresolved dynamic ARP entries.
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

2.17 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

2.18 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

2.19 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

2.20 show ip arp

Use this command to display the Address Resolution Protocol (ARP) cache table.

show ip arp

Parameter Description

Parameter	Description
N/A	N/A

Defaults N/A.

Command Mode Privileged EXEC mode.

Usage Guide N/A.

Configuration Examples The following example displays the output of **show ip arp**:

```
Ruijie# show ip arp
Protocol Address Age(min)Hardware Type Interface
Internet 192.168.7.233 23 0007.e9d9.0488 ARPA FastEthernet 0/0
Internet 192.168.7.112 10 0050.eb08.6617 ARPA FastEthernet 0/0
Internet 192.168.7.79 12 00d0.f808.3d5c ARPA FastEthernet 0/0
Internet 192.168.7.1 50 00d0.f84e.1c7f ARPA FastEthernet 0/0
Internet 192.168.7.215 36 00d0.f80d.1090 ARPA FastEthernet 0/0
Internet 192.168.7.127 0 0060.97bd.ebee ARPA FastEthernet 0/0
Internet 192.168.7.195 57 0060.97bd.ef2d ARPA FastEthernet 0/0
Internet 192.168.7.183 -- 00d0.f8fb.108b ARPA FastEthernet 0/0
```

Each field in the ARP cache table has the following meanings:

Field	Description
Protocol	Network address protocol, always Internet.
Address	The IP address corresponding to the hardware address.
Age (min)	Age of the ARP cache record, in minutes; If it is not locally or statically configured, the value of the field is represented with “-”.
Hardware	Hardware address corresponding to the IP address
Type	The type of hardware address. The value is ARPA for all Ethernet addresses.
Interface	Interface associated with the IP address.

Related Commands

Command	Description
N/A.	N/A.

Platform Description N/A

3 IPv6 Commands

3.1 clear ipv6 neighbors

Use this command to clear the dynamic IPv6 neighbors.

clear ipv6 neighbors [*interface-id*]

Parameter Description

Parameter	Description
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 the dynamic IPv6 neighbors.

```
Ruijie# clear ipv6 neighbors
```

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 gateway

Use this command to configure the default gateway IPv6 address on the management port.

ipv6 gateway *ipv6-address*

Parameter Description

Parameter	Description
ipv6-address	Configures the default gateway IPv6 address.

Defaults N/A

Command Mode Interface configuration mode

Usage Guide The management port is MGMT in type and 0 in ID.

Configuration Examples The following example configures the default gateway IPv6 address on the management port.

```
Ruijie(config)# interface mgmt 0
Ruijie(config-int)# ipv6 gateway 2001:1::1
Ruijie(config-int)# exit
Ruijie(config)#
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

3.7 ipv6 general-prefix

Use this command to configure the IPv6 general prefix in the global configuration mode.

ipv6 general-prefix *prefix-name ipv6-prefix/prefix-length*

no ipv6 general-prefix *prefix-name ipv6-prefix/prefix-length*

Parameter Description

Parameter	Description
prefix-name	The general prefix name.
pv6-prefix	The network prefix value of the general-prefix following the format defined in RFC4291.
prefix-length	The length of the general prefix.

Defaults N/A

Command Global configuration mode.

Mode

Usage Guide It is convenient to number the network by using the general prefix, which defines a prefix so that many longer specified prefixes could refer to it. These specified prefixes are updated whenever the general prefix changes. If the network number changes, just modify the general prefix.
A general prefix could contain multiple prefixes.
These longer specified prefixes are usually used for the Ipv6 address configuration on the interface.

Configuration Examples The following example configures manually a general prefix as my-prefix.

```
Ruijie(config)# ipv6 general-prefix my-prefix 2001:1111:2222::/48
```

Related Commands

Command	Description
ipv6 address prefix-name sub-bits/prefix-length	Configures the interface address using the general prefix.
show ipv6 general-prefix	Displays the general prefix.

Platform Description N/A

3.8 ipv6 hop-limit

Use this command to configure the default hopcount to send unicast messages in the global configuration mode.
ipv6 hop-limit *value*
no ipv6 hop-limit

Parameter Description

Parameter	Description
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 N/A

Description

3.9 ipv6 mtu

Use this command to configure the MTU of IPv6 packets. Use the **no** form of this command to restore the default setting.

ipv6 mtu *bytes*

no ipv6 mtu

Parameter 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

3.10 ipv6 nd cache interface-limit

Use this command to set the maximum number of neighbors learned on the interface. Use the **no** form of this command to restore the default setting.

ipv6 nd cache interface-limit *value*

no ipv6 nd cache interface-limit

Parameter Description

Parameter	Description
value	Sets the maximum number of neighbors learned on the interface, including the static and dynamic neighbors, in the range from 0 to the number supported by the device. 0 indicates the number is not

	limited.

Defaults The default is 0.

Command Mode Interface configuration mode

Usage Guide This function can prevent neighbor entries generated by malicious neighbor attacks from consuming memory. *limit* must be no smaller than the number of neighbors learned on the interface. Otherwise, the configuration does not take effect.

Configuration Examples The following example sets the number of neighbors learned on the interface to 100.

```
Ruijie(config)# interface GigabitEthernet 0/1
Ruijie(config-if-GigabitEthernet 0/1)# ipv6 nd cache interface-limit 100
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

3.11 ipv6 nd dad attempts

Use this command to set the number of the NS packets to be continuously sent for IPv6 address collision check on the interface. Use the **no** form of this command to restore it to the default setting.
ipv6 nd dad attempts value
no ipv6 nd dad attempts *value*

Parameter Description

Parameter	Description
value	Number of the NS packets. If it is set to 0, it indicates that the IPv6 address collision check is disabled on the interface. The range is 0 to 600.

Defaults The default is 1.

Command Mode Interface configuration mode.

Usage Guide When the interface is configured with a new IPv6 address, the address collision shall be checked before the address is assigned to the interface, and the address shall be in the ”tentative” status. After the address collision check is completed, if no collision is detected, the address can be used normally; if collision is detected and the interface ID of the address is an EUI-64 ID, it indicates that the link-layer address is repeated, and the system will automatically shut down the interface (that is, to prohibit IPv6 operations on the interface). In this case, you shall modify and configure a new

address manually, and restart address collision check for the **down/up** interface. Whenever the state of an interface changes from **down** to **up**, the address collision check function of the interface will be enabled.

Configuration Examples 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

3.12 Ipv6 nd dad retry

Use this command to set the interval for address conflict detection. Use the **no** form of this command to restore the default setting.

ipv6 nd dad retry *value*

no ipv6 nd dad retry

Parameter Description

Parameter	Description
value	Sets the interval for address conflict detection, 60 seconds by default. Setting *value* to 0 indicates that the function is disabled.

Defaults 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 N/A

Description

3.13 ipv6 nd managed-config-flag

Use this command to set the “managed address configuration” flag bit of the RA message. Use the **no** form of this command to restore the default setting.

ipv6 nd managed-config-flag

no ipv6 nd managed-config-flag

Parameter 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

3.14 ipv6 nd ns-interval

Use this command to set the interval for the interface to retransmitting NS (Neighbor Solicitation). Use the **no** form of this command to restore the default setting.

ipv6 nd ns-interval *milliseconds*

no ipv6 nd ns-interval

Parameter 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

3.15 ipv6 nd other-config-flag

Use this command to set “other stateful configuration” flag bit of the RA message. Use the **no** form of this command to delete the flag bit.

ipv6 nd other-config-flag

no ipv6 nd other-config-flag

Parameter 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

3.16 ipv6 nd prefix

Use this command to configure the address prefix included in the RA. Use the **no** form of this command to delete the set prefix or restore the default setting.

ipv6 nd prefix { *ipv6-prefix*/*prefix-length* | **default** } [[*valid-lifetime preferred-lifetime*] | [**at** *valid-date preferred-date*] | [**infinite** | *preferred-lifetime*]] [**no-advertise**] | [[**off-link**] [**no-autoconfig**]]

no ipv6 nd prefix { *ipv6-prefix/prefix-length* | **default** }

Parameter Description

Parameter	Description
ipv6-prefix	IPv6 network ID following the format defined in RFC4291
prefix-length	Length of the IPv6 prefix. "/" shall be added in front of the prefix
valid-lifetime	Valid lifetime of the RA prefix received by the host
preferred-lifetime	Preferred lifetime of the RA prefix received by the host
at valid-date preferred-date	Sets the dead line for the valid lifetime and that of the preferred lifetime, in day, month, year, hour, minute.
infinite	Indicates that the prefix is always valid.
default	Sets the default prefix.
no-advertise	The prefix will not be advertised by the device.
off-link	When the host sends an IPv6 packet, if the prefix of the destination address matches the set prefix, it is considered that the destination is on-link and is directly reachable. If this option is set, it indicates that the prefix is not used for on-link judgment.
no-autoconfig	Indicates that the RA prefix received by the host cannot be used for auto address configuration.

Defaults By default, the advertised prefix is the one set with **ipv6 address** on the interface. The default parameters of the prefix configured in the RA are as follows:
valid-lifetime: 2592000s (30 days)
preferred-lifetime: 604800s (7 days),
The prefix is advertised and is used for on-link judgment and auto address configuration.

Command Mode Interface configuration mode.

Usage Guide This command can be used to configure the parameters of each prefix, including whether to advertise the prefix. By default, the prefix advertised in RA is the one set with **ipv6 address** on the interface. To add other prefixes, use this command.

ipv6 nd prefix default

Set the default parameters to be used by the interface. If no parameter is specified for an added

prefix, the parameters set with **ipv6 nd prefix default** will be used. Note that after a parameter is specified for the prefix, the default configuration will not be used. That is to say, the configuration of the prefix cannot be modified with **ipv6 nd prefix default**; only the prefix that uses all the default configurations can be modified with this command.

at *valid-date preferred-date*

The valid lifetime of a prefix can be specified in two ways. One way is to specify a fixed time for each prefix in the RA; the other way is to specify the end time (in this mode, the valid lifetime of the prefix sent in RA will be gradually reduced until the end time is 0).

Configuration Examples

The following example adds a prefix for SVI 1.

```
Ruijie(config)# interface vlan 1
Ruijie(conifig-if)# ipv6 nd prefix 2001::/64 infinite 2592000
```

The following example sets the default prefix parameters for SVI 1 (they cannot be used for auto address configuration):

```
Ruijie(config)# interface vlan 1

Ruijie(config-if)# ipv6 prefix default no-autoconfig
```

If no parameter is specified, the default parameters will be used, and the prefix cannot be used for auto address configuration.

Related Commands

Command	Description
show ipv6 interface	Displays the RA information of an interface.

Platform Description

N/A

3.17 ipv6 nd ra-hoplimit

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

ipv6 nd ra-hoplimit *value*

no ipv6 nd ra-hoplimit

Parameter Description

Parameter	Description
value	Hopcount

Defaults

The default is 64.

Command Mode

Interface configuration mode.

Usage Guide

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

3.18 ipv6 nd ra-interval

Use this command to set the interval of sending the RA. Use the **no** form of this command to restore the default setting.

ipv6 nd ra-interval { *seconds* | **min-max** *min_value max_value* }

no ipv6 nd ra-interva l

Parameter Description

Parameter	Description
seconds	Interval of sending the RA message in seconds, 3-1800s.
min-max	Maximum and minimum interval sending the RA message in seconds
min_value	Minimum interval sending the RA message in seconds
max_value	Maximum interval sending the RA message in seconds

Defaults 200s. The actual interval of sending the RA message will be fluctuated 20% based on 200s.

Command Mode Interface configuration mode.

Usage Guide If the device serves as the default device, the set interval shall not be longer than the lifetime of the device. Besides, to ensure other devices along the link occupies network bandwidth while sending the RA message, the actual interval for sending the RA message will be fluctuated 20% based on the set value.

If the key word **min-max** is specified, the actual interval for sending the packet will be chosen between the range of minimum value and maximum value.

Configuration Examples 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

3.19 ipv6 nd ra-lifetime

Use this command to set the device lifetime of the RA sent on the interface. Use the **no** form of this command to restore the default setting.

ipv6 nd ra-lifetime *seconds*

no ipv6 nd ra-lifetime

Parameter Description

Parameter	Description
seconds	Default life time of the device on the interface, in the range from 0 to 9000 in the unit of seconds.

Defaults The default is 1800.

Command Mode Interface configuration mode.

Usage Guide The router lifetime field is available in each RA. It specifies the time during which the hosts along the link of the interface can select the device as the default device. If the value is set to 0, the device will not serve as the default device any longer. If it is not set to 0, it shall be larger than or equal to the interval of sending the RA (ra-interval)

Configuration Examples 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 N/A

Description

3.20 ipv6 nd ra-mtu

Use this command to set the MTU of the RA message. Use the **no** form of this command to restore the default setting.
ipv6 nd ra-mtu *value*
no ipv6 nd ra-mtu

Parameter 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

3.21 ipv6 nd reachable-time

Use this command to set the reachable time after the interface checks the reachability of the neighbor dynamically learned through NDP. Use the **no** form of this command to restore the default setting.
ipv6 nd reachable-time *milliseconds*
no ipv6 nd reachable-time

Parameter Description

Parameter	Description
milliseconds	Reachable time for the neighbor in the range from 0 to 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

3.22 ipv6 nd state-time

Use this command to set the period for the neighbor to maintain the state. Use the **no** form of this command to restore the default setting.
ipv6 nd stale-time *seconds*
no ipv6 nd stale-time

Parameter Description

Parameter	Description
Seconds	Sets the period for the neighbor to maintain the state, in the range from 0 to 86400 in the unit of seconds.

Defaults The default is 3600.

Command Mode Global configuration mode

Usage Guide This command is used to set the period for the neighbor to maintain the state. After the period expires, neighbor unreachability detection is performed. The shorter the period, the faster the neighbor is found unreachable. On the other hand, more network bandwidth and device resources are consumed. Therefore, it is recommended to set a value not too small.

Configuration The following example sets the period to 600 seconds for the neighbor to maintain the state.

Examples

```
Ruijie(config)# ipv6 nd stale-time 600
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

3.23 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

3.24 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

3.25 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 Examples The following example configures a static neighbor on SVI 1.

```
Ruijie(config)# ipv6 neighbor 2001::1 vlan 1 00d0.f811.1111
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

3.26 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

3.27 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

3.28 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 Commands

Command	Description
N/A	N/A

Platform Description N/A

3.29 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

3.30 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

3.31 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. In: Indicate the number of the RAs that are received. inconsistent: Indicate the number of the received RAs in which the parameters are different from those contained in the RAs advertised by the device.
RS(input)	Indicate the number of the RSs that are received.
Link-layer address	Link-layer address of the interface.
Physical MTU	Link MTU of the interface.
!M | M	!M indicates the managed-config-flag bit in the RA is not set. M: Conversely
!O | O	!O indicates the other-config-flag bit in the RA is not set. O: Conversely

Description of the fields of the prefix list in **ra-info**:

Field	Meaning
total	The number of the prefixes of the interface.
fec0:1:1:1::/64	A specific prefix.
Def	Indicate that the interfaces use the default prefix.
Auto | CFG	Auto: Indicate the prefix is automatically generated after the interface is configured with the corresponding IPv6 address. CFG: Indicate that the prefix is manually configured.
!Adv	Indicate that the prefix will not be advertised.

vltime	Valid lifetime of the prefix, measured in seconds.
pltime	Preferred lifetime of the prefix, measured in seconds.
L | !L	L: Indicate that the on-link in the prefix is set. !L: Indicate that the on-link in the prefix is not set.
A | !A	A: Indicate that the auto-configure in the prefix is set. !A: It indicates that the auto-configure in the prefix is not set.

The following example displays the brief information of the IPv6 interface.

```
Ruijie#show ipv6 interface brief

GigabitEthernet 0/1          [down/down]
       2222::2
       FE80::1614:4BFF:FE5C:ED3A
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

3.32 show ipv6 neighbors

Use this command to display the IPv6 neighbors.

show ipv6 neighbors [**verbose**] [*interface-id*] [*ipv6-address*] **[static]**

show ipv6 neighbors static

Parameter Description

Parameter	Description
verbose	Displays the neighbor details.
static	Displays the validity status of static neighbors.
interface-id	Displays the neighbors of the specified interface.
ipv6-addres	Displays the neighbors of the specified IPv6 address.
static	Displays reachability of static neighbors.

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) The values of STATE are as below: INCMP (Incomplete): The address resolution of the neighbor is underway, the NS is sent, but the NA is not received. REACH (Reachable): The switch is connected with the neighbor. In this state, the switch takes no additional action when sending packets to the neighbor. STALE: The reachable time of the neighbor expires. In this state, the switch takes no additional action; it only starts NUD (Neighbor Unreachability Detection) after a packet is sent to the neighbor. DELAY: A packet is sent to the neighbor in STALE state. If the STALE state changes to DELAY, DELAY will be changed to PROBE if no neighbor reachability notification is received within DELAY_FIRST_PROBE_TIME seconds (5s), the NS will be sent to the neighbor to start NUD. PROBE: The NUD is started to check the reachability of the neighbor. The NS packets are sent to the neighbor at the interval of RetransTimer milliseconds until the response from the neighbor is received or the number of the sent NSs hits MAX_UNICAST_SOLICIT(3). ?: Unknown state. /R—indicate the neighbor is considered as a device /H: The neighbor is a host.
Age	The reachable time of the neighbor. '-' indicates that the neighbor is always reachable. Note that the reachability of a static neighbor depends on the actual situation. 'expired' indicates that the lifetime of the neighbor expires, and the neighbor is waits for the triggering of NUD.
Asked	The number of the NSs that are sent to the neighbor for the resolution of the link address of the neighbor.

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: The values of STATE are as below: ACTIVE INACTIVE

Related Commands

Command	Description
ipv6 neighbor	Configures a neighbor.

Platform Description N/A

3.33 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

3.34 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

3.35 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

3.36 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

3.37 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)# lease 0 1
```

The following example sets the DHCP lease to 1 minute.

```
Ruijie(dhcp-config)# lease 0 0 1
```

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 N/A

Description

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. String option: Ethernet ieee802 Digits option: 1 (10M Ethernet) 6 (IEEE 802)

Defaults No hardware address is defined by default.
If there is no option when the hardware address is defined, it is the Ethernet by default.

Command Mode DHCP address pool configuration mode.

Usage Guide This command can be used only when the DHCP is defined by manual binding.

Configuration Examples The following example defines the MAC address 00d0.f838.bf3d with the type ethernet.

```
hardware-address 00d0.f838.bf3d
```

Related Commands

Command	Description
client-identifier	Defines the unique ID of the DHCP client (Indicated by the hexadecimal numeral, separated by dot).
host	Defines the IP address and network mask, which is used to configure the DHCP manual binding.
ip dhcp pool	Defines the name of the DHCP address pool and enter the DHCP address pool configuration mode.
default-router	Defines the default route of the DHCP client.

Platform Description N/A

4.19 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

Command	Description

Commands	**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	**Parameter**	**Description**

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 Mode Global configuration mode.

Usage Guide The DHCP client checks the previously used IP address every time it is started and sends a DHCPREQUEST packet to continue leasing this IP address. If the address is not available, the DHCP server sends an NAK packet to let the client resend a DHCPDISCOVER packet to apply for a new IP address. If no corresponding lease record can be found on the server, the client keeps sending DHCPDISCOVER packets. The forcible NAK packet sending function is added to shorten the interval at which the client sends DHCPDISCOVER packets.

Configuration Examples The following example enables the forcible NAK packet sending function in global configuration mode.

```
Ruijie(config)# ip dhcp force-send-nak
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

4.24 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 Description	N/A

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: Digit in hexadecimal form in the range of 0 to FF. Only the following numerals are available: 1: b-node. 2: p-node. 4: m-node. 8: h-node. String: b-node: broadcast node p-node: peer-to-peer node m-node: mixed node

	h-node: hybrid node

Defaults No type of the NetBIOS node is defined by default.

Command Mode DHCP address pool configuration mode.

Usage Guide There are 4 types of the NetBIOS nodes of the Microsoft DHCP client: 1) Broadcast, which carries out the NetBIOS name resolution by the broadcast method, 2) Peer-to-peer, which directly requests the WINS server to carry out the NetBIOS name resolution, 3) Mixed, which requests the name resolution by the broadcast method firstly, and then carry out the name resolution by the WINS server connection, 4) Hybrid, which requests the WINS server to carry out the NetBIOS name resolution firstly, and it will carry out the NetBIOS name resolution by the broadcast method if the response is not received.
By default, the node type for Microsoft operating system is broadcast or hybrid. If the WINS server is not configured, broadcast node is used. Otherwise, hybrid node is used. It is recommended to set the type of the NetBIOS node as Hybrid.

Configuration Examples The following example sets the NetBIOS node of Microsoft DHCP client as Hybrid.

```
netbios-node-type h-node
```

Related Commands

Command	Description
ip dhcp pool	Defines the name of DHCP address pool and enters the DHCP address pool configuration mode.
netbios-name-server	Configures the WINS name server of the Microsoft DHCP client NETBIOS.

Platform Description N/A

4.41 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 Commands	Command	Description
	show ip dhcp server statistics	Displays various statistics information of the DHCP server.
	ip helper-address [**vrf**] *A.B.C.D*	Adds an IP address of the DHCP server.

Platform Description N/A

4.49 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 DHCPv6 Commands

5.1 clear ipv6 dhcp binding

Use this command to clear the DHCPv6 binding information.

clear ipv6 dhcp binding [*ipv6-address*]

Parameter Description

Parameter	Description
ipv6-address	Sets the IPv6 address or the prefix.

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide If the *ipv6-address* is not specified, all DHCPv6 binding information is cleared. If the *ipv6-address* is specified, the binding information for the specified address is cleared.

Configuration Examples The following example clears the DHCPv6 binding information:

```
Ruijie(config)# clear ipv6 dhcp binding
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

5.2 clear ipv6 dhcp client

Use this command to reset the DHCPv6 client.

clear ipv6 dhcp client*interface-type interface-number*

Parameter Description

Parameter	Description
interface-type interface-number	Sets the interface type and the interface number.

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide This command is used to reset the DHCPv6 client, which may lead the client to request for the configurations from the server again.

Configuration Examples The following example resets DHCP client VLAN 1.

```
Ruijie# clear ipv6 dhcp client vlan 1
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

5.3 clear ipv6 dhcp conflict

Use this command to clear the DHCPv6 address conflicts.

clear ipv6 dhcp conflict { *ipv6-address* | *}

Parameter Description

Parameter	Description
ipv6-address	Specifies IPv6 address or prefix.
*	All IPv6 addresses or prefixes

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide If the * parameter is not specified, all conflicts of IPv6 addresses or prefixes will be deleted.
If the *ipv6-address* parameter is specified, only the specified address conflict will be deleted.

Configuration Examples The following example clears a DHCPv6 address conflict.

```
Ruijie# clear ipv6 dhcp conflict 2008:50::2
```

Related Commands

Command	Description
show ipv6 dhcp conflict	Displays address conflicts.

Platform Description N/A

5.4 clear ipv6 dhcp relay statistics

Use this command to clear the packet sending and receiving condition with the DHCPv6 Relay function enabled.

clear ipv6 dhcp relay statistics

Parameter Description	Parameter	Description
	N/A	N/A

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide N/A

Configuration Examples The following example clears the packet sending and receiving condition with the DHCPv6 Relay function enabled.

```
Ruijie# clear ipv6 dhcp relay statistics
```

Related Commands	Command	Description
	show ipv6 dhcp relay statistics	Displays the statistical information.

Platform Description N/A

5.5 clear ipv6 dhcp server statistics

Use this command to clear the DHCPv6 server statistics.

clear ipv6 dhcp server statistics

Parameter Description	Parameter	Description
	N/A	N/A

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide This command is used to clear the DHCPv6 server statistics.

Configuration Examples The following example clears the DHCPv6 server statistics.

```
Ruijie(config)# clear ipv6 dhcp server statistics
```

Related Commands	Command	Description
	N/A	N/A

Platform Description N/A

5.6 dns-server

Use this command to set the DNS Server list information for the DHCPv6 Server.
Use the **no** form of this command to restore the default setting.
dns-server *ipv6-address*
no dns-server *ipv6-address*

Parameter Description

Parameter	Description
ipv6-address	Sets the IPv6 address or the DNS server.

Defaults By default, no DNS server list is configured.

Command Mode DHCPv6 pool configuration mode

Usage Guide To configure several DNS Server addresses, use the **dns-server** command for several times. The newly-configured DNS Server address will not overwrite the former ones.

Configuration Examples The following example configures the DNS server address.

```
Ruijie(config-dhcp)# dns-server 2008:1::1
```

Related Commands

Command	Description
domain-name	Sets the DHCPv6 domain name information.
ipv6 dhcp pool	Sets a DHCPv6 pool.

Platform Description N/A

5.7 domain-name

Use this command to set the domain name for the DHCPv6 server.
Use the **no** form of this command to restore thedefault setting.
domain-name*domain*
no domain-name *domain*

Parameter Description

Parameter	Description
domain	Sets the domain name.

Defaults By default, no domain name is configured.

Command Mode DHCPv6 pool configuration mode

Usage Guide To configure several domain names, use the domain-name command for several times. The newly-configured domain name will not overwrite the former ones.

Configuration Examples The following example sets the domain name for the DHCPv6 server to example.com.

```
Ruijie(config-dhcp)# domain-name example.com
```

Related Commands

Command	Description
dns-server	Sets the DHCPv6 DNS server list.
ipv6 dhcp pool	Sets the DHCPv6 pool.

Platform Description N/A

5.8 iana-address prefix

Use this command to set the IA_NA address prefix for the DHCPv6 Server. Use the **no** form of this command to restore thedefault setting.

iana-address prefix *ipv6-prefix/prefix-length* [**lifetime** { *valid-lifetime* | *preferred-lifetime* }]

no iana-address prefix

Parameter Description

Parameter	Description
ipv6-prefix/prefix-length	Sets the IPv6 prefix and prefix length.
lifetime	Sets the lifetime of the address allocated to the client. With the keyword **lifetime** configured, both parameters *valid-lifetime*and*preferred-lifetime* shall be configured.
valid-lifetime	Sets the valid lifetime of using the allocated address for the client.
preferred-lifetime	Sets the preferred lifetime of the address allocated to the client.

Defaults By default, no IA_NA address prefix is configured.
The default *valid-lifetime* is 3600s(1 hour).
The default *preferred-lifetime is* 3600s(1 hour).

Command Mode DHCPv6 pool configuration mode

Usage Guide This command is used to set the IA_NA address prefix for the DHCPv6 Server, and allocate the IA_NA address to the client.
The Server attempts to allocate a usable address within the IA_NA address prefix range to the client upon receiving the IA_NA address request from the client. That address will be allocated to other

clients if the client no longer uses that address again.

Configuration Examples The following example sets the IA_NA address prefix for the DHCPv6 Server.

```
Ruijie(config-dhcp)# iana-address prefix 2008:50::/64 lifetime 2000 1000
```

Related Commands

Command	Description
ipv6 dhcp pool	Sets the DHCPv6 pool.
show ipv6 dhcp pool	Displays the DHCPv6 pool information.

Platform Description N/A

5.9 ipv6 dhcp client ia

Use this command to enable DHCPv6 client mode and request the IANA address from the DHCPv6 server. Use the **no** form of this command to restore the default setting.

ipv6 dhcp client ia [**rapid-commit**]

no ipv6 dhcp client ia

Parameter Description

Parameter	Description
rapid-commit	Allows the two-message interaction process.

Defaults This function is disabled by default.

Command Mode Interface configuration mode

Usage Guide This command is used to enable DHCPv6 client mode and request the IANA address from the DHCPv6 server,

The **rapid-commit**key allows the two-message interaction process between the client and the server. After the key is configured, the solicit message transmitted by the client contains the rapid-commit option.

Configuration Examples The following example enables the request for the IANA address on the interface.

```
Ruijie(config)# interface fastethernet 0/1
Ruijie(config-if)# ipv6 dhcp client ia
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

5.10 ipv6 dhcp client pd

Use this command to enable the DHCPv6 client and request for the prefix address information.
Use the **no** form of this command to restore the default setting.
ipv6 dhcp client pd *prefix-name* [**rapid-commit**]
no ipv6 dhcp client pd

Parameter Description

Parameter	Description
prefix-name	Defines the IPv6 prefix name.
rapid-commit	Allows the two-message interaction process.

Defaults This function is disabled by default.

Command Mode Interface configuration mode

Usage Guide With the DHCPv6 client mode disabled, use this command to enable the DHCPv6 client mode on the interface.
With the **ipv6 dhcp client pd** command enabled, the DHCPv6 client sends the prefix request to the DHCPv6 server
The keyword **rapid-commit** allows the client and the server two-message interaction process. With this keyword configured, the solicit message sent by the client includes the **rapid-commit** item.

Configuration Examples The following example enables the prefix information request on the interface.

```
Ruijie(config)# interface fastethernet 0/1
Ruijie(config-if)# ipv6 dhcp client pd pd_name
```

Related Commands

Command	Description
clear ipv6 dhcp client	Resets the DHCPv6 client function on the interface.
show ipv6 dhcp interface	Displays the DHCPv6 interface configuration.

Platform Description N/A

5.11 ipv6 dhcp pool

Use this command to set the DHCPv6 server pool.
Use the **no** form of this command to restore thedefault setting.
ipv6 dhcp pool *poolname*
no ipv6 dhcp pool *poolname*

Parameter

Parameter	Description

Description		
	poolname	Defines the DHCPv6 pool name.

Defaults By default, no DHCPv6 server pool is configured.

Command Mode Global configuration mode

Usage Guide This command is used to create a DHCPv6 Server configuration pool. After configuring this command, it enters the DHCPv6 pool configuration mode, in which the administrator can set the pool parameters, such as the prefix and the DNS Server information, ect.
After creating the DHCPv6 Server configuration pool, use the **ipv6 dhcp server** command to associate the pool and the DHCPv6 Server on one interface.

Configuration Examples The following example sets the DHCPv6 server pool.

```
Ruijie# configure terminal
Ruijie(config)# ipv6 dhcp pool pool1
Ruijie(config-dhcp)#
```

Related Commands

Command	Description
ipv6 dhcp server	Enables the DHCPv6 server function on the interface.
show ipv6 dhcp pool	Displays the DHCPv6 pool information.

Platform Description N/A

5.12 ipv6 dhcp relay destination

Use this command to enable the DHCPv6 relay service and configure the destination address to which the messages are forwarded.
Use the **no** form of this command to restore the default setting.
ipv6 dhcp relay destination*ipv6-address* [*interface-type interface-number*]
no ipv6 dhcp relay destination*ipv6-address* [*interface-type interface-number*]

Parameter Description

Parameter	Description
ipv6-address	Sets the DHCPv6 relay destination address.
interface-type interface-number	Specifies the forwarding output interface if the forwarding address is the local link address.

Defaults By default, the relay and forward function is disabled, and the forwarding destination address and the output interface are not configured.

Command Interface configuration mode

Mode

Usage Guide With the DHCPv6 relay service enabled on the interface, the DHCPv6 message received on the interface can be forwarded to all configured destination addresses. Those received DHCPv6 messages can be from the client, or from another DHCPv6 relay service.
The forwarding output interface configuration is mandatory if the forwarding address is the local link address or the multicast address. And the forwarding output interface configuration is optional if the forwarding address is global or station unicast or multicast address.
Without the forwarding output interface configured, the interface is selected according to the unicast or multicast routing protocol.
The relay reply message can be forwarded without the relay function enabled on the interface.

Configuration Examples The following example sets the relay destination address on the interface.

```
Ruijie(config)# interface fastethernet 0/1
Ruijie(config-if)# ipv6 dhcp relay destination 2008:1::1
```

Related Commands

Command	Description
show ipv6 dhcp interface	Displays the DHCPv6 interface information.

Platform Description N/A

5.13 ipv6 dhcp server

Use this command to enable the DHCPv6 server on the interface.
Use the **no** form of this command to restore the default setting.
ipv6 dhcp server *poolname*[**rapid-commit**][**preference** *value*]
no ipv6 dhcp server

Parameter Description

Parameter	Description
poolname	Defines the DHCPv6 pool name.
rapid-commit	Allows the two-message interaction process.
preference *value*	Sets the preference level for the advertise message. The valid range is from 1 to 100 and the default value is 0.

Defaults This function is disabled by default.

Command Mode Interface configuration mode

Usage Guide Use the **ipv6 dhcp server** command to enable the DHCPv6 service.
Configuring the keyword **rapid-commit** allows the two-message interaction for the server and the client when allocating the address prefix and setting other configurations. With this keyword

configured, if the client solicit message includes the **rapid-commit** item, the DHCPv6 Server will send the Reply message immediately.
DHCPv6 Server carries with the **preference** value when sending the advertise message if the **preference** level is not 0.
If the **preference** level is 0, the advertise message will not include this field. If the **preference** value is 255, the client sends the request message to the server to obtain the configurations.
DHCPv6 Client, Server and Relay functions are exclusive, and only one of the functions can be configured on the interface.

Configuration Examples The following example enables the DHCPv6 server on the interface.

```
Ruijie(config)# interface fastethernet 0/1
Ruijie(config-if)# ipv6 dhcp server pool1
```

Related Commands

Command	Description
ipv6 dhcp pool	Sets the DHCPv6 pool.
show ipv6 dhcp pool	Displays the DHCPv6 pool information.

Platform Description N/A

5.14 ipv6 local pool

Use this command to configure the local prefix pool of the DHCPv6 server prefix.
Use the **no** form of this command to restore the default setting.
ipv6 local pool *poolname prefix/prefix-length assigned-length*
no ipv6 local pool *poolname*

Parameter Description

Parameter	Description
poolname	The local prefix pool name
prefix/prefix-length	The prefix and prefix length
assigned-length	The assigned prefix length

Defaults By default, no local prefix pool of the DHCPv6 server prefix is configured.

Command Mode Global configuration mode

Usage Guide The **ipv6 local pool** command is used to create the local prefix pool. If the DHCPv6 server requires prefix delegation, you can use the **prefix-delegation pool** command to specify the local prefix pool and then assign prefixes from the prefix pool.

Configuration Examples The following example configures the local prefix pool.

```
Ruijie(config)# ipv6 local pool client-prefix-pool 2001::db8::/64 80
```

The following example specifies the local prefix pool.

```
Ruijie(config-dhcp)# prefix-delegation pool client-prefix-pool lifetime 2000 1000
```

Related Commands	Command	Description
	N/A	N/A

Platform Description N/A

5.15 option52

Use this command to configure the DHCPv6 Server to set the CAPWAP AC IPv6 address.
Use the **no** form of this command to restore the default setting.
option52 *ipv6-address*
no option52 *ipv6-address*

Parameter Description	Parameter	Description
	ipv6-address	Sets the CAPWAP AC IPv6 address.

Defaults By default, no option52 is created after pool configuration on the DHCPv6 server is complete.

Command Mode DHCPv6 pool configuration mode

Usage Guide This command can be used to set multiple CAPWAP AC IPv6 addresses. The newly added IPv6 address does not overwrite the old one.

Configuration Examples The following example configures thedomain-name address.

```
Ruijie(config-dhcp)# option52 2008:1::1
```

Related Commands	Command	Description
	N/A	N/A

Platform Description N/A

5.16 prefix-delegation

Use this command to set the static binding address prefix information for the DHCPv6 server.
Use the **no** form of this command to restore the default setting.
prefix-delegation *ipv6-prefix/prefix-length client-DUID* [*lifetime*]
no prefix-delegation *ipv6-prefix/prefix-length client-DUID* [*lifetime*]

Parameter Description

Parameter	Description
ipv6-prefix/prefix-length	Sets the IPv6 address prefix and the prefix length.
client-DUID	Sets the client DUID.
lifetime	Sets the interval of using the prefix by the client.

Defaults By default, no address prefix information is configured.
The default*lifetime* is 3600 seconds (one hour).

Command Mode DHCPv6 pool configuration mode

Usage Guide The administrator uses this command to manually set the address prefix information list for the client IA_PD and set the valid lifetime for those prefixes.
The parameter *client-DUID* allocates the address prefix to the first IA_PD in the specified client.
Before receiving the request message for the address prefix from the client, DHCPv6 Server searches for the corresponding static binding first. If it succeeds, the server returns to the static binding; otherwise, the server will attempt to allocate the address prefix from other prefix information sources.

Configuration Examples The following example sets the static binding address prefix information for the DHCPv6 server.

```
Ruijie(config-dhcp)# prefix-delegation 2008:2::/64 0003000100d0f82233ac
```

Related Commands

Command	Description
ipv6 dhcp pool	Sets a DHCPv6 pool.
ipv6 local pool	Sets a local prefix pool.
prefix-delegation pool	Specifies the DHCPv6 local prefix pool.
show ipv6 dhcp pool	Displays the DHCPv6 pool information.

Platform Description N/A

5.17 prefix-delegation pool

Use this command to specify the local prefix pool for the DHCPv6 server.
Use the **no** form of this command to restore the default setting.
prefix-delegation pool *poolname* [**lifetime** { *valid-lifetime* | *preferred-lifetime* }]
no prefix-delegation pool *poolname*

Parameter Description

Parameter	Description
poolname	Sets the local prefix pool name.
lifetime	Sets the lifetime of the address prefix allocated to the client. With the keyword **lifetime** configured, both parameters *valid-lifetime* and

	preferred-lifetime shall be configured.
valid-lifetime	Sets the valid lifetime of using the allocated address prefix for the client.
preferred-lifetime	Sets the preferred lifetime of the address prefix allocated to the client.

Defaults By default, no address prefix pool is specified.
The default *valid-lifetime* is 3600s(1 hour).
The default *preferred-lifetime is* 3600s(1 hour).

Command Mode DHCPv6 pool configuration mode

Usage Guide Use the **prefix-delegation pool** command to set the prefix pool for the DHCPv6 Server and allocate the prefix to the client. Use the **ipv6 local pool** command to set the prefix pool.
The Server attempts to allocate a usable prefix from the prefix pool to the client upon receiving the prefix request from the client. That prefix will be allocated to other clients if the client no longer uses that prefix again.

Configuration Examples The following example specifies the local prefix pool for the DHCPv6 server.

```
Ruijie(config-dhcp)# prefix-delegation pool client-prefix-pool lifetime 2000 1000
```

Related Commands

Command	Description
ipv6 dhcp pool	Sets a DHCPv6 pool.
ipv6 local pool	Sets a local prefix pool.
prefix-delegation	Statically binds the client with the address prefix.
show ipv6 dhcp pool	Displays the DHCPv6 pool information.

Platform Description N/A

5.18 show ipv6 dhcp

Use this command to display the device DUID.
show ipv6 dhcp

Parameter Description

Parameter	Description
N/A	N/A

Defaults N/A

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

Usage Guide The server, client and relay on the same device share a DUID.

Configuration Examples The following example displays the device DUID.

```
Ruijie# show ipv6 dhcp
This device's DHCPv6 unique identifier(DUID): 00:03:00:01:00:d0:f8:22:33:b0
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

5.19 show ipv6 dhcp binding

Use this command to display the address binding information for the DHCPv6 server.

show ipv6 dhcp binding [*ipv6-address*]

Parameter Description

Parameter	Description
ipv6-address	Sets the IPv6 address or the prefix.

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide If the *ipv6-address* is not specified, all prefixes dynamically assigned to the client and IANA address binding information are shown. If the *ipv6-address* is specified, the binding information for the specified address is shown.

Configuration Examples The following example displays the address binding information for the DHCPv6 server.

```
Ruijie# show ipv6 dhcp binding
Client  DUID: 00:03:00:01:00:d0:f8:22:33:ac
  IAPD: iaid 0, T1 1800, T2 2880
    Prefix: 2001:20::/72
          preferred lifetime 3600, valid lifetime 3600
       expires at Jan 1 2008 2:23 (3600 seconds)
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

5.20 show ipv6 dhcp conflict

Use this command to display the DHCPv6 address conflicts.

show ipv6 dhcp conflict

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

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide N/A

Configuration Examples The following example displays the DHCPv6 address conflicts.

```
Ruijie# show ipv6 dhcp conflict
2008:50::2    declined
2108:50::2    declined
2008:50::3    declined
2008:50::4    declined
2108:50::4    declined
2008:50::5    declined
```

Related Commands	**Command**	**Description**
	clear ipv6 dhcp conflict	Clears address conflicts.

Platform Description N/A

5.21 show ipv6 dhcp interface

Use this command to display the DHCPv6 interface information.

show ipv6 dhcp interface [*interface-name*]

Parameter Description	**Parameter**	**Description**
	interface-name	Sets the interface name.

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide If the *interface-name* is not specified, all DHCPv6 interface information isdisplayed. If the *interface-name* is specified, the specified interface information is displayed.

Configuration Examples The following example displays the server-based DHCPv6 interface information.

```
Ruijie# show ipv6 dhcp interface
VLAN 1 is in server mode
  Server pool dhcp-pool
  Rapid-Commit: disable
```

The following example displays the client-based DHCPv6 interface information.

```
Ruijie# show ipv6 dhcp interface
FastEthernet 0/1 is in client mode
  Rapid-Commit: disable
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

5.22 show ipv6 dhcp pool

Use this command to display the DHCPv6 pool information.

show ipv6 dhcp pool [*poolname*]

Parameter Description

Parameter	Description
poolname	Defines the DHCPv6 pool name.

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide If the *poolname* is not specified, all DHCPv6 interface information isdisplayed. If the *poolname* is specified, the specified interface information is displayed.

Configuration Examples The following example displays the DHCPv6 pool information.

```
Ruijie# show ipv6 dhcp pool
DHCPv6 pool: dhcp-pool
  DNS server: 2011:1::1
  DNS server: 2011:1::2
  Domain name: example.com
```

Related Commands	Command	Description
	N/A	N/A

Platform Description N/A

5.23 show ipv6 dhcp relay destination

Use this command to display the destination information about DHCPv6 Relay Agent.

show ipv6 dhcp relay destination { **all** | *interface-type interface-number* }

Parameter description	Parameter	Description
	all	Displays information about all configured destination addresses and relay exits.
	interface*interface-type interface-number*	Displaysthe relay destination address and relay exit configured for a specified interface.

Defaults N/A

Command mode Privileged EXEC mode

Usage guideline Use this command to show the relay destination address to which DHCPv6 packets sent from a client are forwarded through a specified relay exit (optional) by an interface for which the relay function has been enabled by Relay Agent.

Examples The following example displays all the relay destination addresses.

```
Ruijie# show ipv6 dhcp relay destination all
Interface: Vlan1   //interface for which the relay function has been enabled
Destination address(es)                    Output Interface
3001::2
FF02::1:2     //specified destination address          Vlan2   //specified
relay exit
```

Related commands	Command	Description
	N/A	N/A

Platform description N/A

5.24 show ipv6 dhcp relay statistics

Use this command to display the packet sending and receiving condition with the DHCPv6 Relay function enabled.

show ipv6 dhcp relay statistics

Parameter Description

Parameter	Description
N/A.	N/A.

Defaults N/A.

Command Mode Privileged EXEC mode

Usage Guide N/A.

Configuration Examples The following example displays the packet sending and receiving condition with the DHCPv6 Relay function enabled.

```
Ruijie# show ipv6 dhcp relay statistics
Packets dropped             :  2
   Error                   :  2
   Excess of rate limit     :  0
Packets received            :  28
   SOLICIT                 :  0
   REQUEST                 :  0
   CONFIRM                 :  0
   RENEW                   :  0
   REBIND                  :  0
   RELEASE                 :  0
   DECLINE                 :  0
   INFORMATION-REQUEST      :  14
   RELAY-FORWARD           :  0
   RELAY-REPLY             :  14
Packets sent                :  16
   ADVERTISE               :  0
   RECONFIGURE             :  0
   REPLY                   :  8
   RELAY-FORWARD           :  8
 RELAY-REPLY             :  0
```

Related Commands

Command	Description
clear ipv6 dhcp relay statistics	Clears the statistical information.

Platform N/A

Description

5.25 show ipv6 dhcp server statistics

Use this command to display the DHCPv6 server statistics.

show ipv6 dhcp server statistics

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

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide This command is used to display the DHCPv6 server statistics.

Configuration Examples The following example displays the DHCPv6 server statistics.

```
Ruijie# show ipv6 dhcp server statistics
DHCPv6 server statistics:

Packet statistics:
DHCPv6 packets received:          7
Solicit received:                 7
Request received:                 0
Confirm received:                 0
Renew received:                   0
Rebind received:                  0
Release received:                 0
Decline received:                 0
Relay-forward received:           0
Information-request received:     0
Unknown message type received:    0
Error message received:           0

DHCPv6 packet sent:               0
Advertise sent:                   0
Reply sent:                       0
Relay-reply sent:                 0
Send reply error:                 0
Send packet error:                0

Binding statistics:
Bindings generated:               0
IAPD assigned:                    0
IANA assigned:                    0

Configuration statistics:
DHCPv6 server interface:          1
DHCPv6 pool:                      0
DHCPv6 iapd binding:              0
```

Related Commands

Command	Description
ipv6 dhcp pool	Sets a DHCPv6 pool.

Platform Description N/A

5.26 show ipv6 local pool

Use this command to display the local prefix pool configuration and usage.

show ipv6 local pool [*poolname*]

Parameter Description	Parameter	Description
	poolname	The local prefix pool name

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide This command is used to display the local prefix pool configuration and usage.

Configuration Examples The following example displays all local prefix pool information.

```
Ruijie#show ipv6 local pool
Pool                        Prefix
Free          In use
client-prefix-pool             2001:db8::/64
65536          0
```

Field	Description
Pool	The local address pool name.
Prefix	The prefix and prefix length.
Free	The available prefix.
In use	The prefix in use.

The following example displays the information about the specified local prefix pool.

```
Ruijie#show ipv6 local pool client-prefix-pool
Prefix is 2001:db8::/64 assign /80 prefix
1 entries in use, 65535 available
Prefix                                              Interface
2001:db8::/80                                        GigabitEthernet 0/0
```

Filed	Description
Prefix	The assigned prefix and prefix length.
Interface	The assigning interface.

Related Commands	Command	Description
	N/A	N/A

Platform Description N/A

6 DNS Commands

6.1 clear host

Use this command to clear the dynamically learned host name.

clear host [* | *host-name*]

Parameter Description

Parameter	Description
host-name	Deletes the specified dynamic domain name buffer.
*	Deletes all dynamic domain name buffer.

Defaults N/A

Command Mode Privileged EXEC mode.

Usage Guide You can obtain the mapping record of the host name buffer table in two ways: 1) the **ip host** static configuration, 2) the DNS dynamic learning. Execute this command to delete the host name records learned by the DNS dynamically.

Configuration Examples The following configuration deletes the dynamically learned mapping records from the host name-IP address buffer table.

```
Ruijie(config)#clear host *
```

Related Commands

Command	Description
show hosts	Displays the host name buffer table.

Platform Description N/A

6.2 ip domain-lookup

Use this command to enable DNS domain name resolution. Use the **no** form of this command to disable the DNS domain name resolution function.

ip domain-lookup

no ip domain-lookup

Parameter Description

Parameter	Description

N/A	N/A

Defaults This function is enabled by default.

Command Mode Global configuration mode.

Usage Guide This command enables the domain name resolution function.

Configuration Examples The following example disables the DNS domain name resolution function.

```
Ruijie(config)# no ip domain-lookup
```

Related Commands

Command	Description
show hosts	Displays the DNS related configuration information.

Platform Description N/A

6.3 ip host

Use this command to configure the mapping of the host name and the IP address. Use the **no** form of the command to remove the host list.

ip host *host-name ip-address*

no ip host *host*-name *ip-address*

Parameter Description

Parameter	Description
host-name	The host name of the equipment
ip-address	The IP address of the equipment

Defaults N/A

Command Mode Global configuration mode.

Usage Guide N/A

Configuration Examples The following example configures IPv4 address 192.168.5.243 for domain name www .test.com.

```
Ruijie(config)# ip host www.test.com 192.168.5.243
```

Related

Command	Description

Commands

show hosts	Show the DNS related configuration information.

Platform Description N/A

6.4 ip name-server

Use this command to configure the IP address of the domain name server. Use the **no** form of this command to delete the configured domain name server.

ip name-server { *ip-address* | *ipv6-address* }

no ip name-server [*ip-address* | *ipv6-address*]

Parameter Description

Parameter	Description
ip-address	The IP address of the domain name server.
ipv6-address	The IPv6 address of the domain name server.

Defaults 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

6.5 ipv6 host

Use this command to configure the mapping of the host name and the IPv6 address by manual. Use the **no** form of the command to remove the host list.

ipv6 host *host-name ipv6-address*

no ipv6 host *host*-name *ipv6-address*

Parameter Description

Parameter	Description
host-name	The host name of the equipment
ipv6-address	The IPv6 address of the equipment

Defaults N/A

Command Mode Global configuration mode.

Usage Guide

Configuration Examples The following example configures the IPv6 address for the domain name.

```
Ruijie(config)# ipv6 host switch 2001:0DB8:700:20:1::12
```

Related Commands

Command	Description
show hosts	Displays the DNS related configuration information.

Platform Description N/A

6.6 show hosts

Use this command to display DNS configuration.

show hosts [*hostname*]

Parameter Description

Parameter	Description
hostname	Displays the specified domain name information,

Defaults 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: Static resolution and dynamic resolution.
Address	IP address corresponding to the domain name
TTL	TTL of entries corresponding to the domain name/IP address.

Related Commands

Command	Description
ip host	Configures the host name and IP address mapping by manual.
ipv6 host	Configures the host name and IPv6 address mapping by manual.
ip name-server	Configures the DNS server.

Platform Description N/A

7 FTP Server Commands

7.1 ftp-server enable

Use this command to enable the FTP server. Use the **default** form of this command to restore the default setting.

ftp-server enable

default ftp-server enable

Parameter Description

Parameter	Description
N/A	N/A

Defaults This function is disabled by default.

Command Mode Global configuration mode

Usage Guide This command is used to enable the FTP server to connect the FTP client to upload/download the files.

To enable the FTP client to access to the FTP server files, this command shall be co-used with the **ftp-server topdir** command.

Configuration Examples The following example enables the FTP Server and confines the FTP client access to the syslog subdirectory:

```
Ruijie(config)# ftp-server topdir /syslog
Ruijie(config)# ftp-server enable
```

The following example disables the FTP Server:

```
Ruijie(config)# no ftp-server enable
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

7.2 ftp-server login timeout

Use this command to set the timeout interval for login to the FTP server. Use the **no** or **default** form of this command to restore the default setting.

ftp-server login timeout *time*

no ftp-server login timeout

default ftp-server login timeout

Parameter Description

Parameter	Description
time	Sets the timeout interval for login to the FTP server, in the range from 1 to 30 in the unit of minutes.

Defaults The default is 2 minutes.

Command Mode Global configuration mode

Usage Guide The timeout interval refers to the maximum time when your account is allowed online after you login to the server. If you don't perform authentication again before the timeout interval expires, you will be forced offline.

Configuration Examples The following example sets the timeout interval for login to the FTP server to 5 minutes.

```
Ruijie(config)# ftp-server login timeout 5
```

The following example restores the default setting.

```
Ruijie(config)# no ftp-server login timeout
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

7.3 ftp-server login times

Use this command to set the number of login attempts. Use the **no** or **default** form of this command to restore the default setting.

ftp-server login times *time*

no ftp-server login times

default ftp-server login times

Parameter Description

Parameter	Description
time	Sets the number of login attempts, in the range from 1 to 10.

Defaults The default is 3.

Command Mode Global configuration mode

Usage Guide The number of login attempts refers to the maximum count you are allowed to perform authentication. If the number of your login attempts exceeds 3, you will be forced offline.

Configuration Examples The following example sets the number of login attempts to 5.

```
Ruijie(config)# ftp-server login times 5
```

The following example restores the default setting.

```
Ruijie(config)# no ftp-server login times
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

7.4 ftp-server topdir

Use this command to set the directory range for the FTP client to access to the FTP server files. Use the **no** or **default** form of this command to restore the default setting.

ftp-server topdir *directory*

no ftp-server topdir

default ftp-server topdir

Parameter Description

Parameter	Description
directory	Sets the top-directory.

Defaults No top-directory is configured by default.

Command Mode Global configuration mode.

Usage Guide The FTP server top directory specifies the directory range of the files accessed by the client. Can the FTP client accesses to the files on the FTP server with the top directory correctly specified.
Without this command configured, FTP client fails to access to any file or directory on the FTP server.

Configuration Examples The following example enables the FTP Server and confines the FTP client access to the syslog subdirectory.

```
Ruijie(config)# ftp-server topdir /syslog
Ruijie(config)# ftp-server enable
```

The following example restores the default setting.

```
Ruijie(config)# no ftp-server topdir
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

7.5 ftp-server timeout

Use this command to set the FTP session idle timeout. Use the **no** or **default** form of this command to restore the default setting.
ftp-server timeout *time*
no ftp-server timeout
default ftp-server timeout

Parameter Description

Parameter	Description
time	Sets the session idle timeout, in the range from 1 to 3600 in the unit of minutes.

Defaults The default is 10 minutes.

Command Mode Global configuration mode.

Usage Guide Use this command to set the FTP session idle timeout. If the session is idle, the FTP server deems the session connection is invalid and disconnects with the user.

⚠ The session idle time refers to the time for the FTP session between two FTP operations

Configuration The following example sets the session idle timeout to 5 mimutes:

Examples

```
Ruijie(config)# ftp-server timeout 5
```

The following example restores the default setting.

```
Ruijie(config)# no ftp-server timeout
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

7.6 ftp-server username password

Use this command to set the login username and password for the FTP server. Use the **no** form of this command to restore the default setting.

ftp-server username *username* **password** [*type*] *password*

no ftp-server username *username*

default ftp-server username *username*

Parameter Description

Parameter	Description
username	Sets the login username.
password	Sets the log password

Defaults No username or password is set by default.

Command Mode Global configuration mode

Usage Guide Use this command to set the login username for the FTP server. To log in to the FTP server, the correct username and password shall be provided.

The maximum length of the username is 64 characters and the spaces are not allowed in the middle of the username. The username consists of letters, semiangle number and semiangle mark. Up to 10 usernames can be configured for the FTP server.

The password must contain letters or numbers. Spaces before or behind the password are allowed but will be ignored. The spaces within are part of the password.

The plaintext password is in the range from 1 to 25 characters. The encrypted password is in the range from 4 to 52 characters.

⚠ The anonymous user login is not supported on the FTP server. The client fails to pass the identity verification if the username is removed.

Configuration Examples The following example sets the username to user:

```
Ruijie(config)# ftp-server username user password pass
```

The following example restores the default setting:

```
Ruijie(config)# no ftp-server username user
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

7.7 show ftp-server

Use this command to show the status information of the FTP server.

show ftp-server

Parameter Description

Parameter	Description
N/A	N/A

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide The FTP server status information includes:

- Enabled/Disabled server
- The FTP server top directory
- The FTP server user information, including username, password and connection number. If connection is set up, the IP address, port, transmission type, active/passive mode is shown

Configuration Examples The following example displays the related status information of the FTP server:

```
Ruijie#show ftp-server
    ftp-server information
==================================
enable : Y
topdir : tmp:/
timeout: 10min
username:aaaa          password:(PLAINT)bbbb          connect num[2]
    [0]trans-type:BINARY (ctrl)server IP:192.168.21.100[21]
```

```
                              client IP:192.168.21.26[3927]
    [1]trans-type:ASCII (ctrl)server IP:192.168.21.100[21]
                              client IP:192.168.21.26[3929]
username:a1           password:(PLAINT)bbbb         connect num[0]
username:a2           password:(PLAINT)bbbb         connect num[0]
username:a3           password:(PLAINT)bbbb         connect num[0]
username:a4           password:(PLAINT)bbbb         connect num[0]
username:a5           password:(PLAINT)bbbb         connect num[0]
username:a6           password:(PLAINT)bbbb         connect num[0]
username:a7           password:(PLAINT)bbbb         connect num[0]
username:a8           password:(PLAINT)bbbb         connect num[0]
username:a9           password:(PLAINT)bbbb         connect num[0]
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

8 FTP CLIENT Commands

8.1 default ftp-client

Use this command to resort the default FTP client setting.

default ftp-client

Parameter Description

Parameter	Description
N/A	N/A

Defaults N/A

Command Mode Global configuration mode

Usage Guide This command is used to restore the FTP client setting. Specifically, data connection is in PASV mode and file transfer BINARY. The client source IP address is not bound.

Configuration Examples The following example restores the default FTP client setting.

```
Ruijie(config)# default ftp-client
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

8.2 ftp-client ascii

Use this command to use ASCII mode for FTP transfer.

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

ftp-client ascii

no ftp-clientascii

Parameter Description

Parameter	Description
N/A	N/A

Defaults The default FTP transfer mode is binary.

Command Mode Global configuration mode

Usage Guide N/A

Configuration Examples The following example configures ASCII FTP transfer.

```
Ruijie (config)# ftp-client ascii
```

The following example configures binary FTP transfer.

```
Ruijie(config)# no ftp-client ascii
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

8.3 ftp-client port

Use this command to configure PORT mode used for FTP data connection. Use the **no** form of this command to restore the default setting.

ftp-client port

no ftp-client port

Parameter Description

Parameter	Description
N/A	N/A

Defaults The default is PASV mode for FTP data connection.

Command Mode Global configuration mode.

Usage Guide This command is used to configure the connection mode to PORT mode, in which the server will actively connect with the client.

Configuration Examples The following example configures PORT mode used for FTP data connection

```
Ruijie (config)# ftp-client port
```

The following example configures PASV mode for FTP data connection.

```
Ruijie(config)# no ftp-client port
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

8.4 ftp-client source-address

Use this command to bind FTP Client with the source IP address of client and use this IP address to communicate with server. Use the **no** form of this command to disable source IP address binding. Use the **default** form of this command to restore the default setting.

ftp-client source-address {*ip-address* **|** *ipv6-address*}

no ftp-client source-address

Parameter Description

Parameter	Description
ip-address	The IPv4 address of the local interface.
ipv6-address	The IPv6 address of the local interface.

Defaults By default, the IP address is not bound with the client locally. Instead, it is selected by the route.

Command Mode Global configuration mode

Usage Guide N/A

Configuration Examples The following example binds FTP Client with source IP address 192.168.23.236.

```
Ruijie(config)# ftp-client source-address 192.168.23.236
```

The following example binds FTP Client with source IP address 2003:0:0:0::2.

```
Ruijie(config)# ftp-client source-address 2003:0:0:0::2
```

The following example disables source IP address binding.

```
Ruijie(config)# no ftp-client source-address
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

8.5 copy ftp

Use this command to download the file from the server to the device through FTP Client.
copy ftp://*username:password@dest-address* [/*remote-directory*] / *remote-file*
flash:[*local-directory*/] *local-file*]

Parameter Description

Parameter	Description
username	The username for logging into FTP Server. It is limited to 40 bytes and must not contain ":", "@", "/" and space, neither can it be omitted.
password	The password for logging into FTP Server. It is limited to 32 bytes and must not contain ":", "@", "/" and space, neither can it be omitted.
dest-address	IP address of the target FTP Server.
remote-directory	File directory of FTP Server. It is optional and limited to 255 bytes. No space or Chinese character is supported. If left blank, it implies the current directory of FTP server.
remote-file	Filename on the remote server. It is limited to 255 bytes and doesn't support space or Chinese character.
local-directory	Directory of local folder (optional). If this directory is specified, this directory must have been created beforehand. This command doesn't support automatic directory creation. If left blank, it implies the current directory on the local device. It is limited to 255 bytes and doesn't support space or Chinese characters.
local-file	Filename on the local device. It is limited to 255 bytes and doesn't support space or Chinese character.

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide N/A

Configuration Examples The following example uses username of "user" and password of "pass" to download a file named "remote-file" from the directory "root" on FTP Server with IP address 192.168.23.69 to directory "home" on the local device, and changes the name to "local-file".

```
Ruijie# copy ftp://user:pass@192.168.23.69/root/remote-file
flash:home/local-file
```

The following example uploads a file named “local file” from the directory "home" on the local device to the directory "root" on FTP Server, and changes the name to “remote-file”.

```
Ruijie# copy flash:home/local-file
ftp://user:pass@192.168.23.69/root/remote-file
```

Related Commands

Command	Description
copy tftp	Uses the TFTP protocol to transfer files.

Platform Description N/A

8.6 copy flash

Use this command to upload the file from the server to the device through FTP Client.

copy flash:[*local-directory/*] *local-file* **ftp:**//*username:password@dest-address* [/*remote-directory*] / *remote-file*

Parameter Description

Parameter	Description
username	The username for logging into FTP Server. It is limited to 40 bytes and must not contain ":", "@", "/" and space, neither can it be omitted.
password	The password for logging into FTP Server. It is limited to 32 bytes and must not contain ":", "@", "/" and space, neither can it be omitted.
dest-address	IP address of the target FTP Server.
remote-directory	File directory of FTP Server. It is optional and limited to 255 bytes. No space or Chinese character is supported. If left blank, it implies the current directory of FTP server.
remote-file	Filename on the remote server. It is limited to 255 bytes and doesn't support space or Chinese character.
local-directory	Directory of local folder (optional). If this directory is specified, this directory must have been created beforehand. This command doesn't support automatic directory creation. If left blank, it implies the current directory on the local device. It is limited to 255 bytes and doesn't support space or Chinese characters.
local-file	Filename on the local device. It is limited to 255 bytes and doesn't support space or Chinese character.

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide N/A

Configuration Examples The following example uploads the file named "local-file" in directory "home" of local device to directory "root" on the FTP Server whose user name is user, password is pass and IP address is 192.168.23.69, and changes the filename to "remote-file".

```
Ruijie# copy flash:home/local-file
ftp://user:pass@192.168.23.69/root/remote-file
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

9 Tunnel Commands

9.1 keepalive

Use this command to enable the keepalive function and configure the keepalive packet sending interval and retransmission times.

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

keepalive[*seconds* [*retries*]]

nokeepalive

Parameter Description

Parameter	Description
seconds	Sets the interval at which keepalive packets are sent, in the range from 1 to 32,767 in the unit of seconds. The default is 10 seconds.
retries	Sets the keepalive packet transmission times, in the range from 1 to 255. The default is 3. If no response is received after the specified times, the protocol is switched to down.

Defaults This function is disabled by default.

Command Mode Interface configuration mode

Usage Guide This command is used to detect the reachability of the tunnel interface in case that the tunnel packets cannot be sent to the peer end while the physical interface is UP.

Configuration Examples The following example creates a tunnel interface.

```
Ruijie(config)# interface tunnel 1
```

The following example configures the tunnel mode.

```
Ruijie(config-if)# tunnel mode ipv6ip
```

The following example enables the keepalive function.

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

Related Commands

Command	Description
N/A	N/A

Platform Description

9.2 show interfaces tunnel

Use this command to display the tunnel configuration.

show interfaces tunnel [*number*]

Parameter Description

Parameter	Description
number	Specifies the tunnel number.

Defaults N/A

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

Usage Guide N/A

Configuration Examples The following example displays tunnel 1 information.

```
Ruijie#showinterfaces tunnel 1
// Here is the public information about the interface
Tunnel source 1.1.1.2, destination 1.1.1.1, routeable
  Tunnel TOS/Traffic Class not set, Tunnel TTL 254
  Tunnel config nested limit is 0, current nested number is 0
  Tunnel protocol/transport is ipv6ip
  Tunnel transport VPN is no set
```

Field Description

Field	Description
Destination	The tunnel destination address. The address 0.0.0.0 indicates that the destination address is not configured.
Tunnel source	The tunnel source address, which can be either an IPv4 or an IPv6 address. If the **tunnel source interface**command is configured, the tunnel source address is the interface address.
Tunnel TTL	The TTL or hop limit field of the transmission protocol.
Tunnel TOS	The TOS or traffic class field of the transmission protocol. Note that there is an exception. If the field is 0, and the transmission protocol is the same as the payload protocol, the field of the payload protocol is copied to the transmission protocol.
Tunnel nested-limit	The limit to the number of tunnel nested encapsulation times. This filed is displayed by all tunnels except the 6to4, 6rd and isatap tunnels.
Tunnel protocol/transport	Tunnel encapsulation mode
Key	With the key setting, this field is displayed by only the GRE tunnel.

Checksuming	With the checksum setting, this filed is displayed by only the GRE tunnel.
Tunnel VPN	The destination VRF.

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

9.3 show tunnel statistics

Use this command to display the number of configurable tunnel interfaces and configured tunnel interfaces.

show tunnel statistics

Parameter Description

Parameter	Description
N/A	N/A

Defaults N/A

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

Usage Guide This command is used to display the number of configurable tunnel interfaces and configured tunnel interfaces.

Configuration Examples The following example displays the number of configurable tunnel interfaces and configured tunnel interfaces.

```
Ruijie#show tunnel statistics
used: 2,  limit: 1000
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

9.4 tunnel checksum

Use this command to enable data integrity check on the tunnel interface.

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

tunnel checksum

no tunnel checksum

Parameter Description

Parameter	Description
N/A	N/A

Defaults

This function is disabled by default.

Command Mode

Interface configuration mode

Usage Guide

This command is applied on the Generic Route Encapsulation (GRE) interfaces. Some encapsulation protocols add media-attached checksum to the end of packets. The data integrity check should be performed on the tunnel interface as well and the damaged packets are discarded directly.

Configuration Examples

The following example creates the tunnel interface.

```
Ruijie(config)# interface tunnel 1
```

The following example configures the tunnel mode.

```
Ruijie(config-if)# tunnel mode gre ip
```

The following example enables data integrity check.

```
Ruijie(config-if)# tunnel checksum
```

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

9.5 tunnel destination

Use this command to specify the destination IP address of a tunnel interface in interface configuration mode.

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

tunnel destination*ip-address*

no tunnel destination

Parameter

Parameter	Description

Description		
	ip-address	Sets the IP address of the specified tunnel destination.

Defaults No destination IP address is set by default.

Command Mode Interface configuration mode

Usage Guide This command must be used to specify the peer address during tunnel setup. Tunnels cannot be set up if this command is not executed.

Configuration Examples The following example creates a tunnel interface.

```
Ruijie(config)# interface tunnel 1
```

The following example configures the tunnel mode.

```
Ruijie(config-if)# tunnel mode gre ip
```

The following example sets the destination IP address of tunnel interface.

```
Ruijie(config-if)# tunnel destination 61.154.101.3
```

Related Commands

Command	Description
show interface tunnel	Displays tunnel interface information.

Platform Description N/A

9.6 tunnel key

Use this command to set the security key on a tunnel interface. The value of the tunnel keyword is an integer. Use the **no** form of this command to restore the default setting.

tunnel key *value*

no tunnel key

Parameter Description

Parameter	Description
value	Tunnel key value, in the range from 0 to 2,147,483,647.

Defaults No key configuration is setby default.

Command Mode Interface configuration mode

Usage Guide Without key protection, illegal intrusion or packet attack may occur during tunnel setup. This

command takes effect only when the GRE is encapsulated.

Configuration Examples

The following example creates a tunnel interface.

```
Ruijie(config)# interface tunnel 1
```

The following example configures the tunnel mode.

```
Ruijie(config-if)# tunnel mode gre ip
```

The following example sets the key of tunnel interface.

```
Ruijie(config-if)# tunnel key 1234
```

Related Commands

Command	Description
show interface tunnel	Displays tunnel interface information.

Platform Description

N/A

9.7 tunnel mode

Use this command to set the encapsulation mode on a tunnel interface.

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

tunnel mode { **gre ip | ipv6ip** [**6to4 | isatap**] }

no tunnel mode

default tunnel mode

Parameter Description

Parameter	Description
gre ip	The transmission network is IPv4 network, and GRE for the route is at the IP layer.
ipv6ip	The transmission network is IPv4 network, and GRE for the route is not at the IP layer. The user network is manually configured IPv6 network. The IPv4 address of the peer end needs to be configured.
ipv6ip 6to4	The transmission network is IPv4 network, and GRE for the route is not at the IP layer. The user network is IPv6 network. The IPv4 address of the peer end does not need to be configured. It is used for connection between IPv6 networks.
ipv6ip isatap	The transmission network is IPv4 network, and GRE for the route is not at the IP layer. The user network is IPv6 network. The IPv4 address of the peer end does not need to be configured. It is used for quick deployment of IPv6 networks.

Defaults **ipv6ip**.

Command Mode Interface configuration mode

Usage Guide The tunnel encapsulation format is the tunnel carrier protocol. The default encapsulation format of tunnel interfaces is GRE. You can determine the encapsulation format of tunnel interfaces based on the actual usage. By default, IP tunnel GRE can be implemented without any definition of the encapsulation format.

Configuration Examples The following example creates a tunnel interface.

```
Ruijie(config)# interface tunnel 1
```

The following example configures the tunnel mode.

```
Ruijie(config-if-Tunnel 1)# tunnel mode ipv6ip
```

Related Commands

Command	Description
show interface tunnel	Displays tunnel interface information.

Platform Description N/A

9.8 tunnel nested-limit

Use this command to set the maximum number of nested encapsulation layers on a tunnel interface.Use the **no** form of this command to restore the default setting.

tunnel nested-limit *num*

no tunnel nested-limit

Parameter Description

Parameter	Description
num	Maximum number of nested encapsulation layers on a tunnel interface, in the range from 0 to 10

Defaults The default is 4.

Command Mode Tunnel interface configuration mode

Usage Guide Tunnel nested encapsulation indicates that packets are sent after multiple-layer tunnel encapsulation on the local device. The route change on the local device may lead to unlimited tunnel nested encapsulation, which causes continuous fragmentation and re-combination on routers and has serious performance impact. RGOS can automatically prevent unlimited nested encapsulation. The

maximum number of nested encapsulation layers is four by default. You can use this command to change the default value at the inner layer of a tunnel interface.

Configuration Examples

The following example creates a tunnel interface.

```
Ruijie(config)# interface tunnel 1
```

The following example configures the tunnel mode.

```
Ruijie(config-if-Tunnel 1)# tunnel mode ipv6ip
```

The following example sets the maximum number of GRE nested encapsulation layers to five.

```
Ruijie(config-if)# tunnel nested-limit 5
```

Related Commands

Command	Description
show interface tunnel	Displays tunnel interface information.

Platform Description

N/A

9.9 tunnel path-mtu-discovery

Use this command to enable the PMTUD function for the tunnel.

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

tunnel path-mtu-discovery [**age-timer**{*aging-mins* | **infinite** } | **min-mtu***mtu-bytes*]

notunnel path-mtu-discovery

Parameter Description

Parameter	Description
aging-mins	(Optional) Sets MTU aging time, in the range from 1 to 30 in the unit of minutes. The default is 10. Infinite indicates no aging.
mtu-bytes	(Optional) Sets the minimum MTU size, in the range from 92 to65,535 in the unit of bytes. The default is 92.

Defaults

This function is disabled by default.

Command Mode

Interface configuration mode

Usage Guide

This command is used to detect the Path MTU of the peer end automatically and modify the MTU of the tunnel interface accordingly, avoiding packet fragmentation.

If you run the **showinterfacetunnel** command, one of the following three states is displayed:

```
PathMTUDiscoverystate:init
PathMTUDiscoverystate:keep
PathMTUDiscoverystate:learning
```

When the command is just configured, the state is init.
When the probe packets are sent for learning, the state is learning and learning packets are sent.
When the MTU does not change after five probe packets are sent consecutively, the state turns to keep and keep packets are sent.

Configuration Examples

The following example creates the tunnel interface.

```
Ruijie(config)# interface tunnel 1
```

The following example configured the tunnel mode.

```
Ruijie(config-if)# tunnel mode gre ip
```

The following example enables the PMTUD function.

```
Ruijie(config-if)# tunnel path-mtu-discovery
```

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

9.10 tunnel source

Use this command to configure the source IP address for the tunnel.
Use the **no** form of this command to restore the default setting.
tunnel source { *ip-address* **|** *interface-type interface-number* **}**
no tunnel source

Parameter Description

Parameter	Description
ip-address	Source IP address of the tunnel used as the source IP address of the packets to be transmitted through the tunnel.
interface-type interface-number	Interface referenced by the tunnel, which will be used as the source IP address of the packets to be transmitted through the tunnel.

Defaults

No tunnel source address is configured by default.

Command Mode

Interface configuration mode.

Usage Guide

The source IP address of a tunnel can be a specified IP address or an IP address of an interface.
When you configure an auto tunnel (for example, 6to4 and isatap), it is recommended to specify the source address.
A device shall not be configured multiple tunnels with the same encapsulation type, source address and destination address.
If there are multiple auto tunnels, their source addresses shall be different.

Configuration Examples The following example creates a tunnel interface.

```
Ruijie(config)# interface tunnel 1
```

The following example configures the tunnel mode.

```
Ruijie(config-if-Tunnel 1)# tunnel mode ipv6ip
```

The following example configures an IPv6 manual tunnel.

```
Ruijie(config-if)# tunnel source 1.1.1.1
```

Related Commands

Command	Description
tunnel mode	Configures the mode of a tunnel.
tunnel destination	Configures the destination address of a tunnel.
Tunnel ttl	Configures the TTL of the tunnel.

Platform Description N/A

9.11 tunnel tos

Use this command to set the IPv4 ToS byte or IPv6 traffic class 8 bits fin tunnel intefface configruation mode. Use the **no** form of this command to restore the default setting.

tunnel tos *number*

no tunnel tos

Parameter Description

Parameter	Description
number	IPv4 ToS byte or IPv6 traffic class 8 bits, in the range from 0 to 255.

Defaults By default, the inner-layer IPv4 ToS byte is copied to the outer-layer IPv4 header, if both the inner-layer carrier and the outer-layer encapsulation on a tunnel interface use the IPv4 protocol. By default, the inner-layer IPv6 traffic class 8 bits are copied to the outer-layer IPv6 header if both the inner-layer carrier and the outer-layer encapsulation on a tunnel interface use the Ipv6 protocol. In other circumstances, the outer-layer IPv4 ToS and IPv6 traffic class are 0.

Command Mode Interface configuration mode

Usage Guide This command is used to set GRE tunnel packets to a higher priority.

Configuration Examples The following example sets the ToS byte for a GRE tunnel outer-layer encapsulation protocol to 20 on interface tunnel 1.

```
Ruijie(config)# interface tunnel 1
Ruijie(config-if)# tunnel mode ipv6ip
Ruijie(config-if)# tunnel tos 20
```

Related Commands	Command	Description
	show interface tunnel	Displays tunnel interface information.

Platform Description N/A

9.12 tunnel ttl

Use this command to specify the TTL value of the IPv4 header in the encapsulated IPv6 messages.
Use the**no** form of this command to restore the default setting.
tunnel ttl*hop-count*
no tunnel ttl

Parameter Description	Parameter	Description
	hop-count	TTL value ranging from 1 to 254.

Defaults The default is 254.

Command Mode Interface configuration mode

Usage Guide This command is used to specify the TTL value of the IPv4 header in the encapsulated IPv6 messages.

Configuration Examples The following example creates a tunnel interface.

```
Ruijie(config)# interface tunnel 1
```

The following example configures the tunnel mode.

```
Ruijie(config-if-Tunnel 1)# tunnel mode ipv6ip
```

The following example sets the TTL value to 100.

```
Ruijie(config-if)# tunnel ttl 100
```

Related Commands	Command	Description
	tunnel mode	Configures the mode of a tunnel.
	tunnel source	Configures the source IP address of the tunnel.
	tunnel destination	Configures the destination IP address of a tunnel.

Platform Description N/A

9.13 tunnel vrf

Use this command to configure the VRF to which the outer-layer addresses of a tunnel belong. The VRF routing table is used to forward packets to the tunnel interface.

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

tunnel vrf *vrf-name*

no tunnel vrf

Parameter Description

Parameter	Description
vrf-name	Name of the tunnel out-layer VRF.

Defaults The outer-layer source and destination addresses of a tunnel are global addresses.

Command Mode Interface configuration mode

Usage Guide The outer-layer source and destination addresses of a tunnel must be in a VRF. If the specified VRF does not include a route to the destination address, the tunnel interface is down.

Configuration Examples The following example creates a tunnel interface.

```
Ruijie(config)# interface tunnel 1
```

The following example configures the tunnel mode.

```
Ruijie(config-if-Tunnel 1)# tunnel mode ipv6ip
```

The following example sets the outer-layer VRF of a manually IPv6 over IPv4 tunnel.

```
Ruijie(config-if)# tunnel vrf VPN1
```

Related Commands

Command	Description
tunnel mode	Configures the mode of a tunnel.
ip vrf	Configures an IPv4 VRF.
tunnel source	Configures the source IP address of the tunnel.
tunnel destination	Configures the destination IP address of a tunnel.

Platform Description N/A

10 Network Connectivity Test Tool Commands

10.1 clear rping table all

Use this command to clear Rping entries.

clear rping table [**all |** [**ping-object** *owner test-name*] | [**trace-object** *owner test-name*]]

Parameter Description

Parameter	Description
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

10.2 ping

Use this command to test the connectivity of a network to locate the network connectivity problem. The command format is as follows:

ping [**oob** | **ip**] [*address* [**via** *mgmt-name*] [**length** *length*] [**ntimes** *times*] [**timeout** *seconds*] [**data** *data*] [**source** *source*] [**df-bit**] [**validate**] [**detail**] [**interval** millisecond] [**out-interface** interface]

Parameter Description

Parameter	Description

oob	Enables the out-band channel. It must be set when MGMT is specified as the source port.
via	If a device supports multiple MGMT ports, that is, multiple MGMT ports are displayed in the **show interface brief** command output, you are advised to add **via mgmt xxx** to the ping command. This command is supported only on devices with MGMT ports.
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.
next-hop	Specifies the next hop IPv4 address
millisecond	Specifies the ping interval, in the range from 50 to 300，000 milliseconds. Default: 100 milliseconds.

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

Command 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

10.3 ping ipv6

Use this command to test the connectivity of a network to locate the network connectivity problem. The command format is as follows:
ping [**oob** | **ipv6**] [*ip-address* [**via** *mgmt-name*] [**length** *length*] [**ntimes** *times*] [**timeout** *seconds*] [**data** *data*] [**source** *source*] [**detail**] [**interval** millisecond] [**out-interface** interface]

Parameter Description

Parameter	Description
oob	Enables the out-band channel. It must be set when MGMT is specified as the source port.
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.
interface	Specifies the outbound interface
millisecond	Specifies the ping interval, in the range from 10 to 300000 milliseconds. Default: 100 milliseconds.

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

Command Privileged EXEC mode: enables extended functions.

Mode 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

10.4 show rping detail

Use this command to display Rping information.

show rping detail

Parameter Description

Parameter	Description
N/A	N/A

Defaults N/A

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

Usage Guide This command is used to display the Rping information such as numbers of test accounts and users.

Configuration Examples The following example displays Rping information.

```
Ruijie#show rping detail
Total owner number: 2
Total test number: 4
owner: user1
  test name: taget_1       storage type: volatile
test name: taget_2       storage type: nonVolatile
owner: user2
  test name: taget_1       storage type: permanent
```

```
test name: taget_2        storage type: readOnly
```

Field	Description
Total owner number	The number of users
Total test number	The number of Rping accounts
owner	Username
test name	Test name
storage type	Storage type

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

10.5 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 The following is two examples of the application bout traceroute, the one is of the smooth network,

Examples and the other is the network in which some gateways aren't connected successfully.

1. When the network is connected smoothly:

```
Ruijie# traceroute 61.154.22.36
  < press Ctrl+C to break >
Tracing the route to 61.154.22.36

1     192.168.12.1      0 msec   0 msec   0 msec
2     192.168.9.2       4 msec   4 msec   4 msec
3     192.168.9.1       8 msec   8 msec   4 msec
4      192.168.0.10     4 msec   28 msec  12 msec
5      192.168.9.2      4 msec   4 msec   4 msec
6      202.101.143.154      12 msec  8 msec   24 msec
7      61.154.22.36     12 msec  8 msec   22 msec
```

From above result, it's clear to know that the gateways passed by the packets sent to the host with an IP address of 61.154.22.36 (gateways 1~6) and the spent time are displayed. Such information is helpful for network analysis.

2. When some gateways in the network fail:

```
Ruijie# traceroute 202.108.37.42
  < press Ctrl+C to break >
Tracing the route to 202.108.37.42

1     192.168.12.1      0 msec    0 msec  0 msec
2     192.168.9.2       0 msec    4 msec  4 msec
3     192.168.110.1     16 msec  12 msec  16 msec
4     *  *  *
5     61.154.8.129      12 msec   28 msec  12 msec
6     61.154.8.17       8 msec    12 msec  16 msec
7     61.154.8.250      12 msec   12 msec  12 msec
8     218.85.157.222    12 msec   12 msec  12 msec
9      218.85.157.130   16 msec   16 msec  16 msec
10     218.85.157.77    16 msec   48 msec  16 msec
11     202.97.40.65     76 msec   24 msec  24 msec
12     202.97.37.65     32 msec   24 msec  24 msec
13     202.97.38.162    52 msec   52 msec  224 msec
14     202.96.12.38     84 msec   52 msec  52 msec
15     202.106.192.226  88 msec   52 msec  52 msec
16     202.106.192.174      52 msec   52 msec  88 msec
17     210.74.176.158   100 msec  52 msec  84 msec
18     202.108.37.42    48 msec   48 msec  52 msec
```

The above result clearly shown that the gateways passed by the packets sent to the host with an IP address of 202.108.37.42 (gateways 1~17) and the spent time are displayed, and gateway 4 fails.

```
Ruijie# traceroute www.ietf.org

Translating "www.ietf.org"...[OK]
```

```
 < press Ctrl+C to break >
Tracing the route to 64.170.98.32

1     192.168.217.1    0 msec  0 msec  0 msec
2     10.10.25.1       0 msec  0 msec  0 msec
3     10.10.24.1       0 msec  0 msec  0 msec
4     10.10.30.1       10 msec 0 msec  0 msec
5     218.5.3.254      0 msec  0 msec  0 msec
6     61.154.8.49      10 msec 0 msec  0 msec
7     202.109.204.210  0 msec  0 msec  0 msec
8     202.97.41.69     20 msec 10 msec 20 msec
9     202.97.34.65     40 msec 40 msec 50 msec
10    202.97.57.222    50 msec 40 msec 40 msec
11    219.141.130.122  40 msec 50 msec 40 msec
12    219.142.11.10    40 msec 50 msec 30 msec
13    211.157.37.14    50 msec 40 msec 50 msec
14    222.35.65.1      40 msec 50 msec 40 msec
15    222.35.65.18     40 msec 40 msec 40 msec
16    222.35.15.109    50 msec 50 msec 50 msec
17    *      *      *
18    64.170.98.32    40 msec 40 msec 40 msec
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

10.6 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

11 TCP Commands

11.1 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

11.2 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.

11.3 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.

11.4 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.

11.5 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.

11.6 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.

11.7 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.

11.8 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

11.9 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.

11.10 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.

11.11 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

11.12 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

11.13 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: CLOSED: The connection has been closed. LISTEN: Listening state SYNSENT: In the three-way handshake phase when the SYN packet has been sent out. SYNRCVD: In the three-way handshake phase when the SYN packet has been received. ESTABLISHED: The connection has been established. FINWAIT1: The local end has sent the FIN packet. FINWAIT2: The FIN packet sent by the local end has been acknowledged. CLOSEWAIT: The local end has received the FIN packet from the peer end. LASTACK: The local end has received the FIN packet from the peer end, and then sent its own FIN packet. CLOSING: The local end has sent the FIN packet from the peer end, and received the FIN packet from the peer end before the ACK packet for the peer end to respond with this FIN packet is received. TIMEWAIT: The FIN packet sent by the local end has been acknowledged, and the local end has also acknowledged the FIN packet.
Process Name	Process name

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

11.14 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: CLOSED: The connection has been closed. LISTEN: Listening state SYNSENT: In the three-way handshake phase when the SYN packet has been sent out. SYNRCVD: In the three-way handshake phase when the SYN

	packet has been received. ESTABLISHED: The connection has been established. FINWAIT1: The local end has sent the FIN packet. FINWAIT2: The FIN packet sent by the local end has been acknowledged. CLOSEWAIT: The local end has received the FIN packet from the peer end. LASTACK: The local end has received the FIN packet from the peer end, and then sent its own FIN packet. CLOSING: The local end has sent the FIN packet from the peer end, and received the FIN packet from the peer end before the ACK packet for the peer end to respond with this FIN packet is received. TIMEWAIT: The FIN packet sent by the local end has been acknowledged, and the local end has also acknowledged the FIN packet.
Process name	Process name.

The following example displays the current IPv4 TCP connection statistics.

```
Ruijie#show tcp connect statistics
State         Count
-----      -----
ESTABLISHED 1
SYN_SENT     0
SYN_RECV     0
FIN_WAIT1    0
FIN_WAIT2    0
TIME_WAIT    0
CLOSED        0
CLOSE_WAIT   0
LAST_ACK     0
LISTEN        1
CLOSING       0
Total: 2
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

11.15 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

11.16 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: CLOSED: The connection has been closed. LISTEN: Listening state SYNSENT: In the three-way handshake phase when the SYN packet has been sent. SYNRCVD: In the three-way handshake phase when the SYN packet has been received. ESTABLISHED: The connection has been established. FINWAIT1: The local end has sent the FIN packet. FINWAIT2: The FIN packet sent by the local end has been

	acknowledged. CLOSEWAIT: The local end has received the FIN packet from the peer end. LASTACK: The local end has received the FIN packet from the peer end, and then sent its own FIN packet. CLOSING: The local end has sent the FIN packet from the peer end, and received the FIN packet from the peer end before the ACK packet for the peer end to respond with this FIN packet is received. TIMEWAIT: The FIN packet sent by the local end has been acknowledged, and the local end has also acknowledged the FIN packet.

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

12 IPv4/IPv6 REF Commands

12.1 clear ip ref packet statistics

Use this command to clear IPv4 Ruijie Express Forwarding (REF) packet statistics.

clear ip ref packet statistics

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

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide N/A

Configuration Examples The following example clears IPv4 REF packet statistics.

```
Ruijie #clear ip ref packet statistics
```

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

Platform Description N/A

12.2 clear ipv6 ref packet statistics

Use this command to clear IPv6 REF packet statistics.

clear ipv6 ref packet statistics

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

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide N/A

Configuration Examples The following example clears IPv6 REF packet statistics.

```
Ruijie #clear ipv6 ref packet statistics
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

12.3 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

12.4 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.

12.5 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: Unresolved Resolved
type	Adjacent node type Local: local adjacency Forward: forward adjacency Discard: discard adjacency Glean: glean adjacency Mcast: multicast adjacency
rfct	Reference count of the adjacent node
chg	Whether the adjacent node is on the changing link.
ip	IP address of the adjacent node
interface	Interface
linklayer	Layer 2 head

Related Commands	Command	Description
	show ip ref route	Displays all route information in the current REF module.

Platform Description N/A

12.6 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: Unresolved Resolved

type	Adjacency type Local: local adjacency Forward: forward adjacency Discard: discard adjacency Glean: glean adjacency Mcast: multicast adjacency
rfct	Reference count of the adjacency
chg	Whether the adjacency is on the changing link.
ip	Adjacency IP address
interface	Interface
linklayer	Layer 2 head

Related Commands

Command	Description
show ip ref route	Displays all routing information in the current REF module.

Platform Description N/A

12.7 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

12.8 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 res: resolved
flags	0: related to adjacency 1: unrelated to adjacency
interface	Interface

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

12.9 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

12.10 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: Unresolved Resolved
type	Adjacent node type Local: local adjacency Forward: forward adjacency Discard: discard adjacency Glean: glean adjacency Mcast: multicast adjacency
rfct	Reference count of the adjacent node
chg	Whether the adjacent node is on the changing link.
ip	IP address of the adjacent node
interface	Interface
linklayer	Layer 2 head

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

12.11 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: Unresolved Resolved
type	Adjacent node type Local: local adjacency Forward: forward adjacency Discard: discard adjacency Glean: glean adjacency Mcast: multicast adjacency
rfct	Reference count of the adjacent node
chg	Whether the adjacent node is on the changing link.
ip	IP address of the adjacent node
interface	Interface
linklayer	Layer 2 head

Related Commands

Command	Description
N/A	N/A

Platform N/A

Description

12.12 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

12.13 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 res: resolved
flags	0: related to adjacency 1: unrelated to adjacency
interface	Interface

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

12.14 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 This command is used to display all routing information in the IPv6 REF table. 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

13 TFTP Server Commands

13.1 tftp-server enable

Use this command to enable the TFTP server.
Use the **no** form of this command to disable the TFTP server.
tftp-server enable
no tftp-server enable

Parameter Description

Parameter	Description
N/A	N/A

Defaults The TFTP server is disabled by default.

Command Modes Global configuration mode

Usage Guide Only with the TFTP server enabled and the top directory configured meanwhile, TFTP clients are able to upload or download files.

Configuration Examples The following example enables the TFTP server and sets the top directory of the TFTP server to **/syslog**.

```
Ruijie(config)# tftp-server topdir /syslog
Ruijie(config)# tftp-server enable
```

The following example disables the TFTP server.

```
Ruijie(config)# no tftp-server enable
```

Platform Description N/A

13.2 tftp-server topdir

Use this command to configure the top directory for TFTP clients.
Use the **no** or **default** form of this command to restore the default setting.
tftp-server topdir *directory*
no tftp-server topdir
default tftp-server topdir

Parameter Description

Parameter	Description
directory	The top directory for TFTP clients to access. "/" means the root directory.

Defaults The top directory is **flash**:.

Command Modes Global configuration mode

Usage Guide The top directory on the TFTP server defines what files and folders the client is able to access. And the client cannot access the TFTP server before a top directory is correctly configured for the server.

Configuration Examples The following example enables the TFTP servicer and sets the top directory for TFTP clients to **/syslog**.

```
Ruijie(config)# tftp-server topdir /syslog
Ruijie(config)# tftp-server enable
```

The following example restores the default top directory.

```
Ruijie(config)# no tftp-server topdir
```

Platform Description N/A

13.3 show tftp-server

Use this command to display the configuration of the TFTP server.

show tftp-server

Parameter Description

Parameter	Description
N/A	N/A

Defaults N/A

Command Modes Global configuration mode/Privileged configuration mode/Interface configuration mode

Usage Guide N/A

Configuration Examples The following example displays the progress of downloading the TFTP client.

```
Ruijie# show tftp-server

    tftp-server information

================================

enable : Y

topdir : flash:/
```

Platform N/A

Description

13.4 show tftp-server updating-list

Use this command to display the progress of downloading the TFTP client.

show tftp-server updating-list

Parameter Description

Parameter	Description
N/A	N/A

Defaults N/A

Command Modes Global configuration mode/Privileged configuration mode/Interface configuration mode

Usage Guide This command is supported only on AM5528 products.

Configuration Examples The following example displays the progress of downloading the TFTP client.

```
Ruijie# show  tftp-server updating-list
IP Address            Interface             File Name               TX
Elapsed
----------------------  ----------------------  ------------------------
----------  --------
171.208.208.2         GigabitEthernet 0/7    main_map552.bin
```

Platform Description N/A

14 NAT Commands

14.1 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. 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

14.2 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

14.3 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

14.4 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

14.5 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. 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

14.6 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

14.7 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

14.8 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

14.9 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

14.10 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

15 Proxy ARP Commands

15.1 clear proxy_arp

Use this command to clear a specified proxy ARP entry or all proxy ARP entries.
clear proxy-arp [*ip-address vlan-id*]

Parameter Description

Parameter	Description
ip-address	Specifies the IP address of the proxy ARP entry. By default, all proxy ARP entries are cleared.
vlan-id	VLAN ID. The range is from 1 to 4094.

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide When the MAC address of the gateway is changed, you can clear the proxy ARP entry of the gateway to enable the device to learn the correct proxy ARP entry of the gateway as quickly as possible.

Configuration Examples The following example clears all proxy ARP entries.

```
Ruijie# clear proxy_arp
```

The following example clears a specified proxy ARP entry.

```
Ruijie# clear proxy_arp 1.1.1.1 1
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

15.2 proxy_arp enable

Use this command to enable Layer-2 ARP Proxy.
proxy_arp enable

Use the **no** form of this command to disable Layer-2 ARP Proxy.
no proxy_arp enable

Parameter Description

Parameter	Description
N/A	N/A

Defaults By default, Layer-2 ARP Proxy is enabled.

Command Mode Global configuration mode

Usage Guide N/A

Configuration Examples The following example disables Layer-2 ARP Proxy.

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

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

15.3 proxy_arp drop wlan-ip

Use this command to drop ARP packets from WLAN (namely, CTI ports) and the source IP address of these packets is *ip_address*.
proxy_arp drop wlan-ip *ip-address*

Use the **no** form of this command to remove the configuration that drops ARP packets whose source IP address is *ip_address*.
no proxy_arp drop wlan-ip *ip-address*

Parameter Description

Parameter	Description
ip-address	Source IP address of ARP packets to be dropped.

Defaults By default, no ARP packets from WLAN are dropped.

Command Mode Global configuration mode

Usage Guide N/A

Configuration Examples The following example drops ARP packets from WLAN with their source IP address being 192.168.1.1.

```
Ruijie(config)# proxy_arp drop wlan-ip 192.168.1.1
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

15.4 proxy-arp learn only-wlan

Use this command to enable ARP proxy to learn ARP packets only from wireless ports as well as wired ports with excluded IP addresses. Use the **no** form of this command to restore the default setting.

proxy-arp learn only-wlan [**except** *ip_address*]

no proxy_arp drop wlan-ip

Parameter Description

Parameter	Description
ip-address	IP addresses of excluded wired ports.

Defaults By default, this function is disabled.

Command Mode Global configuration mode

Usage Guide The feature can be enabled when both the following conditions are met:

- The AC is in centralized forwarding mode.
- The AC is connected with a gateway. SuperVLAN and subVLANs are deployed on the gateway.

ARP Proxy entries are easily used up due to a large number of users (run the **show proxy-arp statistics** command to display the ARP Proxy statistics).

Configuration Examples The following example learns ARP packets only from wireless ports as well as wired ports with the IP addresses of 192.168.21.1 and 192.168.22.1.

```
Ruijie(config)# proxy-arp learn only-wlan except 192.168.21.1
Ruijie(config)# proxy-arp learn only-wlan except 192.168.22.1
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

15.5 show proxy_arp

Use this command to display all proxy ARP entries.

show proxy_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 all proxy ARP entries.

```
Ruijie# show proxy_arp
total entry:2
ip               vid    mac             interface         type
----------------   ----   ----------------  -------------     ----
192.168.195.68     1      0013.20a5.7a5f    Gi0/1             DYNAMIC
192.168.195.69     2      0013.20a5.7a51    Gi0/2             DYNAMIC
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

15.6 show proxy_arp dynamic

Use this command to display the dynamic proxy ARP entry.

show proxy_arp dynamic

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 dynamic proxy ARP entry.

```
Ruijie# show proxy_arp dynamic
ip               mac             type
---------------    ---------------  ----
192.168.195.68     0013.20a5.7a5f    DYNAMIC
192.168.195.69     0013.20a5.7a51    DYNAMIC
total entry: 2
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

15.7 show proxy_arp statistics

Use this command to display statistics about the proxy ARP entry.

show proxy_arp statistics

Parameter Description

Parameter	Description
N/A	N/A

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide You can use this command to display statistics about the proxy ARP entry, such as: total proxy ARP entries, next aging time, dropped packet count.

Configuration Examples The following example displays statistics about the proxy ARP entry.

```
Ruijie# show proxy_arp statistics
```

```
total entry: 100
next aging time: 5 seconds
dropped packets: 0
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

IP Routing Commands

1 Protocol-independent Commands

1.1 accept-lifetime

Use this command in the encryption key configuration mode to specify the lifetime of an encryption key in its receiving direction. Use the no form of this command to restore the default value.

accept-lifetime *start-time* {**infinite** | *end-time* | **duration** *seconds*}

no accept-lifetime

Parameter description

Parameter	Description
start-time	Start time of the lifetime. The syntax is as follows:
infinite	Indicates that the encryption key is valid for ever.
end-time	*End time of the encryption key. It must be later than the start time.*
duration *seconds*	Duration of the encryption key after the start time. The value ranges from 1 to 2147483646.

Default infinite

Command mode Encryption key configuration mode

Usage guideline

Examples The following example configures the lifetime from 0:00 on September 9, 2000 to 0:00 on October 12, 2011.

```
Ruijie(config)# key chain ripkeys
Ruijie(config-keychain)# key 1
Ruijie(config-keychain-key)#accept-lifetime 00:00:00 Sep 9 2000 00:00:00 Dec 12 2011
```

Related command

Command	Description
-	-

Platform description -

1.2 ip prefix-list

Use this command to create a prefix list or add an entry to the prefix list. Use the **no** form of this

command to remove the prefix list or an entry.

ip prefix-list *prefix-list-name* [**seq** *seq-number*] { **deny** | **permit** } *ip-prefix* [**ge** *minimum-prefix-length*][**le** *maximum-prefix- length*]

no ip prefix-list *prefix-list-name* [**seq** *seq-number*] { **deny** | **permit** } *ip-prefix* [**ge** *minimum-prefix-length*][**le** *maximum-prefix- length*]

Parameter description

Parameter	Description
prefix-list-name	Name of the prefix list
seq-number	Sequence number of an entry in the range of 1 to 2147483647. When you execute this command to add an entry without a sequence number, the system allocates a default sequence number for the entry. The default sequence number of the first entry is 5. Every subsequential entry without a sequence number uses the time of 5 larger than the previous sequence number as the default sequence number.
deny	Deny the route matching the prefix list.
permit	Permit the route matching the prefix list.
ip-prefix	Network address and mask. Network address can be any valid IP address and the mask length is in the range of 0 to 32.
minimum-prefix-length	(Optional) Minimum length of the prefix (the starting length) Note: “ge” indicates the operation of “larger than” and “equivalent to”.
maximum-prefix-length	(Optional) Maximum length of the prefix (the ending length) Note: “le” indicates the operation of “less than” and “equivalent to”.

Default configuration

There is no prefix list by default.

Command mode

Global configuration mode.

Usage guidelines

The ip prefix-list command configures the prefix list, with the permit or deny keyword to determine the action in case of matching.

You can execute this command to define an exact match, or use “ge” or “le” to define a range match for a prefix for flexible configuration. “ge” indicates the range of minimum-prefix-length to 32; “le” indicates the range of the mask length of the IP prefix to maximum-prefix-length; “ge” and “le” indicates the range of minimum-prefix-length to maximum-prefix-length, namely, mask length of IP prefix < minimum-prefix-length < maximum-prefix-length <=32.

Examples

The following example filters the RIP routes the OSPF redistributes by the destination IP address

following the rule defined in the associated IP prefix list, for example, redistribute the routes whose destination IP address is in the range 201.1.1.0/24.

```
Ruijie# configure terminal
Ruijie(config)# ip prefix-list pre1 permit 201.1.1.0/24
Ruijie(config)# router ospf
Ruijie(config-router)# distribute-list prefix pre1 out rip
Ruijie(config-router)# end
```

1.3 ip prefix-list description

Use this command to add the description of a prefix list. Use the **no** form of this command to delete the description.

ip prefix-list *prefix-list-name* **description** *description-text*

no ip prefix-list *prefix-list-name* **description**

Parameter description

Parameter	Description
prefix-list-name	Name of the prefix list
description-text	Description of the prefix list

Default configuration No description is added for a prefix list, by default.

Command mode Global configuration mode

Examples The example below adds the description for the prefix list:

```
Ruijie# configure terminal
Ruijie(config)# ip prefix-list pre description Deny routes from Net-A
```

1.4 ip prefix-list sequence-number

Use this command to enable sort function for a prefix list. Use the **no** form of this command to disable the sort function.

ip prefix-list sequence-number

no ip prefix-list sequence-number

Parameter description Disabled

Default configuration No sequence number is added for a prefix list, by default.

Command mode Global configuration mode

Examples The example below adds a sequence number for the prefix list:

```
Ruijie# configure terminal
Ruijie(config)# ip prefix-list pre description deny routes from Net-A
```

Related commands

Command	Description
ip prefix-list	Configure the prefix list.

Platform description N/A

1.5 ipv6 prefix-list

Use this command to create an IPv6 prefix list or add an entry in the prefix list. Use the **no** form of this command to delete an IPv6 prefix list or an entry in the prefix list.

Ipv6 prefix-list *prefix-list-name***[seq** *seq-number***] { deny | permit}** *ipv6-prefix* **[ge** *minimum-prefix-length***][le** *maximum-prefix- length***]**

no ipv6 prefix-list *prefix-list-name***[seq** *seq-number***] { deny | permit}** *ipv6-prefix* **[ge** *minimum-prefix-length***][le** *maximum-prefix- length***]**

Parameter description

Parameter	Description
prefix-list-name	Name of the prefix list
seq-number	Sequence number of an entry in the prefix list. Its range is 1 to 4294967294. If the sequence number is not specified in this command, the system will allocate a default one for the entry. The default sequence number of the first entry is 5, and that of each subsequent one is the product of adding 5 to the sequence number of the proceeding entry.
permit	Permit the access to the matching result.
deny	Deny the access to the matching result.
ipv6-prefix	Network address and its mask. The network address can be any valid IP address. The mask can be 0 to 32 characters.
minimum-prefix-length	(Optional) Minimum length of the prefix (the starting length) “ge” indicates the operation of “larger than” and “equivalent to”.
maximum-prefix- length	(Optional) Maximum length of the prefix (the ending length) “le” indicates the operation of “less than” and “equivalent to”.

Default configuration No prefix list is created.

Command mode Global configuration mode

Usage guideline The ipv6 prefix-list command configures the prefix list, with the permit or deny keyword to determine the action in case of matching.
You can execute this command to define an exact match, or use “ge” or “le” to define a range match for a prefix for flexible configuration. “ge” indicates the range of minimum-prefix-length to 128; “le” indicates the range of the mask length of the IP prefix to maximum-prefix-length; “ge” and “le” indicates the range of minimum-prefix-length to maximum-prefix-length, namely, Ipv6-prefix mask length < minimum-prefix-length < maximum-prefix-length <= 128

Examples The following example filters the RIP routes the OSPF redistributes by the destination IP address following the rule defined in the associated IP prefix list, for example, redistribute the routes whose destination IP address is in the range 2222::/64.

```
Ruijie# configure terminal
Ruijie(config)# ipv6 prefix-list pre1 permit 2222::64
Ruijie(config)# ipv6 router ospf
Ruijie(config-router)# distribute-list prefix pre out rip
Ruijie(config-router)# end
```

1.6 ipv6 prefix-list description

Use this command to add the description of an IPv6 prefix list. Use the **no** form of this command to delete the description.
ipv6 prefix-list *prefix-lis-name* **description** *description-text*
no ipv6 prefix-list *prefix-lis-name* **description** *description-text*

Parameter description

Parameter	Description
prefix-lis-name	Name of the ipv6 prefix list
description-text	Description of the ipv6 prefix list

Default configuration No description is added for an IPv6 prefix list, by default.

Command mode Global configuration mode

Examples The example below adds the description for the prefix list:

```
Ruijie# configure terminal
Ruijie(config)# ipv6 prefix-list pre description Deny routes from Net-A
```

Related commands

Command	Description
ipv6 prefix-list	Configure the IPv6 prefix list.

1.7 ipv6 prefix-list sequence-number

Use this command to enable the sorting function for an IPv6 prefix list. Use the **no** form of this command to remove the settings.

ipv6 prefix-list sequence-number

no ipv6 prefix-list sequence-number

Parameter description Disabled.

Default configuration No sequence number is added for a prefix list, by default.

Command mode Global configuration mode

Examples The example below adds a sequence number for the prefix list:

```
Ruijie# configure terminal
Ruijie(config)# ipv6 prefix-list pre description Deny routes from Net-A
```

Related commands

Command	Description
ipv6 prefix-list	Configure the IPv6 prefix list.

1.8 key

Use this command to define an encryption key and enter the encryption key chain configuration mode. Use the no form of this command to delete it.

key *key-id*

no key *key-id*

Parameter description

Parameter	Description
key-id	Key ID, ranging from 0 to 2147483647.

Default

Command mode Encryption key chain configuration mode.

Usage

guideline

Examples The following example configures encryption key chain ripkeys and key 1.

```
Ruijie(config)# key chain ripkeys
Ruijie(config-keychain)# key 1
```

Related command	**Command**	**Description**
	-	-

Platform description **-**

1.9 key chain

Use this command to define a key chain and enter the key chain configuration mode. Use the no form of this command to delete it.

key chain *key-chain-name*

no key chain *key-chain-name*

Parameter description	**Parameter**	**Description**
	key-chain-name	Key chain name.

Default

Command mode Global configuration mode.

Usage guideline For a key chain to take effect, you need to configure at least one key.

Examples The following example configures key chain ripkeys and enters the key chain configuration mode.

```
Ruijie(config)# key chain ripkeys
```

Related command	**Command**	**Description**
	-	-

Platform description -

1.10 key-string

Use this command to specify a key string. Use the no form of this command to delete it.

key-string [**0**|**7**] *text*

no key-string

Parameter description

Parameter	Description
0	Use plaintext.
7	Use encryption.
text	Authentication string.

Default

Command mode Encryption key configuration mode.

Usage guideline

Examples The following example configures key chain ripkeys, key 1 and the key string abc:

```
Ruijie(config)# key chain ripkeys
Ruijie(config-keychain)# key 1
Ruijie(config-keychain-key)#key-string abc
```

Related command

Command	Description
-	-

Platform description -

1.11 match interface

Use **match interface** command to redistribute the routes whose next hop is the specified interface.
Use the **no** form of this command to remove the setting.
match interface *interface-type interface-number* [*…interface-type interface-number*]
no match interface *[interface-type interface-number* [*…interface-type interface-number*]]

Parameter description

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

Default configuration None.

Command mode Route map configuration mode.

Usage guidelines

This command can be followed by multiple interfaces.

You can redistribute the routes from one routing process to another routing process. For example, you can redistribute the route in the OSPF routing domain and then advertise it to the RIP routing domain, and vice versa. The mutual route redistribution can be implemented between all the IP routing protocols.

For route redistribution, route maps are usually used to control the mutual route redistribution between two routing domains.

One or more match or set commands can be executed to configure a route map. If the match command is not used, all the routes will be matched. If the set command is not used, no operation will be performed.

The route map can be configured very flexibly for route redistribution and policy-based routing. No matter how the route map is used, the configuration principle is the same, except that different command sets are used. Even if it is used on the route redistribution, different routing protocols can use different commands with the route map.

Examples

The following example redistributes the RIP route with the next hop of fastethernet 0/0 in the OSPF routing protocol.

router ospf

```
redistribute rip subnets route-map redrip
network 192.168.12.0 0.0.0.255 area 0

route-map redrip permit 10
match interface fastethernet 0/0
```

Related commands

Command	Description
match ip address	Match the address in the access list.
match ip next-hop	Match the next-hop IP address in the access list.
match ip route-source	Match the source IP address in the access list.
match metric	Match the metric.
match route-type	Match the route type.
match tag	Match the tag.
set metric	Set the metric.
set metric-type	Set the metric type.
set tag	Set the tag.

1.12 match ip address

Use **match ip address** command to redistribute the routes matching the IP address permitted by the ACL or the prefix list. Use the **no** form of this command to remove the setting.

match ip address {*access-list-number* [*access-list-number...* | *access-list-name...*] |*access-list-name* [*access-list-number...*|*access-list-name*] | **prefix-list** *prefix-list-name [prefix-list-name...*]}

no match ip address [*access-list-number* [*access-list-number...* | *access-list-name...*] |*access-list-name* [*access-list-number...*|*access-list-name*] | **prefix-list** *prefix-list-name [prefix-list-name...*]]

Parameter description

Parameter	Description
access-list-number	Number of the access list
access-list-name	Name of the access list
prefix-list *prefix-list-name*	Specify the prefix list to match.

Default configuration

None.

Command mode

Route map configuration mode.

Usage guidelines

Multiple access list numbers or names may follow match ip address.
You can redistribute the routes from one routing process to another routing process. For example, you can redistribute the route in the OSPF routing domain and then advertise it to the RIP routing domain, and vice versa. The mutual route redistribution can be implemented between all the IP routing protocols.
For route redistribution, route maps are usually used to control the mutual route redistribution between two routing domains.
One or more match or set commands can be executed to configure a route map. If the match command is not used, all the routes will be matched. If the set command is not used, no operation will be performed.
The route map can be configured very flexibly for route redistribution and policy-based routing. No matter how the route map is used, the configuration principle is the same, except that different command sets are used. Even if it is used on the route redistribution, different routing protocols can use different commands with the route map.

Examples

The following example enables the OSPF routing protocol to redistribute RIP routes that match access list 10, with the route type being type-1 external type and the default metric being 40.

```
router ospf
redistribute rip subnets route-map redrip
network 192.168.12.0 0.0.0.255 area 0

access-list 10 permit 200.168.23.0

route-map redrip permit 10
match ip address 10
set metric 40
set metric-type type-1!
```

Related commands

Command	Description
access-list	Set the access list.
match interface	Match the next-hop interface of the route.
match ip next-hop	Match the next-hop address in the access list.

match ip route-source	Match the route source address in the access list.
match metric	Match the metric.
match route-type	Match the route type.
match tag	Match the tag.
set metric	Set the metric.
set metric-type	Set the metric type.
set tag	Set the tag.

1.13 match ip next-hop

Use **match ip next-hop** command to redistribute the routes whose next-hop IP address matches the access list or the prefix list. Use the **no** form of this command to remove the setting.
match ip next-hop {*access-list-number* [*access-list-number...* | *access-list-name...*] |*access-list-name* [*access-list-number...*|*access-list-name*] | **prefix-list** *prefix-list-name [prefix-list-name...*]}
no match ip next-hop [*access-list-number* [*access-list-number...* | *access-list-name...*] |*access-list-name* [*access-list-number...*|*access-list-name*] | **prefix-list** *prefix-list-name [prefix-list-name...*]]

Parameter description

Parameter	Description
access-list-number	Number of the access list
access-list-name	Name of the access list
prefix-list *prefix-list-name*	Specify the prefix list to match.

Default configuration None.

Command mode Route map configuration mode.

Usage guidelines

Multiple access list numbers or names may follow match ip next-hop.
You can redistribute the routes from one routing process to another routing process. For example, you can redistribute the route in the OSPF routing domain and then advertise it to the RIP routing domain, and vice versa. The mutual route redistribution can be implemented between all the IP routing protocols.
For route redistribution, route maps are usually used to control the mutual route redistribution between two routing domains.
One or more match or set commands can be executed to configure a route map. If the match command is not used, all the routes will be matched. If the set command is not used, no operation will be performed.

Examples

In the example below, the OSPF routing protocol redistributes the RIP routes. As long as the next hop address of the RIP route matches the access list 10 or 20, the OSPF allows for redistribution.

```
router ospf
```

```
redistribute rip subnets route-map redrip
network 192.168.12.0 0.0.0.255 area 0

access-list 10 permit 192.168.100.1
access-list 20 permit 172.16.10.1

route-map redrip permit 10
match ip next-hop 10 20
```

Related commands

Command	Description
access-list	Set the access list.
match ip address	Match the IP address in the access list.
match interface	Match the next-hop interface of the route.
match ip route-source	Match the route source address in the access list.
match metric	Match the metric.
match route-type	Match the route type.
match tag	Match the tag.
set metric	Set the metric.
set metric-type	Set the metric type.
set tag	Set the tag.

1.14 match ip route-source

Use **match ip route-source** command to redistribute the routes whose source IP address matches the access list. Use the **no** form of this command to remove the setting.

match ip route-source {*access-list-number* [*access-list-number...* | *access-list-name...*] |*access-list-name* [*access-list-number...*|*access-list-name*] | **prefix-list** *prefix-list-name [prefix-list-name...*]}

no match ip route-source [*access-list-number* [*access-list-number...* | *access-list-name...*] |*access-list-name* [*access-list-number...*|*access-list-name*] | **prefix-list** *prefix-list-name [prefix-list-name...*]]

Parameter description

Parameter	Description
access-list-number	Number of the access list
access-list-name	Name of the access list
prefix-list *prefix-list-name*	Specify the prefix list to match.

Default configuration None.

Command mode Route map configuration mode.

Usage guidelines

Multiple access list numbers may follow match ip route-source.

You can redistribute the routes from one routing process to another routing process. For example, you can redistribute the route in the OSPF routing domain and then advertise it to the RIP routing domain, and vice versa. The mutual route redistribution can be implemented between all the IP routing protocols.

For route redistribution, route maps are usually used to control the mutual route redistribution between two routing domains.

One or more match or set commands can be executed to configure a route map. If the match command is not used, all the routes will be matched. If the set command is not used, no operation will be performed.

Examples

In the example below, the OSPF routing protocol redistributes the RIP routes. As long as the source IP address of the RIP route matches the access list 5, the OSPF allows for redistribution.

```
router ospf
redistribute rip subnets route-map redrip
network 192.168.12.0 0.0.0.255 area 0

access-list 5 permit 192.168.100.1

route-map redrip permit 10
 match ip route-source
```

Related commands

Command	Description
access-list	Set the access list.
match ip address	Match the IP address in the access list.
match interface	Match the next-hop interface of the route.
match ip next-hop	Match the next-hop IP address in the access list.
match metric	Match the metric.
match route-type	Match the route type.
match tag	Match the tag.
set metric	Set the metric.
set metric-type	Set the metric type.
set tag	Set the tag.

1.15 match ipv6 address

Use this command to redistribute the network routes permitted in the IPv6 access list or the IPv6 prefix list. Use the **no** form of this command to delete the setting.

match ipv6 address { *access-list-name*] | **prefix-list** *prefix-list-name* }

no match ipv6 address

Parameter

Parameter	Description

description	*access-list-name*	Name of the access list.
	prefix-list *prefix-list-name*	Specify the IPv6 prefix list to match.

Default configuration None

Command mode Route map configuration mode

Usage guideline

You can redistribute the routing information from one routing process to another routing process. For example, you can redistribute the route in the OSPF routing domain and then advertise it to the RIP routing domain, and vice versa. The mutual route redistribution can be implemented between all the IP routing protocols.

In the route redistribution, route maps are usually used to control the mutual route redistribution between two routing domains.

In configuring one route map, one or more match or set commands can be executed. If the match command is not used, all the routes will be matched. If the set command is not used, no operation will be performed.

The route map can be configured very flexibly to be used for route redistribution and policy-based routing. No matter how the route map is used, the configuration principle is the same, except that different command sets are used. Even if it is used on the route redistribution, different routing protocols can use different commands with the route map.

Examples

The following example enables the OSPF routing protocol to redistribute RIP routes that match access list v6acl, with the default metric being 30.

```
ipv6 router ospf
redistribute rip subnets route-map redrip
ipv6 access-list v6acl
10 permit ipv6 2620::64 any

route-map redrip permit 10
match ipv6 address v6acl
set metric 30
```

Related commands

Command	Description
ipv6 access-list	Set the IPV6 access list.
match interface	Match the next-hop interface of the route.
match ipv6 next-hop	Match the next-hop address in the IPv6 access list.
match ipvr route-source	Match the route source address in the IPv6 access list.
match metric	Match the route metric.
match route-type	Match the route type.
match tag	Match the route tag.

set metric	Set the metric for route redistribution.
set metric-type	Set the type for route redistribution.
set tag	Set the tag for route redistribution.

1.16 match ipv6 next-hop

Use this command to redistribute the network routes whose next-hop IP address matches the IPv6 access list or the IPv6 prefix list. Use the **no** form of this command to delete the setting.

match ipv6 next-hop { *access-list-name*] | **prefix-list** *prefix-list-name*}

no match ipv6 next hop

Parameter description

Parameter	Description
access-list-name	Name of the IPv6 access list.
prefix-list *prefix-list-name*	Specify the IPv6 prefix list to match.

Default configuration

None

Command mode

Route map configuration mode

Usage guideline

You can redistribute the routes from one routing process to another routing process. For example, you can redistribute the route in the OSPF routing domain and then advertise it to the RIP routing domain, and vice versa. The mutual route redistribution can be implemented between all the IP routing protocols.

For route redistribution, route maps are usually used to control the mutual route redistribution between two routing domains.

One or more match or set commands can be executed to configure a route map. If the match command is not used, all the routes will be matched. If the set command is not used, no operation will be performed.

The route map can be configured very flexibly to be used for route redistribution and policy-based routing. No matter how the route map is used, the configuration principle is the same, except that different command sets are used. Even if it is used on the route redistribution, different routing protocols can use different commands with the route map.

Examples

The following example enables the OSPF routing protocol to redistribute RIP routes that only match access list v6acl, with the default metric being 40.

```
ipv6 router ospf
redistribute rip subnets route-map redrip

ipv6 access-list v6acl
10 permit ipv6 2620::64 any
```

```
route-map redrip permit 10
match ipv6 address v6acl
set metric 40
```

Related commands

Command	Description
ipv6 access-list	Set the IPV6 access list.
match interface	Match the next-hop interface of the route.
match ipv6 address	Match the IP address in the IPv6 access list.
match ipv6 route-source	Match the route source address in the IPv6 access list.
match metric	Match the route metric.
match route-type	Match the route type.
match tag	Match the route tag.
set metric	Set the metric for route redistribution.
set metric-type	Set the type for route redistribution.
set tag	Set the tag for route redistribution.

1.17 match ipv6 route-source

Use this command to redistribute the network routes whose next-hop IP address matches the IPv6 access list or the IPv6 prefix list. Use the **no** form of this command to delete the setting.

match ipv6 route-source { *access-list-name*] | **prefix-list** *prefix-list-name* }

no match ipv6 route-source

Parameter description

Parameter	Description
access-list-name	Name of the IPv6 access list.
prefix-list *prefix-list-name*	Specify the IPv6 prefix list to match.

Default configuration None

Command mode Route map configuration mode

Usage guideline

You can redistribute the routing information from one routing process to another routing process. For example, you can redistribute the route in the OSPF routing domain and then advertise it to the RIP routing domain, and vice versa. The mutual route redistribution can be implemented between all the IP routing protocols.

In the route redistribution, route maps are usually used to control the mutual route redistribution between two routing domains.

In configuring one route map, one or more match or set commands can be executed. If the match command is not used, all the routes will be matched. If the set command is not used, no operation will be performed.

The route map can be configured very flexibly to be used for route redistribution and policy-based routing. No matter how the route map is used, the configuration principle is the same, except that different command sets are used. Even if it is used on the route redistribution, different routing protocols can use different commands with the route map.

Examples

The following example enables the OSPF routing protocol to redistribute RIP routes that only match access list v6acl, with the default metric being 50.

```
ipv6 router ospf
redistribute rip subnets route-map redrip

ipv6 access-list v6acl
10 permit ipv6 5200::64 any

route-map redrip permit 10
match ipv6 address v6acl
set metric 50
```

Related commands

Command	Description
ipv6 access-list	Set the IPV6 access list.
match interface	Match the next-hop interface of the route.
match ipv6 address	Match the IP address in the IPv6 access list.
match ipv6 next-hop	Match the next hop in the IPv6 access list.
match metric	Match the route metric.
match route-type	Match the route type.
match tag	Match the route tag.
set metric	Set the metric for route redistribution.
set metric-type	Set the type for route redistribution.
set tag	Set the tag for route redistribution.

1.18 match metric

Use **match metric** command to redistribute the routes of the specified metric. Use the **no** form of this command to remove the setting.

match metric *metric*
no match metric *metric*

Parameter description

Parameter	Description
metric	Route metric, in the range 0 to 4294967295

Default configuration

None.

Command mode

Route map configuration mode.

Usage guidelines

You can redistribute the routing information from one routing process to another routing process. For example, you can redistribute the route in the OSPF routing domain and then advertise it to the RIP routing domain, and vice versa. The mutual route redistribution can be implemented between all the IP routing protocols.
In the route redistribution, route maps are usually used to control the mutual route redistribution between two routing domains.
In configuring one route map, one or more match or set commands can be executed. If the match command is not used, all the routes will be matched. If the set command is not used, no operation will be performed.

Examples

In the example below, the OSPF routing protocol redistributes the RIP routes of metric 10.

```
router ospf 1
redistribute rip subnets route-map redrip
network 192.168.12.0 0.0.0.255 area 0

route-map redrip permit 10
match metric 10
```

Related commands

Command	Description
access-list	Set the access list.
match ip address	Match the IP address.
match interface	Match the interface.
match ip next-hop	Match the next-hop IP address.
match ip route-source	Match the source IP address.
match route-type	Match the route type.
match tag	Match the tag.
set metric	Set the metric.
set metric-type	Set the metric type.
set tag	Set the tag.

1.19 match route-type

Use this command to redistribute the network routes of the specified type. Use the **no** form of this command to delete the setting.

match route-type {**internal | external** [**type-1 | type-2**] }

no match route-type {**internal | external** [**type-1 | type-2**] }

Parameter description

Parameter	Description
internal	Indicates the OSPF internal route type.
external	Indicates the OSPF external route type.
**type-1	type-2**	Indicates the OSPF type-1 or type-2 route type.

Default configuration None

Command mode Route map configuration mode

Usage guideline

You can redistribute the routing information from one routing process to another routing process. For example, you can redistribute the route in the OSPF routing domain and then advertise it to the RIP routing domain, and vice versa. The mutual route redistribution can be implemented between all the IP routing protocols.

In the route redistribution, route maps are usually used to control the mutual route redistribution between two routing domains.

In configuring one route map, one or more match or set commands can be executed. If the match command is not used, all the routes will be matched. If the set command is not used, no operation will be performed.

Examples

In the example below, the RIP routing protocol redistributes only the internal routes in the OSPF routing domain.

```
router rip
redistribute ospf route-map redrip
network 192.168.12.0

route-map redrip permit 10
match route-type internal
!
```

Related commands

Command	Description
access-list	Set the access list.
match ip address	Match the IP address.
match interface	Match the interface.
match ip next-hop	Match the next-hop IP address.

match ip route-source	Match the source IP address.
match metric	Match the metric.
match tag	Match the tag.
set metric	Set the metric.
set metric-type	Set the access list.
set tag	Match the IP address.

1.20 match tag

Use this command to redistribute the network routes with the specified tag. Use the **no** form of this command to delete the setting.

match tag *tag* [*…tag*]

no match tag [*tag* [*…tag*]]

Parameter description

Parameter	Description
tag	Route tag

Default configuration

None

Command mode

Route map configuration mode

Usage guideline

Multiple tags may follow the match tag command.

You can redistribute the routing information from one routing process to another routing process. For example, you can redistribute the route in the OSPF routing domain and then advertise it to the RIP routing domain, and vice versa. The mutual route redistribution can be implemented between all the IP routing protocols.

In the route redistribution, route maps are usually used to control the mutual route redistribution between two routing domains.

In configuring one route map, one or more match or set commands can be executed. If the match command is not used, all the routes will be matched. If the set command is not used, no operation will be performed.

Examples

In the example below, the RIP routing protocol redistributes only the routes with tag 50 and 80 in the OSPF routing domain.

```
Ruijie(config)# router rip
Ruijie(config-router)# redistribute ospf 100 route-map redrip
Ruijie(config-router)# network 192.168.12.0
Ruijie(config-router)# exit
Ruijie(config)# route-map redrip permit 10
Ruijie(config-route-map)# match tag 50 80
```

Related commands

Command	Description
access-list	Set the access list.
match ip address	Match the IP address.
match interface	Match the next-hop IP interface.
match ip route-source	Match the source IP address.
match metric	Match the metric.
match ip next-hop	Match the next-hop IP address.
match route-type	Match the route type.
set metric	Set the metric.
set metric-type	Set the metric type.
set tag	Set the tag.

1.21 memory-lack exit-policy

Use this command to configure a policy to preferentially exit a routing protocol when the memory reaches the lower limit. Use the **no** form of this command to restore the default policy, namely, exit the routing protocol which occupies the largest memory.

memory-lack exit-policy {**ospf** | **rip** }

no memory-lack exit-policy

Parameter description

Parameter	Description
ospf	Preferentially exit OSPF when the memory is insufficient.
rip	Preferentially exit RIP when the memory is insufficient.

Default By default, the routing protocol which occupies the largest memory exits preferentially.

Command mode Global configuration mode

Usage guideline When the memory reaches the lower limit, you can disable a routing protocol to release the memory to ensure the normal running of other protocols.

When the system runs out of memory, disable a routing protocol which has the minimal impact on the system to ensure the operation of main services.

Configuring the policy to preferentially exit the routing protocols which are disabled cannot help the system release memory.

This command ensures the operation of main services to some extent when the memory is insufficient. If the memory is further consumed, all routing protocols will exit and stop running.

Examples The following example configures a policy to preferentially exit the RIP protocol when the memory reaches the lower limit.

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

Related command

Command	Description
-	-

Platform description -

1.22 route-map

Use **route-map** to enter the route map configuration mode and define a route map. Use the **no** form of this command to remove the setting.

route-map *route-map-name* [**permit** | **deny**] [*sequence-number*]

no route-map *route-map-name* [{**permit** | **deny**}*sequence-number*]

Parameter description

Parameter	Description
route-map-name	Name of the route map. The redistribute command references the route map according to its name. Multiple routing policies can be defined in a route map, and each policy corresponds to one sequence number.
permit	(Optional) If the permit keyword is defined and the rule defined by match is met, The set command controls the redistributed routes. For policy-based routing, the set command controls the packet forwarding, and exits the route map operation. If the permit keyword is defined but the rule defined by match is not met, the system performs the routing policy of the second route map till the set command is executed finally.
deny	(Optional) If the deny keyword is defined and the rule defined by match is met, no operation will be performed. Neither route redistribution nor policy-based routing is supported in the route map. The system exits the route map operation. If the deny keyword is defined but the rule defined by match is not met, the system performs the routing policy of the second route map till the set command is executed finally.
sequence-number	Sequence number of the route map. The policy with a lower sequence number is preferred, so it's noted when setting the sequence number.

Default configuration No route map is configured by default.

Command mode Global configuration mode.

Usage guidelines

At present, the RGOS software primarily uses the route map for route redistribution and policy-based routing.

1. Route redistribution control

You can redistribute the routes from one routing process to another routing process. For example, you can redistribute the route in the OSPF routing domain and then advertise it to the RIP routing domain, and vice versa. The mutual route redistribution can be implemented between all the IP routing protocols.

For route redistribution, route maps are usually used to control the mutual route redistribution between two routing domains.

One or more match or set commands can be executed to configure a route map. If the match command is not used, all the routes will be matched. If the set command is not used, no operation will be performed.

When configuring route maps, pay attention to the following when using the sequence number of a route map:

When you create the first route map policy, if *sequence-number* is not specified, it is 10 by default;

If only one route map policy exists and *sequence-number* is not specified, no new route map policy will be created, and the existing route map policy will be accessed for configuration;

If more than one route map policy is available, the sequence number of each policy shall be specified; otherwise an error message will be displayed.

2. policy-based routing

Policy-based routing refers to a routing mechanism based on user defined policies. Compared with traditional destination IP address-based routing, policy-based routing offers a flexibility for routing based on source IP address, length and port of IP packets. Policy-based routing can apply to the IP packets received on an interface or the IP packets sent from the local device.

Policy-based routing utilizes route map to define routing and forwarding policy. The match command defines packet filtering rule and the set command defines the action for the packets matching the filtering rules. The match command used includes match ip address and match length; the set command includes set ip tos, set ip precedence, set ip dscp, set ip [default] nexthop, set ip next-hop verify-availability, set [default] interface.

Examples

The following example enables the OSPF routing protocol to redistribute the RIP routes with the hop count of 4. In the OSPF route domain, the route type is the external route type-1, the default metric is 40 and the tag is 40.

```
!
router ospf
 redistribute rip subnets route-map redrip
 network 192.168.12.0 0.0.0.255 area 0
!
!
route-map redrip permit 10
 match metric 4
 set metric 40
```

```
set metric-type type-1
set tag 40
```

Related commands	Command	Description
	redistribute	Redistribute the routes.

1.23 send-lifetime

Use this command in the encryption key configuration mode to specify the lifetime of an encryption key in its send direction. Use the no form of this command to restore the default value.

send-lifetime *start-time* {**infinite** | *end-time* | **duration** *seconds*}

no send-lifetime

Parameter description	Parameter	Description
	start-time	Start time of the lifetime.
	infinite	Indicates that the encryption key is valid for ever.
	end-time	*End time of the encryption key. It must be later than the start time.*
	duration *seconds*	Duration of the encryption key after the start time. The value ranges from 1 to 2147483646.

Default infinite

Command mode Encryption key configuration mode

Usage guideline

Examples The following example configures the lifetime from 0:00 on September 9, 2000 to 0:00 on October 12, 2011

```
Ruijie(config)# key chain ripkeys
Ruijie(config-keychain)# key 1
Ruijie(config-keychain-key)# send-lifetime 00:00:00 Sep 9 2000 00:00:00 Dec 12
2011
```

Related command	Command	Description
	-	-

Platform description -

1.24 set level

Use this command to set the level of the area where the routes matching the rule are redistributed in the route map configuration command. Use the **no** form of this command to remove the setting.

set level {stub-area | backbone}

no set level

Parameter description

Parameter	Description
stub-area	Redistributes to OSPF Stub Area.
backbone	Redistributes to OSPF backbone Area.

Default configuration

None

Command mode

Route map configuration mode

Examples

In the example below, the OSPF routing protocol redistributes the RIP protocol to the backbone area.

```
Ruijie(config)# router ospf
Ruijie(config-router)# redistribute rip subnets route-map redrip
Ruijie(config-router)# network 192.168.12.0 0.0.0.255 area 0
Ruijie(config-router)# exit
Ruijie(config)# route-map redrip permit 10
Ruijie(config-route-map)# set level backbone
```

Related commands

Command	Description
match interface	Match the interface.
match ip address	Match the IP address.
match ip next-hop	Match the next-hop IP address.
match ip route-source	Match the source IP address.
match metric	Match the metric.
match route-type	Match the route type.
match tag	Match the tag.
set metric-type	Set the metric type.
set tag	Set the tag.

1.25 set metric

Use **set metric** to set the metric for the routes to be redistributed. Use the **no** form of this command to remove the setting.

set metric [+ *metric-value* | **-** *metric-value* | *metric-value*]

no set metric

Parameter description

Parameter	Description
+	Increase based on the metric of the original route
-	Decrease based on the metric of the original route
metric-value	Metric for the route to be redistributed

Default configuration

Command mode

Route map configuration mode

Usage guideline

You should set the metric according to the actual network topology, because the routing depends on the metric of routes. Attentions should be paid to the upper and lower limits of the routing protocols when you execute the set metric, + metric or – metric commands. When the RIP protocol redistributes the routes of other protocols, the range of the metric after increase or decrease is 1 to 16.
You can redistribute the routes from one routing process to another routing process. For example, you can redistribute the route in the OSPF routing domain and then advertise it to the RIP routing domain, and vice versa. The mutual route redistribution can be implemented between all the IP routing protocols.
For route redistribution, route maps are usually used to control the mutual route redistribution between two routing domains.
One or more match or set commands can be executed to configure a route map. If the match command is not used, all the routes will be matched. If the set command is not used, no operation will be performed.

Examples

The following example enables the OSPF routing protocol to redistribute the RIP routes and sets the default metric to 40.

```
Ruijie(config)# router ospf
Ruijie(config-router)# redistribute rip subnets route-map redrip
Ruijie(config-router)# network 192.168.12.0 0.0.0.255 area 0
Ruijie(config-router)# exit
Ruijie(config)# route-map redrip permit 10
Ruijie(config-route-map)# set metric 40
```

Related commands

Command	Description
match interface	Match the interface.
match ip address	Match the IP address.
match ip next-hop	Match the next-hop IP address.
match ip route-source	Match the source IP address.
match metric	Match the metric.
match route-type	Match the route type.

match tag	Match the tag.
set metric-type	Set the metric type.
set tag	Set the tag.

1.26 set metric-type

Use **set metric-type** to set the type of the routes to be redistributed. Use the **no** form of this command to remove the setting.

set metric-type *type*

no set metric-type

Parameter description

Parameter	Description
type	Type of the routes to be redistributed. At present, you can set the type of the routes that the OSPF protocol redistributes. type-1: Type-1 external route; type-2: Type-2 external route.

Default configuration

Command mode

Route map configuration mode

Usage guideline

You can redistribute the routing information from one routing process to another routing process. For example, you can redistribute the route in the OSPF routing domain and then advertise it to the RIP routing domain, and vice versa. The mutual route redistribution can be implemented between all the IP routing protocols.

In the route redistribution, route maps are usually used to control the mutual route redistribution between two routing domains.

In configuring one route map, one or more match or set commands can be executed. If the match command is not used, all the routes will be matched. If the set command is not used, no operation will be performed.

Examples

The following example enables the OSPF routing protocol to redistribute the RIP route and sets the type as type-1.

```
Ruijie(config)# router ospf
Ruijie(config-router)# redistribute rip subnets route-map redrip
Ruijie(config-router)# network 192.168.12.0 0.0.0.255 area 0
Ruijie(config-router)# exit
Ruijie(config)# route-map redrip permit 10
Ruijie(config-route-map)# set metric-type type-1
```

Related commands

Command	Description
match interface	Match the interface.
match ip address	Match the IP address.
match ip next-hop	Match the next-hop IP address.
match ip route-source	Match the source IP address.
match metric	Match the metric.
match route-type	Match the route type.
match tag	Match the tag.
set metric	Set the metric.
set tag	Set the tag.

1.27 set next-hop

Use this command to specify the next-hop IP address for the routes that match the rule. Use the **no** form of this command to remove the setting. This command is only used to configure routing policies.

set next-hop *ip-address*

no set next-hop

Parameter description

Parameter	Description
ip-address	IP address of the next hop.

Default configuration

None

Command mode

Route map configuration mode

Usage guideline

You can redistribute the routing information from one routing process to another routing process. For example, you can redistribute the route in the OSPF routing domain and then advertise it to the RIP routing domain, and vice versa. The mutual route redistribution can be implemented between all the IP routing protocols.

In the route redistribution, route maps are usually used to control the mutual route redistribution between two routing domains.

In configuring one route map, one or more match or set commands can be executed. If the match command is not used, all the routes will be matched. If the set command is not used, no operation will be performed.

Examples

The following example enables the OSPF routing protocol to redistribute the RIP route and sets the next-hop to 192.168.1.2.

```
Ruijie(config)# route-map redrip permit 10
Ruijie(config-route-map)# match ip address 1
Ruijie(config-route-map)# set next-hop 192.168.1.2
```

Related commands

Command	Description
match interface	Match the interface.
match ip address	Match the IP address.
match ip next-hop	Match the next-hop IP address.
match ip route-source	Match the source IP address.
match metric	Match the metric.
match route-type	Match the route type.
match tag	Match the tag.
set metric-type	Set the metric type.
set tag	Set the tag.

1.28 set tag

Use this command to set the tag for the routes to be redistributed. Use the **no** form of this command to remove the setting.

set tag *tag*

no set tag

Parameter description

Parameter	Description
tag	Tag of the route to be redistributed

Default configuration

Command mode

Route map configuration mode

Usage guideline

This command can only be used for route redistribution. If this command is not configured, the default route tag is used.

Examples

The following example enables the OSPF routing protocol to redistribute the RIP route and sets the tag as 100.

```
Ruijie(config)# router ospf
Ruijie(config-router)# redistribute rip subnets route-map redrip
Ruijie(config-router)# network 192.168.12.0 0.0.0.255 area 0
Ruijie(config-router)# exit
Ruijie(config)# route-map redrip permit 10
Ruijie(config-route-map)# set tag 100
```

Related commands

Command	Description
match interface	Match the interface.
match ip address	Match the IP address.

match ip next-hop	Match the next-hop IP address.
match ip route-source	Match the source IP address.
match metric	Match the metric.
match route-type	Match the route type.
match tag	Match the tag.
set metric	Set the metric.
set metric-type	Set the metric type.

1.29 show ip prefix-list

Use **show ip prefix-list** to display the prefix list or the entries.

show ip prefix-list [*prefix-name*]

Parameter description

Parameter	Description
prefix-name	Name of the prefix list.

Default configuration

Command mode Privileged EXEC mode, global configuration mode, interface configuration mode, routing protocol configuration mode, route map configuration mode.

Usage guidelines If no prefix list is specified, the configurations of all the prefix lists are displayed, otherwise only the configuration of the specified prefix list is displayed.

Examples

```
Ruijie# show ip prefix-list
seq pre: 2 entries
seq 5 permit 192.168.564.0/24
seq 10 permit 192.2.2.0/24
```

1.30 show ip protocols

Use this command to display information about the status of the currently running IPv4 routing protocol.

show ip protocols { **ospf | rip** }

Parameter Description

Parameter	Description
ospf	Displays information about the status of the OSPF protocol.
rip	Displays information about the status of the RIP protocol.

Command Mode Privileged EXEC mode, global configuration mode, interface configuration mode, routing protocol configuration mode, and routing map configuration mode

Default Level 14

Usage Guide Information about the status of only the currently running routing protocol is displayed, and the information about a routing protocol that is not running is not displayed.

Examples The following example displays the status of routing protocols.

```
Ruijie# show ip protocols
Routing Protocol is "ospf 1"
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Router ID 57.57.57.57
  Memory Overflow is enabled
  Router is not in overflow state now
  It is an autonomous system boundary router
  Redistributing External Routes from,
    connected, includes subnets in redistribution
    bgp, includes subnets in redistribution
  Number of areas in this router is 2: 2 normal 0 stub 0 nssa
  Routing for Networks:
    57.57.57.57 0.0.0.0 area 0
    163.18.4.0 0.0.0.255 area 0
    163.18.57.0 0.0.0.255 area 0
    192.100.1.0 0.0.0.255 area 0
    192.101.1.0 0.0.0.255 area 1
    192.102.1.0 0.0.0.255 area 0
  Reference bandwidth unit is 100 mbps
  Distance: (default is 110)

Routing Protocol is "bgp 10"
  IGP synchronization is disabled
  Default-information originate is disabled
  Default local-preference applied to incoming route is 100
  Redistributing: connected
  Neighbor(s):
    Address           AddressFamily  FiltIn  FiltOut  DistIn  DistOut  RouteMapIn
RouteMapOut  Weight
  Distance: external 20(default) internal 200(default) local 200(default)
```

Field description:

Field	Description

Routing Protocol is "ospf 1"	Name of a routing protocol
Redistributing External Routes from	Route redistribution status of a routing protocol
Distance:	Distance information of a routing protocol

1.31 show ipv6 prefix-list

Use this command to display the information about the IPv6 prefix list or its entries.

show ipv6 prefix-list [*prefix-name*]

Parameter description

Parameter	Description
prefix-name	Name of the IPv6 prefix list.

Default configuration

Command mode Privileged EXEC mode, global configuration mode, interface configuration mode, route protocol configuration mode, route map configuration mode

Usage guideline If no prefix list is specified, the configurations of all the prefix lists are displayed, otherwise only the configuration of the specified prefix list is displayed.

Examples

```
Ruijie# show ipv6 prefix-list
ipv6 prefix-list p6: 2 entries
      seq 5 permit 13::/20
      seq 10 permit 14::/20
```

1.32 show key chain

Use this command to display the key chain configuration.

show key chain [*key-chain-name*]

Parameter description

Parameter	Description
key-chain-name	(Optional) Display the configuration of the specified key chain.

Default

Command mode Privileged EXEC mode, global configuration mode, interface configuration mode, routing protocol configuration mode, and key chain configuration mode.

Usage guideline If no key chain is specified, the configuration information of all key chains is displayed.

Examples

```
Ruijie# show key chain
```

```
route-map AAA, permit, sequence 10
Match clauses:
ip address 2
Set clauses:
metric 10
Ruijie(config)#show key chain
key chain kc
    key 1 -- text "ruijie"
        accept-lifetime (12:11:00 May  2 2001) - (infinite)
        send-lifetime (always valid) - (always valid) [valid now]
```

Field	Description
key chain	Key chain name.
key	Key ID.
text	Key string.
accept-lifetime	Lifetime in the accept direction.
send-lifetime	Lifetime in the send direction.

Related command

Command	Description
-	-

Platform description -

1.33 show route-map

Use the command to display the configuration of the route map.

show route-map [*route-map-name*]

Parameter description

Parameter	Description
route-map-name	(Optional) Display the configuration information of the specified the route map.

Default configuration

Command mode Privileged EXEC mode, global configuration mode, interface configuration mode, routing protocol configuration mode, route map configuration mode.

Usage guidelines If no route map is specified, the configurations of all the route maps will be displayed, otherwise only the configuration of the specified route map is displayed.

```
Ruijie# show route-map
route-map AAA, permit, sequence 10
Match clauses:
ip address 2
Set clauses:
metric 10
```

Examples

Field	Description
route-map	Name of the route map.
Permit	The route map contains the permit keyword.
sequence 10	Sequence number of the route map.
Match clauses	Set the matching rule. Whether to perform the set operation depends on the permit or deny keyword in the route map.
Set clauses	Set the operation when the rule is matched.

2 PBR Commands

2.1 clear ip pbr statistics

Use this command to clear the IPv4 PBR forwarded packet count.

clear ip pbr statistics [**interface** *if-name* **| local**]

Parameter Description

Parameter	Description
interface *if-name*	Specifies the interface name. If the interface name is specified, the device clears the IPv4 PBR forwarded packet count on that interface. Otherwise, the device clears the IPv4 PBR forwarded packet count on every interface where IPv4 PBR is enabled.
local	Clears the IPv4 PBR forwarded packet count on the local interface.

Defaults N/A

Command Mode Privileged EXEC mode.

Usage Guide Use this command to clear the IPv4 PBR forwarded packet count.

Configuration Examples The following example clears the IPv4 PBR forwarded packet count.

```
Ruijie#clear ip pbr statistics
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

2.2 clear ipv6 pbr statistics

Use this command to clear the IPv6 PBR forwarded packet count.

clear ipv6 pbr statistics [**interface** *if-name* **| local**]

Parameter Description

Parameter	Description
interface *if-name*	Specifies the interface name. If the interface name is specified, the device clears the IPv6 PBR forwarded packet count on that interface.

	Otherwise, the device clears the IPv6 PBR forwarded packet count on every interface where IPv6 PBR is enabled.
local	Clears the IPv6 PBR forwarded packet count on the local interface.

Defaults N/A

Command Mode Privileged EXEC mode.

Usage Guide Use this command to clear the IPv6 PBR forwarded packet count.

Configuration Examples The following example clears the IPv6 PBR forwarded packet count.

```
Ruijie#clear ipv6 pbr statistics
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

2.3 ip local policy route-map

Use this command to apply the policy-based routing (PBR) on the packets sent locally. Use the **no** form of this command to restore the default setting.

ip local policy route-map *route-map-name*

no ip local policy route-map

Parameter Description

Parameter	Description
route-map	Name of the route map

Defaults This function is disabled by default.

Command Mode Global configuration mode

Usage Guide This command is valid for the IP packets sent locally, but not the IP packets received locally. The IP packets received by the local are free from this command.

To use the policy-based routing, you must specify the route map for it and create the route map. A route map contains multiple policies, and each policy defines one or more match rules and the corresponding operations. After policy-based routing is applied to an interface, the packets received by the interface will be checked. The packets that do not match any policy in the route map will be forwarded to the usual route. The packets that match a policy in the route map will be processed according to the operation defined in the policy.

The **set interface** command for the policy-based routing does not support the load-balancing and only supports the redundancy backup.

Configuration Examples

The following examples send the packets with the source address 192.168.217.10 from the serial 2/0.

The following example defines an ACL that match the IP packet.

```
Ruijie(config)#access-list 1 permit 192.168.217.10
```

The following example defines the route map.

```
Ruijie(config)#route-map lab1 permit 10
Ruijie(config-route-map)#match ip address 1
Ruijie(config-route-map)#set interface serial 2/0
Ruijie(config-route-map)#exit
```

The following example applies PBR on the local interface.

```
Ruijie(config)#ip local policy route-map lab1
```

Related Commands

Command	Description
access-list	Defines the access list rule.
route-map	Defines the route map.
set vrf	Defines the VRF instance of the policy-based IP packet.
set ip next-hop	Defines the next hop of the policy-based routing.
set ip default next-hop	Defines the default next hop of the policy-based routing.
set interface	Defines the output port of the policy-based routing.
set default interface	Defines the default policy-based routing output port.
set ip tos	Sets the TOS in the head of the IP packet.
set ip dscp	Sets the DSCP of the IP packet.
set ip precedence	Sets the priority level in the head of the IP packet.
match ip address	Sets the filtering rule.
match length	Matches the packet length.

Platform Description

N/A

2.4 ip policy

Use this command to set the policy: redundant backup or load balancing used between multiple next hops of the PBR applied for the **set ip [default] nexthop** command in global configuration mode.

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

ip policy { load-balance | **redundance }**

no ip policy

Parameter Description

Parameter	Description
load-balance | redundance	Specifies the policy: load balancing or redundant backup.

Defaults Redundant backup is adopted by default.

Command Mode Global configuration mode

Usage Guide When you configure the **set ip next-hop** command in sub-route map, it is possible to configure multiple next hops. However, when you set redundant backup, only the first resolved next hop of the policy-based routing takes effect. When the load balancing is set, multiple resolved next hops of the policy-based routing take effect. The WCMP can be set up to 8 next hops, and the ECMP can be set up to 32 next hops. The resolved next hop refers to the ARP message learned by the next hop and the MAC address corresponding to this ARP exists in the MAC address table.

NPE80 does not support this command.

Configuration Examples In the example below, there are multiple next hops configured in the route map. After the redundant backup is set in global configuration mode, only the first next hop among the sub-route map of the policy-based routing applied on the interface FastEthernet 0/0 takes effect.

The following example sets the ACL that match the IP packet.

```
Ruijie(config)#access-list 1 permit 10.0.0.1
Ruijie(config)#access-list 2 permit 20.0.0.1
```

The following example defines the route map.

```
Ruijie(config)#route-map lab1 permit 10
Ruijie(config-route-map)#match ip address 1
Ruijie(config-route-map)#set ip next-hop 196.168.4.6
Ruijie(config-route-map)#set ip next-hop 196.168.4.7
Ruijie(config-route-map)#set ip next-hop 196.168.4.8
Ruijie(config-route-map)#exit
Ruijie(config)#route-map lab1 permit 20
Ruijie(config-route-map)#match ip address 2
Ruijie(config-route-map)#set ip next-hop 196.168.5.6
Ruijie(config-route-map)#set ip next-hop 196.168.5.7
Ruijie(config-route-map)#set ip next-hop 196.168.5.8
Ruijie(config-route-map)#exit
```

The following example applies the policy-based routing on the interface.

```
Ruijie(config)#interface FastEthernet 0/0
```

```
Ruijie(config-if)#ip policy route-map lab1
Ruijie(config-if)#exit
Ruijie(config)#ip policy redundance
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

2.5 ip policy route-map

Use this command to apply the policy-based routing on an interface. Use the **no** form of this command to restore the default setting.

ip policy route-map *route-map*

no ip policy route-map

Parameter Description

Parameter	Description
route-map	Name of the route map

Defaults This function is disabled by default.

Command Mode Interface configuration mode

Usage Guide The policy-based routing must be applied on the specified interface. That interface performs the policy-based routing only on the received packets.

To use the policy-based routing, you must specify the route map for it and create the route map. A route map contains multiple policies, and each policy defines one or more match rules and the corresponding operations. After policy-based routing is applied to an interface, the packets received by the interface will be checked. The packets that do not match any policy in the route map will be forwarded to the usual route. The packets that match a policy in the route map will be processed according to the operation defined in the policy.


Up to one route map can be configured on an interface. When you configure a route map on the interface for many times, the latter will overwrite the former.

Configuration Examples In the example below, when the interface FastEthernet0/0 receives a datagram, if the source address of the datagram is 10.0.0.1, it sets the next-hop as 196.168.4.6; if the source address is 20.0.0.1, it sets the next-hop as 196.168.5.6;, otherwise, the general forwarding will be performed.

The following example sets the ACL matched with the IP packets.

```
Ruijie(config)#access-list 1 permit 10.0.0.1
Ruijie(config)#access-list 2 permit 20.0.0.1
```

The following example defines the route map.

```
Ruijie(config)#route-map lab1 permit 10
Ruijie (config-route-map)#match ip address 1
Ruijie(config-route-map)#set ip next-hop 196.168.4.6
Ruijie(config-route-map)#exit
Ruijie(config)#route-map lab1 permit 20
Ruijie(config-route-map)#match ip address 2
Ruijie(config-route-map)#set ip next-hop 196.168.5.6
Ruijie(config-route-map)#exit
```

The following example applies the route map on the interface.

```
Ruijie(config)#interface FastEthernet 0/0
Ruijie(config-if)#ip policy route-map lab1
Ruijie(config-if)#exit
```

Related Commands

Command	Description
access-list	Defines the access list rule.
route-map	Defines the route map.
set vrf	Defines the VRF instance of the policy-based IP packet.
set ip next-hop	Defines the next hop of the policy-based routing.
set ip default next-hop	Defines the default next hop of the policy-based routing.
set interface	Defines the policy-based routing output port.
set default interface	Defines the default policy-based routing output port.
set ip tos	Sets the TOS in the head of the IP packet.
set ip dscp	Sets the DSCP of the IP packet.
set ip precedence	Sets the priority level in the head of the IP packet.
match ip address	Sets the filtering rule.
match length	Matches the packet length.

Platform Description N/A

2.6 ipv6 local policy route-map

Use this command to enable the policy-based routing on the packets sent locally. Use the **no** form of

this command to restore the default setting.

ipv6 local policy route-map *route-map-name*

no ipv6 local policy route-map

Parameter Description

Parameter	Description
route-map-name	Name of the router map applied locally, which is configured by the **router-map** command.

Defaults This function is disabled by default.

Command Mode Global Configuration mode

Usage Guide This command is valid only for the IPv6 packets in accordance with the policy (for example, ping packets used for management) sent locally, but not the packets received locally.

To use the policy-based routing, you must specify the route map for it and create the route map. A route map contains multiple policies, and each policy defines one or more match rules and the corresponding operations. After policy-based routing is applied to an interface, the packets received by the interface will be checked. The packets that do not match any policy in the route map will be forwarded to the usual route. The packets that match a policy in the route map will be processed according to the operation defined in the policy.

Configuration Examples The following examples display the PBR application process: The device sends the packets from the source address 2003:1000::10/80 to the 2001:100::/64, the packets will match ACL6 of aaa and be sent to the device 2003:1001::2.

- The following example defines the ACL matched with the IPv6 packet:

```
Ruijie(config)#ipv6 access-list aaa
Ruijie(config)#permit ipv6 2003:1000::10/80 2001:100::/64
```

- The following example defines the router map.

```
Ruijie(config)#route-map pbr-aaa permit 10
Ruijie(config-route-map)#match ipv6 address aaa
Ruijie(config-route-map)#set ipv6 next-hop 2003::1001::2
```

- The following example applies the PBR on the device.

```
Ruijie(config)#ipv6 local policy route-map pbr-aaa
```

Related Commands

Command	Description
match ipv6 address	Sets the ACL6 used to match the IPv6 packets in the IPv6 PBR.
match length	Defines the length of matched packets.
route-map	Defines the route map for PBR.
set default interface	Defines the default next hop output port.
set interface	Defines the next hop output port.

set ipv6 default next-hop	Sets the default next hop of packet forwarding.
set ipv6 next-hop	Sets the next hop of packet forwarding.
set ipv6 precedence	Sets the priority field in the head of IPv6 packets.
show ipv6 policy	Displays the current PBR application.
show route-map	Displays the current router map configuration.

Platform Description N/A

2.7 ipv6 policy

Use this command to set the policy: redundant backup or load balancing, applied for the **set ip nexthop** command in global configuration mode. Use the **no** form of this command to restore the default setting.

ipv6 policy { load-balance | redundance }

no ipv6 policy

Parameter Description

Parameter	Description
load-balance	Sets the policy as load balancing.
redundance	Sets the policy as redundant backup.

Defaults Redundant backup is adopted by default.

Command Mode Global configuration mode

Usage Guide This command is valid for the IP packets sent locally, but not the IP packets received locally. The IP packets received by the local are free from this command.

To use the policy-based routing, you must specify the route map for it and create the route map. A route map contains multiple policies, and each policy defines one or more match rules and the corresponding operations. After policy-based routing is applied to an interface, the packets received by the interface will be checked. The packets that do not match any policy in the route map will be forwarded to the usual route. The packets that match a policy in the route map will be processed according to the operation defined in the policy.

The **set interface** command for the policy-based routing does not support the load-balancing and only supports the redundancy backup.

This function is valid for the multiple next-hops.

When you configure the set ip next-hop command in sub-route map, it is possible to configure multiple next hops. However, when you set redundant backup, only the first resolved next hop takes effect. The second configured next hop will take effect only when the first one fails and the first next hop will take effect again if it recovers.

When the load balancing is set, multiple next hops of the policy-based routing take effect.

The WCMP can be set up to 8 next hops, and the ECMP can be set up to 32 next hops.

The resolved next hop refers to the learned MAC address for the next-hop.

Configuration Examples

The following example sets load-balancing mode for multiple nexthops.

The following example configures an ACL matching with IP packets.

```
Ruijie(config)# ipv6 access-list 1
Ruijie(config-ipv6-acl )# permit ipv6 1000::1 any
Ruijie(config)# ipv6 access-list 2
Ruijie(config-ipv6-acl )# permit ipv6 2000::1 any
```

The following example defines a route map.

```
Ruijie(config)# route-map lab1 permit 10
Ruijie(config-route-map)# match ipv6 address 1
Ruijie(config-route-map)# set ipv6 next-hop 2002::1
Ruijie(config-route-map)# set ipv6 next-hop 2002::2
Ruijie(config-route-map)# set ipv6 next-hop 2002::3
Ruijie(config-route-map)# exit
Ruijie(config)# route-map lab1 permit 20
Ruijie(config-route-map)# match ipv6 address 2
Ruijie(config-route-map)# set ipv6 next-hop 2002::5
Ruijie(config-route-map)# set ipv6 next-hop 2002::6
Ruijie(config-route-map)# set ipv6 next-hop 2002::7
Ruijie(config-route-map)# exit
```

The following example applies policy-based routing on the interface.

```
Ruijie(config)# interface FastEthernet 0/0
Ruijie(config-if)# ipv6 policy route-map lab1
Ruijie(config-if)# exit
Ruijie(config)# ipv6 policy load-balance
```

Related Commands

Command	Description
set ipv6 default next-hop	Defines the default next hop for forwarding the packets.
set ipv6 next-hop	Defines the next hop for forwarding the packets.
show ipv6 policy	Displays the current policy-based routing application.

Platform Description

N/A

2.8 ipv6 policy route-map

Use this command to apply the policy-based routing on an interface in interface configuration mode.

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

ipv6 policy route-map *route-map-name*

no ip policy route-map

Parameter Description

Parameter	Description
route-map-name	Name of the PBR router map applied locally, which is configured by the **router-map** command.

Defaults This function is disabled by default..

Command Mode Interface configuration mode

Usage Guide The policy-based routing must be applied on the specified interface. That interface performs the policy-based routing only on the received packets.

To use the policy-based routing, you must specify the route map for it and create the route map. A route map contains multiple policies, and each policy defines one or more match rules and the corresponding operations. After policy-based routing is applied to an interface, the packets received by the interface will be checked. The packets that do not match any policy in the route map will be forwarded to the usual route. The packets that match a policy in the route map will be processed according to the operation defined in the policy.

⚠ Up to one route map can be configured on an interface. When you configure a route map on the interface for many times, the latter will overwrite the former.

Configuration Examples An IPv6 packet is received on the fastEthernet 0/0. If the packet is sent from 10::/64 network segment, it is forwarded to the next hop of 2000:1; if the packet is sent from 20::/64 network segment, it is forwarded to the next hop of 2000:2 or forwarded as usual.:

The following example configures an ACL matched with the IP packet.

```
Ruijie(config)# ipv6 access-list acl_for_pbr1
Ruijie (config-ipv6-acl)# permit ipv6 10::/64  any
Ruijie(config)# ipv6 access-list acl_for_pbr2
Ruijie (config-ipv6-acl)# permit ipv6 20::/64  any
```

The following example defines a route map.

```
Ruijie(config)# route-map rm_pbr  permit 10
Ruijie (config-route-map)# match ipv6 address acl_for_pbr1
Ruijie(config-route-map)# set ipv6 next-hop 2000::1
Ruijie(config-route-map)# exit
Ruijie(config)# route-map rm_pbr  permit 20
Ruijie(config-route-map)# match ipv6 address acl_for_pbr2
Ruijie(config-route-map)# set ipv6 next-hop 2000::2
Ruijie(config-route-map)# exit
```

The following example applies the route map to the interface.

```
Ruijie(config)# interface FastEthernet 0/0
```

```
Ruijie(config-if)# no switchport
Ruijie(config-if)# ipv6 policy route-map rm_pbr
Ruijie(config-if)# exit
```

Related Commands

Command	Description
route-map	Defines the route map.
match ipv6 address	Sets the IPv6 ACL used to match the IPv6 packets in the IPv6 PBR.
set ipv6 default next-hop	Defines the default next hop of the packet forwarding.
set ipv6 next-hop	Defines the next hop of the packet forwarding.
show ipv6 policy	Displays the current policy-based routing application.
show route-map	Displays the current route map configurations.

Platform Description N/A

2.9 show ip pbr bfd

Use this command to display the correlation between the IPv4 policy router and BFD.

show ip pbr bfd

Parameter Description

Parameter	Description
N/A	N/A

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide N/A

Configuration Examples The following example displays the correlation between the IPv4 policy router and BFD.

```
Ruijie# show ip pbr bfd
VRF ID  Ifindex  Host           State  Refcnt
    0       13  192.168.8.100      Up      2
```

Field Description

Field	Description
VRF ID	VRF of BFD neighbors correlated with the policy router

Ifindex	The interface index of BFD neighbors correlated with the policy router
Host	The peer IPv4 address
State	Up/Down status of BFD neighbors correlated with the policy router
Refcnt	Calculation referred by BFD neighbors

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

2.10 show ip pbr route

Use this command to display the IPv4 PBR information on the interface.

show ip pbr route [**interface** *if-name* **| local**]

Parameter Description

Parameter	Description
interface *if-name*	Specifies the interface name. If the interface name is specified, the IPv4 BPR information of this interface is displayed. Otherwise, the IPv4 BPR information of all interfaces where the IPv4 PBR is enabled is displayed.
local	Displays the IPv4 PBR information on the local interface

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide Use this command to display the IPv4 PBR information.

Configuration Examples The following example displays the IPv4 PBR information on the interfaces.

```
Ruijie#show ip pbr route
PBR IPv4 Route Summay : 1
Interface       : GigabitEthernet 0/1
  Sequence      : 10
  ACL[0]        : 2900
ACL_CLS[0]     : 0
  VRF ID        : 0
  Route Flags    :
```

```
  Route Type    : PBR
  Direct       : Permit
  Priority     : High
  Tos_Dscp     : None
  Precedence    : None
 Precedence    : 0
 Mode          : redundance
 Nexthop Count  : 1
  Nexthop[0]    : 192.168.8.100
  Weight[0]     : 1
  Ifindex[0]    : 2
```

Parameter	Description
PBR IPv4 Route Summay	IPv4 PBR route count.
Interface	Interface where IPv4 PBR is enabled.
Sequence	The PBR serial number.
ACL	The ACL ID used in the match rule.
ACL_CLS	The ACL type used in the match rule, such as the IP standard ACL.
VRF ID	Port-correlated VRF ID.
Route Flags	PBR flag bit: Route Type: “PBR” indicates PBR routes. “Normal” indicates common routes. Direct: PBR matching action, **permit** or **deny** Priority: PBR priority, **High** or **Low** Tos_Dscp: Displays whether the **tos** rule or the **dscp** rule is configured. Precedence: Displays whether the **set ip precedence** rule is configured.
Mode	Specifies the redundancy mode or the next hop load balancing mode.
Nexthop Count	Specifies the next hop number. ECMP supports up to 32 next hops.
Weight	Specifies the next hop weight.
Ifindex	Specifies the outbound interface index corresponding to the next hop.

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

2.11 show ip pbr route-map

Use this command to display the IPv4 PBR route-map information.

show ip pbr route-map *route-map-name*

Parameter Description

Parameter	Description
route-map-name	The route-map name.

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide N/A

Configuration Examples The following example displays the IPv4 PBR route-map information.

```
Ruijie#show ip pbr route-map rm
Pbr VRF: GLOBAL, ID: 0
 Forward Mode: redundance
 Forwarding: On

route-map rm
  route-map index: sequence 10, permit
    Match rule:
      ACL ID :     0, ACL CLS: 0, Name: acl1
    Set rule:
      IPv4 Nexthop: 192.168.8.100, (VRF Name: , ID: 0), Weight: 0, Flags: 0
      PBR state info ifx: GigabitEthernet 0/1, Connected: true, Track State:
valid, Flags: 0
```

Field	Description
Pbr VRF	VRF name and VRF ID.
Forward Mode	Sets the load balance mode or the redundancy mode for the next hop.
Forwarding	Displays whether the IP route forwarding is enabled.
Route-map index	The serial number and the type of the sub-map.
Match rule	Match rule.
Set rule	Set rule.
PBR state info	PBR private data information, such as outbound interface and the link state of the next hop.

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

2.12 show ip pbr statistics

Use this command to display the IPv4 PBR forwarded packet count.

show ip pbr statistics [**interface** *if-name* **| local**]

Parameter Description

Parameter	Description
interface *if-name*	Specifies the interface name. If the interface name is specified, the IPv4 PBR forwarded packet count of this interface is displayed. Otherwise, the IPv4 PBR forwarded packet count of all interfaces where the IPv4 PBR is enabled is displayed.
local	Displays the IPv4 PBR forwarded packet count on the local interface.

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide N/A

Configuration Examples The following example displays the IPv4 PBR forwarded packet count.

```
Ruijie#show ip pbr statistics
IPv4 Policy-based route statistic
 gigabitEthernet 0/1
   statistics : 10
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

2.13 show ip policy

Use this command to display the interface configured with the policy-based routing and the name of

route map applied on the interface.

show ip policy [*route-map-name*]

Parameter Description

Parameter	Description
route-map-name	Indicates the name of a route map.

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide You can use this command to verify the current PBR configured in the system.

Configuration Examples The following example displays the current PBR configured in the system.

```
Ruijie#show ip policy
Banlance Mode: redundance
Interface           Route map
local               test
FastEthernet 0/0    test
```

Related Commands

Command	Description
ip policy route-map	Applies the policy-based routing on the interface.
ip local policy route-map	Applies the policy-based routing on the local interface.

Platform Description N/A

2.14 show ipv6 pbr bfd

Use this command to display the correlation between the IPv6 policy router and BFD.

show ipv6 pbr bfd

Parameter Description

Parameter	Description
N/A	N/A

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide N/A

Configuration Examples The following example displays the correlation between the IPv6 policy router and BFD.

```
Ruijie# show ipv6 pbr bfd
VRF ID  Ifindex  Host                                State  Refcnt
    0       13  2000::2                              Up       1
```

Field Description

Field	Description
VRF ID	VRF of BFD neighbors correlated with the policy router
Ifindex	The interface index of BFD neighbors correlated with the policy router
Host	The peer IPv6 address
State	Up/Down status of BFD neighbors correlated with the policy router
Refcnt	Calculation referred by BFD neighbors

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

2.15 show ipv6 pbr route

Use this command to display the IPv6 PBR information on the interface.

show ipv6 pbr route [**interface** *if-name* **| local**]

Parameter Description

Parameter	Description
interface *if-name*	Specifies the interface name. If the interface name is specified, the IPv6 BPR information of this interface is displayed. Otherwise, the IPv6 BPR information of all interfaces where the IPv6 PBR is enabled is displayed.
local	Displays the IPv6 PBR information on the local interface.

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide N/A

Configuration Examples The following example displays the IPv6 PBR information on the interfaces.

```
Ruijie#show ipv6 pbr route
PBR IPv6 Route Summary : 1
Interface       : GigabitEthernet 0/2
  Sequence      : 10
  ACL[0]        : 2901
ACL_CLS[0]     : 0
  VRF ID        : 0
  Route Flags    :
   Route Type    : PBR
   Direct       : Permit
   Priority     : High
   Precedence    : None
  Precedence     : 0
  Mode          : redundance
  Nexthop Count  : 1
   Nexthop[0]    : 10::1
   Weight[0]     : 1
   Ifindex[0]    : 3
```

Parameter	Description
PBR IPv4 Route Summay	IPv4 PBR route count.
Interface	Interface where IPv4 PBR is enabled.
Sequence	The PBR serial number.
ACL	The ACL ID used in the match rule.
ACL_CLS	The ACL type used in the match rule, such as the IP standard ACL.
VRF ID	Port associated VRF ID.
Route Flags	PBR flag bit: Route Type: “PBR” indicates PBR routes. “Normal” indicates common routes. Direct: PBR matching action, **permit** or **deny** Priority: PBR priority, **High** or **Low** Tos_Dscp: Displays whether the **tos** rule or the **dscp** rule is configured. Precedence: Displays whether the **set ip precedence** rule is configured.
Mode	Specifies the redundancy mode or the load balance mode for the next hop.
Nexthop Count	Specifies the next hop number. ECMP supports up to 32 next hops.
Weight	Specifies the next hop weight.

Ifindex	Specifies the outbound interface index corresponding to the next hop

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

2.16 show ipv6 pbr route-map

Use this command to display the IPv6 PBR route-map information.

show ipv6 pbr route-map *route-map-name*

Parameter Description

Parameter	Description
route-map-name	The route-map name.

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide N/A

Configuration Examples The following example displays the IPv6 PBR route-map information.

```
Ruijie#show ipv6 pbr route-map rm6
Pbr VRF: GLOBAL, ID: 0
 Forward Mode: redundance
 Forwarding: On

route-map rm6
  route-map index: sequence 10, permit
Match rule:
  ACL ID :     0, ACL CLS: 0, Name: acl6
    Set rule:
      IPv6 Nexthop: 10::1, (VRF Name: , ID: 0), Weight: 0, Flags: 0
      PBR state info ifx: GigabitEthernet 0/0, Connected: true, Track State:
valid, Flags: 0
```

Field	Description
Pbr VRF	VRF name and VRF ID.

Forward Mode	Sets the load balancing mode or to the redundancy mode for the next hop.
Forwarding	Displays whether the IP route forwarding is enabled.
Route-map index	The serial number and the type of the sub-map.
Match rule	Match rule
Set rule	Set rule.
PBR state info	PBR private data information, such as outbound interface and the link state of the next hop.

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

2.17 show ipv6 pbr statistics

Use this command to display the IPv6 PBR forwarded packet count.

show ip pbr statistics [**interface** *if-name* **| local**]

Parameter Description

Parameter	Description
interface *if-name*	Specifies the interface name. If the interface name is specified, the IPv6 PBR forwarded packet count of this interface is displayed. Otherwise, the IPv6 PBR forwarded packet count of all interfaces where the IPv6 PBR is enabled is displayed.
local	Displays the IPv6 PBR forwarded packet count on the local interface.

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide N/A

Configuration Examples The following example displays the IPv6 PBR forwarded packet count.

```
Ruijie#show ipv6 pbr statistics
IPv6 Policy-based route statistic
 gigabitEthernet 0/1
   statistics : 20
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

2.18 show ipv6 policy

Use this command to display which interfaces are configured with IPv6 PBR.

show ipv6 policy [*route-map-name*]

Parameter Description

Parameter	Description
route-map-name	Name of the PBR router map.

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide N/A

Configuration Examples The following example displays the current PBR applied in the system.

```
Ruijie#show ipv6 policy
Banlance Mode: redundance
Interface               Route map
VLAN 1                   RM_for_Vlan_1
VLAN 2                   RM_for_Vlan_2
```

Field	Description
Balance Mode	The current PBR running mode.
Interface	The name of interface with PBR applied.
Route map	The name of route map applied on the interface.

Related Commands

Command	Description
show route-map	Displays the current configured route map.

Platform Description N/A

3 RIP Commands

3.1 auto-summary

Use this command to enable automatic summary of RIP routes. Use the **no** form of this command to disable this function

auto-summary

no auto-summary

Parameter Description

Parameter	Description
N/A	N/A

Defaults Automatic summary of RIP routes is enabled by default

Command Mode Routing progress configuration mode

Usage Guide Automatic RIP route summary means the subnet routes will be automatically summarized into the routes of the classified network when they traverse through the subnet. Automatic route summary is enabled by default for RIPv1 and RIPv2.

Automatic RIP route summary improves the flexibility and effectiveness of the network. If the summarized route exists, the sub-routes contained in the summarized route cannot be seen in the

routing table, reducing the size of the routing table significantly.

Advertising the summarized route is more efficient than advertising individual routes in light of the following factors:

- The summarized route is always processed preferentially when you query the RIP database.
- Any sub-route is ignored when you query the RIP database, reducing the processing time.
- If you want to learn the specific sub-routes instead of the summarized route, disable the automatic route summary function. Only when RIPv2 is configured, the automatic route summary function can be disabled. For the RIPv1, the automatic route summary function is always enabled.

The range of the supernet route is wider than that of the classful network. Therefore, this command takes no effect on the supernet route.

Configuration Examples

The following example disables automatic route summary of RIPv2.

```
Ruijie (config)# router rip
Ruijie (config-router)# version 2
Ruijie (config-router)# no auto-summary
```

Related Commands

Command	Description
version	Defines the RIP software versions: v1 or v2. Both v1 and v2 are supported by default.

Platform Description

N/A

3.2 default-information originate

Use this command to generate a default route in the RIP progress. Use the **no** form of this command to delete the generated default route.

default-information originate [**always] [metric** *metric-value*] [**route-map** *map-name*]

no default-information originate [**always**] [**metric**] [**route-map** *map-name*]

Parameter Description

Parameter	Description
always	(Optional) Enables RIP to generate the default route, no matter whether the default route exists or not.
metric *metric-value*	(Optional) The original metric value of the default route with the value range 115 of metric-value.
route-map *map-name*	(Optional) Name of the associated route-map. Route-map is not associated by default.

Defaults No default route is generated by default.

The default metric value is 1.

Command Mode Routing process configuration mode

Usage Guide

By default, RIP will not advertise the default route if the default route exists in the routing table of the router. In this case, use the **default-information originate** command to notify the neighbor of the default route.

With the parameter always configured, no matter whether the default route exists in the RIP routing process or not, the default route will be advertised to the neighbor but is not shown in the local routing table. You can use the **show ip rip database** command to view the RIP routing information database to confirm whether the default route is generated.

Use the parameter **route-map** to control more about the default route advertised to RIP. For example, use the **set metric** command to set the metric value of the default route.

The route-map set metric rule takes precedence over the parameter metric value configuration of the default route. If the parameter metric is not configured, the default metric value is used by the default route.

If the default route can be generated in the RIP process by using this command, RIP will not learn the default route advertised from the neighbor.

For the default route generated by using the ip default-network command, the default-information originate command is required to add the default route to RIP.

Configuration Examples

The following example generates a default route to the RIP routing table.

```
Ruijie(config-router)# default-information originate always
```

Related Commands

Command	Description
ip rip default-information	Notifies the default route through an interface.
redistribute	Redistributes the routes from other protocols to RIP.

Platform

N/A

Description

3.3 default-metric

Use this command to define the default RIP metric value. Use the **no** form of this command to restore the default setting.

default-metric *metric-value*

no default-metric

Parameter Description

Parameter	Description
metric-value	Indicates the default metric value with the range from 1 to 16. If the metric value is greater than or equal to 16, the RGNOS regards the route unreachable.

Defaults The default is 1.

Command Mode Routing process configuration mode

Usage Guide This command needs to work with the command **redistribute**. When the routes are redistributed to the RIP routing process from a routing protocol process, the route metric value cannot be converted due to the incompatibility of the metric calculation mechanisms for different protocols. During the conversion, therefore, it is required to redefine the metric values of redistributed routes in the RIP routing domain. If there is no clear definition of the metric value in redistributing a routing protocol process, the RIP uses the metric value defined with **default-metric**. If the metric value is defined, this

value overwrites the metric value defined with default-metric. If this command is not configured, the default value of default-metric is 1.

Configuration Examples The following example enables the RIP routing protocol to redistribute the routes learned by the OSPF routing protocol, whose initial RIP metric value is set to 3.

```
Ruijie (config)# router rip
Ruijie (config-router)# default-metric 3
Ruijie (config-router)# redistribute ospf 100
```

Related Commands

Command	Description
redistribute	Redistributes the routes from one routing domain to another routing domain.

Platform Description N/A

3.4 distance

Use this command to set the management distance of the RIP route. Use the **no** form of this command to restore the default setting.

distance *distance* [*ip-address wildcard*]

no distance [*distance ip-address wildcard*]

Parameter

Parameter	Description

Description

distance	Sets the management distance of a RIP route, an integer in the range from 1 to 255.
ip-address	Indicates the prefix of the source IP address of the route.
wildcard	Defines the comparison bit of the IP address, where 0 means accurate matching and 1 means no comparison.

Defaults The default is 120.

Command Mode Routing process configuration mode

Usage Guide Use this command to set the management distance of the RIP route.

You can use this command to create several management distances with source address prefixes. When the source address of the RIP route is within the range specified by the prefixes, the corresponding management distance is applied; otherwise, the route uses the management distance configured by the RIP.

Configuration Examples The following example sets the management distance of the RIP route to 160, and specifies the management distance of the route learned from 192.168.2.1 as 123.

```
Ruijie(config)# router rip
Ruijie(config-router)# distance 160
Ruijie(config-router)# distance 123 192.168.12.1 0.0.0.0
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

3.5 distribute-list in

Use this command to control route update for route filtering. Use the **no** form of this command to restore the default setting.

distribute-list { [*access-list-number* | *name*] | **prefix** *prefix-list-name* [**gateway** *prefix-list-name*] | [**gateway** *prefix-list-name*] } **in** [*interface-type interface-number*]

no distribute-list { [*access-list-number* | *name*] | **prefix** *prefix-list-name* [**gateway** *prefix-list-name*] | [**gateway** *prefix-list-name*] } **in** [*interface-type interface-number*]

Parameter Description

Parameter	Description
access-list-number | *name*	Specifies the ACL. Only the routes that are allowed by the ACL can be accepted.
prefix *prefix-list-name*	Uses the prefix list to filter the routes.
gateway *prefix-list-name*	Uses the prefix list to filter the source of the routes.
interface-type interface-number	(Optional) Applies the distribution list only to a specified interface.

Defaults The distribution list is not defined by default.

Command Mode Routing process configuration mode

Usage Guide To deny receiving some specified routes, you can process all the received route update packets by configuring the route distribute control list.

Without any interface specified, the system will process the route update packets received on all the interfaces.

Configuration Examples The following example enables RIP to control the routes received from the Fastethernet 0/0, only permitting the routes starting with 172.16.

```
Ruijie (config)# router rip
Ruijie (config-router)# network 200.168.23.0
Ruijie (config-router)# distribute-list 10 in fastethernet 0/0
Ruijie (config-router)# no auto-summary
Ruijie (config-router)# access-list 10 permit 172.16.0.0 0.0.255.255
```

Related Commands

Command	Description
access-list	Defines the ACL rule.
prefix-list	Defines the prefix list.

Platform Description N/A

3.6 distribute-list out

Use this command to control route update advertisement for filtering routes. Use the **no** form of this command to restore the default setting.

distribute-list { [*access-list-number* | *name*] **| prefix** *prefix-list-name* } **out** [*interface* **|** [**connected | ospf** *process-id* **| rip | static**]]

no distribute-list { [*access-list-number* | *name*] | **prefix** *prefix-list-name* } **out** [*interface* **|** [**connected | ospf** *process-id* **| rip | static**]]

Parameter Description

Parameter	Description
access-list-number | *name*	Specifies the ACL.
prefix *prefix-list-name*	Uses the prefix list to filter routes.
interface	(Optional) Applies route update advertisement control to a specified interface in the distribution list.
connected	(Optional) Applies route update advertisement control to only connected routes in this distribution list.
ospf *process-id*	(Optional) Applies route update advertisement control to only routes introduced from OSPF in this distribution list. *process-id* specifies an OSPF instance.
rip	(Optional) Applies route update advertisement control to only RIP routes in this distribution list.

static	(Optional) Applies route update advertisement control to only static routes in this distribution list.

Defaults No route update advertisement is configured by default.

Command Mode Routing process configuration mode

Usage Guide If this command relates to none of optional parameters, route update advertisement control applies to all interfaces. If this command relates to interface options, route update advertisement control applies to only the specified interface. If this command relates to other route process parameters, route update advertisement control applies to only the specific route process.

Configuration Examples The following example advertises only the 192.168.12.0/24 route.

```
Ruijie (config)# router rip
Ruijie (config-router)# network 200.4.4.0
Ruijie (config-router)# network 192.168.12.0
Ruijie (config-router)# distribute-list 10 out
Ruijie (config-router)# version 2
Ruijie (config-router)#access-list 10 permit 192.168.12.0 0.0.0.255
```

Related Commands

Command	Description
access-list	Defines the ACL rule.
prefix-list	Defines the prefix list.

redistribute	Configures route redistribution.

Platform Description N/A

3.7 enable mib-binding

Use this command to bind a MIB with a specified RIP instance. Use the **no** form of this command to restore the default setting

enable mib-binding

no enable mib-binding

Parameter Description

Parameter	Description
N/A	N/A

Defaults By default, the MIB is bound with the RIP instance.

Command Mode Routing process configuration mode.

Usage Guide As RIP MIB does not have RIP instance information, you can only operate only one RIP instance using SNMP. By default, RIP MIB is bound with the RIP instance. You can only operate this RIP instance. If you want to operate another RIP instance of a specified VRF through SNMP, you can use this command to bind the MIB with this instance.

Configuration Examples The following example operates the RIP instance.

```
Ruijie(config)# router rip
Ruijie(config-router-af)# enable mib-binding
```

Related Commands

Command	Description
show ip rip	Displays the global configuration of RIP.

Platform Description N/A

3.8 graceful-restart

Use this command to configure the RIP graceful restart (GR) function for a device. Use the **no** form of this command to restore the default configuration.

graceful-restart [**grace-period** *grace-period*]

no graceful-restart [**grace-period**]

Parameter

Parameter	Description

Description

graceful-restart	Enables the GR function.
grace-period	(Optional) Configures the grace period.
grace-period	(Optional) Indicates the user-defined GR period. The default value is the smaller value between twice the update time and 60 seconds. The range is from 1 to 1,800. The unit is second.

Defaults This function is disabled by default.

Command Mode Routing process configuration mode

Usage Guide The GR function is configured on the RIP instances. Different parameters can be configured for different RIP instances.

The GR period refers to the time from the startup to the end of RIP GR. During this period, the forwarding table remains unchanged and the RIP route is restored to the state before protocol restart. When the GR period expires, RIP exits the GR state and performs normal RIP operation.

The **graceful-restart grace-period** command enables users to modify GR period. Note: Make sure that GR is completed before the RIP route is validate and after an RIP route update cycle elapses. If an improper value is configured, non-stop data forwarding cannot be ensured during the GR process. For example, if the GR period is longer than the time when the neighbor's route is unavailable and GR is not completed before the route is validated, then the neighbor is not re-informed of the route and forwarding of the neighbor's route is terminated when it is validated, which results in data forwarding interruption. Therefore, unless otherwise specified, it is not recommended to adjust the GR period. If the period needs to changed, determine that the grace period is longer than the route update cycle and shorter than the time when the route is unavailable in combination with the configuration of the

timers basic command.

During the RIP GR period, the network must be stable.

Configuration Examples

The following example enables the RIP GR function and configures the GR period parameters of the GR function.

```
Ruijie(config)# router rip
Ruijie(config-router)# graceful-restart grace-period 90
```

Related Commands

Command	Description
timers basic	Configures RIP timers.

Platform Description

N/A

3.9 ip rip authentication key-chain

Use this command to enable RIP authentication and specify the keychain used for RIP authentication. Use the **no** form of this command to restore the default setting.

ip rip authentication key-chain *name-of-keychain*

no ip rip authentication key-chain

Parameter

Parameter	Description

Description

name-of-keychain	Indicates the name of the keychain, which specifies the keychain used for RIP authentication.

Defaults The keychain is not associated by default.

Command Mode Interface configuration mode

Usage Guide If the keychain is specified in the interface configuration, use the key chain global configuration command to define the keychain. Otherwise, RIP data packet authentication fails.

RIPv2 instead of RIPv1 supports authentication of the RIP data packet.

Configuration Examples The following example enables RIP authentication on the fastEthernet 0/1 with the associated keychain ripchain.

```
Ruijie (config)#interface fastEthernet 0/1
Ruijie (config-if-FastEthernet 0/1)#ip rip authentication key-chain ripchain
```

Meanwhile, use the **key chain** command to define this keychain in global configuration mode.

```
Ruijie(config)#key chain ripchain
Ruijie(config-keychain)#key 1
Ruijie(config-keychain-key)#key-string Hello
```

Related Commands

Command	Description

ip rip authentication mode	Defines the RIP authentication mode.
ip rip authentication text-password	Enables RIP authentication, and sets the password string of RIP plaintext authentication. RIP data packet authentication is supported only by RIPv2.
ip rip receive version	Defines the version of RIP packets received on the interface.
ip rip send version	Defines the version of RIP packets sent on the interface.
key chain	Defines the keychain and enters keychain configuration mode.

Platform Description N/A

3.10 ip rip authentication mode

Use this command to define the RIP authentication mode. Use the **no** form of this command to restore the default setting.

ip rip authentication mode { **text | md5** }

no ip rip authentication mode

Parameter Description

Parameter	Description

text	Configures RIP authentication as plaintext authentication.
md5	Configures RIP authentication as MD5 authentication.

Defaults It is plaintext authentication by default.

Command Mode Interface configuration mode

Usage Guide During the RIP authentication configuration process, the RIP authentication modes of all devices requiring exchange of RIP routing information must be the same. Otherwise, RIP packet exchange will fail.

If the plaintext authentication mode is adopted, but the password string of the plaintext authentication or the associated keychain is not configured, no authentication occurs. In the same way, if the MD5 authentication mode is adopted, but the associated keychain is not configured, no authentication occurs.

RIPv2 instead of RIPv1 supports authentication of the RIP data packet.

Configuration Examples The following example configures the RIP authentication mode on the fastEthernet 0/1 as MD5.

```
Ruijie (config)#interface fastEthernet 0/1
Ruijie (config-if-FastEthernet 0/1)# ip rip authentication mode md5
```

Related Commands

Command	Description

ip rip authentication key-chain	Enables the RIP authentication mode and specifies the keychain used for RIP authentication. Only RIPv2 supports authentication of the RIP data packet.
ip rip authentication text-password	Enables the RIP authentication mode, and sets the password string of RIP plaintext authentication. Only RIPv2 supports authentication of the RIP data packet.
key chain	Defines the keychain and enters the keychain configuration mode

Platform Description N/A

3.11 ip rip authentication text-password

Use this command to enable RIP authentication and set the password string of RIP plaintext authentication. Use the **no** form of this command to restore the default setting.

ip rip authentication text-password [**0** | **7**] *password-string*

no ip rip authentication text-password

Parameter Description

Parameter	Description
0	Specifies that the key is displayed as plaintext.
7	Specifies that the key is displayed as cipher text.

password-string	Indicates the password string of the plaintext authentication, in the length of 1-16 bytes.

Defaults No password string of RIP plaintext authentication is configured by default.

Command Mode Interface configuration mode

Usage Guide This command works only in plaintext authentication mode.

To enable the RIP plaintext authentication function, use this command to configure the corresponding password string, or use the associated key chain to obtain the password string. The latter takes the precedence over the former one.

RIPv1 does not support RIP authentication but RIPv2 does.

Configuration Examples The following example enables the RIP plaintext authentication on fastEthernet 0/1 and sets the password string to hello.

```
Ruijie(config)#interface fastEthernet 0/1
Ruijie(config-if-FastEthernet 0/1)# ip rip authentication text-password hello
```

Related Commands

Command	Description
ip rip authentication mode	Defines the RIP authentication mode.
ip rip authentication key-chain	Enables the RIP authentication mode and

	specifies the keychain used for RIP authentication. Only RIPv2 supports authentication.

Platform Description N/A

3.12 ip rip default-information

Use this command to advertise the default route through a RIP interface. Use the **no** form of this command to restore the default setting.

ip rip default-information { **only** | **originate** } [**metric** *metric-value*]

no ip rip default-information

Parameter Description

Parameter	Description
only	Notifies the default route rather than other routes.
originate	Notifies the default route and other routes.
metric *metric-value*	Specifies the metric value of the default route, in the range from1 to 15.

Defaults No default route is configured by default. The default metric value is 1.

Command Mode Interface configuration mode

Usage Guide After you configure this command on a specified interface, a default route is generated and notified through the interface. If the **ip rip default-information** command of the interface and the **default-information originate** command of the RIP process are configured at the same time, only the default route of the interface is advertised.

RIP will no longer learn the default route notified by the neighbor if any interface is configured with the ip rip default-information command.

Configuration Examples The following example creates a default route which is notified on ethernet0/1 only.

```
Ruijie(config)#interface ethernet 0/1
Ruijie(config-if-Ethernet 0/1)#ip rip default-information only
```

Related Commands

Command	Description
default-information originate	Generates a default route in the RIP process.

Platform Description N/A

3.13 ip rip receive enable

Use this command to enable RIP to receive the RIP data package on a specified interface. Use the **no** form of this command to restore the default setting.

ip rip receive enable

no ip rip receive enable

Parameter Description

Parameter	Description
N/A	N/A

Defaults RIP packages can be received through the interface by default.

Command Mode Interface configuration mode

Usage Guide To prevent an interface from receiving RIP packets, use the no form of this command in interface configuration mode. This command works on interfaces configured with this command. You can use the **default** form of this command to enable the interface to receive the RIP data package.

Configuration Examples The following example prohibits receiving RIP data packages on fastEthernet 0/1.

```
Ruijie (config)# interface fastEthernet 0/1
Ruijie (config-if-FastEthernet 0/1)# no ip rip receive enable
```

Related Commands

Command	Description

ip rip send enable	Enables or disables the interface to send RIP data packages.
passive-interface	Configures a passive RIP interface.

Platform Description N/A

3.14 ip rip receive version

Use this command to define the version of RIP packets received on an interface. Use the **no** form of this command to restore the default setting.

ip rip receive version [**1**] [**2**]

no ip rip receive version

Parameter Description

Parameter	Description
1	(Optional) Receives only RIPv1 packets.
2	(Optional) Receives only RIPv2 packets.

Defaults The default behavior depends on the configuration with the version command.

Command Mode Interface configuration mode

Usage Guide This command overwrites the default configuration of the **version** command. It affects only RIP packet receiving through the interface and allows RIPv1 and RIPv2 packets to be received on the interface at the same time. If the command is configured without parameters, data package receiving depends on the configuration of the version.

Configuration Examples The following example enables receiving both RIPv1 and RIPv2 data packages.

```
Ruijie (config)#interface fastEthernet 0/1
Ruijie (config-if-FastEthernet 0/1)# ip rip receive version 1 2
```

Related Commands

Command	Description
version	Defines the default version of the RIP packets received/sent on the interface.

Platform Description N/A

3.15 ip rip send enable

Use this command to enable RIP to send a RIP data package on a specified interface. Use the **no** form of this command to restore the default setting.

ip rip send enable

no ip rip send enable

Parameter Description

Parameter	Description
N/A	N/A

Defaults RIP packages can be sent through the interface by default.

Command Mode Interface configuration mode

Usage Guide To prevent an interface from sending RIP packets, use the **no** form of this command in interface configuration mode. This command works on interfaces configured with this command. You can use the **default** form of this command to enable the interface to send the RIP data package.

Configuration Examples The following example prohibits sending RIP data packages on fastEthernet 0/1.

```
Ruijie (config)# interface fastEthernet 0/1
Ruijie (config-if-FastEthernet 0/1)# no ip rip send enable
```

Related Commands

Command	Description
ip rip receive enable	Enables or disables receiving RIP packets on

	the interface.
passive-interface	Configures a passive RIP interface.

Platform Description N/A

3.16 ip rip send supernet-routes

Use this command to enable RIP to send the supernet route on a specified interface. Use the **no** form of this command to disable this function.

ip rip send supernet-routes

no ip rip send supernet-routes

Parameter Description

Parameter	Description
N/A	N/A

Defaults This function is enabled by default.

Command Mode Interface configuration mode

Usage Guide When the RIPv1 router monitors a RIPv2 router response packet and if the supernet routing information is monitored, incorrect route information is learned because the RIPv1 ignores the subnet mask of the routing information. In this case, you are advised to use the no form of this command on the RIPv2 router to disable advertising the supernet route on the corresponding interface. This command works only on interfaces configured with this command.

This command is only valid upon sending the RIPv2 packets on the interface and it is used to control sending the supernet route.

Configuration Examples The following example disables sending RIP supernet routes on the fastEthernet 0/1 interface.

```
Ruijie(config)# interface fastEthernet 0/1
Ruijie(config-if-FastEthernet 0/1)# no ip rip send supernet-routes
```

Related Commands

Command	Description
version	Defines the RIP version
ip rip send enable	Enables or disables sending the RIP package on the interface.

Platform Description N/A

3.17 ip rip send version

Use this command to define the version of the RIP packets sent on the interface. Use the **no** form of this command to restore the default setting.

ip rip send version [**1**] [**2**]

no ip rip send version

Parameter Description

Parameter	Description
1	(Optional) Receives only RIPv1 packets.
2	(Optional) Receives only RIPv2 packets.

Defaults The default behavior depends on the configuration with the version command.

Command Mode Interface configuration mode

Usage Guide This command overwrites the default configuration of the **version** command. It affects only RIP packet sending through the interface and allows RIPv1 and RIPv2 packages sent on the interface at the same time. If the command is configured without parameters, package receiving depends on the configuration of the version.

Configuration Examples The following example enables sending both RIPv1 and RIPv2 packages on the fastEthernet 0/1 interface.

```
Ruijie (config)# interface fastEthernet 0/1
Ruijie (config-if-FastEthernet 0/1)# ip rip send version 1 2
```

Related Commands

Command	Description
version	Defines the default version of the RIP packets received/sent on the interfaces.

Platform Description N/A

3.18 ip rip split-horizon

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

ip rip split-horizon [**poisoned-reverse**]

no ip rip split-horizon [**poisoned-reverse**]

Parameter Description

Parameter	Description
poisoned-reverse	(Optional) Enables split horizon with poisoned reverse.

Defaults This function is enabled by default.

Command Mode Interface configuration mode

Usage Guide When multiple devices are connected to the IP broadcast network and run a distance vector routing protocol, the split horizon mechanism is required to prevent loop. The split horizon prevents the device from advertising routing information from the interface that learns that information, which optimizes routing information exchange between multiple devices.

For non-broadcast multi-path access networks (such as frame relay and X.25), split horizon may cause some devices to be unable to learn all routing information. Split horizon may need to be disabled in this case. If an interface is configured the secondary IP address, attentions shall be paid also for split horizon.

If the **poisoned-reverse** parameter is configured, split horizon with poisoned reverse is enabled. In this case, devices still advertise the route information through the interface from which the route information is learned. However, the metric value of the route information is set to unreachable.

The RIP routing protocol is a distance vector routing protocol, and the split horizon issue shall be cautioned in practical applications. If it is unsure whether split horizon is enabled on the interface, use the show ip rip command to judge. This function makes no influence on the neighbor defined with the **neighbor** command.

Configuration Examples The following example disables the RIP split horizon function on the interface fastethernet 0/0.

```
Ruijie (config)# interface fastethernet 0/1
Ruijie (config-if)# no ip rip split-horizon
```

Related Commands

Command	Description
neighbor (RIP)	Defines the IP address of the neighbor of RIP.
validate-update-source	Enables the source address authentication of the RIP route update message.

Platform Description N/A

3.19 ip rip summary-address

Use this command to configure port-level convergence through an interface. Use the **no** form of this command to disable this function.

ip rip summary-address *ip-address ip-network-mask*

no ip rip summary-address *ip-address ip-network-mask*

Parameter Description

Parameter	Description
ip-address	Indicates the IP addresses to be converged.
ip-network-mask	Indicates the subnet mask of the specified IP address for route convergence.

Defaults The RIP routes are automatically converged to the classful network edge by default.

Command Mode Interface configuration mode

Usage Guide The **ip rip summary-address** command converges an IP address or a subnet on a specified port. RIP routes are automatically converged to the classful network edge. The classful subnet can be configured through only port convergence.

The summary range configured by this command cannot be a super class network, that is, the configured mask length is greater than or equal to the natural mask length of the network.

Configuration Examples The following example disables the automatic route convergence function of RIPv2. Interface convergence is configured so that fastEthernet 0/1 advertises the converged route 172.16.0.0/16.

```
Ruijie (config)# interface fastEthernet 0/1
Ruijie (config-if-FastEthernet 0/1)# ip rip summary-address 172.16.0.0
255.255.0.0
Ruijie (config-if-FastEthernet 0/1)# ip address 172.16.1.1 255.255.255.0
Ruijie (config)# router rip
Ruijie (config-router)# network 172.16.0.0
Ruijie (config-router)# version 2
Ruijie (config-router)# no auto-summary
```

Related Commands

Command	Description
auto-summary	Enables the automatic convergence of RIP routes.

Platform Description N/A

3.20 ip rip triggered

Use this command to enable triggered RIP based on links. Use the **no** form of this command to restore the default setting.

ip rip triggered

ip rip triggered retransmit-timer *timer*

ip rip triggered retransmit-count *count*

no ip rip triggered

no ip rip triggered retransmit-timer

no ip rip triggered retransmit-count

Parameter Description

Parameter	Description
retransmit-timer *timer*	Configures the interval at which the Update Request and Update Response packets are retransmitted. The range is from 1 to 3,600. The unit is second. The default is five.
retransmit-count *count*	Configures the maximum times that the Update Request and Update Response packets are retransmitted. The range is from 1 to 3600. The default is 36.

Defaults This function is disabled by default.

Command Mode Interface configuration mode

Usage Guide Triggered RIP (TRIP) is the extension of RIP on the wide area network (WAN), mainly used for demand-based links.

With the TRIP function enabled, RIP no longer sends route updates periodically and sends route updates to the WAN interface only if:

Update Request packets are received.

RIP routing information is changed.

Interface state is changed.

The router is started.

As periodical RIP update is disabled, the confirmation and retransmission mechanism is required to ensure that update packets are sent and received successfully over the WAN. The **retransmit-timer** and **retransmit-count** commands can be used to specify the retransmission interval and maximum retransmission times for request and update packets.

- The function can be enabled in the case of the following conditions: a) The interface has only one neighbor. b) There are multiple neighbors but they interact information using unicast packets. You are advised to enable the function for link layer protocols such as PPP, frame relay, and X.25.
- You are advised to enable split horizon with poison reverse on the interface enabled with the function; otherwise invalid routing information might be left.
- Make sure that the function is enabled on all routers on the same link; otherwise the function will be invalid and the routing information cannot be exchanged correctly.
- To enable the function, make sure that the RIP configuration is the same on both ends of the link, such as RIP authentication and the RIP version supported by the interface.
- If this function is enabled on this interface, the source address of packets on this interface will be checked no matter whether the source IP address verification function (validate-update-source) is enabled.

Configuration Examples The following example enables TRIP and sets the retransmission interval and maximum retransmission time to 10 seconds and 18 respectively for Update Request and Update Response packets.

```
Ruijie(config)# interface fastEthernet 0/1
```

```
Ruijie(config-if-FastEthernet 0/1)# ip rip triggered
Ruijie(config-if-FastEthernet 0/1)# ip rip triggered retransmit-timer 10
Ruijie(config-if-FastEthernet 0/1)# ip rip triggered retransmit-count 18
```

Related Commands

Command	Description
show ip rip database	Displays the summarized routing information of the RIP database.
show ip rip interface	Displays the RIP interface information.
ip rip split-horizon	Configures RIP split horizon.

Platform Description N/A

3.21 ip rip v2-broadcast

Use this command to send RIPv2 packets in broadcast rather than multicast mode. Use the **no** form of this command to restore the default setting.

ip rip v2-broadcast

no ip rip v2-broadcast

Parameter Description

Parameter	Description
N/A	N/A

Defaults The default behavior depends on the configuration of the version command.

Command Mode Interface configuration mode

Usage Guide This command overwrites the default of the **version** command. This command affects only sending RIP packets on the interface. This command allows RIPv1 and RIPv2 packages sent on the interface simultaneously. If this command is configured without parameters, package receiving depends on the version setting.

Configuration Examples The following example sends RIPv2 packets in broadcast mode on the fastEthernet 0/1 interface.

```
Ruijie(config)# interface fastEthernet 0/1
Ruijie(config-if-FastEthernet 0/1)# no ip rip split-horizon
```

Related Commands

Command	Description
version	Defines the default version of the RIP packets received and sent on the interface.

Platform Description N/A

3.22 neighbor

Use this command to define the IP address of a RIP neighbor. Use the **no** form of this command to restore the default setting.

neighbor *ip-address*

no neighbor *ip-address*

Parameter Description

Parameter	Description
ip-address	Indicates the IP address of the neighbor. The IP address must be that of the network connected to the local device.

Defaults The neighbor is not defined by default.

Command Mode Routing process configuration mode

Usage Guide By default, RIPv1 uses the IP broadcast address (255.255.255.255) to advertise routing information, and RIPv2 uses the multicast address 224.0.0.9 to do so. If you do not want to allow all the devices on the broadcast network or non-broadcast multi-path access network to receive routing information, use the **passive-interface** command to configure related interfaces as passive interfaces and then define only some neighbors who can receive the routing information. This command has no impact on the receiving of RIP information. The passive interface is configured. No request packet is sent after the interface is enabled.

Configuration Examples The following example creates a VRF with the name of vpn1 and creates its RIP instance.

```
Ruijie(config)# ip vrf vpn1
Ruijie(config-vrf)# exit
Ruijie(config)# interface fastEthernet 1/0
Ruijie(config-if-FastEthernet 0/1)# ip vrf forwarding vpn1
Ruijie(config-if-FastEthernet 0/1)# ip address 192.168.1.1 255.255.255.0
Ruijie(config)# router rip
Ruijie(config-router)# address-family ipv4 vrf vpn1
Ruijie(config-router)# network 192.168.1.0
Ruijie(config-router)# exit-address-family
```

Related Commands

Command	Description
passive-interface	Configures the interface as a passive interface.

Platform Description N/A

3.23 network

Use this command to define the list of networks to be advertised in the RIP routing process. Use the **no** form of this command to delete the defined network.

network *network-number* [*wildcard*]

no network *network-number* [*wildcard*]

Parameter Description

Parameter	Description
network-number	Indicates the network number of the directly-connected network. The network number is a natural one. All interfaces whose IP addresses belong to that natural network can send/receive RIP packages.
wildcard	Defines the IP address comparing bit: 0 refers to accurate matching, and 1 refers to no comparison.

Defaults N/A

Command Mode Routing process configuration mode

Usage Guide The *network-number* and *wildcard* parameters can be configured simultaneously to enable the IP address of the interface within the IP address range to join RIP running.

Without the *wildcard* parameter, RGOS make the interface IP address within the classful address range join the RIP running.

Only when the IP address of an interface is in the network list defined by RIP, RIP route update packets can be received and sent on the interface.

Configuration Examples The following example defines two network numbers associated with RIP and allows the interface IP address between 192.168.12.0/24 and 172.16.0.0/24 to join RIP running.

```
Ruijie (config)# router rip
Ruijie (config-router)# network 192.168.12.0
Ruijie(config-router)# network 172.16.0.0 0.0.0.255
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

3.24 offset-list

Use this command to increase the metric value of received or sent RIP routes. Use the **no** form of this command to restore the default setting.

offset-list { access-list-number | name } { **in** | **out** } offset [interface-type interface-number]

no offset-list { access-list-number | name { **in** | **out** } offset [interface-type interface-number]

Parameter Description

Parameter	Description
access-list-number	*name*	Specifies the ACL.
in	Modifies the metric of the received routes using the ACL.
out	Modifies the metric of the sent routes using the ACL.
offset	Indicates the offset of changed metric values. The value is in the range from 0 to16.

interface-type	Applies the ACL to a specified interface.
interface-number	Specifies the interface number.

Defaults No offset is specified by default.

Command Mode Routing process configuration mode

Usage Guide If a RIP route matches against both the offset-list of the specified interface and the global offset-list, it will increase the metric value of the offset-list of the specified interface.

Configuration Examples The following example increases the metric of the RIP routes by 7 in the range specified by ACL 7.

```
Ruijie (config-router)# offset-list 7 out 7
```

The following example increases the metric of the RIP routes by 7 in the range specified by ACL 7 and learned by fastethernet 0/1.

```
Ruijie (config-router)# offset-list 8 in 7 fastethernet 0/1
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

3.25 output-delay

Use this command to modify the delay to send RIP update packets. Use the **no** form of this command to restore the default setting.

output-delay *delay*

no output-delay

Parameter Description

Parameter	Description
delay	Sets the delay to send RIP update packets, in the range from 8 to 50 in the unit of milliseconds.

Defaults No sending delay is configured by default.

Command Mode Routing process configuration mode

Usage Guide In normal cases, the size of a RIP update packet is 512 bytes including 25 routes. If the number of updated routes is greater than 25, update packets will be sent through multiple routes. Note that the update packets should be sent as fast as possible.

However, when a high-speed device sends a large number of packets to a low-speed device, the

low-speed device may not process all the packets timely, resulting in packet loss. In this case, you can use this command to increase the delay to send packets on the high-speed device so that the low-speed device can process all the update packets.

Configuration Examples The following example sets the delay to send RIP update packets to 30 milliseconds.

```
Ruijie(config)# router rip
Ruijie(config-router)# output-delay 30
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

3.26 passive-interface

Use this command to disable the function of sending update packets on an interface. Use the **no** form of this command to restore the default setting.

passive-interface { **default |** *interface-type interface-num* }

no passive-interface { **default |** *interface-type interface-num* }

Parameter Description

Parameter	Description

default	Sets all interfaces to the passive interfaces.
interface-type interface-num	Indicates the interface type and number.

Defaults Interfaces are set to the non passive interfaces by default.

Command Mode Routing process configuration mode

Usage Guide The **passive-interface default** command sets all interfaces to the passive interfaces. You can use **no passive-interface** *interface-type interface-num* command to set specified interfaces as non-passive interfaces.

After you set an interface to the passive interface, RIP route update packets will no longer be sent but can be received through the interface. In this case, route update packets can be sent to a specified neighbor through the interfaces by using the **neighbor** command. You can use the **ip rip send enable** and **ip rip receive enable** commands to control whether route update packets can be sent or received through the interface.

Configuration Examples The following example sets all interfaces to the passive interfaces and then sets ethernet0/1 to the non-passive interface.

```
Ruijie(config-router)# passive-interface default
Ruijie(config-router)# no passive-interface gigabitEthernet 0/1
```

Related Commands

Command	Description

ip rip receive enable	Enables or disables receiving RIP packets on the interface.
ip rip send enable	Enables or disables sending RIP packets on the interface.

Platform Description N/A

3.27 redistribute

Use this command to redistribute external routes in route configuration mode. Use the **no** form of this command to restore the default setting.

redistribute { **connected** | **ospf** *process-id* | **static** } [**match** { i**nternal** | **external** [**1|2**] | **nssa-external** [**1|2**] }] [**metric** *metric-value*] [**route-map** *route-map-name*]

no redistribute { **connected** | **ospf** *process-id* | **static** } [**match** { **internal** | **external** [**1|2**] | **nssa-external** [**1|2**] }] [**metric** *metric-value*] [**route-map** *route-map-name*]

Parameter Description

Parameter	Description
connected	Is redistributed from a connected route.
ospf *process-id*	Is redistributed from OSPF and specifies an OSPF instance through process-id. The value is in the range from 1 to 65535.
static	Is redistributed from static routes.
match	Is used when OSPF route redistribution is configured and filters a

	route with a specific level for redistribution.
metric *metric-value*	Sets the metric value of the redistributed route and specifies the metric value by using the metric-value parameter. The value is in the range from 1 to 16.
route-map *route-map-name*	Sets the redistribution filtering rule.

Defaults By default:

All the routes of the sub types of the instance are redistributed when you configure redistributing OSPF.

All the routes of the protocol are redistributed for other routing protocols.

The metric of the redistributed routes is 1 by default.

The route-map is not associated.

Command Mode Routing process configuration mode

Usage Guide This command is executed to redistribute external routes to RIP.

It is unnecessary to convert the metric of one routing protocol into that of another routing protocol for route redistribution, since different routing protocols use different metric measurement methods. For RIP, the metric value is calculated based on hop counts; for OSPF, the metric value is calculated based on bandwidths. Therefore, their metrics are not comparable. However, a symbolic metric value must be set for route redistribution. Otherwise, route redistribution will fail.

When you configure redistribution of OSPF routes without the match parameter, the OSPF routes of all sub types are redistributed by default. Then the first configured match parameter is used as the original one. Only the routes matching the specific type can be redistributed. The no form of this command restores the setting to the default value.

The rule of configuring the no form of the redistribute command is as follows:

1. If the no form of this command specifies certain parameters, the parameters must be restored to the default configuration.

2. If the **no** form of this command does not specify any parameter, the command must be deleted.

⚠ The redistribute command cannot redistribute the default route of other protocol to the RIP process. To this end, use the **default-information originate** command.

Configuration Examples

The following example redistributes static routes to RIP.

```
Ruijie(config-router)# redistribute static
```

Related Commands

Command	Description
default-metric *metric*	Sets the default metric of the route to be redistributed.
default-information originate	Generates the default route in the RIP process.

Platform Description

N/A

3.28 router rip

Use this command to create the RIP routing process and enter the routing process configuration mode. Use the **no** form of this command to restore the default setting.

router rip

no router rip

Parameter Description

Parameter	Description
N/A	N/A

Defaults No RIP process is running by default.

Command Mode Global configuration mode

Usage Guide One RIP routing process must be defined with one network number. If a dynamic routing protocol runs on asynchronous lines, configure the **async default routing** command on the asynchronous interface.

Configuration Examples The following example creates the RIP routing process and enters the routing process configuration mode.

```
Ruijie (config)# router rip
Ruijie(config-router)#
```

Related Commands

Command	Description

network (RIP)	Defines the network number of the RIP process.

Platform Description N/A

3.29 show ip rip

Use this command to display the RIP process information.

show ip rip

Parameter Description

Parameter	Description
N/A	N/A

Defaults N/A

Command Mode Privileged EXEC mode/ Global configuration mode/ Routing process configuration mode

Usage Guide It is used to display the three timers, routing distribution status, routing re-distribution status, interface RIP version, RIP interface and network range, metric, and distance of the RIP process quickly.

Configuration Examples The following example displays the basic information of the RIP process such as the update time and management distance.

```
Ruijie#show ip rip
Routing Protocol is "rip"
  Sending updates every 10 seconds, next due in 4 seconds
  Invalid after 20 seconds, flushed after 10 seconds
  Outgoing update filter list for all interface is: not set
  Incoming update filter list for all interface is: not set
  Default redistribution metric is 2
  Redistributing: connected
  Default version control: send version 2, receive version 2
    Interface            Send  Recv
    FastEthernet 0/1      2     2
    FastEthernet 0/2      2     2
  Routing for Networks:
    192.168.26.0 255.255.255.0
    192.168.64.0 255.255.255.0
  Distance: (default is 50)
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

3.30 show ip rip database

Use this command to display the route summary information in the RIP routing database.

show ip rip database [*network-number network-mask*] [**count**]

Parameter Description

Parameter	Description
network-number	(Optional) Indicates the ID of the subnet on which route information is to be displayed.
network-mask	Indicates the subnet mask. It must be specified if the network number is specified.
count	(Optional) Displays the abstract of the route statistics in the RIP database.

Defaults N/A

Command Mode Privileged EXEC mode/ Global configuration mode/ Routing process configuration mode

Usage Guide Only when the related sub-routes are converged, the converged address entries appear in the RIP routing database. When the last sub-route information in the converged address entries becomes invalid, the converged address information will be deleted from the database.

Configuration Examples The following example displays all converged address entries in the RIP routing database.

```
Ruijie# show ip rip database
192.168.1.0/24    auto-summary
```

```
192.168.1.0/30    directly connected, Loopback 3
192.168.1.8/30    directly connected, FastEthernet 0/1
192.168.121.0/24    auto-summary
192.168.121.0/24    redistributed
[1] via 192.168.2.22, FastEthernet 0/2
192.168.122.0/24    auto-summary
192.168.122.0/24
[1] via 192.168.4.22, Serial 0/1  00:28    permanent
```

The following example displays the converged address entries related with 192.168.121.0/24 in the RIP routing database.

```
Ruijie# show ip rip database 192.168.121.0 255.255.255.0
192.168.121.0/24    redistributed
[1] via 192.168.2.22, FastEthernet 0/1
```

The following example displays the statistical information summary of various routes in the RIP routing database.

```
Ruijie# show ip rip database count
              All    Valid   Invalid
database       5      5      0
auto-summary    5      5      0

connected      1      1      0
rip            4      4      0
```

Related Commands

Command	Description
show ip rip	Displays the information of the currently-running routing protocol process.

Platform Description N/A

3.31 show ip rip external

Use this command to display the information of the external routes redistributed by the RIP protocol.

show ip rip external [connected |ospf process-id | static]

Parameter Description

Parameter	Description
connected	Displays redistributed directly-connected routes.
ospf *process-id*	Displays redistributed OSPF routes. The process-id parameter indicates OSPF process ID. The range is from 1 to 65535.
static	Displays redistributed static routes.

Defaults N/A

Command Mode Privileged EXEC mode/ Global configuration mode/ Routing process configuration mode

Usage Guide N/A

Configuration Examples The following example displays direct routes redistributed by the RIP process.

```
Ruijie# show ip rip external
```

```
Protocol connected route:
[connected] 192.100.3.0/24 metric=0
    nhop=0.0.0.0, if=2
 [connected] 192.101.1.0/24 metric=0
    nhop=0.0.0.0, if=3
Protocol static route:
 [static] 10.1.1.1/32 metric=0
    nhop=0.0.0.0, if=4096
 [static] 10.1.2.1/32 metric=0
    nhop=0.0.0.0, if=4096
Protocol ospf 1 route:
 [ospf] 1.1.1.1/32 metric=2
    nhop=192.100.3.2, if=2
 [ospf] 90.1.1.1/32 metric=2
    nhop=192.100.3.2, if=2
```

Related Commands

Command	Description
show ip rip	Displays the information of the currently running routing protocol process.
ip vrf	Creates a VRF.

Platform Description N/A

3.32 show ip rip interface

Use this command to display the RIP interface information.

show ip rip interface [interface-type interface-number]

Parameter Description

Parameter	Description
[*interface-type interface-number*]	Displays the specified interface type and interface number (optional).

Defaults N/A

Command Mode Privileged EXEC mode/ Global configuration mode/ Routing process configuration mode

Usage Guide This command is used to display the information about RIP interfaces. If no RIP interface exists, no information is displayed.

Configuration Examples The following example displays the RIP interface information.

```
Ruijie# show ip rip interface
FastEthernet 0/1 is up, line protocol is up
Routing Protocol: RIP
Receive RIPv2 packets only
Send RIPv2 packets only
Recv RIP packet total: 0
Send RIP packet total: 3
Passive interface: Disabled
Split Horizon with Poisoned Reverse: Enabled
Triggered RIP Enabled:
Retransmit-timer: 5, Retransmit-count: 36
V2 Broadcast: Disabled
Multicast registe: Registed
Interface Summary Rip:
Not Configured
```

```
Authentication mode: Text
Authentication key-chain: ripk1
Authentication text-password: ruijie
Default-information: only, metric 5
IP interface address:
192.168.64.100/24, next update due in 14 seconds
2.2.1.1/24, next update due in 24 seconds
   neighbor 2.2.1.6, next update due in 3 seconds
   neighbor 2.2.1.77, next update due in 13 seconds
2.2.2.57/24, next update due in 16 seconds
```

Related Commands

Command	Description
show ip rip	Displays the information of the currently running routing protocol process.

Platform Description N/A

3.33 show ip rip peer

Use this command to show the RIP peer information. RIP records a summary for the RIP routing information source learnt (source addresses of RIP route update packets) for the convenience of user monitoring. This routing information source is called RIP neighbor information.

show ip rip peer [*ip-address*]

Parameter Description

Parameter	Description
ip-address	(Optional) Displays the IP address of a specified RIP neighbor.

Defaults N/A

Command Mode Privileged EXEC mode/ Global configuration mode/ Routing process configuration mode

Usage Guide This command is used to display the RIP neighbor information. If no RIP neighbor exists, no information will be displayed.

Related Commands

Command	Description
show ip rip	Displays the information of the routing protocol process that is running.

Platform Description N/A

3.34 timers basic

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

timers basic *update invalid flush*

no timers basic

Parameter Description

Parameter	Description
update	Indicates the route update time in seconds. The update keyword defines the period at which the device sends route update packets. Each time an update packet is received, the "Invalid" and "Flush" clocks are reset. By default, a route update packet is sent every 30 seconds.
invalid	Indicates the route invalid time in seconds, starting from the last valid update packet. The "invalid" defines the period when the route in the routing table becomes invalid due to no update. The invalid period of route shall be at least three times the route update period. If no update packet is received within the route invalid period, the related route becomes invalid and enters into the "invalid" state. If an update packet is received within the period, the clock resets. By default, the Invalid time is 180 seconds.
flush	Indicates the route flushing time in seconds, starting when a RIP route enters into the invalid status. When the flush time is due, the routes in the invalid status will be cleared out of the routing table. The default Flush time is 120 seconds.

Defaults By default, the update time is 30 seconds, the invalid time is 180 seconds, and the flushing time is 120 seconds.

Command Mode Routing process configuration mode

Usage Guide Adjusting the above clocks may speed up routing protocol convergence and fault recovery. Devices

connected to the same network must have consistent RIP clock values. Adjustment of RIP clocks is not recommended unless otherwise specified.

To check the current RIP clock parameters, use the **show ip rip** command.

If you set the clock to a small value on low-speed links, some risks will be caused because numerous update packets may use up the bandwidth. In general, the clocks can be configured with smaller values on Ethernet or the lines of above 2 Mbit/s to reduce the convergence time of routes.

Configuration Examples

The following example enables the RIP update packets that are sent every 10 seconds. If no update packet is received within 30 seconds, related routes become invalid and enter the invalid status. When another 90s elapses, they will be cleared.

```
Ruijie (config)# router rip
Ruijie (config-router)# timers basic 10 30 90
```

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

3.35 validate-update-source

Use this command to validate the source address of the received RIP route update packet. Use the **no** form of the command to disable this function.

validate-update-source

no validate-update-source

Parameter Description

Parameter	Description
N/A	N/A

Defaults This function is enabled by default.

Command Mode Routing process configuration mode

Usage Guide You can validate the source address of the RIP route update packet. The validation aims to ensure that the RIP routing process receives only the route update packets from the same IP subnet neighbor.

Disabling split horizon on the interface causes the RIP routing process to enable update message source address validation, no matter whether it has been configured with the **validate-update-source** command in routing process configuration mode.

In addition, for the ip unnumbered interface, the RIP routing process does not implement update message source address validation, no matter whether it has been configured with the command **validate-update-source**.

Configuration Examples The following example disables verification of the source IP address of the update packet.

```
Ruijie (config)# router rip
Ruijie (config-router)# no validate-update-source
```

Related Commands

Command	Description
ip split-horizon	Enables split horizon.
ip unnumbered	Defines the IP unnumbered interface.
neighbor (RIP)	Defines the IP address of a RIP neighbor.

Platform Description N/A

3.36 version

Use this command to define the RIP version of a device. Use the **no** form of this command to restore the default setting.

version { **1 | 2** }

no version

Parameter Description

Parameter	Description
1	Defines the RIP version 1.
2	Defines the RIP version 2.

Defaults The route update packets of RIPv1 and are received by default, but only the RIPv1 route update packets are sent.

Command Mode Routing process configuration mode

Usage Guide This command defines the RIP version running on the device. It is possible to redefine the messages of which RIP version are processed on every interface by using the **ip rip receive version** and **ip rip send version** commands.

Configuration Examples The following example configures the RIP version as version 2.

```
Ruijie (config)# router rip
Ruijie (config-router)# version 2
```

Related Commands

Command	Description
ip rip receive version	Defines the version of RIP packets received on the interface.
ip rip send version	Defines the version of RIP packets sent on the interface.
show ip rip	Displays RIP information.

Platform N/A

Description

4 RIPNG

4.1 clear ipv6 rip

Use this command to clear the RIPng routes.

clear ipv6 rip

Parameter Description

Parameter	Description
N/A	N/A

Defaults None

Command mode Privileged EXEC mode

Usage Guide Running this command removes all RIPng routes and this operation may have great impact on the RIPng protocol. This command should be used with caution.

Configuration Examples The following example clears the RIPng routes:

```
Ruijie# clear ipv6 rip
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

4.2 default-metric

Use this command to configure the default metric for RIPng. Use the **no** form of this command to restore the default value.

default-metric *metric*

no default-metric

Parameter Description

Parameter	Description
metric	Sets the default metric value. The valid range is from 1 to 16. The route is unreachable if the metric value is larger than or equal to 16.

Defaults The default value is 1.

Command mode Routing process configuration mode.

Usage Guide This command shall be used with the **redistribute** command. When redistributing the route from one route process to RIPng, due to the incompatibility of metric calculation mechanisms of different routing protocols, it fails to translate the routing metric values. To this end, the RIPng metric value shall be defined when translating the metric values. If there is no defined metric value, use the **default-metric** command to define one; and the defined metric value will overwrite the value of the **default-metric** command. By default, the **default-metric** value is 1.

Configuration Examples The following example shows how to set the RIPng metric value as 3 when redistributing OSPF process 100:

```
Ruijie(config-router)# default-metric 3
Ruijie(config-router)# redistribute ospf 100
```

Related Commands

Command	Description
redistribute	Redistributes the route from one route domain to another route domain.

Platform Description N/A

4.3 distance

Use this command to set the administrative distance of RIPng. Use the **no** form of this command to restore the default value.

distance *distance*

no distance

Parameter Description

Parameter	Description
distance	Sets the RIPng administrative distance. The range is from 1 to 254.

Defaults The default distance is 120

Command mode Routing process configuration mode.

Usage Guide N/A

Configuration The following example shows how to set the RIPng administrative distance as 160:

Examples

```
Ruijie(config)# ipv6 router rip
Ruijie(config-router)# distance 160
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

4.4 distribute-list

Use this command to filter the in/out route in the prefix list. Use the **no** form of this command to remove route filtering.

distribute-list prefix-list *prefix-list-name* { **in** | **out** } [*interface-type interface-name*]

no distribute-list prefix-list *prefix-list-name* { **in** | **out** } [*interface-type interface-name*]

Parameter Description

Parameter	Description
prefix-list *prefix-list-name*	Name of the prefix list which is used to filter the route.
in | **out**	Filters the in or out route in the distribute list.
interface-type interface-name	(Optional) Applies the distribute list to the specified interface.

Defaults By default, no distribute list is defined.

Command mode Routing process configuration mode.

Usage Guide This command is used to configure the route distribution control list to filter all update routes for the purpose of refusing to receive or send the specified routes. If the interface is not specified, the update routes on all interfaces are filtered.

Configuration Examples The following example shows how to filter the received update route on the interface eth0 (only those update routes within the **prefix-list** *allowpre* prefix list range can be received)

```
Ruijie(config)# ipv6 router rip
Ruijie(config-router)# distribute-list prefix-list allowpre in eth0
```

Related Commands

Command	Description
redistribute	Sets route redistribution.

Platform Description N/A

4.5 graceful-restart

Use this command to configure the graceful restart (GR) function for the RIPng process.
graceful-restart [**grace-period** *grace-period*]

Use the **no** form of this command restore the default configurations.
no graceful-restart [**grace-period**]

Parameter Description

Parameter	Description
graceful-restart	Enables the GR function.
grace-period	Displays the configured grace period.
grace-period	Indicates the configured GR period, ranging from 1 to 1800 seconds. The default value is the smaller between twice of the update time and 60s.

Defaults The GR function is enabled by default.

Command Mode Routing process configuration mode

Default Level 14

Usage Guide The GR function is configured based on RIPng instances. Different parameters can be configured for different RIPng instances as required.
The GR period indicates the maximum duration from RIPng restart to RIPng GR completion. In this time period, the forwarding table before restart is used and the RIPng route is restored to the status before restart. After the GR period expires, the RIPng process exits the GR status and the common RIPng operation is performed.
The **graceful-restart grace-period** command allows a user to modify the GR period in explicit mode. Note that GR is completed and the RIPng route is updated once before the RIPng route becomes invalid. If the GR period is improperly set, continuous data forwarding in the GR process cannot be ensured. A typical case is as follows:
If the GR period is greater than the invalid time of the neighbor route, GR is not completed before the route becomes invalid and the route is not advertised to the neighbor again. The neighbor route stops forwarding data after the route becomes invalid, resulting in data forwarding interruption. Therefore, unless otherwise specified, it is not recommended to adjust the GR period. If the GR period needs to be configured, check configuration of the **timers** command to ensure that the GR period value is greater than the route update time and smaller than the route invalid time.
When GR is performed for the RIPng process, ensure that the network environment is stable.

Configuration Examples The following example enables the GR function for the RIPng process and configures the GR period.

```
Ruijie(config)# ipv6 router rip
Ruijie(config-router)# graceful-restart grace-period 90
```

Verification Run the **show ipv6 rip** command to check whether the GR function is configured and query the configured grace period.

Prompts N/A

Common Errors N/A

Platform Description N/A

4.6 ipv6 rip default-information

Use this command to generate a default IPv6 route to the RIPng. Use the **no** form of this command to remove the default route.

ipv6 rip default-information { **only** | **originate**} [**metric** *metric-value*]

no ipv6 rip default-information

Parameter Description

Parameter	Description
only	Advertises the IPv6 default route only.
originate	Advertises both of the IPv6 default route and other routes.
metric *metric-value*	Sets the metric value for the default route. The valid range is from 1 to 15. The default metric is 1.

Defaults By default, no default route is configured.

Command mode Interface configuration mode

Usage Guide With this command configured on an interface, the interface advertises an IPv6 default route and the route itself is not to join the device route forwarding table and the RIPng route database.

To avoid the route loop, once this command has been configured on the interface, RIPng refuses to receive the default route update message advertised from the neighbor.

Configuration Examples The following example shows how to create a default route to the RIPng routing process on the interface ethernet0/0 and enable this interface to advertise the default route only:

```
Ruijie(config)# interface ethernet 0/0
Ruijie(config-if)# ipv6 rip default-information only
```

Related Commands

Command	Description
show ipv6 rip	Displays the RIPng process and statistics.
show ipv6 rip database	Displays the RIPng route.

Platform Description N/A

4.7 ipv6 rip enable

Use this command to enable the RIPng on the interface. Use the **no** form of this command to disable RIPng on the interface.

ipv6 rip enable

no ipv6 rip enable

Parameter Description

Parameter	Description
N/A	N/A

Defaults It is disabled by default.

Command mode Interface configuration mode.

Usage Guide This command is used to add the RIPng interface. Before this command is configured, if the RIPng is not enabled, use this command to enable the RIPng automatically.

Configuration Examples The following example shows how to enable the RIPng on the interface 0/0:

```
Ruijie(config)# interface ethernet 0/0
Ruijie(config-if)# ipv6 rip enable
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

4.8 ipv6 rip metric-offset

Use this command to set the interface metric value. Use the **no** form of this command to remove the metric configurations.

ipv6 rip metric-offset *value*

no ipv6 rip metric-offset

Parameter Description

Parameter	Description

value	Sets the interface metric value on the interface. The valid range is from 1 to 16.

Defaults The default value is 1.

Command mode Interface configuration mode.

Usage Guide Before the route is added to the routing list, the interface metric value shall be upon the route metric. To this end, the interface metric value influences the route usage.

Configuration Examples The following example shows how to set the metric value of the interface Ethernet 0/1 as 5:

```
Ruijie(config)# interface ethernet 0/1
Ruijie(config-if)# ipv6 rip metric-offset 5
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

4.9 ipv6 router rip

Use this command to create the RIPng process and enter routing process configuration mode. Use the **no** form of this command to remove the RIPng process.

ipv6 router rip

no ipv6 router rip

Parameter Description

Parameter	Description
N/A	N/A

Defaults No RIPng process is configured by default.

Command mode Global configuration mode.

Usage Guide N/A.

Configuration Examples The following example shows how to create the RIPng process and enter routing process configuration mode:

```
Ruijie(config)# ipv6 router rip
```

Related Commands

Command	Description
ipv6 rip enable	Enables the RIPng on the specified interface.

Platform Description N/A

4.10 passive-interface

Use this command to disable the interface to send update packets. Use the **no** form of this command to enable the interface to send update packets.

passive-interface { **default** | *interface-type interface-num* }

no passive-interface { **default** | *interface-type interface-num* }

Parameter Description

Parameter	Description
default	Enables the passive mode on all interfaces.
interface-type interface-num	Interface type and interface number.

Defaults No passive interface is configured by default.

Command mode Routing process configuration mode.

Usage Guide You can use the **passive-interface default** command to enable the passive mode on all interfaces. Then ,use the **no passive-interface** *interface-type interface-num* command to remove the specified interface from the passive mode.

Configuration Examples The following example shows how to enable the passive mode on all interfaces and remove interface ethernet 0/0 from the passive mode:

```
Ruijie(config-router)# passive-interface default
Ruijie(config-router)# no passive-interface ethernet 0/0
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

4.11 redistribute

Use this command to redistribute the route of other routing protocols to RIPng. Use the **no** form of this

command to remove the redistribution configuration.

redistribute { **bgp** | **connected** | **isis** [*area-tag*] | **ospf** *process-id* | **static**} [**metric** *metric-value* | **route-map** *route-map-name*]

no redistribute { **bgp** | **connected** | **isis** [*area-tag*] | **ospf** *process-id* | **static**} [**metric** *metric-value* | **route-map** *route-map-name*]

Parameter Description

Parameter	Description
bgp	Redistributes the BGP routes to RIPng.
connected	Redistributes the connected routes to RIPng.
isis [*area-tag*]	Redistributes the ISIS routes to RIPng. *area-tag* indicates the ISIS process number.
ospf *process-id*	Redistributes the OSPF routes to RIPng. *process-id* indicates the OSPF process number, and the range is from 1 to 65,535.
static	Redistributes the static routes to RIPng.
metric *metric-value*	(Optional) Sets the metric value for the route redistributed to RIPng.
route-map *route-map-name*	(Optional) Sets the redistribution route filtering.

Defaults

By default, the routes of other routing protocols are not redistributed.

If the **default-metric** command is not configured, the default metric value is 1;

By default, the **route-map** is not configured;

By default, all sub-type routes in the specified routing process are redistributed.

Command mode

Routing process configuration mode.

Usage Guide

This command is used to redistribute the external routes to RIPng.

It is unnecessary to transform the metric of one routing protocol into another routing protocol in the process of the route redistribution, for the metric calculation methods of the different routing protocols are different. The RIP and OSPF metric calculations are incomparable for the reason that the RIP metric calculation is hop-based while the OSPF one is bandwidth-based.

The instance, from where the routing information is redistributed to the RIPng, must be specified in the process of configuring the multi-instance protocol redistribution.

Configuration Examples

The following example shows how to redistribute the static route, use the route map *mymap* to filter and set the metric value as 8:

```
Ruijie(config)# ipv6 router rip
Ruijie(config-router)# redistribute static route-map
mymap metric 8
```

Related Commands

Command	Description
default-metric	Defines the default RIPng metric value when

	redistributing other routing protocols.
distribute-list	Filters the RIPng routing update packets.

Platform Description N/A

4.12 show ipv6 rip

Use this command to show the parameters and each statistical information of the RIPng routing protocol process.

show ipv6 rip

Parameter Description

Parameter	Description
N/A	N/A

Defaults N/A

Command mode Privileged EXEC mode or user mode.

Usage Guide N/A

Configuration Examples

```
Ruijie# show ipv6 rip
Routing Protocol is "RIPng"
Sending updates every 10 seconds with +/-50%, next due in 8 seconds
Timeout after 30 seconds, garbage collect after 60 seconds
Outgoing update filter list for all interface is:
distribute-list prefix aa out
Incoming update filter list for all interface is: not set
Default redistribution metric is 1
Default distance is 120
Redistribution:
Redistributing protocol connected route-map rm
Redistributing protocol static
Redistributing protocol ospf 1
Default version control:  send version 1, receive version 1
Interface              Send   Recv
VLAN 1             1     1
Loopback 1          1     1
Routing Information Sources:
None
```

Related

Command	Description

Commands

show ipv6 rip	Displays the parameters and each statistical information of the RIPng process.

Platform Description N/A

4.13 show ipv6 rip database

Use this command to display the RIPng route entries.

show ipv6 rip database

Parameter Description

Parameter	Description
N/A	N/A

Defaults N/A

Command mode Privileged EXEC mode or user mode.

Usage Guide N/A

Configuration Examples

```
Ruijie# show ipv6 rip database
Codes: R - RIPng,C - Connected,S - Static,O - OSPF,B - BGP
sub-codes:n - normal,s - static,d - default,r - redistribute,
i - interface, a/s - aggregated/suppressed
S(r)   2001:db8:1::/64, metric 1, tag 0
Loopback 0/::
S(r)   2001:db8:2::/64, metric 1, tag 0
Loopback 0/::
C(r)   2001:db8:3::/64, metric 1, tag 0
VLAN 1/::
S(r)   2001:db8:4::/64, metric 1, tag 0
Null 0/::
C(i)   2001:db8:5::/64, metric 1, tag 0
Loopback 1/::
S(r)   2001:db8:6::/64, metric 1, tag 0
Null 0/::
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

4.14 split-horizon

Use the **split-horizon** command to enable the RIPng split-horizon function in routing process configuration mode. Use the **no** form of this command to disable this function. Use the **split-horizon poisoned-reverse** command to enable the RIPng poisoned reverse horizontal split function in routing process configuration mode. Use the no form of this command to disable this function.
split-horizon [**poisoned-reverse**]
no split-horizon [**poisoned-reverse**]

Parameter Description

Parameter	Description
poisoned-reverse	(Optional) Enables the poisoned-reverse horizontal split.

Defaults RIPng split horizon is enabled by default.

Command mode Routing process configuration mode.

Usage Guide In the process of packet updating, split-horizon function prevents some routing information from being advertised through the interface learning those routing information. The poisoned reverse horizontal split function advertises some routing information to the interface learning those routing information, and the metric value is set as 16. The RIPng routing protocol belongs to the distance vector routing protocol, so the horizontal split shall be noticed in the actual application. You can use the **show ipv6 rip** command to determine whether the RIPng split-horizon function is enabled or not.

Configuration Examples The following example shows how to disable the RIPng horizontal split:

```
Ruijie(config)# ipv6 router rip
Ruijie(config-router)# no split-horizon
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

4.15 timers

Use this command to adjust the RIPng timer. Use the **no** form of this command to restore the default settings.

timers *update invalid flush*
no timers

Parameter Description

Parameter	Description
update	Sets the routing update time, in seconds. The update parameter defines the period of sending the routing update packets by the device. The invalid and flush parameter reset once the update packets are received.
invalid	Sets the routing invalid time, in seconds, starting from receiving the last valid update packet. The invalid parameter defines the invalid time for the un-updated routing in the routing list. The routing invalid time shall be three times larger than the routing update time. The routing will be invalid if no update packets are received within the routing invalid time, and it will reset if the update packets are received within the invalid time.
flush	Sets the routing flush time, in seconds, starting from RIPng entering to invalid state. The invalid routing will be removed from the routing list if the flush time expires.

Defaults The default update time is 30 seconds; the default invalid time is 180 seconds; and the default flush time is 120 seconds.

Command mode Routing process configuration mode.

Usage Guide Adjusting the above time may speed up the RIPng convergence time and the troubleshooting time. The RIPng time must be consistent for the devices connecting to the same network. You are not recommended to adjust the RIP time, except for the specific requirement.
Use the **show ipv6 rip** command to view the current RIPng time parameter setting.
In the low-speed link, with the short time configured, large amount of the update packets consumes a lot of bandwidth. Generally, the short time can be configured in the Ethernet or 2Mbps-higher line to shorten the convergence time of the network routing.

Configuration Examples The following example shows how to send the RIP update packets every 10 seconds. The routing will be invalid if no update packets are received within 30 seconds, and the routing will be removed after being invalid for 90 seconds.

```
Ruijie(config)# ipv6 router rip
Ruijie(config-router)# timers 10 30 90
```

Related Commands

Command	Description
show ipv6 rip	Displays the parameters and the statistical

	information of the RIPng process.
show ipv6 rip database	Displays the RIPng routes.

Platform Description N/A

5 OSPFv2 Commands

5.1 area

Use this command to configure the specified OSPF area. Use the **no** form of this command to restore the default setting.

area *area-id*

no area *area-id*

Parameter Description

Parameter	Description
area-id	ID of the OSPF area. The value can be a decimal integer or an IP address.

Defaults No OSPF area is configured by default.

Command Mode Routing process configuration mode

Usage Guide Use the no form of this command to remove the specified OSPF area and its configuration, including the area-based **area authentication, area default-cost, area filter-list, and area nssa** commands.

- Do not remove the OSPF area configuration under the following conditions:
- Virtual links exist in the backbone area. The virtual links must be removed at first.
- The corresponding network area command exists in any area. All network segment commands added to an area must be removed at first.

Configuration Examples The following example removes the configuration of OSPF area 2.

```
Ruijie(config)# router ospf 2
Ruijie(config-router)# no area 2
```

Related Commands

Command	Description
network area	Defines the interface where OSPF runs and the belonging area of the interface.

Platform Description N/A

5.2 area authentication

Use this command to enable OSPF area authentication. Use the **no** form of this command to restore the default setting.

area *area-id* **authentication** [**message-digest**]

no area *area-id* **authentication**

Parameter Description

Parameter	Description
area-id	Specifies ID of the area enabled with OSPF. The value can be a decimal integer or an IP address.
message-digest	(Optional) Enables MD5 (message digest 5) authentication mode.

Defaults No authentication is enabled by default.

Command Mode Routing process configuration mode

Usage Guide The RGOS software supports three authentication types:
1) 0, no authentication. The authentication type in the OSPF packet is 0when this command is not executed to enable OSPF authentication. 2) 1, plain text authentication mode. When this command is configured, the message-digest option is not used.3) 2, MD5 authentication mode. When this command is configured, the message-digest option is used.

All devices in the same OSPF area must use the same authentication type. If authentication is enabled, the authentication password must be configured on an interface connecting neighbors. You can use the **ip ospf authentication-key** command to configure the plain text authentication password, and the **ip ospf message-digest-key** command to configure the MD5 authentication password in interface configuration mode.

Configuration Examples The following example uses MD5 authentication and the authentication password backbone in area 0 (backbone area) of the OSPF routing process.

```
Ruijie(config)# interface fastEthernet 0/1
Ruijie(config-if-FastEthernet 0/1)# ip address 192.168.12.1 255.255.255.0
Ruijie(config-if-FastEthernet 0/1)# ip ospf message-digest-key 1 md5 backbone
Ruijie(config)# router ospf 1
Ruijie(config-router)# network 192.168.12.0 0.0.0.255 area 0
Ruijie(config-router)# area 0 authentication message-digest
```

Related Commands

Command	Description
ip ospf authentication-key	Defines the OSPF plain text authentication password.
ip ospf message-digest-key	Defines the OSPF MD5 authentication password.
area virtual-link	Defines a virtual link.

Platform Description N/A

5.3 area default-cost

Use this command to define the cost (OSPF metric) of the default aggregate route advertised to the stub area or not-so-stubby area (NSSA) in routing process configuration mode. Use the **no** form of this command to restore the default setting.

area *area-id* **default-cost** *cost*

no area *area-id* **default-cost**

Parameter Description

Parameter	Description
area-id	ID of the stub area or NSSA
cost	Cost of the default aggregate route advertised to the stub area or NSSA. The range is from 0 to 16777215.

Defaults The default is 1.

Command Mode Routing process configuration mode

Usage Guide This command takes effect only on the Area Border Router (ABR) of the stub area or the ABR/Autonomous System Border Router (ASBR) of the NSSA.

The ABR can advertise a Link State Advertisement (LSA) indicating the default route in the stub area. The ABR/ASBR can advertise an LSA indicating the default route in the NSSA. You can use the **area default-cost** command to modify the LSA cost.

Configuration Examples The following example sets the cost of the default aggregate route to 50.

```
Ruijie(config)# router ospf 1
Ruijie(config-router)# network 172.16.0.0 0.0.255.255 area 0
Ruijie(config-router)#network 192.168.12.0 0.0.0.255 area 1
Ruijie(config-router)# area 1 stub
```

```
Ruijie(config-router)# area 1 default-cost 50
```

Related Commands

Command	Description
area stub	Sets an OSPF area as a stub area.
area nssa	Sets an OSPF area as an NSSA.

Platform Description N/A

5.4 area filter-list

Use this command to filter the inter-area routes on the ABR. Use the **no** form of this command to restore the default setting.

area *area-id* **filter-list** { **access** *acl-name*| **prefix** *prefix-name* } { **in** | **out** }

no area *area-id* **filter-list** { **access** *acl-name* | **prefix** *prefix-name* } { **in** | **out** }

Parameter Description

Parameter	Description
area-id	Area ID
acl-name	Name of an Access Control List (ACL)
prefix-name	Prefix-list name

in | **out**	Applies the ACL rule to the routes incoming/outgoing the area.

Defaults No filtering is configured by default.

Command Mode Routing process configuration mode

Usage Guide This command can be configured only on an ABR.

You can use this command when it is required to filter the inter-area routes on the ABR.

Configuration Examples The following example sets area 1 to learn only the inter-area routes of 172.22.0.0/8.

```
Ruijie# configure terminal
Ruijie(config)# access-list 1 permit 172.22.0.0 0.255.255.255
Ruijie(config)# router ospf 100
Ruijie(config-router)# area 1 filter-list access 1 in
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

5.5 area nssa

Use this command to set an OSPF area as an NSSA in routing process configuration mode. Use the **no** form of this command to delete the NSSA or the NSSA configuration.

area *area-id* **nssa** [**no-redistribution**] [**default-information-originate** [**metric** *value*] [**metric-type** *type*]] [**no-summary**] [**translator** [**stability-interval** *seconds* | **always**]]

no area *area-id* **nssa** [**no-redistribution**] [**default-information-originate** [**metric** *value*] [**metric-type** *type*]] [**no-summary**] [**translator** [**stability-interval** | **always**]]

Parameter Description

Parameter	Description
area-id	NSSAID
no-redistribution	Imports the routing information to a common area other than the NSSA for the NSSA ABR.
default-information originate	Generates and imports the default Type 7 LSA to the NSSA. This option takes effect only on the NSSA ABR or ASBR.
metric *value*	Sets the metric of the generated default LSA. The range is from 0 to 16777214. The default value is 1.
metric-type *type*	Sets the type of the generated LSA to N-1 or N-2. The default value is N-2.
no-summary	Prevents the NSSA ABR from sending summary LSAs (Type-3 LSA).
translator	Configures the translator for the NSSA ABR.
stability-interval *seconds*	Configures the stability interval in seconds for the NSSA ABR that functions as a translator to change to a non-translator. The range is

	from 0 to 2147483647. The default value is 40.
always	Configures that an NSSA ABR always functions as a translator. The NSSA ABR is the backup translator by default.

Defaults No NSSA is defined by default.

Command Mode Routing process configuration mode

Usage Guide The default-information-originate parameter is used to generate the default Type-7 LSA. However, on the NSSA ABR, the default Type-7 LSA will always be generated; On the ASBR (which is not an ABR at the same time), the default Type-7 LSA is generated only when the default route exists in the routing table.

The no-redistribution parameter prevents the OSPF from advertising the external routes imported with the redistribute command to the NSSA on the ASBR. This option is generally used when the NSSA device is both an ASBR and an ABR.

To reduce the number of LSAs sent to the NSSA, you can configure the no-summary parameter on the ABR to prevent it from advertising summary LSAs (Type-3 LSAs) to the NSSA. In addition, you can use the area default-cost command on the NSSA ABR to configure the cost of the default route advertised to the NSSA. By default, this cost is 1.

If an NSSA has multiple ABRs, the ABR with the greatest ID is selected as the Type-7 or Type-5 translator. To configure that an NSSA ABR always functions as a translator, you can use the translator always parameter. If the translator role of an ABR is taken away by another ABR, the ABR still possesses the conversion capability within stability-interval. If the ABR fails to take back its translator role when stability-interval expires, the LSA that changes from Type-7 to Type-5 will be removed from the autonomous domain.

To avoid route loops, Type-5 LSAs generated from Type-7 convergence will be eliminated immediately after the current device stopped serving as a translator, with no need to wait until the stability-interval expires.

In a same NSSA, you are recommended to configure the **translator always** parameter on only one ABR.

Configuration Examples

The following example sets area 1 as an NSSA on all routers of the area.

```
Ruijie(config)#router ospf1
Ruijie(config-router)#network 172.16.0.0 0.0.255.255 area0
Ruijie (config-router)#network 192.168.12.0 0.0.0.255 area 1
Ruijie(config-router)# area1nssa
```

Related Commands

Command	Description
area default-cost	Defines the cost (OSPF metric) of the default aggregate route advertised to the NSSA.

Platform Description

N/A

5.6 area range

Use this command to configure inter-area route aggregation for OSPF. Use the **no** form of this command to delete route aggregation. Use the **no** form with the cost parameter to restore the default metric of the aggregate route, but not delete route aggregation.

area *area-id* **range** *ip-address net-mask* [**advertise** | **not-advertise**] [c**ost** *cost*]

no area *area-id* **range** *ip-address net-mask* [cost]

Parameter Description

Parameter	Description
area-id	ID of the area where the aggregate route is injected into. The value can be a decimal integer or an IP address.
ip address net-mask	Network segment whose routes are to be aggregated
advertise | not-advertise	Whether to advertise the aggregate route
cost *cost*	Sets the priority of the interface. The range is from 0 to 16777215.

Defaults No inter-area route aggregation is configured by default.

The configured aggregation range is advertised by default.

The default metric of the aggregate route depends on whether the device is compatible with RFC1583. If yes, the default metric is the smallest cost of the aggregate route. If no, the default metric is the largest cost of the aggregate route.

Command Mode Routing process configuration mode

Usage Guide This command takes effect only on the ABR to aggregate multiple routes of an area into a route and advertise it to other areas. Route combination occurs only on the border of an area. The devices inside an area see the specific routing information, but the devices outside the area see only one aggregate route. The advertise and not-advertise options can set whether to advertise the aggregate route for filtering and masking. The aggregate route is advertised by default.

You can use the cost option to set the metric of the aggregate route.

You can define route aggregate in multiple areas to simplify the routes in the whole OSPF routing

area. This improves the network forwarding performance, especially in large networks.

The area range of route aggregation is determined according to the longest match when multiple aggregate routes with direct inclusion relationships are configured.

Configuration Examples The following example aggregate the routes of area 1 into a route 172.16.16.0/20.

```
Ruijie(config)#router ospf 1
Ruijie(config-router)#network 172.16.0.0 0.0.15.255area0
Ruijie((config-router)#network 172.16.17.0 0.0.15.255area1
Ruijie(config-router)#area1range 172.16.16.0 255.255.240.0
```

Related Commands

Command	Description
discard-route	Enables a discarded route to be added to a routing table.
summary-address	Configures the OSPF external route aggregation.

Platform Description N/A

5.7 area stub

Use this command to set an OSPF area as a stub area or full stub area. Use the **no** form of this command to restore the default setting.

area *area-id* **stub** [**no-summary**]

no area *area-id* **stub** [**no-summary**]

Parameter Description

Parameter	Description
area-id	Stub area ID
no-summary	(Optional) Prevents the ABR from advertising the network summary link to the stub area. Here the stub area is called the full stub area. Only the ABR needs this parameter.

Defaults No stub area is defined by default.

Command Mode Routing process configuration mode

Usage Guide All devices in the OSPF stub area must be configured with the area stub command. The ABR only sends three types of link state advertisement (LSA) to the stub area: 1) type 1, device LSA; 2) type 2, network LSA; 3) type 3, network summary LSA. For the routing table, the devices in the stub area can learn only the routes inside the OSPF routing domain, including the internal default routes generated by the ABR.

To configure a full stub area, use the area stub command with the no-summary keyword on the ABR. The devices in the full stub area can learn only the routes in the local area and the internal default routes generated by the ABR.

Two commands can configure an OSPF area as a stub area: the area stub and area default-cost commands. All devices connected to the stub area must be configured with the area stub command, but the area default-cost command can be executed only on the ABR. The area default-cost command defines the initial cost (metric) of the internal default route.

Configuration Examples The following example sets area 1 as the stub area on all devices in area 1.

```
Ruijie(config)# router ospf1
Ruijie(config-router)# network172.16.0.0 0.0.255.255 area 0
Ruijie (config-router)# network 192.168.12.0  0.0.0.255 area 1
Ruijie(config-router)# area 1 stub
```

Related Commands

Command	Description
area default-cost	Defines the cost (OSPF metric value) of the default aggregate route advertised to the stub area.

Platform Description N/A

5.8 area virtual-link

Use this command to define the OSPF virtual link in routing process configuration mode. Use the **no** form of this command to restore the default setting.

area *area-id* **virtual-link** *router-id* [**authentication** [**message-digest** | **null**]] [**dead-interval** | *seconds*] [**hello-interval** *seconds]* [**retransmit-interval** *seconds]* [**transmit-delay** *seconds*] [[**authentication-key** [**0|7**] *key*] | [**message-digest-key** *key-id* **md5** [**0|7**] *key*]]

no area *area-id* **virtual-link** *router-id* [**authentication**] [**dead-interval**] [**hello-interval**] [**retransmit-interval**] [**transmit-delay**] [[**authentication-key**] | [**message-digest-key** *key-id]]*

Parameter Description

Parameter	Description

area-id	ID of the OSPF transition area. The value can be a decimal integer or an IP address.
router-id	ID of the router neighboring to the virtual link. It can be viewed with the show ip ospf command.
dead-interval *seconds*	(Optional) Defines the time to declare neighbor loss in seconds. The range is 0 to 2147483647.This value must be consistent with that of the neighbor.
hello-interval *seconds*	(Optional)Defines the interval at which the HELLO packet is sent by the OSPF to the virtual link in seconds. The range is from1 to 65535.This value must be consistent with that of the neighbor.
retransmit-interval *seconds*	(Optional) OSPF LSA retransmission interval in seconds. The range is from 0 to 65535. The parameter setting must consider the round-trip time of packets on the link.
transmit-delay *seconds*	(Optional) OSPF LSA transmission delay in seconds. The range is from 0 to 65535. This value adds the LSA keep alive period. When the LSA keep alive period reaches a threshold, the LSA will be refreshed.
authentication-key [0|7]*key*	(Optional) Defines the OSPF plain text authentication key. The plain text authentication key between neighbors must be the same. The service password-encryption command enables the key to be displayed in encrypted manner. 0 indicates that the key is displayed in plain text. 7 indicates that the key is displayed in cipher text.
message-digest-key *key-id***md5 [0|7]***key*	(Optional) Defines the OSPF MD5 authentication key and key ID. The MD5 authentication key ID and key between neighbors must be the same. The service password-encryption command enables the key to be displayed in encrypted manner. 0 indicates that the key is displayed in plain text.

	7 indicates that the key is displayed in cipher text.
authentication	Sets the authentication type to plain text.
message-digest	Sets the authentication type to MD5.
null	Sets the authentication type to no authentication.

Defaults The following are the default values:

dead-interval: 40seconds

hello-interval: 10seconds

retransmit-interval: 5seconds

transmit-delay: 1second

authentication: null

The other parameters do not have default values.

Command Mode Routing process configuration mode

Usage Guide A virtual link can connect an area to the backbone area, or another non-backbone area. In the OSPF routing domain, all areas must connect to the backbone area. If an area disconnects from the backbone area, a virtual link to the backbone area is required. Otherwise, the network communication will become abnormal. The virtual link is created between two ABRs. The area that belongs to both ABRs is called the transition area, which can never be a stub area or NSSA.

The router-id parameter indicates the ID of OSPF neighbor router and can be displayed with the show ip ospf neighbor command. You can configure the loopback address as the router ID.

The area virtual-link command defines only the authentication key for a virtual link. You can use the area authentication command to enable the OSPF packet authentication in areas connected over the virtual link in routing process configuration mode.

Configuration Examples

The following example sets area 1 as the transition area to establish virtual link with neighbor *2.2.2.2.*

```
Ruijie(config)# router ospf 1
Ruijie(config-router)# network 172.16.0.0 0.0.15.255 area0
Ruijie(config-router)# network 172.16.17.0 0.0.15.255 area1
Ruijie(config-router)#area1 virtual-link2.2.2.2
```

The following example sets area 1 as the transition area to establish a virtual link with neighbor *1.1.1.1*. This virtual link connects area 10 and the backbone area, and works with the OSPF packet authentication inMD5 mode.

```
Ruijie(config)# routerospf1
Ruijie(config-router)# network172.16.17.0 0.0.15.255area1
Ruijie(config-router)# network172.16.252.0 0.0.0.255 area10
Ruijie(config-router)# area 0 authentication message-digest
Ruijie(config-router)# area1virtual-link 1.1.1.1message-digest-key1md5hello
```

Related Commands

Command	Description
area authentication	Enables the OSPF area packet authentication and define the authentication mode.
show ip ospf	Displays the OSPF process information, including the router ID.
show ip ospf virtual-links	Monitors information about a virtual link.

Platform Description

N/A

5.9 auto-cost

Use this command to enable the auto-cost function and set the reference bandwidth according to the reference bandwidth. Use the **no** form of this command to restore the default setting.

auto-cost [**reference-bandwidth** *ref-bw*]

no auto-cost [**reference-bandwidth**]

Parameter Description

Parameter	Description
ref-bw	Reference bandwidth, in the range from1 to 4294967 Mbps.

Defaults The default is 100Mbps.

Command Mode Routing process configuration mode

Usage Guide By default, the cost of an OSPF interface is equal to the reference value of the auto cost divided by the interface bandwidth.

Run the **auto-cost** command to obtain the reference value of the auto cost. The default value is 100 Mbps.

Run the **bandwidth** command to set the interface bandwidth.

The costs of OSPF interfaces on several typical lines are as follows:

64Kbps serial line: The cost is 1562.

E1 line: The cost is 48.

10M Ethernet: The cost is 10.

100M Ethernet: The cost is 1.

If you run the **ip ospf cost** command to configure the cost of an interface, the configured cost will automatically overwrite the cost that is computed based on the auto cost.

Configuration Examples

The following example configures the reference bandwidth as 10 Mbps.

```
Ruijie(config)# routerospf1
Ruijie(config-router)# network172.16.10.0 0.0.0.255 area0
Ruijie(config-router)# auto-costreference-bandwidth10
```

Related Commands

Command	Description
show ip ospf	Displays the OSPF global configuration information
ip ospf cost	Sets the cost value of the OSPF interface.
bandwidth	Sets the interface bandwidth. This setting does not affect data transmission rate.

Platform Description

N/A

5.10 capability opaque

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

capability opaque

no capability opaque

Parameter Description

Parameter	Description
N/A	N/A

Defaults Opaque LSA is enabled by default.

Command Mode Routing process configuration mode.

Usage Guide N/A

Configuration Examples The following example disables Opaque LSA capability.

```
Ruijie(config)# router ospf 1
Ruijie(config-router)# no capability opaque
```

Related Commands

Command	Description
show ip ospf	Displays the global configuration of OSPF.

Platform Description N/A

5.11 clear ip ospf process

Use this command to clear and restart the OSPF instance.

clear ip ospf *(process-id)* **process**

Parameter Description

Parameter	Description
process-id	OSPF instance ID. When the ID is specified, the command clears data related to the specified instance and restarts the OSPF instance. When no ID is specified, the command clears data related to all running OSPF instances and restarts all the running OSPF instances.

Defaults

Command Mode Privileged EXEC mode

Usage Guide Resetting the entire OSPF process causes that all neighbors are re-established and OSPF is greatly affected. Therefore, you are prompted to confirm the execution for deliberation.

Configuration Examples The following example clears data of OSPF instance 1 and restarts OSPF instance 1.

```
Ruijie#clearipospf1process
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

5.12 compatible rfc1583

Use this command to determine the RFC 1583 or RFC 2328 rule for selecting the optimal route among route table several routes to the same destination out of the Autonomous System (AS).

compatible rfc1583

no compatible rfc1583

Parameter Description

Parameter	Description
N/A	N/A

Defaults The RFC 1583 rule is used by default.

Command Mode Routing process configuration mode

Usage Guide N/A

Configuration Examples The following example determines the best route with the RFC 2328 rule.

```
Ruijie(config)# routerospf1
Ruijie(config-router)# nocommpatiblerfc1583
```

Related Commands

Command	Description
show ip ospf	Displays the OSPF global configuration information

Platform Description N/A

5.13 default-information originate

Use this command to generate a default route to be injected into the OSPF routing domain in routing process configuration mode. Use the **no** form of this command to restore the default setting.

default-information originate [**always**] [**metric** *metric*] [**metric-type** *type*] [**route-map** *map-name*]

no default-information originate [**always**] [**metric**] [**metric-type**] [**route-map** *map-name*]

Parameter Description

Parameter	Description
always	(Optional) Generates the default route unconditionally, no matter whether the default route exists locally or not.
metric *metric*	(Optional) Initial metric of the default route in the range from0 to 16777214
metric-type *type*	(Optional) Type of the default route. There are two type of OSPF external routes: type 1, different metrics on different devices; type 2, same metric on different devices. An external route of type 1 is more trustworthy than that of type 2.
route-map *map-name*	Associated route map name. No route map is associated by default.

Defaults No default route is generated by default.

The default value of metric is 1.

The default value of metric-type is 2.

Command Mode Routing process configuration mode

Usage Guide When the **redistribute** or **default-information** command is executed, the OSPF-enabled device automatically turns into the ASBR. The ASBR cannot generate the default route automatically or advertise it to all the devices in the OSPF routing domain. The ASBR can generate the default route with the **default-information originate** command in routing process configuration mode.

If the always parameter is used, the OSPF routing process advertises an external default route to neighbors, no matter the default route exists or not. However, the local device does not display the default route. To make sure whether the default route is generated, use the **show ip ospf database** command to display the OSPF link state database. The external link identified with 0.0.0.0 indicates the default route. You can use the show ip route command on the OSPF neighbor to display the default route.

The metric of the external default route can be defined only with the **default-information originate** command.

There are two types of OSPF external routes: type 1 external routes have changeable routing metrics, while type 2 external routes have constant routing metrics. For two parallel routes with the same route metric to the same destination network, the type 1 route takes precedence over the type 2 route. As a result, the **show ip route** command displays only the type 1 route.

This command generates a default route of Type-5 LSA, which will not be flooded to the NSSA area.

To generate a default route in the NSSA area, use the **area nssa default-information-originate** command.

The routers in the stub area cannot generate external default routes.

The range of set metric is 0 to 16777214 for the associated route map. If the value exceeds the range, introducing a route fails.

Configuration Examples The following example configures that OSPF generates an external default route and injects it to the OSPF routing domain. The default route is of type 1 and the metric 50.

```
Ruijie(config)#routerospf 1
Ruijie(config-router)#network172.16.24.0 0.0.0.255 area 0
```

```
Ruijie(config-router)#default-information originate
alwaysmetric50metric-type1
```

Related Commands

Command	Description
show ip ospf database	Displays OSPF link state database.
show ip route	Displays the IP route table.
redistribute	Redistributes routes of other routing processes.

Platform Description N/A

5.14 default-metric

Use this command to set the **default metric** of OSPF redistribution route. Use the **no** form of this command to restore the default setting.

default-metric *metric*

no default-metric

Parameter Description

Parameter	Description
metric	Default metric of the OSPF redistribution route in the range from1 to 16777214

Defaults The default metric is not configured by default.

Command Mode Routing process configuration mode

Usage Guide The **default-metric** command must work with the **redistribute** command in routing process configuration mode to modify the initial metric of all redistributed routes.

The configuration result of the **default-metric** command does not take effect for the external routes injected into the OSPF routing domain with the **default-information originate** command.

Configuration Examples The following example configures the default metric of the OSPF redistribution route as 50.

```
Switch(config)# router rip
Ruijie(config-router)# network192.168.12.0
Switch(config-router)# version 2
Ruijie(config-router)# exit
Ruijie(config)# routerospf1
Ruijie(config-router)# network172.16.10.0 0.0.0.255area0
Switch(config-router)# default-metric 50
Ruijie(config-router)# redistribute rip subnets
```

Related Commands

Command	Description
redistribute	Redistributes the routes of other routing processes.

show ip ospf	Displays the OSPF global configuration information.

Platform Description N/A

5.15 discard-route

Use this command to enable adding the discard-route into the core route table. Use the **no** form of this command to disable this function.

discard-route { **internal | external** }

no discard-route { **internal** | **external** }

Parameter Description

Parameter	Description
internal	Enables adding the discard-route generated with the area range command
external	Enables adding the discard-route generated with the summary-address command.

Defaults Adding the discard-route is enabled by default.

Command Routing process configuration mode

Mode

Usage Guide After route aggregation, the range may exceed the actual network range of the route table, and sending the data to the nonexistent network may cause loops or increase router loads. To prevent this situation, the discard-route is added to the route table on the ABR or the ASBR. The discard-route is generated automatically and will not be transmitted.

Configuration Examples The following example disables adding the discard routes generated with the area range command.

```
Ruijie(config)# router ospf 1
Ruijie(config-router)# no discard-route internal
```

Related Commands

Command	Description
area range	Configures the route aggregation between OSPF areas.
summary-address	Configures the route aggregation out of the OSPF routing domain.

Platform Description N/A

5.16 distance ospf

Use this command to set the Administration Distance (AD) of different types of OSPF routes. Use the **no** form of this command to restore the default setting.

distance { *distance* | **ospf** { [**intra-area** *distance*] [**inter-area** *distance*] [**external** *distance*] } }

no distance [**ospf**]

Parameter Description

Parameter	Description
distance	Sets the route AD in the range from1 to 255.
intra-area *distance*	Sets the AD of the intra-area route in the range from1 to 255.
inter-area *distance*	Sets the AD of the inter-area route in the range from1 to 255.
External *distance*	Sets the AD of the external route in the range from1 to 255.

Defaults The default value is 110.

The default intra-area distance is 110.

The default inter-area distance is 110.

The default external distance is 110.

Command Mode OSPF Routing process configuration mode

Usage Guide

Configuration Examples The following example sets the OSPF external route AD to 160.

```
Ruijie(config)# routerospf1
Ruijie(config-router)# distance ospf external 160
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

5.17 distribute-list in

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

distribute-list *{ [access-list-number* | *name]* | *prefix prefix-list-name [* **gateway** *prefix-list-name]* | **route-map** *route-map-name } in [interface-type interface-number]*

no distribute-list *{ [access-list-number* | *name]* | *prefix prefix-list-name [* **gateway** *prefix-list-name]* | route-map *route-map-name } in [interface-type interface-number]*

Parameter Description

Parameter	Description
access-list-number	**name**	Uses the ACL filtering rule.

gateway *prefix-list-name*	Uses the gateway filtering rule.
Prefix *prefix-list-name*	Uses the prefix-list filtering rule.
route-map *route-map-name*	Uses the route-map filtering rule.
interface-type interface-number	Configures the LSA route filtering on the interface.

Defaults No filtering is configured by default.

Command Mode Routing process configuration mode

Usage Guide This configuration filters the received LSAs, and only those matching the filtering conditions are involved in the Shortest Path First (SPF) calculation to generate the corresponding routes. It does not affect the link status database or the route table of the neighbors. It only affects the routing entries calculated by local OSPF. This function is used to control routes that enter the ABR or ASBR.

The following route-map rules will be supported if the route-map parameter is configured:

match interface

match ip address

match ip address prefix-list

match ip next-hop

match ip next-hop prefix-list

match metric

match route-type

match tag

Filtering routes by using the **distribute-list in** command affects forwarding of local routes, but does not affect route computation based on LSAs. Therefore, if route filtering is configured on the ABR, Type 3 LSAs will still be generated and advertised to other areas because routes can still be computed based on LSAs. As a result, black-hole routes are generated. In this case, you can run the **area filter-list** or **area range** (containing the **not-advertise** parameter) command on the ABR to prevent generation of black-hole routes.

Configuration Examples

The following example configures LSA filtering.

```
Ruijie(config)# access-list3permit172.16.0.00.0.127.255
Ruijie(config)# router ospf 25
Ruijie(config-router)# distribute-list 3 in ethernet 0/1
```

Related Commands

Command	Description
distribute-list out	Filters redistribution routes.

Platform Description

N/A

5.18 distribute-list out

Use this command to configure filtering redistribution routes. The function is similar to that of the **redistribute** command. Use the **no** form of this command to restore the default setting.

distribute-list *{ [access-list-number* | *name]* | **prefix** *prefix-list-name }* **out** [**connected**| **ospf** *process-id* | **rip** | **static**]

no distribute-list *{ [access-list-number* | *name]* | **prefix** *prefix-list-name }* **out** [**connected** | **ospf** *process-id* | **rip** | **static**]

Parameter Description

Parameter	Description
access-list-number | name	Uses the ACL filtering rule.
prefix prefix-list-name	Uses the prefix-list filtering rule.
connected | **ospf** process-id| **rip | static**	Source of the routes to be filtered

Defaults No filtering is configured by default.

Command Mode Routing process configuration mode

Usage Guide Similar to the redistribute route-map command, the distribute-list out command filters the routes that other protocols redistribute to the OSPF. However, the distribute-list out command does not redistribute routes by itself. It works with the redistribute command in most cases. The ACL filtering rule and the prefix-list filtering rule cannot coexist in the configuration, that is, the two rules cannot be configured at the same time for routes from the same source.

Configuration Examples The following example filters the redistributed static routes.

```
Ruijie(config)# routerospf1
```

```
Ruijie(config)# redistribute static subnets
Ruijie(config-router)# distribute-list 22 outstatic
Ruijie(config-router)# distribute-list prefix jjj out static
% Access-list filter exists, please de-config first
```

Related Commands

Command	Description
distribute-list in	Configures LSA filtering.
redistribute	Redistributes routes of other routing processes.

Platform Description N/A

5.19 enable mib-binding

Use this command to bind the Management Information Base (MIB) with the specified OSPFv2 process. Use the **no** form of this command to restore the default setting.

enable mib-binding

no enable mib-binding

Parameter Description

Parameter	Description
N/A	N/A

Defaults The MIB is bound with the OSPFv2 process with the smallest ID by default.

Command Mode Routing process configuration mode

Usage Guide OSPFv2 MIB has no OSPFv2 process information, so the user operates a sole OSPFv2 process by SNMP. By default, OSPFv2 MIB is bound with the OSPFv2 process with the smallest ID. User operations take effect for this process.

To operate the specified OSPF process over Simple Network Management Protocol(SNMP), use this command to bind the MIB to SNMP.

Configuration Examples The following example operates OSPFv2 process 100 over SNMP:

```
Ruijie(config)# routerospf100
Ruijie(config-router)# enable mib-binding
```

Related Commands

Command	Description
show ip ospf	Displays the OSPF global configuration information.
enable traps	Configures the OSPF TRAP function.

Platform Description N/A

5.20 enable traps

The OSPFv2 process supports 16 kinds of TRAP packets, which are classified into four categories. Use this command to enable sending the specified TRAP messages. Use the **no** form of this command to restore the default setting.

enable traps [**error** [**IfAuthFailure** | **IfConfigError** | **IfRxBadPacket** | **VirtIfAuthFailure** | **VirtIfConfigError** | **VirtIfRxBadPacket**] | **lsa** [**LsdbApproachOverflow** | **LsdbOverflow** | **MaxAgeLsa** | **OriginateLsa**] | **retransmit** [**IfTxRetransmit** | **VirtIfTxRetransmit**] | **state-change** [**IfStateChange** | **NbrRestartHelperStatusChange** | **NbrStateChange** | **NssaTranslatorStatusChange** | **RestartStatusChange** | **VirtIfStateChange** | **VirtNbrRestartHelperStatusChange | VirtNbrStateChange**]]

no enable traps [**error** [**IfAuthFailure** | **IfConfigError** | **IfRxBadPacket** | **VirtIfAuthFailure** | **VirtIfConfigError** | **VirtIfRxBadPacket**] | **lsa** [**LsdbApproachOverflow** | **LsdbOverflow** | **MaxAgeLsa** | **OriginateLsa**] | **retransmit** [**IfTxRetransmit** | **VirtIfTxRetransmit**] | **state-change** [**IfStateChange** | **NbrRestartHelperStatusChange** | **NbrStateChange** | **NssaTranslatorStatusChange** | **RestartStatusChange** | **VirtIfStateChange** | **VirtNbrRestartHelperStatusChange | VirtNbrStateChange**]]

Parameter Description

Parameter	Description
error	Configures all traps switches related to errors. Use this parameter to set the following specified error traps switches. **Ifauthfailure** — Interface authentication error **Ifconfigerror** — Interface parameter configuration error **Ifrxbadpacket** — Error packets received on the interface **Virtifauthfailure** — Authentication error on the virtual interface **Virtifconfigerror** — Parameter configuration error on the virtual

		interface
	Virtifrxbadpacket	Error packets received on the virtual interface

isa	Configures all traps switches related to the LSA. Use this parameter to set the following specified LSA traps switches.

Lsdbapproachoverflow	External LSA count has reached the 90% of the upper limit.
Lsdboverflow	External LSA count has reached the upper limit.
Maxagelsa	LSA reaching the aging time
Originatelsa	Generates new LSA

retransmit	Configures all traps switches related to the retransmission. Use this parameter to set the following specified retransmit traps switches.

Iftxretransmit	Packet retransmission on the interface
Virtiftxretransmit	Packet retransmission on the virtual interface

state-change	Configures all traps switches related to the state change. Use this parameter to set the following specified state-change switches.

Ifstatechange	Interface state change
NbrRestartHelper StatusChange	State change during the neighbor GR process
Nbrstatechange	Neighbor state change

	NssaTranslatorStatusChange	State change of the NSSA translator
	RestartStatusChange	State change of the GR Restarter on the device
	Virtifstatechange	State change on the virtual interface
	VirtNbrRestartHelper StatusChange	Status change of the virtual neighbor GR process
	Virtnbrstatechange	State change on the virtual neighbor

Defaults All TRAP switches are disabled by default.

Command Mode Routing process configuration mode

Usage Guide The **snmp-server enable traps ospf** command must be configured before you configure this command, for it is limited by the **snmp-server** command.

This command is not limited by the binding of process and MIB, allowing to enable the TRAP switch for different processes simultaneously.

Configuration Examples The following example enables all TRAP switches of OSPFv2 process 100.

```
Ruijie(config)# routerospf100
```

```
Ruijie(config-router)# enable traps
```

Related Commands

Command	Description
show ip ospf	Displays the OSPF global configuration information.
enable mib-binding	Binds the OSPFv2 process with MIB.
snmp-server enable traps ospf	Enables the OSPF TRAP notification function.

Platform Description N/A

5.21 graceful-restart

Use this command to enable the graceful restart (GR) of OSPF on the device. Use the **graceful-restart grace-period** command to configure the grace period parameter and enable the OSPF GR function. Use the **no** form of this command to disable this function.

graceful-restart [**grace-period** *grace-period* | **inconsistent-lsa-checking**]

no graceful-restart [**graceful-period**]

Parameter Description

Parameter	Description
grace-period *grace-period*	Indicates the grace period, which is the maximum time from occurrence of an OSPF failure to completion of the OSPF GR. The value of the graceperiod varies from 1s to 1800s. The default value is

	120s.
inconsistent-lsa-checking	Enables topological change detection. If any topological change is detected, OSPF exits the GR process to complete convergence. After GR is enabled, topological change detection is enabled by default.

Defaults This function is enabled by default.

Command Mode Routing process configuration mode

Usage Guide GR is configured based on the OSPF instance. Different instances could be configured with different parameters according to the actual situation.

The graceful restart interval is the longest time between the OSPF restart and the graceful restart. In this period, you can perform link status reconstruction to restore the OSPF status to the original. With the interval times out, the OSPF will exit GR and perform common OSPF operations.

The GR interval is 120 seconds set with the graceful-restart command, and the graceful-restart grace-period command allows you to change the interval explicitly.

Configuration Examples The following example enables GR for the OSPF instance 1 and sets the restart interval for GR.

```
Ruijie(config)# router ospf 1
Ruijie(config-router)# graceful-restart
Ruijie(config-router)# graceful-restart grace-period 60
```

Related Commands

Command	Description
graceful-restart helper	Enables the OSPF graceful-restart helper.

Platform Description N/A

5.22 graceful-restart helper

Use this command to enable the graceful restart helper function. Use the **no** form of this command to restore the default setting.

graceful-restart helper disable

no graceful-restart helper disable

graceful-restart helper { **strict-lsa-checking** | **internal-lsa-checking**}

no graceful-restart helper {**strict-lsa-checking** | **internal-lsa-checking**}

Parameter Description

Parameter	Description
disable	Prohibits a device from acting as a GR helper for another device.
strict-lsa-checking	Indicates that changes in Type 1 to Type 5 and Type 7 LSAs will be checked during the period that the device acts as a GR helper to determine whether the network changes. If the network changes, the device will stop acting as the GR helper.

internal-lsa-checking	Indicates that changes in Type 1 to Type 3 LSAs will be checked during the period that the device acts as a GR helper to determine whether the network changes. If the network changes, the device will stop acting as the GR helper.

Defaults The GR helper is enabled by default.

The router enabled with the GR helper does not check the LSA change by default.

Command Mode Routing process configuration mode

Usage Guide This command is used to configure the GR helper capability of a router. When a neighbor router implements GR, it sends a Grace-LSA to notify all neighbor routers. If the GR helper function is enabled on the local router, the local router becomes the GR helper on receiving the Grace-LSA, and helps the neighbor to complete GR. The **disable** option indicates that GR helper is not provided for any device that implements GR.

After a device becomes the GR helper, the network changes are not detected by default. If any change takes place on the network, the network topology converges after GR is completed. If you wish that network changes can be quickly detected during the GR process, you can configure **strict-lsa-checking** to check Type 1 to 5 and Type 7 LSAs that indicate the network information or **internal-lsa-checking** to check Type 1 to 3 LSAs that indicate internal routes of the AS domain. When the network scale is large, it is recommended that you disable the LSA checking options (**strict-lsa-checking** and **internal-lsa-checking**) because regional network changes may trigger termination of GR and consequently reduce the convergence of the entire network.

Configuration Examples The following example disables the GF helper and modifies the policy of checking network changes.

```
Ruijie(config)# router ospf1
Ruijie(config-router)# graceful-restart helper disable
Ruijie(config-router)# no graceful-restart helper disable
```

```
Ruijie(config-router)# graceful-restart helper
strict-lsa-checking
```

Related Commands

Command	Description
graceful-restart	Enables GR on the device.

Platform Description N/A

5.23 ip ospf authentication

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

ip ospf authentication [**message-digest** | **null**]

no ip ospf authentication

Parameter Description

Parameter	Description
message-digest	Enables MD5 authentication on the interface.
null	Enables no authentication.

Defaults No authentication mode is configured and that of the local area is used on the interface by default.

Command Mode Interface configuration mode

Usage Guide Plaintext authentication is applicable when **no** option is used with the command. Note that the no form of this command restores the default value. Whether authentication is used actually depends on authentication mode configured for the local area of the interface. If authentication mode is configured as **null,** no authentication is enabled. When both the interface and its area are configured with authentication, the one for the interface takes precedence.

Configuration Examples The following example configures MD5 authentication for OSPF on fastEthernet 0/1.

```
Ruijie (config)#interface fastEthernet0/1
Ruijie(config-if-FastEthernet 0/1)# ipaddress172.16.1.1
255.255.255.0
Ruijie(config-if-FastEthernet 0/1)# ip ospf authentication
message-digest
```

Related Commands

Command	Description
area authentication	Enables authentication and defines authentication mode in the OSPF area.
ip ospf authentication-key	Configures the plain text authentication key.
ip ospf message-digest-key	Configures the MD5 authentication key.

Platform N/A

Description

5.24 ip ospf authentication-key

Use this command to configure the OSPF plain text authentication key in interface configuration mode. Use the **no** form of this command to restore the default setting.

ip ospf authentication-key [**0 | 7**] *key*

no ip ospf authentication-key

Parameter Description

Parameter	Description
0	Displays the key in plain text.
7	Displays the key in cipher text.
key	Key containing at most eight characters.

Defaults It is disabled by default.

Command Mode Interface configuration mode

Usage Guide The **ip ospf authentication-key** command configures the key that will be inserted in all OSPF packet headers. As a result, if the keys are inconsistent, the OSPF neighbor relationship cannot be established between two devices directly connected, and thus route information exchange is

impossible.

The keys may vary by interface, but the devices that are connected to the same physical network segment must use the same key.

To enable the OSPF area authentication, execute the area authentication command in routing process configuration mode.

The authentication can be enabled separately on an interface by executing the ip ospf authentication command in interface configuration mode. When both the interface and the area are configured with authentication, the one for the interface takes precedence.

Configuration Examples

The following example configures the OSPF authentication key ospfauth for fast Ethernet *0/1*.

```
Ruijie (config)#interfacefastEthernet0/1
Ruijie(config-if-FastEthernet 0/1)# ipaddress172.16.1.1
255.255.255.0
Ruijie(config-if-FastEthernet 0/1)# ip ospf authentication-key ospfauth
```

Related Commands

Command	Description
area authentication	Enables OSPF area authentication and defines authentication mode
ip ospf authentication	Enables authentication on the interface and defines authentication mode

Platform Description

N/A

5.25 ip ospf cost

Use this command to configure the cost (OSPF metric) of the OSPF interface for sending a packet in interface configuration mode. Use the **no** form of this command to restore the default setting.

ip ospf cost *cost*

no ip ospf cost

Parameter Description

Parameter	Description
cost	OSPF interface cost in the range from 0 to 65535

Defaults The default interface cost is calculated as follows:
Reference bandwidth/Bandwidth
The reference bandwidth is *100* Mbps by default.

Command Mode Interface configuration mode

Usage Guide By default, the OSPF interface cost is 100Mbps/Bandwidth, where Bandwidth is the interface bandwidth configured with the bandwidth command in interface configuration mode.

The default costs of different types of lines are as follows:

- 64K serial line: 1562
- E1 line: 48
- 10M Ethernet: 10

- 100M Ethernet: 1

The OSPF cost configured with the **ip ospf cost** command will overwrite the default configuration.

Configuration Examples

The following example configures the OSPF cost of fastEthernet 0/1 to100.

```
Ruijie(config)# interfacefastEthernet0/1
Ruijie(config-if-FastEthernet 0/1)# ipospfcost100
```

Related Commands

Command	Description
bandwidth	Specifies the interface bandwidth. This setting does not affect the data transmission rate.
show ip ospf	Displays the OSPF global configuration information

Platform Description

N/A

5.26 ip ospf database-filter all out

Use this command to stop advertising LSAs of an interface, that is, the LSA update packets are not sent on the interface. Use the **no** form of the command to restore the default setting.

ip ospf database-filter all out

no ip ospf database-filter

Parameter Description

Parameter	Description
N/A	N/A

Defaults This function is disabled and all LSA update packets can be sent on the interface by default.

Command Mode Interface configuration mode

Usage Guide To stop sending LSA update packets on the interface, enable this function on the interface.

Then, the device maintains the neighboring connections and accepts LSAs from neighbors, but stops sending LSAs to neighbors.

Configuration Examples The following example stops sending LSA update packets of fastEthernet 0/1.

```
Ruijie(config)# interface fastEthernet 0/1
Ruijie(config-if-FastEthernet 0/1)# ip address 172.16.10.1 255.255.255.0
Ruijie(config-if-FastEthernet 0/1)# ip ospf database-filter all out
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

5.27 ip ospf dead-interval

Use this command to configure the interval for determining the death of an interface neighbor in interface configuration mode. Use the **no** form of this command to restore the default setting.

ip ospf dead-interval *seconds*

no ip ospf dead-interval

Parameter Description

Parameter	Description
seconds	Defines the interval for determining the neighbor death in seconds. The range is from 0 to 2,147,483,647.

Defaults The value of dead-interval is 4 times the interval configured with the **ip ospf hello-interval** command by default.

Command Mode Interface configuration mode

Usage Guide The OSPF dead interval is contained in the Hello packet. If OSPF does not receive a Hello packet from a neighbor within the dead interval, it declares that the neighbor is invalid and deletes this neighbor record form the neighbor list. By default, the dead interval is four times the Hello interval. If

the Hello interval is modified, the dead interval is modified automatically.

When using this command to manually modify the dead interval, pay attention to the following issues:

1. The dead interval cannot be shorter than the Hello interval.

2. The dead interval must be the same on all routers in the same network segment.

Configuration Examples The following example configures the interval for determining the death of the OSPF neighbor on fastEthernet 0/1 to30seconds.

```
Ruijie(config)# interface fastEthernet 0/1
Ruijie(config-if-FastEthernet 0/1)# ip address 172.16.10.1 255.255.255.0
Ruijie(config-if-FastEthernet 0/1)# ip ospf dead-interval30
```

Related Commands

Command	Description
ip ospf hello-interval	Specifies the interval at which the OSPF sends Hello packets
show ip ospf interface	Displays OSPF interface information.

Platform Description N/A

5.28 ip ospf disable all

Use this command to prevent the specified interface from generating OSPF packets. Use the **no** form of this command to restore the default setting.

ip ospf disable all

no ip ospf disable all

Parameter Description

Parameter	Description
N/A	N/A

Defaults OSPF packets are generated on the specified interface by default.

Command Mode Interface configuration mode

Usage Guide The interface configured with this command will ignore whether the network areas are matched. After this command is configured, an interface will not generate OSPF packets even if the interface belongs to the network; therefore, the interface does not receive or send any OSPF packets or participate in OSPF calculation.

Configuration Examples The following example prevents the specified interface from generating OSPF packets.

```
Ruijie(config)# interface fastEthernet 0/1
Ruijie(config-if-FastEthernet 0/1)# ip address172.16.10.1 255.255.255.0
Ruijie(config-if-FastEthernet 0/1)# ip ospf disable all
```

Related Commands

Command	Description

N/A	N/A

Platform Description N/A

5.29 ip ospf hello-interval

Use this command to set the interval for sending Hello packets in interface configuration mode. Use the **no** form of this command to restore the default setting.

ip ospf hello-interval *seconds*

no ip ospf hello-interval

Parameter Description

Parameter	Description
seconds	Interval for sending Hello packets in seconds. The range is from1 to 65535.

Defaults The defaults are as follows:

10secons for Ethernet

10seconsfor PPP or HDLC encapsulated interfaces

10secons for frame relay PTP interfaces

30secons for non-frame relay PTP sub-interface and X.25 interfaces

Command Mode Interface configuration mode

Usage Guide The interval of sending the Hello packets is included in the Hello packet. A shorter interval means that OSPF detects the topological change faster, which will increase network traffic. The Hello packet sending intervals for all the devices in the same network segment must be the same. To manually modify the interval to determine neighbor death, ensure that the Hello packet sending interval cannot be greater than dead-interval of the neighbor.

Configuration Examples The following example configures the interval of sending the Hello packets on fastEthernet 0/1 to15.

```
Ruijie(config)# interface fastEthernet 0/1
Ruijie(config-if-FastEthernet 0/1)# ip address172.16.10.1 255.255.255.0
Ruijie(config-if-FastEthernet 0/1)# ip ospf hello-interval15
```

Related Commands

Command	Description
ip ospf dead-interval	Sets the interval for determining the death of the OSPF neighbor.

Platform Description N/A

5.30 ip ospf message-digest-key

Use this command to configure the MD5 authentication key in interface configuration mode. Use the

no form of this command to restore the default setting.

ip ospf message-digest-key *key-id* **md5** [**0 | 7**] *key*

no ip ospf message-digest-key *key-id*

Parameter Description

Parameter	Description
key	Key of up to 16 characters
0	Displays the key in plain text.
7	Displays the key in cipher text.
key-id	Key identifier in the range from1 to 255

Defaults No MD5 key is configured by default.

Command Mode Interface configuration mode

Usage Guide The **ip ospf message-digest-key** command configures the key that will be inserted in all OSPF packet headers. As a result, if the keys are inconsistent, the OSPF neighboring relationship cannot be established between two devices directly connected, and thus route information exchange is impossible.

The keys can be different for different interfaces, but the devices that are connected to the same physical network segment must be configured with the same key. For neighbors, the same key

identifier must correspond to the same key.

To enable OSPF area authentication, execute the **area authentication** command in routing process configuration mode. The authentication can be enabled separately on an interface by executing the **ip ospf authentication** command in interface configuration mode. When both the interface and the area are configured with authentication, the one for the interface takes precedence.

The RGOS software supports smooth modification of MD5 authentication keys, which shall be added before deleted. When an MD5 authentication key of the device is added, the device will regard other devices have not had new keys and thus send multiple OSPF packets by using different keys, till it confirms that the neighbors have been configured with new keys. When all devices have been configured with new keys, it is possible to delete the old key.

Configuration Examples

The following example adds a new OSPF authentication key "hello5" with key ID 5 for fastEthernet 0/1.

```
Ruijie(config)# interface fastEthernet 0/1
Ruijie(config-if-FastEthernet 0/1)# ip address 172.16.24.2 255.255.255.0
Ruijie(config-if-FastEthernet 0/1)# ip ospf authentication message-digest
Ruijie(config-if-FastEthernet 0/1)# ip ospf message-digest-key 10 md5 hello10
Ruijie(config-if-FastEthernet 0/1)# ip ospf message-digest-key 5md5 hello5
```

When all neighbors are added with new keys, the old keys shall be deleted for all devices.

```
Ruijie(config)# interface fastEthernet 0/1
Ruijie(config-if-FastEthernet 0/1)# no ip ospf message-digest-key10md5
hello10
```

Related Commands

Command	Description
area authentication	Enables OSPF area authentication and defines authentication mode.
ip ospf authentication	Enables authentication on the interface and defines authentication mode.

Platform Description N/A

5.31 ip ospf mtu-ignore

Use this command to disable the MTU check when an interface receives the database description packet. Use the **no** form of this command to restore the default setting.

ip ospf mtu-ignore

no ip ospf mtu-ignore

Parameter Description

Parameter	Description
N/A	N/A

Defaults MTU check is disabled by default.

Command Mode Interface configuration mode

Usage Guide After receiving the database description packet, the device will check whether the MTU of the neighbor interface is the same as its own MTU. If the received database description packet indicates an MTU greater than the interface's MTU, the neighboring relationship cannot be established. This can be fixed by disabling the MTU check.

Configuration Examples The following example disables the MTU check function on fastEthernet 0/1.

```
Ruijie(config)# interface fastEthernet 0/1
Ruijie(config-if-FastEthernet 0/1)# ip ospf mtu-ignore
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

5.32 ip ospf network

Use this command to configure the OSPF network type in interface configuration mode. Use the **no** form of this command to restore the default setting.

ip ospf network { **broadcast | non-broadcast |**

point-to-multipoint [**non-broadcast**] **| point-to-point** }

no ip ospf network

Parameter Description

Parameter	Description
broadcast	Sets the OSPF network type as the broadcast type.

non-broadcast	Sets the OSPF network type as the non-broadcast multi-path access type, i.e. NBMA network.
point-to-multipoint [non-broadcast]	Sets the OSPF network type as the point-to-multipoint type. The value is the point-to-multipoint broadcast type by default. The non-broadcast option means the point-to-multipoint non-broadcast type.
point-to-point	Sets the OSPF network type as the point-to-point type.

Defaults The default configurations are as follows:

PTP network type: Point-to-Point Protocol(PPP), Serial Line Internet Protocol(SLIP), frame relay point-to-point (PTP) sub-interface, X.25 PTP sub-interface encapsulation

NBMA network type: frame relay (except for PTP sub-interface), X.25 encapsulation (except for PTP sub-interface)

Broadcast network type: Ethernet encapsulation

By default, the network type is the point-to-multipoint network type.

Command Mode Interface configuration mode

Usage Guide The broadcast type requires that the interface must have the broadcast capability.

The P2P type requires that the interfaces are interconnected in one-to-one manner.

The NBMA type requires full-meshed connections, and all interconnected routers can directly communicate with each other.

The P2MP type does not raise any requirement.

Configuration Examples

The following example configures the frame relay interface network as the P2P type.

```
Ruijie(config)# interface Serial 1/0
Ruijie(config-Serial 1/0)#ip address 172.16.24.4 255.255.255.0
Ruijie(config-Serial 1/0)# encapsulation frame-relay
Ruijie(config-Serial 1/0)# ip ospf network point-to-point
```

The following example configures the frame relay interface network as the NBMA type.

```
Ruijie(config)# interface Serial 1/0
Ruijie(config-Serial 1/0)# ip address 172.16.24.4 255.255.255.0
Ruijie(config-Serial 1/0)# encapsulation frame-relay
Ruijie(config-Serial 1/0)# ip ospf network non-broadcast
Ruijie(config-Serial 1/0)#exit
Ruijie(config)# router ospf 20
Ruijie(config-router)# neighbor 172.16.24.2 priority 1 poll-interval 150
```

Related Commands

Command	Description
dialer map ip	Defines the mapping between IP address and dialing number.
frame-relay map	Defines the mapping between IP address and frame DLCI.
neighbor(OSPF)	Defines the IP address of neighbor applicable to NBMA network type and point-to-multipoint non-broadcast type only.
X25 map	Defines the mapping between IP address and X.25 network address.

Platform Description N/A

5.33 ip ospf priority

Use this command to configure the OSPF priority in interface configuration mode. Use the **no** form of this command to restore the default setting.

ip ospf priority *priority*

no ip ospf priority

Parameter Description

Parameter	Description
priority	Sets the OSPF priority of the interface in the range from 0 to 255.

Defaults The default is 1.

Command Mode Interface configuration mode

Usage Guide The interface priority is included in the Hello packet. When DR/BDR election occurs in the OSPF broadcast type network, the device with higher priority will become the DR or BDR. If the devices have the same priority, the one with higher ID will become the DR or BDR. The device with priority 0 cannot become DR or BDR. This command is valid only for OSPF broadcast and non-broadcast network types.

Configuration Examples The following example configures the priority offastethernet 0/1 as 0.

```
Switch(config)#interface fastethernet 0/1
Ruijie(config-if-FastEthernet 0/1)# ipospfpriority0
```

Related Commands

Command	Description
ip ospf network	Configures the network type of the interface.

Platform Description N/A

5.34 ip ospf retransmit-interval

Use this command to define the interval for sending the link state update (LSU) packet on the interface in interface configuration mode. Use the **no** form of this command to restore the default setting.

ip ospf retransmit-interval *seconds*

ip ospf retransmit-interval

Parameter Description

Parameter	Description
seconds	Interval for sending the LSU packets in seconds. The range is from 0to 65535. This interval must be greater than the round trip delay of

	packets between two neighbors.

Defaults The default is 5.

Command Mode Interface configuration mode

Usage Guide After the device sends an LSU packet, the LSU packet stays in the transmission buffer queue. If no confirmation from the neighbor is obtained in the interval defined with the **ip ospf retransmit-interval** command, the LSU will be sent once again.

In serial lines or virtual links, the retransmission interval shall be slightly larger. The LSU packet retransmission interval of virtual links is defined with the area virtual-link command followed with the keyword retransmit-interval.

Configuration Examples The following example configures the LSU packet retransmission interval on fastEthernet 0/1 as 10 seconds.

```
Ruijie(config)# interface fastEthernet 0/1
Ruijie(config-if-FastEthernet 0/1)# ip ospf retransmit-interval 10
```

Related Commands

Command	Description
area virtual-link	Defines an OSPF virtual link.

Platform Description N/A

5.35 ip ospf source-check-ignore

Use this command to disable the source address check in the point-to-point link. Use the **no** form of this command to restore the default setting

ip ospf source-check-ignore

no ip ospf source-check-ignore

Parameter Description

Parameter	Description
N/A	N/A

Defaults This function is enabled by default.

Command Mode Interface configuration mode

Usage Guide For OSPF, the source address of the received packet is required to be in the same network segment with the receiving interface. However, in a point-to-point link, the addresses of two ends of the link are individually set, and they are not required to be in the same network segment. The peer address is informed during the process of point-to-point link negotiation; therefore, OSPF will check whether the source address of the packet is the informed one. If no, the OSPF regards this packet as illegal and drops it. In some applications, the addresses informed during the negotiation are shielded. You need

to disable the source address check to ensure the normal establishment of OSPF neighbors.

Configuration Examples The following example disables the source address check function in the point-to-point link.

```
Ruijie(config)# interface serial 1/0
Ruijie(config-if)# ip ospf source-check-ignore
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

5.36 ip ospf transmit-delay

Use this command to define the LSU packet transmission delay in interface configuration mode. Use the **no** form of this command to restore the default setting.

ip ospf transmit delay *seconds*

no ip ospf transmit delay

Parameter Description

Parameter	Description
seconds	LSU packet transmission delay in seconds in the range from 0 to 65535.

Defaults The default is 1.

Command Mode Interface configuration mode

Usage Guide Before the LSU packet is transmitted, the Age field in all the LSAs of the packet will be increased by the value defined with the **ip ospf transmit-delay** command in interface configuration mode. The configuration of this parameter shall consider the transmission and line transmission delay of the interface. For low-rate lines, the transmission delay of the interface shall be slightly larger. The LSU packet transmission delay of the virtual link is defined with the **area virtual-link** command followed with the keyword retransmit-interval.

The RGOS software will resend or request resending the LSA with Age up to 3600. If no update is obtained in time, the aged LSA will be cleared from the link state database.

Configuration Examples The following example configures the transmission delay of fastEthernet 0/1 as 10.

```
Ruijie(config)# interface fastEthernet 0/1
Ruijie(config-if-FastEthernet 0/1)# ip ospf transmit-delay 10
```

Related Commands

Command	Description
area virtual-link	Defines an OSPF virtual link.

Platform N/A

Description

5.37 log-adj-changes

Use this command to enable the logging of the neighbor state changes. Use the **no** form of the command to disable this function.

log-adj-changes [**detail**]

no log-adj-changes [**detail**]

Parameter Description

Parameter	Description
detail	Records the detail of changes.

Defaults This function is enabled by default. Without the detail parameter, the system records the logs that the neighbor enters or exits the full state.

Command Mode Routing process configuration mode

Usage Guide N/A

Configuration The following example logs the neighbor state changes.

Examples

```
Ruijie(config)# router ospf 1
Ruijie(config-router)# log-adj-changes detail
```

Related Commands

Command	Description
show ip ospf	Displays the OSPF global configuration information.

Platform Description N/A

5.38 max-concurrent-dd

Use this command to specify the maximum number of DD packets that can be processed (initiated or accepted) at the same time. Use the **no** form of this command to restore the default setting.

max-concurrent-dd *number*

no max-concurrent-dd

Parameter Description

Parameter	Description
number	Maximum number of DD packets in the range from1 to 65535

Defaults The default is 5.

Command Mode Routing process configuration mode

Usage Guide When a router is exchanging data with multiple neighbors, its performance will be affected. This command is configured to limit the maximum number of DD packets that each OSPF instance can have at the same time.

Configuration Examples The following example sets the maximum number of DD packets to 4.

After the configuration, the device can initiate to interact with four neighbors and can concurrently accept the interaction. That is, the device can interact with a maximum of eight neighbors.

```
Ruijie(config)# routerospf10
Ruijie(config-router)# max-concurrent-dd4
```

Related Commands

Command	Description
router ospf max-concurrent-dd	Sets the maximum number of neighbors allowed in concurrent interaction for all OSPF routing processes.

Platform Description N/A

5.39 max-metric

Use this command to set the maximum metric of the router-lsa, so that this routing device will not firstly be used as the transmission node by other devices in SPF computing. Use the **no** form of this command to restore the default setting.

max-metric router-lsa [external-lsa *[max-metric-value]]* [**include-stub**] [**on-startup** *[seconds]]* [**summary-lsa** *[max-metric-value]]*

no max-metric router-lsa [external-lsa *[max-metric-value]]* [**include-stub**] [**on-startup** *[seconds]]* [**summary-lsa** *[max-metric-value]]*

Parameter Description

Parameter	Description
router-lsa	Configures the maximum metric (0XFFFF) of non-stub links in the Router LSA.
external-lsa	Uses the maximum metric instead of the external-lsa metric (including the Type-5 and Type-7).
max-metric-value	Maximum metric of the LAS. The range is 1 to 16777215.The default value is 16711680,
include-stub	Configures the maximum metric of the stub links in the Router LSA.
on-startup	Advertises the maximum metric when the routing device starts up.
seconds	Interval of advertising the maximum metric. The range is 5 to 86400. The default value is 600 seconds.
summary-lsa	Uses the maximum metric to replace the summary LSA metric. (including Type-3 and Type-4)

Defaults The normal metric LSAs are used by default.

Command Mode Routing process configuration mode

Usage Guide With the **max-metric router-lsa** command enabled, the maximum metric of non-stub links in the Router LSA generated by the routing device is set. The link's normal metric is restored after canceling this configuration or reaching the timer.

By default, with this command enabled, the normal metric of the stub links is still advertised, which is the output interface cost. If the **include-stub** parameter is configured, the maximum metric of the stub links will be advertised.

When the device acts as an ABR, if no interval flow transmission is expected, use the **summary-lsa** parameter to set the summary LSA as the maximum metric.

When the device acts as an ASBR device, if no external flow transmission is expected, use the **external lsa** parameter to set the external LSA as the maximum metric.

The **max-metric router-lsa** command is usually used in the following scenes:

The device is restarted, which generally makes the IGP protocol converge faster, so that other devices attempt forwarding the dataflow through the new started-up device. The device is added into the network without being used for dataflow transmission. If the backup path exists, the current device is not used for the dataflow transmission. Otherwise, this device is still used to transmit the dataflow.

Remove the device from the network gracefully. With this command enabled, the current device advertises the maximum metric to all devices, as that the other devices in this network can choose the backup path to for the dataflow transmission before the current device is removed.

For the OSPF implementation in the earlier versions (RFC 1247 or earlier versions), the links with the maximum metric (0xFFFF) in the LSA will not participate in the SPF calculation, that is, no dataflow will be sent to the router that have generated these LSAs.

Configuration Examples The following example configures the LSA maximum metric as 100 seconds after starting the device.

```
Ruijie(config)# router ospf 20
Ruijie(config-router)# max-metric router-lsa on-startup 100
```

Related Commands

Command	Description
show ip ospf	Displays the OSPF related configurations.

Platform Description N/A

5.40 neighbor

Use this command to define the OSPF neighbor in routing process configuration mode. Use the **no** form of this command to restore the default setting.

Neighbor *ip-address* [**poll-interval** *seconds*] [**priority** *priority*] [**cost** *cost*]]

no neighbor *ip-address* [[**poll-interval**] [**priority**] | [cost]]

Parameter Description

Parameter	Description
ip address	IP address of the neighbor
poll-interval *seconds*	(Optional) Specifies the interval of polling neighbors in seconds. The

	range is from 0 to 2147483647. Only the non-broadcast (NBMA) network type supports this option.
priority *priority*	(Optional) Configures the priority of non-broadcast network neighbors. The range is from 0 to 255. Only the non-broadcast (NBMA) network type supports this option.
cost *cost*	(Optional) Configures the cost to each neighbor in point-to-multipoint network, not defined by default, where the cost configured on the interface will be used. The range is from 0 to 65535. Only the point-to-multipoint [non-broadcast] network type supports this option.

Defaults No neighbor is defined by default.

The default neighbor polling interval is 120 seconds.

The default NBMA neighbor priority is 0.

Command Mode Routing process configuration mode

Usage Guide The RGOS software must explicitly configure the neighbor information for every non-broadcast network neighbor. The IP address of a neighbor must be the master IP address of that neighbor interface.

In the NBMA network, if the neighbor device becomes inactive, in other words, if the Hello packet is not received within the device dead-interval, the OSPF will send more Hello packets to the neighbor. The interval at which the Hello packets are sent is called the polling interval. When the OSPF starts to work for the first time, it sends Hello packets only to the neighbor whose priority is not 0, so that the neighbor whose priority is set as 0 will not participate in the DR/BDR election. When the DR/BDR is generated, the DR/BDR sends the Hello packets to all neighbors to establish the neighbor

relationship.

Since the point-to-multipoint non-broadcast network has no broadcast capability, neighbors cannot be found dynamically. So, it is required to use this command to manually configure neighbor. In addition, it is possible to configure the cost to each neighbor through the cost option for the point-to-multipoint network type.

Configuration Examples The following example declares an OSPF non-broadcast network neighbor, with the IP address 172.16.24.2, priority 1 and polling interval 150 seconds.

```
Ruijie(config)# routerospf 20
Ruijie(config-router)# network 172.16.24.0 0.0.0.255 area 0
Ruijie(config-router)# neighbor 172.16.24.2 priority 1 poll-interval 150
```

Related Commands

Command	Description
ip ospf priority	Sets the interface priority.
ip ospf network	Sets the network type

Platform Description N/A

5.41 network area

Use this command to define which interfaces run OSPF and the OSPF areas they belong to in routing process configuration mode. Use the **no** form of this command to restore the default setting.

network *ip-address wildcard* **area** *area-id*

no network *ip-address wildcard* **area** *area-id*

Parameter Description

Parameter	Description
ip-address	IP address of the interface
wildcard	Defines the comparison bits in the IP address, with 0 for exact match and 1 for no comparison
area-id	OSPF area identifier. An OSPF area is always associated with an address range. For easy of management, a subnet can be used as the OSPF area identifier.

Defaults No OSPF area is configured by default.

Command Mode Routing process configuration mode

Usage Guide The ip-address and wildcard parameters allow associating multiple interfaces with one OSPF area. To run OSPF on an interface, it is required to include the primary IP address and secondary IP address of the interface in the IP address range defined by the network area command. If only the secondary IP address is included, OSPF cannot be enabled on the interface.

You can determine the OSPF process that the interface takes part in by the means of the best match if the IP address of the interface matches the IP address ranges defined by the network command in multiple OSPF processes.

Configuration The following example defines:

Examples Three areas: 0, 1 and 172.16.16.0
The interfaces whose IP addresses fall into the 192.168.12.0/24 range to area 1
The interfaces whose IP addresses fall into the 172.16.16.0/20 range to area 2
The remaining interface being assigned to area 0.

```
Ruijie(config)# routerospf 20
Ruijie(config-router)# network172.16.16.0
0.0.15.255 area172.16.16.0
Ruijie(config-router)# network192.168.12.0
0.0.0.255 area 1
Ruijie(config-router)# network0.0.0.0 255.255.255.255 area0
```

Related Commands

Command	Description
router ospf	Creates the OSPF routing process.

Platform Description N/A

5.42 overflow database

Use this command to configure the maximum number of LSAs supported by the current OSPF instance. Use the **no** form of this command to restore the default setting.

overflow database *number* [**hard | soft**]

no overflow database

Parameter Description

Parameter	Description

number	Maximum number of LSAs. The range is from 1 to 4294967294.
hard | soft	hard: shuts down the OSPF instance when the number of LSAs exceeds that number. soft: issues an alarm when the number of LSAs exceeds that number.

Defaults The maximum number of LSAs supported by the current OSPF instance is not restricted by default.

Command Mode Routing process configuration mode

Usage Guide To shut down the OSPF instance when the number of LSAs exceeds that number, use the hard parameter; otherwise, use the soft parameter.

Configuration Examples The following example configures that OSPF instance 10 will be shut down when there are more than 10 LSAs.

```
Ruijie(config)# router ospf 10
Ruijie(config-router)# overflow database 10 hard
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

5.43 overflow database external

Use this command to configure the maximum number of external LSAs and the waiting time from the overflow state to the normal state. Use the **no** form of this command to restore the default setting.

overflow database external *max-dbsize wait-time*

no overflow database external

Parameter Description

Parameter	Description
max-dbsize	Maximum number of external LSAs (the value shall be the same for all routing devices in the same AS). The range is from 0 to 2147483647.
wait-time	Waiting time of the routing device from the overflow status to normal status. The range is from 0 to 2147483647.

Defaults The maximum number of external-LSAs is not restricted by default.

If the maximum number of external-LSAs is restricted, the normal status cannot be restored when the maximum number is exceeded.

Command Mode Routing process configuration mode

Usage Guide When the number of external-LSAs exceeds the value of max-db size, the device enters the overflow state. Then no more external-LSA will be loaded and the external-LSAs generated locally will be cleared. After wait-time expires, the device restores to the normal state and external-LSAs are reloaded.

⚠ When using this function, ensure that all routers of the OSPF backbone area and common areas use the same max-db size value. Otherwise, the following situations occur:

⚠ The link status is inconsistent on the entire network and neighbors fail to achieve the Full state.

⚠ Incorrect routes occur, including loops.

⚠ AS-External-LSAs may be frequently retransmitted.

Configuration Examples The following example configures that the maximum number of external LSAs is 10, and it turns to the overflow status upon timeout, and the time interval attempting to restore from the overflow state to the normal state is 3 seconds.

```
Ruijie(config)# routerospf10
Ruijie(config-router)# overflow database external10 3
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

5.44 overflow memory-lack

Use this command to allow OSPF to enter the OVERFLOW state when the memory lacks. Use the **no**

form of this command to disable this function.

overflow memory-lack

no overflow memory-lack

Parameter Description

Parameter	Description
N/A	N/A

Defaults This function is enabled by default

Command Mode Routing process configuration mode

Usage Guide The action of OSPF entering the OVERFLOW state is to discard the newly-learned external route and effectively prevent the memory from increasing.

It is possible that enabling this function causes the route loop in the whole network. To reduce that possibility, OSPF will generate a default route directing to the NULL port and this default route will exist in the OVERFLOW state.

Use the **clear ip ospf process** command to reset the OSPF and remove the OSPF OVERFLOW state.

Use the no form of this command to prevent the OSPF to enter the OVERFLOW state when the memory is insufficient, which may result in the constantly consumption of the memory resources. If the memory is exhausted to some degree, the OSPF instance will stop and all learned routes will be removed.

Configuration Examples The following example prevents the OSPF from entering the OVERFLOW state when the memory is insufficient.

```
Ruijie(config)# router ospf 1
Ruijie(config-router)# no overflow memory-lack
```

Related Commands

Command	Description
clear ip ospf process	Resets the OSPF instances.
show ip protocols ospf	Displays the OSPF information.

Platform Description N/A

5.45 passive-interface

Use this command to configure the specified network interface or all interface as the passive interfaces. Use the **no** form of this command to restore the default setting.

passive-interface { **default |** *interface-type interface-number* | *interface-type interface-number ip-address* }

no passive-interface { **default |** *interface-type interface-number* | *interface-type interface-number ip-address* }

Parameter

Parameter	Description

Description

interface-type *interface-number*	Interface to be set as a passive interface
default	Sets all the interfaces as passive interfaces
interface-type *interface-number* *ip-address*	Sets the address of the specified interface as a passive address.

Defaults No interface is configured as a passive interface by default. All interfaces are allowed to receive or send OSPF packets.

Command Mode Routing process configuration mode

Usage Guide To prevent other devices in the network from dynamically learning the routing information of the device, set the specified network interface of this device as a passive interface or the IP address of the specified network interface as a passive address

Configuration Examples The following example configures fastEthernet 0/1 as a passive interface and the IP address of the interface 1.1.1.1 as the passive address.

```
Ruijie(config)# routerospf 30
Ruijie(config-router)# passive-interface fastEthernet 0/1
Ruijie(config-router)# passive-interface fastEthernet 0/1 1.1.1.1
```

Related Commands

Command	Description
show ip ospf interface	Displays the configuration information of the interface.

Platform Description N/A

5.46 redistribute

Use this command to redistribute the external routing information. Use the **no** form of this command to restore the default setting.

redistribute { **connected | ospf** *process-id* **| rip | static** } [**match { internal | external** [**1|2**] **|nssa-external** [**1|2**] }] [**metric** *metric-value*] [**metric-type** { *1|2* }] [**route-map** *route-map-name* **] [subnets] [tag** *tag-value* **]**

no redistribute { connected | ospf *process-id* **| rip | static } [match { internal | external [1|2] | nssa-external [1|2]}] [metric** *metric-value* **] [metric-type {** *1|2* **}] [route-map** *route-map-name*] [**subnets**] [**tag** *tag-value*]

Parameter Description

Parameter	Description
connected	Redistribution from direct routes
ospf *process-id*	Redistribution from an ospf instance specified in process-id in the range from 1 to 65,535
rip	Redistribution from rip

static	Redistribution from static routes
match	Filters specified routes for configuring OSPF route redistribution. By default, all the OSPF routes are redistributed.
metric *metric-value*	Specifies the metric of an OSPF external LSA in the range from 0 to 16777214.
metric-type{1|2}	Sets the external routing type as E-1 or E-2.
route-map *route-map-name*	Redistribution filter rule
subnets	Redistributes the routes of non standard networks.
tag *tag-value*	Sets the tag value of the routes redistributed to the OSPF in the range from 0 to 4294967295.

Defaults Redistribution configuration is not supported by default.

If you configure OSPF redistribution, all subtype routes of the instance are redistributed.

In other cases, all routings of this type are redistributed.

The default metric of LSAs generated by routes of other types is 20.

The default value of metric-type is E-2.

No route-map is associated by default.

Command Mode Route configuration mode

Usage Guide

After the command is configured, the router will become an ASBR, and the related routing information is imported into the OSPF domain and broadcasted to other OSPF routers through type-5 LSAs.

When you configure OSPF router distribution without the match parameter, the OSPF routes of all sub types are redistributed by default. Then the first configured match parameter is used as the original one. Only the routes matching the specific type can be redistributed. Use the no form of this command to restore the default configuration.

When you filter routes for redistribution by following the route-map rule, the match rule of the route-map rule is specific for the original redistribution parameters. The route-map rule works only when the redistributed OSPF routes follow the match rule.

The range of set metric is from 0 to 16777214 for the associated route-map. If the value exceeds the range, introducing a route fails.

The following are the rules for configuring the no form of the redistribute command:1. If the **no** form specifies some parameters, restore their default values.2. If the **no** form contains no parameter, delete the whole command.

Configuration Examples

The following example redistributes routes of **ospf2** to the OSPF area.

```
Ruijie(config)# router ospf1
Ruijie(config-router)# redistribute ospf 2 subnets
Ruijie(config-router)# redistribute ospf2match
external 1 internal
```

The following example displays the output of the **show run** command.

```
router ospf 1
redistribute ospf 2 match external 1 internal subnets
```

Related Commands

Command	Description
summary-address	Configures the aggregate route for the external route of the OSPF route area.
default-metric	Sets the default metric of the OSPF redistribution route.

Platform Description N/A

5.47 router ospf

Use this command to create the OSPF routing process in global configuration mode. Use the **no** form of this command to restore the default setting.

router ospf

router ospf *process-id*

no router ospf *process-id*

Parameter Description

Parameter	Description
process-id	ID of an OSPF process. If the process ID is not configured, process 1 is configured.

Defaults No OSPF routing process exists by default.

Command Mode Global configuration mode

Usage Guide Based on the original implementation, the RGOS10.1 adds the routing process ID to multi-instance OSPF. Different OSPF instances are mutually independent and can be approximately considered as two routing protocols that run independently.

Configuration Examples The following example creates the OSPF routing process 10

```
Ruijie(config)# router ospf10
```

Related Commands

Command	Description
show ip protocols	Displays the routing protocol information.
show ip ospf	Displays the OSPF information.

Platform Description N/A

5.48 router ospf max-concurrent-dd

Use this command to specify the maximum number of DD packets that can be processed (initiated or accepted) at the same time. Use the **no** form of this command to restore the default setting.

router ospf max-concurrent-dd *number*

no router ospf max-concurrent-dd

Parameter

Parameter	Description

Description

number	Maximum number of DD packets in the range from 1 to 65535.

Defaults The default is 10.

Command Mode Global configuration mode

Usage Guide When a routing device is exchanging data with multiple neighbors, its performance will be affected. This command is configured to limit the maximum number of DD packets that each OSPF instance can have (initiated or accepted) at the same time.

Configuration Examples The following example sets the maximum number of DD packets to 4.

After the configuration, the device can initiate to interact with four neighbors and can concurrently accept the interaction. That is, the device can interact with a maximum of eight neighbors.

```
Ruijie# configure terminal
Ruijie(config)# router ospfmax-concurrent-dd4
```

Related Commands

Command	Description
max-concurrent-dd	Sets the maximum number of the neighbors that the OSPF routing process can concurrently interact with.

Platform Description N/A

5.49 router-id

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

router-id *router-id*

no router-id

Parameter Description

Parameter	Description
router-id	Router ID in IP address form

Defaults The OSPF routing process will select the maximal interface IP address as the router ID by default.

If the loopback interface of an IP address is not configured, the OSPF routing process will select the maximum IP address among all its physical interfaces as the router ID.

Command Mode Routing process configuration mode

Usage Guide You can configure any IP address as the router ID. However, the router ID should be unique. Note that once the router ID changes, the OSPF protocol will do a lot of processing. Therefore, it is not recommended to change the router ID. The device can be changed only when no LSA is generated.

Configuration Examples The following example modifies the router ID to 0.0.0.36.

```
Ruijie(config)# router ospf 20
Ruijie(config-router)# router-id0.0.0.36
```

Related Commands

Command	Description
show ip protocols	Displays the routing protocol information.

Platform Description N/A

5.50 show ip ospf

Use this command to display the OSPF information.

show ip ospf [*process-id*]

Parameter Description

Parameter	Description
process-id	OSPF process ID

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide This command displays the information of the OSPF routing process.

Configuration Examples The following example displays the output of the **show ip ospf** command.

```
Ruijie# show ip ospf
Routing Process "ospf 1" with ID 1.1.1.1
Domain ID type 0x0105, value 0x010101010101
Process uptime is 4 minutes
Process bound to VRF default
Memory Overflow is enabled.
Router is not in overflow state now.
Conforms to RFC2328, and RFC1583Compatibility flag isenabled
Supports only single TOS(TOS0) routes
Enable two-way-maintain
Supports opaque LSA
Supports Graceful Restart
This router is an ASBR (injecting external routing information)
Originating router-LSAs with maximum metric
Condition:on startup for 100 seconds, State:inactive
Advertise stub links with maximum metric in router-LSAs
Advertise summary-LSAs with metric 16711680
Advertise external-LSAs with metric 16711680
Unset reason:timer expired, Originated for 100 seconds
Unset time:00:02:02.080, Time elapsed: 00:23:54.656
SPF schedule delay 5 secs, Hold time between two SPFs 10 secs
Initial LSA throttle delay 0 msecs
Minimum hold time for LSA throttle 5000 msecs
```

```
Maximum wait time for LSA throttle 5000 msecs
Lsa Transmit Pacing timer 40 msecs, 10 LS-Upd
Minimum LSA arrival 1000 msecs
Pacing lsa-group:240 secs
Number of incomming current DD exchange neighbors 0/5
Number of outgoing current DD exchange neighbors 0/5
Number of external LSA 4. Checksum 0x0278E0
Number of opaque AS LSA 0. Checksum 0x000000
Number of non-default external LSA 4
External LSA database is unlimited.
Number of LSA originated 6
Number of LSA received 2
Log Neighbor Adjency Changes :Enabled
Graceful-restart disabled
Graceful-restart helper support enabled
Number of areas attached to this router: 1
Area 0 (BACKBONE)
Number of interfaces in this area is 1(1)
Number of fully adjacent neighbors in this area is 1
Area has no authentication
SPF algorithm last executed 00:01:26.640 ago
SPF algorithm executed 4 times
Area 1 (NSSA)
Number of interfaces in this area is 1(1)
Number of fully adjacent neighbors in this area is 0
Number of fully adjacent virtual neighbors through this area is 0
Area has no authentication
SPF algorithm last executed 02:09:23.040 ago
SPF algorithm executed 4 times
Number of LSA 6. Checksum 0x028638
NSSA Translator State is disabled, Stability Interval expired in 00:00:03
```

Field	Description
Router ID	ID of a router.
Process uptime	Effective time of the current OSPF process (the process does not take effect when device-id is 0.0.0.0)
Bou to VRF	VRF of the current OSPF

Conforms to RFC2328	Same as the RFC2328
RFC1583Compatibilit flag	Whether the RFC1583 or RFC2328 is adopted for the calculation of external routes. This policy is used in the selection of best ASBR and in the route comparison.
Support Tos	Supports Only TOS0.
Supports opaque LSA	Supports opaque-LSA.
Graceful-restart	GR Restart capability described in the RFC3623 Graceful Restart
Graceful-restart helper	GR Help capability described in the RFC3623 Graceful Restart
Router Type	OSPF device type, including normal, ABR, and ASBR
SPF Delay	Delay before the SPF calculation is invoked after the topology change is received
SPF-holdtime	Minimum holdtime between two SPF calculations
LsaGroupPacing	Parameter used for LSA pacing, checksum calculation, and aging interval
Incomming current DD exchange neighbors	Number of neighbors under interaction. The incoming neighbors are those entering the exstart status for the first time.
Outgoing current DD exchange neighbors	Number of neighbors under interaction. The outgoing neighbors are those exiting from the higher status to the exstart status for re-interaction.

Number of external LSA	Number of external LSAs stored in the database
External LSA Checksum Sum	Checksum sum of external LSAs stored in the database
Number of opaque LSA	Number of external LSAs stored in the database
Opaque LSA Checksum Sum	Checksum sum of external LSAs stored in the database
Number of non-default external LSA	Number of external LSAs with non-default routes
External LSA database limit	Limit of external LSA number
Exit database overflow state interval	Time of exiting the overflow status
Database overflow state	Whether the current OSPF process is in the overflow status
Number of LSA originated	Number of LSAs generated
Number of LSA received	Number of LSAs received
Log Neighbor Adjency Changes	Whether the record switch for neighbor status change is enabled
Number of areas attached to this router	Total number of areas on the devices
Area type	Area type, including normal, stub, and nssa
Number of interfaces in this area	Number of interfaces in this area

Number of fully adjacent neighbors in this area	Number of Full neighbors of the area
Number of fully adjacent virtual neighbors through this area	Number of Full neighbors with virtual connections in the area. It is effective only in the non-backbone default-type areas.
Area authentication	Authentication mode of the area
SPF algorithm last executed	Time from the previous SPF calculation to the current time
SPF algorithm executed times	Times of SPF calculations
Number of LSA	Total number of LSAs in this area
Checksum Sum	Checksum sum of the LSAs in the area
NSSATranslatorState	Whether to convert the NSSA LSA to External LSA. It is effective on the ABR OSPF process in the NSSA.

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

5.51 show ip ospf border-routers

Use this command to display the OSPF internal routing table on the ABR/ASBR.

show ip ospf [*process-id***] border-routers**

Parameter Description

Parameter	Description
process-id	OSPF process ID

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide This command displays the OSPF internal routes from the local routing device to the ABR or ASBR. The OSPF internal routing table is different from the one displayed with the show ip route command. The OSPF internal routing table has the destination address of the router ID instead of the destination network.

Configuration Examples The following example displays the output of the **show ip ospf border-mrouters** command.

```
Ruijie# show ip ospf border-routers
OSPF internal Routing Table
Codes:i - Intra-area route, I - Inter-area route
i 1.1.1.1 [2] via 10.0.0.1, FastEthernet 0/1, ABR, ASBR, Area 0.0.0.1 select
```

The following table describes fields in the output.

Field	Description
Codes	Route type code, where “i” means intra-area routes, while “I” means inter-area routes.
I	Intra-area routes
1.1.1.1	Displays the OSPF ID of the border device.
[2]	Displays the cost to the border device.
via 10.0.0.1	Displays the next-hop gateway to the border device.
FastEthernet 0/1	Displays the interface to the border device.
ABR, ASBR	Displays the type of the border device, including ABR, ASBR, or both.
Area 0.0.0.1	Displays the area that learns the route.
select	Indicates the currently selected optimal path when there are multiple paths to the ASBR.

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

5.52 show ip ospf database

Use this command to display the OSPF link state database information. Use the **no** form of this command to restore the default setting. Different formats of the command will display different LSA information.

show ip ospf [*process-id* [*area-id* | *ip-address*]] **database** [{ **asbr-summary | external | network | nssa-external | opaque-area | opaque-as | opaque-link | router | summary** }] [{ **adv-router** *ip-address* **| self-originate } |** *link-state-id* **| brief**] [**database-summary | max-age | detail**]

Parameter Description

Parameter	Description
area-id	(Optional) Displays the area ID.
adv-device	(Optional) Displays the LSA information generated by the specified advertising device.
link-state-id	(Optional) Displays the LSA information of the specified OSPF link state identifier.
self-originate	(Optional) Displays the LSA information generated by the device itself.
Max-age	(Optional) Displays the LSAs aged.
router	(Optional) Displays the OSPF device LSA information.
network	(Optional) Displays the OSPF network LSA information.
summary	(Optional) Displays the OSPF summary LSA information.
asbr-summary	(Optional) Displays the ASBR summary LSA information.

external	(Optional) Displays the OSPF external LSA information.
nssa-external	(Optional) Displays the category 7 OSPF external LSA information.
opaque-area	(Optional) Displays type 10 LSAs.
opaque-as	(Optional) Displays type 11 LSAs.
opaque-link	(Optional) Displays type 9 LSAs.
database-summary	(Optional) Displays the statistics of LSAs of the link state database.
detail	Displays detailed information of LSAs of the OSPF.
brief	Displays the brief information of the LSAs of the specified type.

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide When the OSPF link state database is very large, you should display the information on the link state database by item. Proper use of commands may help OSPF troubleshooting.

Configuration Examples The following example displays the output of the **show ip ospf database** command.

```
Ruijie# show ip ospf database
OSPF Device with ID (1.1.1.1) (Process ID 1)
```

```
Device Link States (Area 0.0.0.0)
Link ID        ADV Device     Age  Seq#      CkSum  Link count
1.1.1.1        1.1.1.1        2    0x80000011 0x6f39 2
3.3.3.3        3.3.3.3        120  0x80000002 0x26ac 1
Network Link States (Area 0.0.0.0)
Link ID        ADV Device     Age  Seq#      CkSum
192.88.88.27    1.1.1.1        120  0x80000001 0x5366
Summary Link States (Area 0.0.0.0)
Link ID        ADV Device     Age  Seq#      CkSum  Route
10.0.0.0       1.1.1.1        2    0x80000003 0x350d 10.0.0.0/24
100.0.0.0      1.1.1.1        2    0x8000000c 0x1ecb 100.0.0.0/16
Device Link States (Area 0.0.0.1 [NSSA])
Link ID        ADV Device     Age  Seq#      CkSum  Link count
1.1.1.1        1.1.1.1        2    0x80000001 0x91a2 1
         Summary Link States (Area 0.0.0.1 [NSSA])
Link ID        ADV Device     Age  Seq#      CkSum  Route
100.0.0.0      1.1.1.1        2    0x80000001 0x52a4 100.0.0.0/16
192.88.88.0     1.1.1.1        2    0x80000001 0xbb2d 192.88.88.0/24
NSSA-external Link States (Area 0.0.0.1 [NSSA])
Link ID        ADV Device     Age  Seq#      CkSum  Route            Tag
20.0.0.0       1.1.1.1        1    0x80000001 0x033c E2 20.0.0.0/24    0
100.0.0.0      1.1.1.1        1    0x80000001 0x9469 E2 100.0.0.0/28   0
AS External Link States
Link ID        ADV Device     Age  Seq#      CkSum  Route            Tag
20.0.0.0       1.1.1.1        380  0x8000000a 0x7627 E2 20.0.0.0/24    0
100.0.0.0      1.1.1.1        620  0x8000000a 0x0854 E2 100.0.0.0/28   0
```

The following table describes the fields in the output of the **show ip ospf database** command.

Field	Description
OSPF Device with ID	Displays the Router ID.
Device Link States	Displays the device LSA information.
Net Link States	Displays the network LSA information.
Summary Net Link States	Displays the summary network LSA information.

NSSA-external Link States	Displays the type 7 autonomous external LSA information.
AS External Link States	Displays the type 5 autonomous external LSA information.
Link ID	Displays the Link ID.
ADV Device	Displays the ID of the device that advertises the LSAs.
Age	Displays the keepalive period of the LSA.
Seq#	Displays the sequence number of the LSA, which is used to check aged or duplicate LSAs.
Cksum	Displays the checksum of LSAs.
Link-Count	Displays the number of links in the device LSA information.
Route	Displays the device information included in the LSA.
Tag	Displays the tag of the LSA.

The following example displays the output the **show ip ospf database asbr-summary** command.

```
Ruijie# show ip ospf database asbr-summary
     OSPF Device with ID (1.1.1.35) (Process ID 1)
         ASBR-Summary Link States (Area 0.0.0.1)
LS age: 47
Options: 0x2 (*|-|-|-|-|-|E|-)
LS Type: ASBR-summary-LSA
Link State ID: 3.3.3.3 (AS Boundary Device address)
Advertising Device: 1.1.1.1
LS Seq Number: 80000001
Checksum: 0xbe8c
Length: 28
Network Mask: /0
```

```
    TOS: 0  Metric: 1
```

The following table describes the fields in the output of the **show ip ospf database asbr-summary** command.

Field	Description
OSPF Device with ID	Displays the router ID.
AS Summary Link States	Displays the summary LSA information in the AS.
LS age	Displays the keepalive period of the LSA.
Options	Option
LS Type	Displays the type of the LSA.
Link State ID	Displays the link ID of the LSA.
AdvertisingRouter	Displays the device advertising the LSA.
LS Seq Number	Displays the sequence number of the LSA.
Checksum	Displays the checksum of the LSAs.
Length	Displays the length (in bytes) of the LSA.
Network Mask	Displays the network mask of the route corresponding to the LSA.
TOS	TOS value, which can be only 0 now.
Metric	Displays the metric of the route corresponding to the LSA.

The following example displays the output of the **show ip ospf database external** command.

```
Ruijie# show ip ospf database external
     OSPF Device with ID (1.1.1.35) (Process ID 1)
         AS External Link States
LS age: 752
Options: 0x2 (*|-|-|-|-|-|E|-)
LS Type: AS-external-LSA
Link State ID: 20.0.0.0 (External Network Number)
Advertising Device: 1.1.1.1
LS Seq Number: 8000000a
Checksum: 0x7627
Length: 36
Network Mask: /24
     Metric Type: 2 (Larger than any link state path)
     TOS: 0
     Metric: 20
     Forward Address: 0.0.0.0
     External Route Tag: 0
```

The following table describes the fields in the output of the **show ip ospf database external** command.

Field	Description
OSPF Device with ID	Displays the router ID.
Type-5 AS External Link States	Displays autonomous external LSA information.
LS age	Displays the keepalive period of the LSA.
Options	Option
LS Type	Displays the type of the LSA.
Link State ID	Displays the link ID of the LSA.

Advertising Router	Displays the device advertising the LSA
LS Seq Number	Displays the sequence number of the LSA.
Checksum	Displays the checksum of the LSAs.
Length	Displays the length (in bytes) of the LSA.
Network Mask	Displays the network mask of the route corresponding to the LSA.
Metric Type	Indicates the external link type.
TOS	TOS value, which can be 0 only now.
Metric	Displays the metric of the route corresponding to the LSA.
Forward Address	IP address through which traffic is forwarded to the destination network. If this address is 0.0.0.0, the data traffic will be forwarded to the device that generates the link state.
External Route Tag	External route tag. Each external route has a 32-byte route tag. The OSPF does not use the route tag by itself, but it will be used by other routing processes to redistribute OSPF routes.

The following example displays the output of the **show ip ospf database network** command:

```
Ruijie# show ip ospf database network
OSPF Router with ID (1.1.1.1) (Process ID 1)
Network Link States (Area 0.0.0.0)
LS age: 572
Options:0x2 (*|-|-|-|-|-|E|-)
LS Type:network-LSA
Link State ID:192.88.88.27 (address of Designated Router)
Advertising Router:1.1.1.1
LS Seq Number: 80000001
```

```
Checksum:0x5366
Length: 32
Network Mask: /24
Attached Router:1.1.1.1
Attached Router:3.3.3.3
```

The following table describes the fields in the output of the **show ip ospf database network** command.

Field	Description
OSPF Router with ID	Displays the router ID corresponding to the follow-up information and the process ID corresponding to the OSPF.
Network LinStates	Displays the network LSA information.
LS age	Displays the keepalive period of the LSA.
Options	Option
LS Type	Displays the type of the LSA.
Link State ID	Displays the link ID of the LSA.
Advertising Device	Displays the device advertising the LSA.
LS Seq Number	Displays the sequence number of the LSA.
Checksum	Displays the checksum of LSAs.
Length	Displays the length (in bytes) of the LSA.
Network Mask	Displays the network mask of the network corresponding to the LSA.

Attached Router	Displays the device that is connected with the network.

The following example displays the output of the **show ip ospf database device** command:

```
Ruijie# show ip ospf database router
OSPF Router with ID (1.1.1.1) (Process ID 1)
Router Link States (Area 0.0.0.0)
LS age: 322
Options:0x2 (*|-|-|-|-|-|E|-)
Flags:0x3 :ABR ASBR
LS Type:router-LSA
Link State ID:1.1.1.1
Advertising Router:1.1.1.1
LS Seq Number: 80000012
Checksum:0x6d3a
Length: 48
Number of Links: 2
Link connected to:Stub Network
(Link ID) Network/subnet number: 100.0.1.1
(Link Data) Network Mask: 255.255.255.255
Number of TOS metrics: 0
TOS 0 Metric: 0
```

The following table describes the fields in the output of the **show ip ospf database device** command.

Field	Description
OSPF Device with ID	Displays the router ID.
Device Link States	Displays the device LSA information.
LS age	Displays the keepalive period of the LSA.
Options	Option

Flag	Flag
LS Type	Displays the type of the LSA.
Link State ID	Displays the link ID of the LSA.
Advertising Router	Displays the device advertising the LSA.
LS Seq Number	Displays the sequence number of the LSA.
Checksum	Displays the checksum of LSAs.
Length	Displays the length (in bytes) of the LSA.
Number of Links	Displays the number of links associated with the device.
Link connected to	Displays what the link is connected to and the network type.
(Link ID)	Link identifier
(Link Data)	Link data
Number of TOS metrics	TOS value, supporting TOS0 only
TOS 0 Metrics	TOS0 metric

The following example displays the output of the **show ip ospf database summary** command:

```
Ruijie# show ip ospf database summary
     OSPF Device with ID (1.1.1.1) (Process ID 1)
         Summary Link States (Area 0.0.0.0)
```

```
LS age: 499
Options: 0x2 (*|-|-|-|-|-|E|-)
LS Type: summary-LSA
Link State ID: 10.0.0.0 (summary Network Number)
Advertising Device: 1.1.1.1
LS Seq Number: 80000004
Checksum: 0x330e
Length: 28
Network Mask: /24
     TOS: 0  Metric: 11
```

The following table describes the fields in the output of the **show ip ospf database summary** command.

Field	Description
OSPF Router with ID	Displays the router ID.
Summary Net Link States	Displays the summary network LSA information.
LS age	Displays the keepalive period of the LSA.
Options	Option
LS Type	Displays the type of the LSA.
Link State ID	Displays the link ID of the LSA.
Advertising Router	Displays the device advertising the LSA.
LS Seq Number	Displays the sequence number of the LSA.

Checksum	Displays the checksum of LSAs.
Length	Displays the length (in bytes) of the LSA.
Network Mask	Displays the network mask of the route corresponding to the LSA.
TOS	TOS value, supporting only 0 now
Metric	Displays the metric of the route corresponding to the LSA.

The following example displays the output of the **show ip ospf database nssa-external** command:

```
Ruijie# show ip ospf database nssa-external
     OSPF Device with ID (1.1.1.1) (Process ID 1)
NSSA-external Link States (Area 0.0.0.1 [NSSA])
LS age: 1
Options: 0x0 (*|-|-|-|-|-|-|-)
LS Type: AS-NSSA-LSA
Link State ID: 20.0.0.0 (External Network Number For NSSA)
Advertising Device: 1.1.1.1
LS Seq Number: 80000001
Checksum: 0x033c
Length: 36
Network Mask: /24
     Metric Type: 2 (Larger than any link state path)
     TOS: 0
     Metric: 20
     NSSA: Forward Address: 100.0.2.1
     External Route Tag: 0
```

The following table describes the fields in the output of the **show ip ospf database nssa-external** command.

Field	**Description**

OSPF Router with ID	Displays the router ID.
NSSA-external Link States	Displays the type 7 autonomous external LSA information.
LS age	Displays the keepalive period of the LSA.
Options	Option
LS Type	Displays the type of the LSA.
Link State ID	Displays the link ID of the LSA.
Advertising Router	Displays the device advertising the LSA.
LS Seq Number	Displays the sequential number of the LSA.
Checksum	Displays the checksum of the LSAs.
Length	Displays the length (in bytes) of the LSA.
Network Mask	Displays the network mask of the route corresponding to the LSA.
Metric Type	Displays the metric type.
TOS	TOS value, which can be 0 only now.
Metric	Displays the metric of the route corresponding to the LSA.

NSSA:Forward Address	IP address through which traffic is forwarded to the destination network. If this address is 0.0.0.0, the data traffic will be forwarded to the device that generates the link state.
External Route Tag	External route tag. Each external route has a 32-byte route tag. The OSPF does not use the route tag by itself, but it will be used in redistributing OSPF routes by other routing process.

The following example displays the output of the **show ip ospf database external** command:

```
Ruijie# show ip ospf database external
     OSPF Device with ID (1.1.1.1) (Process ID 1)
         AS External Link States
LS age: 1290
Options: 0x2 (*|-|-|-|-|-|E|-)
LS Type: AS-external-LSA
Link State ID: 20.0.0.0 (External Network Number)
Advertising Device: 1.1.1.1
LS Seq Number: 8000000a
Checksum: 0x7627
Length: 36
Network Mask: /24
     Metric Type: 2 (Larger than any link state path)
     TOS: 0
     Metric: 20
     Forward Address: 0.0.0.0
     External Route Tag: 0
```

The following table describes the fields in the output of the **show ip ospf database external** command.

Field	Description
OSPF Device with ID	Displays the router ID.

Type-7 AS External Link States	Displays the type 7 autonomous external LSA information.
LS age	Displays the keepalive period of the LSA.
Options	Option
LS Type	Displays the type of the LSA.
Link State ID	Displays the link ID of the LSA.
Advertising Router	Displays the device advertising the LSA.
LS Seq Number	Displays the sequence number of the LSA.
Checksum	Displays the checksum of the LSAs.
Length	Displays the length (in bytes) of the LSA.
Network Mask	Displays the network mask of the route corresponding to the LSA.
Metric Type	Displays the metric type.
TOS	TOS value, which can be 0 only now.
Metric	Displays the metric of the route corresponding to the LSA.
Forward Address	IP address through which traffic is forwarded to the destination network. If this address is 0.0.0.0, the data traffic will be forwarded to the device that generates the link state.

External Route Tag	External route tag. Each external route has a 32-byte route tag. The OSPF does not use the route tag by itself, but it will be used in redistributing OSPF routes by other routing process.

The following example displays the output of the **show ip ospf database database-summary** command:

```
Ruijie# show ip ospf database database-summary
OSPF process 1:
Device Link States      : 4
Network Link States     : 2
Summary Link States     : 4
ASBR-Summary Link States : 0
AS External Link States  : 4
NSSA-external Link States: 2
```

The following table describes the fields in the output of the command **show ip ospf database database-summary**.

Field	Description
OSPF Process	OSPF process ID
Router Link	Number of device LSAs in the area
Network Link	Number of network LSAs in the area
Summary Link	Number of summary LSAs in the area
ASBR-Summary Link	Number of ASBR summary LSAs in the area
AS External Link	Number of NSSA LSAs in the area

NSSA-external Link	Number of NSSA LSAs in the area

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

5.53 show ip ospf interface

Use this command to display the OSPF-associated interface information.

show ip ospf [*process-id* **] interface [** *interface-type interface-number* **| brief]**

Parameter Description

Parameter	Description
process-id	OSPF process ID
interface-type	(Optional) type of the specified interface
interface-number	(Optional) number of the specified interface
brief	Displays the summary of the interface.

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide This command displays the OSPF information on the interface.

Configuration Examples The following example displays the output of the **show ip ospf interface fastEthernet** *0/1* command:

```
Ruijie# show ip ospf interface fastEthernet0/1
FastEthernet 0/1 is up, line protocol is up
Internet Address 192.88.88.27/24, Ifindex 4, Area 0.0.0.0, MTU 1500
Matching network config: 192.88.88.0/24
Process ID 1, Router ID 1.1.1.1, Network Type BROADCAST, Cost: 1
Transmit Delay is 1 sec, State DR, Priority 1,BFD enabled
Designated Router (ID) 1.1.1.1, Interface Address 192.88.88.27
Backup Designated Router (ID) 3.3.3.3, Interface Address 192.88.88.72
Timer intervals configured,Hello 10,Dead 40,Wait 40,Retransmit 5
Hello due in 00:00:03
Neighbor Count is 1, Adjacent neighbor count is 1
Crypt Sequence Number is 70784
Hello received 1786 sent 1787, DD received 13 sent 8
LS-Req received 2 sent 2, LS-Upd received 29 sent 53
LS-Ack received 46 sent 23, Discarded 1
```

The following table describes the fields in the output of the **show ip ospf interface serial***1/0* command.

Field	Description

FastEthernet 0/1 State	State of the network interface; UP means normal working and Down means faults.
Internet Address	Interface IP address
Area	OSPF area of the interface
MTU	Corresponding MTU
Matching network config	Network area configured for the corresponding OSPF
Process ID	Corresponding process ID
Router ID	OSPF router id
Network Type	OSPF network type
Cost	OSPF interface cost
Transmit Delay is	OSPF interface transmit delay
State	DR/BDR state ID
Priority	Priority of the interface
Designated Router(ID)	DR ID of the interface
DR's Interface address	Address of the DR of the interface
Backup designated device(ID)	Router ID of the BRD of the interface

BDR's Interface address	Address of the BDR of the interface
Time intervals configured	Hello, Dead, Wait, and Retransmit intervals of the interface
Hello due in	Time when the previous Hello is sent
Neighbor count	Total number of neighbors
Adjacent neighbor count	Number of Full neighbors
Crypt Sequence Number	The corresponding md5 authentication number of the interface
Hello received send	Statistics on the Hello packets sent and received
DD received send	Statistics on the DD packets sent and received
LS-Req received send	Statistics on the LS request packets sent and received
LS-Upd received send	Statistics on the LS update packets sent and received
LS-Ack received send	Statistics on the LS response packets sent and received
Discard	Statistics on the discarded OSPF packets

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

5.54 show ip ospf neighbor

Use this command to display the OSPF neighbor list.

show ip ospf [*process-id*] **neighbor**[**statistics** | { [*interface-type interface-number*] | [*neighbor-id*] | [**detail**] }]

Parameter Description

Parameter	Description
detail	(Optional) Displays the neighbor details.
interface-type interface-number	(Optional) Displays the neighbor information of the specified interface
neighbor-id	(Optional) Displays the information of the specified neighbor
statistics	(Optional) Displays the neighbor statistics.

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide This command displays neighbor information usually used to check whether the OSPF is running normally.

Configuration Examples The following example displays the output of the **show ip ospf neighbor** command.

```
Ruijie# show ip ospf neighbor
OSPF process 1, 1 Neighbors, 1 is Full:
Neighbor ID   Pri   State    Dead Time   Address       Interface
3.3.3.3       1     Full/BDR  00:00:32   192.88.88.72   FastEthernet 0/1

Ruijie# show ip ospf neighbor detail
Neighbor 3.3.3.3, interface address 192.88.88.72
In the area 0.0.0.0 via interface FastEthernet 0/1
Neighbor priority is 1, State is Full, 11 state changes
DR is 192.88.88.27, BDR is 192.88.88.72
Options is 0x52 (*|O|-|EA|-|-|E|-)
Dead timer due in 00:00:32
Neighbor is up for 05:11:27
Database Summary List 0
Link State Request List 0
Link State Retransmission List 0
Crypt Sequence Number is 0
Thread Inactivity Timer on
Thread Database Description Retransmission off
Thread Link State Request Retransmission off
Thread Link State Update Retransmission off
Thread Poll Timer on
Graceful-restart helper disabled
```

The following table describes the fields in the output of the **show ip ospf neighbor** command.

Field	Description
Neighbor ID	Neighbor ID
Pri	Neighbor priority (for selection of DR)

State	Neighbor status
Dead Time	Remaining time for the neighbor to enter the Dead status
Address	Interface address of the neighbor
Interface	Interface of the neighbor
interface address	Interface address of the neighbor device
In the area	Displays the area that learns the neighbor.
via interface	Displays the interface that learns the neighbor
Neighbor priority	Priority of the neighbor OSPF
State	OSPF neighbor connection state. FULL means the stable state; DR indicates that the neighbor is the designated device; BDR indicates that the neighbor is the backup designated device; DROTHER indicates that the neighbor is not a DR/BDR. Point-to-point network type has no DR or DBR.
State changes times	Times of state changes
Dead Time	Dead time of the neighbor
DR	Interface address of the DR elected by the neighbor device (that is, the DR field of the Hello packet)
BDR	Interface address of the BDR elected by the neighbor device (that is, the BDR field of the Hello packet)

Options	Hello packet E-bit option, where 0 indicates that the area is a STUB area; 2 indicates that the area is not a STUB area.
Dead timer due in	Dead time of the neighbor device
Neighbor up time	Period from when the device is discovered till now
Database Summary List	Statistics on the neighbor DD packets
LinkState Request List	Statistics on the neighbor LS request packets
LinkState Retransmission List	Statistics on the neighbor re-transmit packets
Crypt Sequence Number	Area MD5 authentication code
Thread Inactivity Timer	Status of invalid neighbor timer
Thread Database Description Retransmission	Status of DD packet timer of the interface
ThreadLinkState Request Retransmission	Status of LS request packet timer of the interface
ThreadLinkState Update Retransmission	Status of LS update packet timer of the interface
Thread Poll Timer	Poll Timer start status of the static neighbor

Graceful-restart helper	Whether it is able to function as the GR Helper of a specified neighbor

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

5.55 show ip ospf route

Use this command to display the OSPF routes.

show ip ospf [*process-id*] **route** [**count |** *ip-address mask*]

Parameter Description

Parameter	Description
process-id	OSPF process ID. All OSPF routes will be displayed without an ID specified.
count	Statistics of various OSPF routes
ip-address mask	Statistics of routes which have a specified prefix and mask.

Defaults N/A

Command Mode Privileged mode

Usage Guide This command displays the OSPF routing information. The count option displays the OSPF routing statistics.

Configuration Examples The following example displays the output of the **show ip ospf route** command.

```
OSPF process 1:
Codes: C - connected, D - Discard , O - OSPF,
IA - OSPF inter area  N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external
type 2
E1 - OSPF external type 1, E2 - OSPF external type 2
E2 100.0.0.0/24 [1/20] via 192.88.88.126, FastEthernet 0/1
C  192.88.88.0/24 [1] is directly connected,FastEthernet 0/1,Area 0.0.0.1
```

The following table describes the fields in the output of the **show ip ospf route** command.

Field	Description
codes	Route type and corresponding abbreviation and description
100.0.0.0/24	Route prefix
[1]	Route cost
via	Route next hop and interface

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

5.56 show ip ospf spf

Use this command to display the routing count in the OSPF area.

show ip ospf [*process-id*] **spf**

Parameter Description

Parameter	Description
process-id	OSPF process ID

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide This command displays the routing counts within the latest 30 minutes in the OSPF area and current routing total counts.

Configuration Examples The following example displays the output of the **show ip ospf [***process-id***] spf** command:

```
Ruijie# show ip ospf 1 spf

OSPF process 1:
Area_id     30min_counts   Total_counts
0               32             1235
1               6               356
```

The following table describes the fields in the output of the **show ip ospf [***process-id***] spf** command.

Field	Description
Area_id	OSPF area ID
30min_counts	OSPF routing counts within the latest 30 minutes
Total_counts	Total counts of the OSPF routing till now

Related Commands

Command	Description
show ip ospf	Displays the OSPF summary.

Platform N/A

Description

5.57 show ip ospf summary-address

Use this command to display the converged route of all redistributed routes.

show ip ospf [*process-id***] summary-address**

Parameter Description

Parameter	Description
process-id	ID of the OSPF process. All OSPF routing processes will be displayed if this parameter is not configured.

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide This command is valid only on the NSSA ABR, and displays only the routes with local aggregation operations.

Configuration Examples The following example displays the output of the **show ip ospf summary-address** command:

```
Ruijie# show ip ospf summary-address
OSPF Process 1, Summary-address:
172.16.0.0/16, Metric 20, Type 2, Tag 0, Match count 3, advertise
```

Field	Description
Summary Address	IP address to be aggregated
Summary Mask	Mask to be aggregated
Advertise	Whether to advertise the aggregated route
Status	Whether the aggregation range takes effect
Aggregated subnets	Number of external routes included in the aggregation range

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

5.58 show ip ospf virtual-link

Use this command to display the OSPF virtual link information.

show ip ospf [*process-id*] **virtual-link** [*ip-address*]

Parameter

Parameter	Description

Description

process-id	ID of the OSPF process. All OSPF routing processes will be displayed if this parameter is not configured.
ip-address	Associated ID of a virtual link neighbor

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide If no virtual link is configured, the command displays the neighbor status and other related information. The show ip ospf neighbor command does not display the neighbor of the virtual link.

Configuration Examples The following is the output of the **show ip ospf virtual-links** command:

```
Ruijie# show ip ospf virtual-links
Virtual Link VLINK0 to device 1.1.1.1 is up
Transit area 0.0.0.1 via interface FastEthernet 0/1
Local address 10.0.0.37/32
Remote address 10.0.0.27/32
Transmit Delay is 1 sec, State Point-To-Point,
Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
Hello due in 00:00:05
Adjacency state Full
```

The following table describes the fields in the output.

Field	Description

Virtual Link VLINK0 to router	Displays the virtual link neighbors and their status.
Virtual Link State	Displays the virtual link state.
Transit area	Displays the transit area of the virtual link.
via interface	Displays the associated interface of the virtual link.
Local address	Local interface address
Remote Address	Peer interface address
Transmit Delay	Displays the transmit delay of the virtual link.
State	Interface state
Time intervals configured	Hello, Dead, Wait, and Retransmit interval of the interface
Adjacency State	Neighbor state, where FULL means the stable state

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

5.59 summary-address

Use this command to configure the aggregate route out of the OSPF routing domain. Use the **no** form of this command to restore the remove the aggregate route.

summary-address *ip-address net-mask* [**not-advertise** | **tag** *value* | **cost** *cost*]

no summary-address *ip-address net-mask* [**not-advertise** | **tag** | **cost**]

Parameter Description

Parameter	Description
ip address	IP address of the aggregate route
net-mask	Network mask of the aggregate route
not-advertise	Does not advertise the aggregate route. If the parameter is not configured, the aggregate route is advertised.
tag *value*	Sets the tag value of an aggregate route. The range is from 0 to 4,294,967,295.
cost *cost*	Cost value of the aggregate route. The range is from 0 to 16,777,214.

Defaults No aggregate route is configured by default.

Command Mode Routing process configuration mode

Usage Guide

When routes are redistributed by another routing process into the OSPF routing process, every route is advertised to the OSPF-enabled device separately in external LSAs. If the incoming routes are continuous addresses, the autonomous border device can advertise only one aggregate route, reducing the scale of routing table greatly.

Unlike the **area range** command, the area range command aggregates inter-OSPF-area routes, while the summary-address command aggregates external routes of the OSPF routing domain.

For the NSSA, the **summary-address** command is valid only on the NSSA ABR now, and aggregates only redistributed routes.

Configuration Examples

The following example generates an external aggregate route 100.100.0.0/16.

```
Ruijie(config)# router ospf20
Ruijie(config-router)# summary-address100.100.0.0 255.255.0.0
Ruijie(config-router)# redistribute static subnets
Ruijie(config-router)# network200.2.2.0 0.0.0.255 area 1
Ruijie(config-router)# network172.16.24.0 0.0.0.255area 0
Ruijie(config-router)# area1nssa
```

Related Commands

Command	Description
area-range	Configures route convergence on the OSPF area border device.
redistribute	Redistributes routes of other routing processes.

Platform Description

N/A

5.60 timers lsa arrival

Use this command to configure the time delay for the same LSA received. Use the **no** form of this command to restore the default setting.

timers lsa arrival *arrival-time*

no timers lsa arrival

Parameter Description

Parameter	Description
arrival-time	Configures the time delay when receiving the same LSA. The range is from 0 to 600000 in the unit of milliseconds.

Defaults The default is 1000.

Command Mode Routing process configuration mode

Usage Guide No action is done when the same LSA is received within the specified time.

Configuration Examples The following example configures the time delay for the same LSA as 2seconds.

```
Ruijie(config)# routerospf1
Ruijie(config-router)# timers lsa arrival 2000
```

Related Commands

Command	Description
show ip ospf	Displays the OSPF information.

Platform Description N/A

5.61 timers pacing lsa-group

Use this command to configure the LSA grouping and then refresh the whole groups as well as the update interval for the aged link state. Use the **no** form of this command to restore the default setting.

timers pacing lsa-group *seconds*

no timers pacing lsa-group

Parameter Description

Parameter	Description
seconds	Parameter used for LSA pacing, checksum calculation, and aging interval. The range is from 10 to1800 in the unit of seconds.

Defaults The default is 30.

Command Mode Routing process configuration mode

Usage Guide Each LSA has its own update and aging time (LSA age). If you update and age LSAs separately, many CPU resources will be consumed. To effectively use CPU resources, you can update LSAs of a device in batches.

You can use this command to modify the value of seconds, whose default value is 240 seconds. This parameter needs not to be adjusted often. The optimal group pacing interval is inversely proportional to the number of LSAs that need to be calculated. For example, if you have approximately 10000 LSAs in the database, decreasing the pacing interval would be better. If the switch has a small database (40 to 100 LSAs), increasing the pacing interval to 10 to 20 minutes might be better.

Configuration Examples The following example configures the pacing time as 120 seconds.

```
Ruijie(config)# deviceospf 20
Ruijie (config-router)# timers paing lsa-group 120
```

Related Commands

Command	Description
show ip ospf	Displays the OSPF information.

Platform Description N/A

5.62 timers pacing lsa-transmit

Use this command to transmit the LSA grouping updating. Use the **no** form of this command to restore the default setting.

timers pacing lsa-transmit *transmit-time transmit-count*

no timers pacing lsa-transmit

Parameter Description

Parameter	Description
transmit-time	Configures the interval of sending the LSA grouping. The range is from 10 to 1000.
transmit-count	Configures the number of LS-UPD packets per group. The range is from 1 to 200.

Defaults The default configurations are as follows:

Transmit-time: 40 milliseconds.

Transmit-count: 1

Command Mode Routing process configuration mode

Usage Guide If there are a large number of LSAs and the load on the system is heavy, you can properly use the

transmit-time and **transmit-count** to inhibit the flooding LS-UPD packet number in the network.

If the CPU and network bandwidth loads are not too much, reduce **transimi-time** and increase **transimit-count** to quicken the environment convergence.

Configuration Examples

The following example sets the interval of sending the LS-UPD packets as 50ms, the packets number as 20.

```
Ruijie(config)# routerospf1
Ruijie(config-router)# timers pacing lsa-transmit 50 20
```

Related Commands

Command	Description
show ip ospf	Displays the OSPF process information, including the router ID.

Platform Description

N/A

5.63 timers spf

Use this command to configure the delay for SPF calculation after the OSPF receives the topology change as well as the interval between two SPF calculations. Use the **no** form of this command to restore the default setting.

timers spf *spf-delay spf-holdtime*

no timers spf

Parameter Description

Parameter	Description
spf-delay	Defines the SPF calculation waiting period in seconds. The range is from 0 to 2147483647.After receiving the topology change, the OSPF routing process must wait for the specified period to start the SPF calculation.
spf-holdtime	Defines the interval between two SPF calculations in seconds. The range is from 0 to 2147483647.When the waiting time is up but the interval between two calculations is still elapsing, the SPF calculation cannot start.

Defaults

For the RGOS not supporting the timers throttle spf command, the default values are as follows:

spf-delay: 5seconds;

spf-holdtime: 10 seconds.

For the RGOS supporting the timers throttle spf command, by default, the timers spf command takes no effect. Spf-delay depends on the default configuration of the timers throttle spf command.

Command Mode

Routing process configuration mode

Usage Guide

Smaller values of *spf-delay* and *spf-holdtime* mean that OSPF adapts to the topology change faster, and the network convergence period is shorter, but this will occupy more CPU of the router.

⚠ The configurations of the **timers spf command** and the timers throttle spf command may overwrite each other.

Configuration Examples The following example configures the delay and holdover period of the OSPF as 3 and 9 seconds respectively.

```
Ruijie(config)# deviceospf20
Ruijie(config-router)# timersspf 3 9
```

Related Commands

Command	Description
show ip ospf	Displays the configuration information of the ospf.
timers throttle spf	Configures the exponential back off delay for SPF calculation. The command is recommended to replace the timers spf command because it is more powerful.

Platform Description N/A

5.64 timers throttle lsa all

Use this command to configure the exponential back off algorithm for the LSA. Use the **no** form of this command to restore the default setting.

timers throttle lsa all *delay-time hold-time max-wait-time*

no timers throttle lsa all

Parameter Description

Parameter	Description

delay-time	Configures the time delay of generating the LSA first. The range is from 1 to 600000.
hold-time	Configures the minimum interval of refreshing the LSA between the first time and second time. The range is from1 to 600000.
max-wait-time	Configures the maximum interval of successive refreshing the LSA., which determines whether the LSA is refreshed successively. The range is from1 to 600000

Defaults The default configurations are as follows:

Delay-time: 0 millisecond,

Hold-time: 5000 milliseconds,

Max-wait-time: 5000 milliseconds.

Command Mode Routing process configuration mode

Usage Guide If high convergence performance is required for the link change, the value of delay-time can be relatively small. if you expect to reduce the CPU consumption, increase appropriately several values.

The value of hold-time cannot be smaller than that of delay-time, and the value of max-wait-time cannot be smaller than that of hold-time.

Configuration The following example configures the first delay as 10ms, hold-time as 1second and the longest delay

Examples as 5seconds.

```
Ruijie(config)# routerospf1
Ruijie(config-router)# timers throttle lsa all 10 1000 5000
```

Related Commands

Command	Description
show ip ospf	Displays the configuration information of the ospf

Platform Description N/A

5.65 timers throttle route

Use this command to configure the delay time of route calculation on receiving the ASBR summary LSA and the external summary LSA. Use the **no** form of this command to restore the default setting.

timers throttle route { **inter-area** *ia-delay* | **ase** *ase-delay* }

no timers throttle route { **inter-area** | **ase** }

Parameter Description

Parameter	Description
inter-area	Calculates the inter area routes.
ia-delay	Sets the delay time of the inter-area route calculation, in the range from 0 to 600,000 in the unit of milliseconds. On receiving the ASBR summary LSA, the router will not calculate the inter-area routes until

	the ia-delay time runs out.
ase	Calculates the external routes.
ase-delay	Defines the delay time of the external route calculation, in the range from 0 to 600,000 in the unit of milliseconds. On receiving the external summary LSA, the router will not calculate the external routes until the ase-delay time runs out.

Defaults The default values are as follows:

ia-delay: 0,

ase-delay: 0,

Command Mode Routing process configuration mode

Usage Guide The default setting is recommended if the network needs to be fast converged. For the instable network where multiple inter-area and external routes exist, if you want to optimize the route calculation and save the CPU resources, increase the delay time.

Configuration Examples The following example sets the .delay time of the inter-area route calculation to one second.

```
Ruijie(config)# router ospf 1
Ruijie(config-router)# timers throttle route inter-area 1000
```

Related Commands

Command	Description

N/A	N/A

Platform Description N/A

5.66 timers throttle spf

Use this command to configure the topology change information for OSPF, including the delay for SPF calculation as well as the interval between two SPF calculations in routing process configuration mode. Use the **no** form of this command to restore the default setting.

timers throttle spf *spf-delay spf-holdtime spf-max-waittime*

no timers throttle spf

Parameter Description

Parameter	Description
spf-delay	Defines the SPF calculation waiting period, in the unit of milliseconds, in the range from1 to 600,000. After receiving the topology change, the OSPF routing process must wait for the specified period to start the SPF calculation.
spf-holdtime	Defines the interval between two SPF calculations in seconds in the range from1 to 600,000.
spf-max-waittime	Defines the maximum interval between two SPF calculations, in milliseconds in the range from1 to 60,0000.

Defaults The default configurations are as follows:

spf-delay: 1000ms;

spf-holdtime: 5000ms;

spf-max-waittime: 10000ms.

Command Mode Routing process configuration mode

Usage Guide The spf-delay parameter indicates the delay time of the topology change to the SPF calculation. The spf-holdtime parameter indicates the minimum interval between two SPF calculations. Then, the interval of the consecutive SPF calculations is at least twice as the last interval until it reaches to spf-max-waittime. If the interval between two SPF calculations has exceeded the required value, the SPF calculation will restart from spf-holdtime.

Smaller spf-delay and spf-holdtime values can make the topology converge faster. A greater spf-max-waittime value can reduce the system resource consumption of SPF calculation. Those configurations can be flexibly adjusted according to the actual stability of the network topology.

Compared with the timers spf command, this command is more flexible. It speeds up the SPF calculation convergence, and reduces the system resource consumption of SPF calculation due to the topology change. To this end, the timers throttle spf command is recommended.

The value of spf-holdtime cannot be smaller than the value of spf-delay, or the value ofspf-holdtime will be set to be equal to the value of spf-delay;
The value of spf-max-waitime cannot be smaller than the value of spf-holdtime, or the value of spf-max-waittime will be set to be equal to the value of spf-holdtime automatically;
The configurations of the timers spf command and the timers throttle spf command may overwrite each other.
If both the timers spf command and the timers throttle spf command are not configured, the default value of the timers throttle spf command is used.

Configuration The following example configures the delay and holdtime and the maximum time interval of the OSPF

Examples as 5ms, 1000ms and 90000ms respectively. If the topology changes consecutively, the SPF calculation intervals are: 5ms, 1second, 3 seconds, 7 seconds, 15 seconds, 31 seconds, 63 seconds, 89 seconds, 179 seconds, 179+90seconds…

```
Ruijie(config)# routerospf20
Ruijie(config-router)# timersspf 5 1000 90000
```

Related Commands

Command	Description
show ip ospf	Displays the configuration information of OSPF
timers spf	Configures the SPF calculation delay. This command is supported in versions earlier than RGOS 10.4. It is recommended to replace the timers spf command with the timers throttle spf command.

Platform Description N/A

5.67 two-way-maintain

Use this command to enable the OSPF two-way-maintain function. Use the **no** form of this command to disable this function.

two-way-maintain

no two-way-maintain

Parameter Description

Parameter	Description

N/A	N/A

Defaults This function is enabled by default.

Command Mode Routing process configuration mode

Usage Guide In the large-scale network, partial packets delay or dropped may exist due to much CPU and memory are occupied caused by lots of packet transmission. If the Hello packets are handled over dead-interval, the corresponding adjacency will be disconnected. In this case, you can enable the two-way-maintain function for the packets such as DD, LSU, LSR and LSAck packets from a neighbor in the network (except for the Hello packets), avoiding the neighbor invalidation caused by delayed or dropped Hello packets.

Configuration Examples The following example disables the OSPF two-way-maintain function.

```
Ruijie(config)# routerospf1
Ruijie(config-router)# notwo-way-maintain
```

Related Commands

Command	Description
show ip ospf	Displays the configuration information of the OSPF

Platform N/A

Description

6 OSPFv3 Commands

6.1 area authentication

Use this command to configure OSPFv3 area authentication. Use the **no** form of this command to restore the default settings.

area *area-id* **authentication ipsec spi** *spi* [**md5 | sha1**] [**0 | 7**] *key*

no area *area-id* **authentication**

Parameter Description

Parameter	Description
area-id	Specifies an area ID. It can be an integer or the prefix of an IPv4 address.
spi	Specifies a security parameter index, in the range from 256 to 4294967295.
md5	Specifies a message digest 5 (MD5) authentication mode.
sha1	Specifies a secure hash algorithm 1 (SHA1) authentication mode.
0	Indicates that a key is displayed in a plain-text format.
7	Indicates that a key is displayed in a cipher-text format.
key	Specifies an authentication key.

Defaults Authentication is not performed by default.

Command Mode Routing process configuration mode

Usage Guide RGOS supports three authentication modes:

- null authentication mode, which is configured when authentication is not needed
- MD5 authentication mode
- SHA1 authentication mode

If OSPFv3 area authentication is configured, the configuration takes effect on all interfaces (except for those of virtual links) in the area. Interface authentication configuration, however, takes precedence over area authentication configuration.

Configuration Examples The following example specifies MD5 authentication for area 1 where OSPFv3 routing processes reside, and sets the authentication password to aaaaaaaaaaaaaaaaaaaaaaaaaaaaaa.

```
Ruijie(config-router)# area 1 authentication ipsec spi 300 md5
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
```

Related Commands

Command	Description
ipv6 ospf authentication	Specifies interface authentication.
area virtual-link authentication	Specifies virtual link authentication.

Platform Description N/A

6.2 area default-cost

Use this command to set the cost of the default route for the ABR in the stub or NSSA area. Use the **no** form of this command to restore the default settings.

area *area-id* **default-cost** *cost*

no area *area-id* **authentication**

Parameter Description

Parameter	Description
area-id	Area ID of the stub or NSSA area. It can be an integer or an IPv4 prefix.
cost	Cost of the default route of the stub or NSSA area in the range from 0 to 16777215.

Defaults The default cost is 1.

Command Mode Routing process configuration mode.

Usage Guide This command can only work in the ABR connected to the stub area.

Configuration Examples The following example sets the cost of the default route of stub area 50 to 100.

```
ipv6 router ospf 1
area 50 stub
area 50 default-cost 100
```

Related Commands

Command	Description
area stub	Sets a stub area.

Platform Description N/A

6.3 area encryption

Use this command to enable encryption authentication for an OSPFv3 area. Use the **no** form of this command to restore the default settings.

area *area-id* **encryption ipsec spi** *spi* **esp null** [**md5** | **sha1**] [**0 | 7**] *key*

no area *area-id* **encryption**

Parameter Description

Parameter	Description

area-id	Specifies an area ID. It can be an integer or the prefix of an IPv4 address.
spi	Specifies a security parameter index, in the range from 256 to 4294967295.
null	Specifies the null encryption mode.
md5	Specifies the MD5 authentication mode.
sha1	Specifies the SHA1 authentication mode.
0	Indicates that a key is displayed in the plain-text format.
7	Indicates that a key is displayed in the cipher-text format.
Key	Specifies an authentication key.

Defaults Encryption authentication is not performed by default.

Command Mode Routing process configuration mode

Usage Guide RGOS supports the null encryption mode and two authentication modes: MD5 and SHA1.

If encryption authentication is configured for an OSPFv3 area, the configuration takes effect on all interfaces (except for those of virtual links) in the area. Encryption authentication configuration on interfaces, however, takes precedence over that of the OSPFv3 area.

Configuration Examples The following example specifies null encryption and MD5 authentication for area 1 where OSPFv3 routing processes reside, and sets the authentication password to aaaaaaaaaaaaaaaaaaaaaaaaaaaaaa.

```
Ruijie(config-router)# area 1 encryption ipsec spi 300 esp null md5
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
```

Related Commands

Command	Description
ipv6 ospf encryption	Specifies interface encryption authentication.
area virtual-link encryption	Specifies virtual link encryption authentication.

Platform Description N/A

6.4 area-range

Use this command to set the range of the converged inter-area addresses. Use the **no** form of this command to restore the default settings.

area *area-id* **range** *ipv6-prefix*/*prefix-length* [**advertise|not-advertise**]

no area *area-id* **range** *ipv6-prefix*/*prefix-length*

Parameter Description

Parameter	Description

area-id	ID of the area in which the addresses are converged. It can be an integer or an IPv4 prefix.
ipv6-prefix/prefix-length	Range of the converged addresses.
advertise	Advertises the range of converged addresses.
not-advertise	The range of the converged addresses is not advertised. By default, the function is enabled.

Defaults No converged inter-area address range is defined by default.

Command Mode Routing process configuration mode

Usage Guide This command applies only to ABR. Use this command to converge multiple routes of an area into one route and advertise it to other areas. This command applies only to ABR. Use this command to converge multiple routes of an area into one route and advertise it to other areas. The routing information combination only takes place on the area border. The specific routing information is seen on the intra-area routers, but only one converged route can be seen on the devices in other areas. By configuring the two options of advertise and not-advertise, you can decide whether to advertise the convergence range to enable blocking and filtering. By default, the range is advertised to the outside. The option cost can be used to set the metric value of convergence routing.

A number of route convergence commands can be defined. In this way, the number of the routes in the OSPF AS is reduced. Particularly for a large network, the forwarding performance will be improved.

When a number of routes are converged, and the containment relationship exists between items, the area range converged is determined by the longest match principle.

Configuration Examples The following example converges the routes in area 1.

```
ipv6 router ospf 1
area 1 range 2001:abcd:1:2::/64
```

Related Commands

Command	Description
summary-prefix	Sets the range of the external routes to be converged.

Platform Description N/A

6.5 area stub

Use this command to create a stub area or set its attributes. Use the **no** form of this command to restore the default settings.

area *area-id* **stub** [**no-summary**]

no area *area-id* **stub** [**no-summary**]

Parameter Description

Parameter	Description
area-id	ID of the stub area.

	It can be an integer or an IPv6 prefix.
no-summary	This option applies only to the ABR in the stub area, indicating that the ABR only advertises the type 3 LSA indicating the default route to the stub area, not other type 3 LSAs.

Defaults No stub area is defined by default.

Command Mode Routing process configuration mode

Usage Guide If an area is at the end of an entire network, it can be designed as the stub area, in which all the routers must execute the area stub command. If the area is designed as the stub area, it cannot learn the AS external routing information (type 5 LSAs). In practical application, the external routing information takes a large proportion of the link state database, so the devices in the stub area can only learn very little routing information, thus reducing the system resources required for the running of the OSPFv3 protocol.

By default, a type 3 LAS advertisement indicating default routing on the ABR in the stub area is generated, then the devices in the stub area can get to the outside of the AS.

If a totally stub area needs to be configured, just select the keyword **no-summary** when executing the **area stub** command on the ABR.

Configuration Examples The following example enables the ABR in stub area 10 to advertise the default route to the stub area.

```
ipv6 router ospf 1
area 10 stub
area 10 stub no-summary
```

Related Commands

Command	Description
area default-cost	Sets the cost of the default route in the stub area.

Platform Description N/A

6.6 area virtual-link

Use this command to create a virtual link or set its parameters. Use the **no** form of this command to restore the default settings.

area *area-id* **virtual-link** *router-id* [**hello-interval** *seconds*] [**dead-interval** *seconds*] [**retransmit-interval** *seconds*] [**transmit-delay** *seconds*] [**instance** *instance-id*] [**authentication ipsec spi** *spi* [**md5** | **sha1**] [**0** | **7**] *key*] [**encryption ipsec spi** *spi* **esp null** [**md5** | **sha1**] [**0** | **7**] *key*]

no area *area-id* **virtual-link** *router-id* [**hello-interval**] [**dead-interva**l] [**retransmit-interval**] [**transmit-delay**] [**instance**] [**authentication**] [**encryption**]

Parameter Description

Parameter	Description
area-id	ID of the area in which the virtual link is located. It can be an integer or an IPv6 prefix.
Router-id	Neighbor router ID of the virtual link.
hello-interval *seconds*	Sets the interval to send the hello message on the local virtual link

	interface in the range from 1 to 65535 in the unit of seconds.
dead-interval *seconds*	Interval for the local interface of the virtual link to wait before considering that the neighbor fails. It is in the range from 1 to 65535 in the unit of seconds.
retransmit-interval *seconds*	Interval for retransmitting LSA on the local interface of the virtual link . The range is from 1 to 65535 in the unit of seconds.
transmit-delay *seconds*	Delay on the local interface of the virtual link in sending LSA. The range is from 1 to 65535 in the unit of seconds.
instnace *instance-id*	Specifies the instance corresponding to the virtual link. No virtual link can be established between different instances. Range: 0.-255
authentication ipsec spi *spi* [**md5 | sha1**] [**0 | 7**] *key*	Specifies OSPFv3 authentication. Authentication configuration on two neighboring devices must be consistent. The **service password-encryption** command enables a key to be displayed in the cipher-text format. *spi* specifies a security parameter index, in the range from 256 to 4294967295. **md5** specifies the MD5 authentication mode. **sha1** specifies the SHA1 authentication mode. 0 indicates that a key is displayed in the plain-text format. 7 indicates that a key is displayed in the cipher-text format. *key* specifies an authentication key.
encryption ipsec spi *spi* **esp null** [**md5| sha1**] [**0|7**] *key*	Specifies OSPFv3 encryption authentication. Authentication configuration on two neighboring devices must be consistent. The **service password-encryption** command

	enables a key to be displayed in the cipher-text format. *spi* specifies a security parameter index, in the range from 256 to 4294967295. **null** specifies the null encryption mode. **md5** specifies the MD5 authentication mode. **sha1** specifies the SHA1 authentication mode. 0 indicates that a key is displayed in the plain-text format. 7 indicates that a key is displayed in the cipher-text format. *key* specifies an authentication key.
authentication ipsec spi *spi* [**md5 | sha1**] [**0 | 7**] *key*	Specifies OSPFv3 authentication. Authentication configuration on two neighboring devices must be consistent. The **service password-encryption** command enables a key to be displayed in the cipher-text format. *spi* specifies a security parameter index, in the range from 256 to 4294967295. **md5** specifies the MD5 authentication mode. **sha1** specifies the SHA1 authentication mode. 0 indicates that a key is displayed in the plain-text format. 7 indicates that a key is displayed in the cipher-text format. *key* specifies an authentication key.

Defaults No virtual link is defined by default

hello-interval: 10 seconds; dead-interval: four times of the hello-interval; retransmit-interval: five seconds; transmit-interval: one second.

Authentication and encryption are not performed by default.

Command Mode Routing process configuration mode

Usage Guide In the OSPFv3 AS, all the areas must be connected with the backbone area to ensure that they can learn the routes of the whole OSPFv3 AS. If an area cannot be directly connected with the backbone area, it can connect it through a virtual link.

- The virtual link shall not be in the stub or NSSA area.
- configuration, **dead-interval** and **instance** shall be configured consistently on both sides of the virtual link neighbors, otherwise neighboring relationship cannot be set up between the virtual neighbors.

Configuration Examples The following example configures a virtual link.

```
Ruijie(config)# ipv6 router ospf 1
Ruijie(config-router)# area 1 virtual-link 192.1.1.1
```

Related Commands

Command	Description
show ipv6 ospf	Displays the OSPFv3 routing process information.
show ipv6 ospf neighbor	Displays the OSPFv3 neighbor information.
show ipv6 ospf virtual-links	Displays the OSPFv3 virtual link information.

Platform Description N/A

6.7 auto-cost

The metric of the OSPFv3 protocol is the interface-based bandwidth. Use this command to enable the bandwidth-based interface metric calculation or modify the reference bandwidth. Use the **no** form of this command to restore the default settings.

auto-cost [**reference-bandwidth** *ref-bw*]

no auto-cost [**reference-bandwidth**]

Parameter Description

Parameter	Description
reference-bandwidth *ref-bw*	Reference bandwidth in the range from 1 to 4294967 Mbps.

Defaults The interface metric is calculated based on the reference bandwidth, which is 100Mbps.

Command Mode Routing process configuration mode

Usage Guide Use **no auto-cost reference-bandwidth** to restore it to the default reference bandwidth.

You can use **ipv6 ospf cost** in the interface configuration mode to set the cost of the specified interface, and it takes precedence over the metric calculated based on the reference bandwidth.

Configuration Examples

The following example changes the reference bandwidth to 10M.

```
ipv6 router ospf 1
auto-cost reference-bandwidth 5
```

Related Commands

Command	Description
ipv6 ospf cost	Sets the cost of an interface.
show ipv6 ospf	Displays the OSPFv3 routing process information.

Platform Description

N/A

6.8 clear ipv6 ospf process

Use this command to clear and restart the OSPF process.

clear ipv6 ospf { **process** | *process-id*]

Parameter Description

Parameter	Description

process-id	OSPF process ID, in the range from 1 to 65535

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide In normal case, it is not necessary to use this command.

Use the parameter *process-id* to clear only one specific OSPFv3 instance. If no *process-id* is specified, all the OSPFv3 instances will be cleared.

Configuration Examples The following example restarts the OSPF process.

```
enble
clear ipv6 ospf process
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

6.9 default-information originate

Use this command to generate a default route to the OSPFv3 routing domain in the routing process mode. Use the **no** form of this command to restore the default settings.

default-information originate [**always**] [**metric** *metric*] [**metric-type** *type*] [**route-map** *map-name*]

no default-information originate [**always**] [**metric**] [**metric-type**] [**route-map** *map-name*]

Parameter Description

Parameter	Description
always	(Optional) It makes OSPFv3 generate the default route unconditionally, no matter whether the default route exists locally or not.
metric *metric*	(Optional) Initial metric value of the default route, in the range from 0 to 16777214
metric-type *type*	(Optional) Type of the default route. There are two type of OSPF external routes: type 1, different metrics seen on different routers; type 2, the same metric seen on different routers.
route-map *map-name*	Associated route-map name, no associated route-map by default

Defaults No default route is created;

The initial metric value is 1;

The default route type is type 2.

Command Mode	Routing process configuration mode

Usage Guide

When the **redistribute** or default-information command is executed, the OSPFv3-enabled router automatically turns into the autonomous system border router (ASBR). But the ASBR cannot generate the default route automatically or advertise it to all the routers in the OSPFv3 routing domain. The ASBR generates default routes by default. It is required to configure with the routing process configuration command **default-information originate**.

If the always parameter is used, the OSPF routing process advertises an external default route to the neighbors, no matter whether the default route in the core routing table exists or not. However, the local router does not display the default route. To make sure whether the default route is generated, execute **show ipv6 ospf database** to observe the OSPF link state database. The execution of the **show ipv6 route** command on the OSPF neighbor will display the default route.

The metric of the external default route can be defined only with the **default-information originate** command and cannot be set with the **default-metric** command.

There are two types of OSPFv3 external routes: type 1 external routes have changeable routing metrics, while type 2 external routes have constant routing metrics. For two parallel routes with the same route metric to the same destination network, type 1 takes precedence over type 2. As a result, the **show ipv6 route** command displays only the type 1 route.

This command generates a default route of Type-5 LSA, which will not be flooded to the NSSA area.

To generate a default route in the NSSA area, use the **area nssa default-information-originate** command.

The routers in the stub area cannot generate external default routes.

Configuration Examples

The following example generates a default route.

```
default-information originate always
```

Related

Command	Description

Commands

redistribute	Redistribute routes.
show ipv6 ospf	Displays the OSPFv3 routing process information.
show ipv6 ospf database	Displays the OSPFv3 link state database information.

Platform Description N/A

6.10 default-metric

Use this command to set the default metric for the routes to be redistributed. Use the **no** form of this command to restore the default settings.

default-metric *metric-value*

no default-metric

Parameter Description

Parameter	Description
metric-value	Default metric for the routes to be redistributed. Its range is from 1 to 16777214.

Defaults The default is 20.

Command Mode The default route type is type 2.

Usage Guide This command can be used together with **redistribute** to set the default metric for the routes to be redistributed. But this command does not apply to two types of routes:

- The **default route generated** with default-information originate;
- The redistributed direct route, for which 20 is always the default metric value.

Configuration Examples The following example sets the default metric for the routes to be redistributed to 10.

```
default-metric 10
```

Related Commands

Command	Description
redistribute	Redistributes the routes.
show ipv6 ospf	Displays the OSPFv3 routing process information.

Platform Description N/A

6.11 distance

Use this command to set the management distance corresponding to different types of OSPFv3

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

distance { *distance* | **ospf** { **intra-area** *distance* | **inter-area** *distance* | **external** *distance* } }

no distance [**ospf**]

Parameter Description

Parameter	Description
distance	Sets the management distance of the route, in the range from 1 to 255.
intra-area *distance*	Sets the management distance of the intra-area route, in the range from1 to 255.
inter-area *distance*	Sets the management distance of the inter-area route, in the range from 1 to 255.
external *distance*	Sets the management distance of the external route, in the range from 1 to 255.

Defaults

The default value is 110.

Management distance of the intra-area route :110,

Management distance of the inter-area route :110

Management distance of the external-area route: 110.

Command Mode

Routing process configuration mode.

Usage Guide This command is used to specify different management distances for different types of OSPFv3 routes. The management distance of the route is used for the comparison of routing priority, the smaller the management distance is, the higher the routing priority.

⚠ The priority of the route generated by different OSPFv3 processes must be compared using the management distance.

⚠ Setting the management distance as 255 indicates the routing entry is unreliable and will not for the packet forwarding.

Configuration Examples the following example sets the OSPFv3 external route management distance to 160.

```
Ruijie(config)# ipv6 router ospf 20
Ruijie(config-router)# distance ospf external 160
```

Related Commands

Command	Description
ipv6 router ospf	Enables the OSPFv3 routing process .

Platform Description N/A

6.12 distribute-list in

Use this command to filter routes that are computed based on Link State Advertisement (LSA). Use the **no** form of this command to restore the default settings.

distribute-list { *name* | **prefix-list** *prefix-list-name* } **in** [*interface-type interface-number*]

no distribute-list { *name* | **prefix-list** *prefix-list-name* } **in** [*interface-type interface-number*]

Parameter Description

Parameter	Description
name	Specifies an ACL filtering rule.
prefix-list *prefix-list-name*	Specifies a prefix list filtering rule.
interface-type interface-number	Specifies an interface on which LSA-based routes are filtered.

Defaults Routes are not filtered by default.

Command Mode Routing process configuration mode

Usage Guide Filter the routes computed based on LSA. Only the routes meeting filtering conditions can be forwarded. Route filtering does not affect the link state database and the routing tables of the neighbors. The ACL and prefix list filtering rules cannot be set at the same time. You can set only the ACL filtering rule or the prefix list filtering rule for a specific interface.

The routing filtering rules affect only forwarding of local routes but not route computation based on LSA. When route filtering is configured on an ABR, LSA can still compute routes and generate and send inter-area LSAs with prefixes to other areas. This will cause blackhole routes. To prevent the generation of blackhole routes, you can run the **area range** command with the **not-advertise** keyword.

Configuration Examples The following example filters routes that are computed based on Link State Advertisement (LSA).

```
Ruijie(config)# ipv6 prefix-list aaa seq 10 permit 2001::/64
Ruijie(config)# ipv6 router ospf 25
Ruijie(config-router)# redistribute rip metric 100
Ruijie(config-router)# distribute-list prefix-list aaa in ethernet 0/1
```

Related Commands

Command	Description
area range	Configures route aggregation in an area.

Platform Description N/A

6.13 distribute-list out

Use this command to filter routes that are re-distributed. This command has the similar function as the **redistribute** command. Use the **no** form of this command to restore the default settings.

distribute-list { *name* | **prefix-list** *prefix-list-name* } **out** [**bgp** | **connected** | **isis** [*area-tag*] | **ospf** *process-id* | **rip** | **static**]

no distribute-list { *name* | **prefix-list** *prefix-list-name* } **out** [**bgp** | **connected** | **isis** [*area-tag*] | **ospf** *process-id* | **rip** | **static**]

Parameter Description

Parameter	Description
name	Specifies the ACL filtering rule.

prefix-list *prefix-list-name*	Specifies the prefix list filtering rule.
bgp | connected | isis [*area-tag*] | **ospf** process-id | **rip** | **static**	Specifies the source from which the routes are filtered.

Defaults Routes are not filtered by default.

Command Mode Routing process configuration mode

Usage Guide The **distribute-list out** command has the similar function as the **redistribute route-map** command. It can be used to filter the routes that are re-distributed based on other protocols into an OSPFv3 area. It does not directly re-distribute routes but works with the **redistribute** command to re-distribute routes. The ACL and prefix list filtering rules cannot be configured at the same time. You can set only the ACL filtering rule or the prefix list filtering rule to filter the routes from a specific source.

Configuration Examples The following example filters static routes that are re-distributed.

```
Ruijie(config)# ipv6 router ospf 1
Ruijie(config-router)# redistribute static
Ruijie(config-router)# distribute-list prefix-list jjj out static
```

Related Commands

Command	Description
redistribute	Re-distributes routes that are carried by other routing processes.

Platform Description N/A

6.14 enable mib-binding

Use this command to bind MIB to a specific OSPFv3 process. Use the **no** form of this command to restore the default settings.

enable mib-binding

no enable mib-binding

Parameter Description

Parameter	Description
N/A	N/A

Defaults MIB is bound to an OSPFv3 process with the smallest process number by default.

Command Mode Routing process configuration mode

Usage Guide OSFPv3 MIB has no configuration information about OSFPv3 processes. You can operate only one OSFPv3 process through SNMP. OSFPv3 MIB is bound to the OSFPv3 process with the smallest process number by default. Users' operations take effect on this process.

To operate a specific OSFPv3 process through SNMP, you can bind OSFPv3 MIB to the process.

Configuration Examples The following example enables users to operate the OSPFv3 process with the process number of 100 through SNMP.

```
Ruijie(config)# ipv6 router ospf 100
Ruijie(config-router)# enable mib-binding
```

Related Commands

Command	Description
show ipv6 ospf	Displays global OSPFv3 configuration information.
enable traps	Enables the OSPFv3 trap function.

Platform Description N/A

6.15 enable traps

OSPFv3 processes support eight types of trap information, which are classified into two categories. Use this command to send specific trap information. Use the **no** form of this command to restore the default settings.

enable traps [**error** [**IfConfigError | IfRxBadPacket | VirtIfConfigError | VirtIfRxBadPacket**] | **state-change** [**IfStateChange | NbrStateChange | NssaTranslatorStatusChange | VirtIfStateChange | VirtNbrStateChange**]]

no enable traps [**error** [**IfConfigError | IfRxBadPacket | VirtIfConfigError | VirtIfRxBadPacket**] | **state-change** [**IfStateChange | NbrStateChange | NssaTranslatorStatusChange |**

VirtIfStateChange | VirtNbrStateChange]]

Parameter Description

Parameter	Description
Error	Configures all error-related trap types. This keyword can also specify the following types of error traps: **IfConfigError** — Specifies an interface parameter error; **IfRxBadPacket** — Specifies incorrect packets received by an interface; **VirtIfConfigError** — Specifies a parameter error on a virtual interface; **VirtIfRxBadPacket** — Specifies incorrect packets received by a virtual interface.
state-change	Configures all traps related to state change. This keyword can also specify the following traps related to state change: **IfStateChange** — Specifies state change of an interface; **NbrStateChange** — Specifies state change of a neighbor; **NssaTranslatorStatusChange** — Specifies status change of the NSSA translator. **VirtIfStateChange** — Specifies state change of a virtual interface; **VirtNbrStateChange** — Specifies state change of a

		virtual neighbor.

Defaults All traps are disabled by default.

Command Mode Routing process configuration mode

Usage Guide Before configuring this command, you must run the **snmp-server enable traps ospf** command; otherwise, OSPFv3 trap information cannot be sent correctly**.** This is because the function of this command is restricted by the **snmp-server** command.

You can synchronously enable the trap function of different processes even if MIB is not bound to these processes.

Configuration Examples The following example enables all traps of OSPFv3 process 100.

```
Ruijie(config)#ipv6 router ospf 100
Ruijie(config-router)# enable traps
```

Related Commands

Command	Description
show ipv6 ospf	Displays global OSPFv3 configuration information.
enable mib-binding	Binds MIB to an OSPFv3 process.
snmp-server enable traps ospf	Enables OSPFv3 to send trap information.

Platform Description N/A

6.16 graceful-restart

Use this command to enable the OSPFv3 graceful restart (GR) function and to set the GR period. Use the **no** form of this command to restore the default settings.

graceful-restart [**grace-period** *grace-period* | **inconsistent-lsa-checking**]

no graceful-restart [*graceful-period*]

Parameter Description

Parameter	Description
grace-period *grace-period*	Configures the GR period. The GR period is the longest interval that lasts from the moment when OSPFv3 fails to the moment when OSPFv3 gracefully restarts. The GR period is in the range from 1 to 1800 in the unit of seconds. The default is 120.
inconsistent-lsa-checking	Configures the topology change detection. Once the topology change is detected, the device will exit GR and finish the convergence, This function is enabled by default after GR is enabled.

Defaults This function is enabled by default.

Command Mode Routing process configuration mode

Usage Guide GR is configured based on the OSPFv3 instance. Different instances could be configured with different parameters.

Use this command to configure the GR period. The GR period is the longest interval that lasts from the moment when OSPFv3 fails to the moment that OSPFv3 gracefully restarts. In this period, the device will perform link reconstruction to restore OSPFv3. When the GR period expires, OSPFv3 exits GR and finishes regular operation.

To enable the GR function and set the GR period to the 120 seconds, use the **graceful-restart** command. To modify the GR period, use the **graceful-restart grace-period** command. Topology stability is indispensable for uninterrupted forwarding. If topology changes, OSPFv3 finishes convergence instead of continuing GR to avoid long time interruption

1) Disabling the topology change detection: If the topology cannot converge in time in the hot backup process, the long term forwarding interruption may occur.

2) Enabling the topology change detection: Forwarding interruption may occur but the interruption time is much shorter than the time it takes to disable topology detection.

It is not recommended to disable the topology change detection. In some scenario where long term forwarding interruption does not occur, disabling the topology change detection minimizes the forwarding interruption time.

The GR function is unavailable when the Fast Hello function is enabled.

Configuration Examples The following example enables GR for OSPFv3 instance 1 and sets the GR period to 60 seconds.

```
Ruijie(config)# ipv6 router ospf 1
Ruijie(config-router)# graceful-restart
Ruijie(config-router)# graceful-restart grace-period 60
```

Related

Command	Description

Commands

N/A	N/A

Platform Description N/A

6.17 graceful-restart helper

Use this command to enable the OSPFv3 graceful restart helper function. Use the **no** form of this command to disable this function.

graceful-restart helper disable

no graceful-restart helper disable

Use this command configure the topology change detection method of OSPFv3 GR helper. Use the **no** form of this command to cancel the configuration.

graceful-restart helper { **strict-lsa-checking** | **internal-lsa-checking**}

no graceful-restart helper {**strict-lsa-checking** | **internal-lsa-checking**}

Parameter Description

Parameter	Description
disable	Disables the device to assist other devices in performing GR.
strict-lsa-checking	Checks the change of the LSA of types 1-5 and 7 to judge whether the network topology changes. If the topology changes, the GR helper function will be disabled.

internal-lsa-checking	Checks the change of the LSA of types 1–3 to judge whether the network topology changes. If the topology changes, the GR helper function will be disabled.

Defaults The GR helper is enabled by default.

The device where the GR helper is enabled does not check the LSA change by default.

Command Mode Routing process configuration mode

Usage Guide Use this command to enable the GR helper function. When one neighbor device performs graceful restart, the Grace-LSA is advertised to all neighbors. If the device enabled with the GR helper receives the Grace-LSA, it will become the GR Helper to help the neighbors perform GR. The **disable** option means that it is not allowed to perform the GR helper function for any device in GR.

The GR helper does not perform the network change detection by default. The convergence is not performed again until the GR is implemented even if the network changes. Use the **strict-lsa-checking orinternal-lsa-checking** command to enable the device to detect the change of network topology during the GR. The former checks any LSA (types 1-5,7) that stands for the network information, the latter checks the LSA that stands for the AS inner-area route. In the large scale network, it is not recommended to enable the LSA check option because the partial network changes trigger the ending of the GR, decreasing the convergence speed of the entire network.

Configuration Examples The following example disables the GF helper function of the OSPFv3 instance 1 and modifies the topology change detection policy.

```
Ruijie(config)# ipv6 router ospf 1
Ruijie(config-router)# graceful-restart helper disable
Ruijie(config-router)# no graceful-restart helper disable
Ruijie(config-router)# graceful-restart helper strict-lsa-checking
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

6.18 ipv6 ospf area

Use this command to enable the interface to participate in the OSPFv3 routing process. Use the **no** form of this command to restore the default settings.

ipv6 ospf *process-id* **area** *area-id* [**instance** *instance-id*]

no ipv6 ospf *process-id* **area** [**instance** *instance-id*]

Parameter Description

Parameter	Description
process-id	OSPF process ID.
area *area-id*	OSPFv3 area in which the interface participates. It can be an integer or an IPv4 prefix.
instance *instance-id*	Configures the specific OSPFv3 instance on the interface. Range: 0-255.

Defaults This function is disabled by default.

Command Mode Interface configuration mode.

Usage Guide You can use this command to enable the OSPFv3 on an interface, and then configure the OSPFv3 process with **ipv6 router ospf**. it will be automatically started after this command is used., it will be automatically started after this command is used.

Use **no ipv6 ospf area** to disable the specified interface to participate in the OSPFv3 routing process.

Use **no ipv6 router ospf** to disable all the interfaces to participate in the OSPFv3 routing process.

The neighbor relationship can only be established between the routers with the same instance ID.

After this command is configured, all the prefix information on the interface will be used in the operation of the OSPFv3.

Configuration Examples The following example starts the OSPFv3 process on int fastethernet 0/0 for the specified area of the specified instance.

```
int fastethernet 0/0
ipv6 ospf 1 area 2 instance 2
```

Related Commands

Command	Description
ipv6 router ospf	Starts the OSPFv3 routing process.

passive-interface	Setsthe a passive interface.
show ipv6 ospf interface	Displays the OSPFv3 interface information.

Platform Description N/A

6.19 ipv6 ospf authentication

Use this command to configure OSPFv3 interface authentication. Use the **no** form of this command to restore the default settings.

ipv6 ospf authentication [**null | ipsec spi** *spi* [**md5 | sha1**] [**0 | 7**] *key*]

no ipv6 ospf authentication

Parameter Description

Parameter	Description
null	Indicates that authentication is not performed.
spi	Specifies a security parameter index, in the range from 256 to 4294967295.
md5	Specifies the MD5 authentication mode.
sha1	Specifies the SHA1 authentication mode.
0	Indicates that a key is displayed in the plain-text format.

7	Indicates that a key is displayed in the cipher-text format.
key	Specifies an authentication key.

Defaults Authentication is not performed by default.

Command Mode Interface configuration mode

Usage Guide RGOS supports three authentication modes:

- null authentication mode, which is configured when authentication is not needed
- MD5 authentication mode
- SHA1 authentication mode

OSPFv3 authentication parameters configured on interconnected interfaces must be consistent.

Configuration Examples The following example specifies MD5 authentication in OSPFv3 interface configuration mode and sets the authentication password to aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa.

```
Ruijie(config-if)# ipv6 ospf authentication ipsec spi 300 md5
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
```

Related Commands

Command	Description
ipv6 ospf authentication	Specifies interface authentication.

area virtual-link authentication	Specifies virtual link authentication.

Platform Description N/A

6.20 ipv6 ospf cost

Use this command to set the cost of the interface. Use the **no** form of this command to restore the default settings.

ipv6 ospf cost *cost* [**instance** *instance-id*]

no ipv6 ospf cost [**instance** *instance-id*]

Parameter Description

Parameter	Description
Cost	Cost of interface, in the range from 0 to 65535.
instance *instance-id*	Configures the specific OSPFv3 instance on the interface, in the range from 0 to 255.

Defaults The default interface cost is the reference bandwidth/Bandwidth (100Mbps by default).

Command Mode Interface configuration mode.

Usage Guide By default, the cost of the OSPFv3 interface is 100Mbps/Bandwidth, in which the Bandwidth is the bandwidth of the interface and configured with the command **bandwidth** in the interface configuration mode.

The default costs of OSPFv3 interfaces for several typical lines are:

- 64K serial line: 1562;
- E1 line: 48
- 10M Ethernet: 10
- 100M Ethernet: 1

The OSPFv3 cost configured with the command **ipv6 ospf cost** will overwrite the default configuration.

Configuration Examples The following example sets the cost of the interface to 1:

```
Ruijie(config)# int fastethernet 0/0
Ruijie(config-if)# ipv6 ospf cost 1
```

Related Commands

Command	Description
show ipv6 ospf interface	Displays the OSPFv3 interface information.
ipv6 ospf area	Sets the interface to participate in the OSPFv3 routing process.

Platform Description N/A

6.21 ipv6 ospf dead-interval

Use this command to set a dead interval of neighbors on an interface. If no hello packet is received from a neighbor within the interval, the neighboring relationship is considered to fail. Use the **no** form of this command to restore the default settings.

ipv6 ospf dead-interval { *seconds* | **minimal hello-multiplier** *multiplier* } [**instance** *instance-id*]

no ipv6 ospf dead-interval [**instance** *instance-id*]

Parameter Description

Parameter	Description
seconds	Dead interval of neighbors. Its range is from 1 to 65535 in the unit of seconds.
minimal hello-multiplier *multiplier*	Enables the fast hello function, which takes 1s as the dead interval of neighbors. *Multiplier* specifies the number of hello packets sent in one second, in the range from 3 to 20.
instance *instance-id*	Configures the specific OSPFv3 instance on the interface, in the range from 0 to 255.

Defaults

If the fast hello function is not enabled, the dead interval of neighbors is four times longer than the hello interval.

If the hello interval is changed, the dead interval of neighbors varies automatically.

Command Mode Interface configuration mode

Usage Guide The dead interval of neighbors must be longer than the hello interval.

The OSPFv3 fast hello function allows OSPFv3 to fast discovery neighbors and detect whether neighboring relationships are valid. To enable the OSPFv3 fast hello function, you can specify the **minimal** and **hello-multiplier** keywords and the *multiplier* parameter in this command. **minimal** specifies the deal interval of neighbors to be 1s; **hello-multiplier** specifies the number of times that hello packets are sent in a second. Therefore, this configuration reduces the hello interval to be shorter than 1s.

If an interface is enabled with the fast hello function, the **hello-interval** field of hello packets to be advertised by this interface is set to 0, and that of hello packets received from this interface is omitted**.**

dead-interval, **minimal**, and **hello-multiplier** that are introduced to enable the fast hello function cannot be configured together with **hello-interval**.

No matter whether the fast hello function is configured, the dead interval of neighbors on the interconnected interfaces of neighbors must be consistent. The values of **hello-multiplier** on the interconnected interfaces can be different but you must ensure that at least one hello packet is received within the dead interval of neighbors.

You can use the **show ipv6 ospf interface** command to monitor the dead interval of neighbors and the fast hello interval on an interface.

Configuration Examples The following example sets the dead interval of neighbors to 60 seconds on an interface.

```
ipv6 ospf dead-interval 60
```

Related

Command	Description

Commands

ipv6 ospf hello-interval	Sets the interval for sending the Hello message on an interface.
show ipv6 ospf interface	Displays the OSPFv3 interface information.
ipv6 ospf area	Sets the interface to participate in the OSPFv3 routing process

Platform Description N/A

6.22 ipv6 ospf encryption

Use this command to enable OSPFv3 encryption authentication on an interface. Use the **no** form of this command to restore the default settings.

ipv6 ospf encryption [**null | ipsec spi** *spi* **esp null** [**md5 | sha1**] [**0 | 7**] *key*]

no ipv6 ospf encryption

Parameter Description

Parameter	Description
null	Indicates that encryption authentication is not performed.
spi	Specifies a security parameter index, in the range from 256 to 4294967295.
null	Specifies the null encryption mode.

md5	Specifies the MD5 authentication mode.
sha1	Specifies the SHA1 authentication mode.
0	Indicates that a key is displayed in the plain-text format.
7	Indicates that a key is displayed in the cipher-text format.
key	Specifies an authentication key.

Defaults Encryption authentication is not performed by default.

Command Mode Interface configuration mode

Usage Guide RGOS supports the null encryption mode and two authentication modes: MD5 and SHA1.

OSPFv3 encryption authentication parameters configured on interconnected interfaces must be consistent.

Configuration Examples The following example specifies null encryption and MD5 authentication in OSPFv3 interface configuration mode and sets the authentication password to aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa.

```
Ruijie(config-if)# ipv6 ospf encryption ipsec spi 300 esp null md5
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
```

Related

Command	Description

Commands

area encryption	Specifies area encryption authentication.
area virtual-link encryption	Specifies virtual link encryption authentication.

Platform Description N/A

6.23 ipv6 ospf hello-interval

Use this command to set the interval for the interface to send the Hello message. Use the **no** form of this command to restore the default settings.

ipv6 ospf hello-interval *seconds* [**instance** *instance-id*]

no ipv6 ospf hello-interval [**instance** *instance-id*]

Parameter Description

Parameter	Description
seconds	Interval for sending the Hello message. Its range is from 1 to 65535 in the unit of seconds.
instance i*nstance-id*	Configures the specific OSPFv3 instance on the interface.

Defaults The broadcast network and point-to-point network :10 seconds. The point-to-multipoint network and NBMA network :30 seconds.

Command Mode Interface configuration mode.

Usage Guide The same hello sending intervals must be set for the neighbors, otherwise the normal adjacency cannot be established.

> The dead-interval minimal hello-multiplier and hello-interval parameters for Fast Hello cannot be configured simultaneously.

Configuration Examples The following example sets the interval for the interface to send the Hello message to 20 seconds.

```
ipv6 ospf hello-interval 20
```

Related Commands

Command	Description
ipv6 ospf dead-interval	Sets the interval for the interface to consider that the neighbor fails.
show ipv6 ospf interface	Displays the OSPFv3 interface information.
ipv6 ospf area	Sets the interface to participate in the OSPFv3 routing process.

Platform Description N/A

6.24 ipv6 ospf mtu-ignore

Use this command to ignore the MTU check when an interface receives the database description message. Use the **no** form of this command to restore the default settings.

ipv6 ospf mtu-ignore [**instance** *instance-id*]

no ipv6 ospf mtu-ignore [**instance** *instance-id*]

Parameter Description

Parameter	Description
instance *instance-id*	Configures the specific OSPFv3 instance on the interface, in the range from 0 to 255.

Defaults The MTU check is enabled by default.

Command Mode Interface configuration mode.

Usage Guide After receiving the database description message, the OSPFv3 device will check whether the MTU of neighbor interface is the same as its own MTU. If the received database description message indicates an MTU greater than its own interface's MTU, the neighbor relationship cannot be established. This can be fixed by disabling the MTU check.

Configuration The following example disables the MTU check function on the ethernet 1/0.

Examples

```
Ruijie(config)# interface ethernet 1/0
Ruijie(config-if)# ipv6 ospf mtu-ignore
```

Related Commands

Command	Description
ipv6 router ospf	Starts the OSPFv3 routing process.
ipv6 mtu	Sets the value of IPv6 MTU of the interface.

Platform Description N/A

6.25 ipv6 ospf neighbor

Use this command to configure the OSPFv3 neighbor manually. Use the **no** form of this command to restore the default settings.

ipv6 ospf neighbor *ipv6-address* [[**cost** <1-65535>] [poll-interval <0-2147483647> | priority <0-255>]] [instance *instance-id*]

no ipv6 ospf neighbor *ipv6-address* [[cost <1-65535>] [**poll-interval** < 0-2147483647 > | **priority** < 0-255 >]] [**instance** *instance-id*]

Parameter Description

Parameter	Description
cost *cost*	(Optional) Configures the cost to each neighbor in point-to-multipoint network. It is not defined by default, where the cost configured on the interface will be used. It ranges from 1 to 65535.

	Only the networks of the point-to-multipoint type support this option.
poll-interval *seconds*	(Optional) Interval for polling the neighbors (in seconds), which ranges from 1 to 2147483647. Only the networks of the non-broadcast (NBMA) type support this option.
priority *priority*	(Optional) Configures the priority value of non-broadcast network neighbors, which ranges from 0 to 255. Only the non-broadcast (NBMA) type network supports this option.
instance *instance-id*	(Optional) Configures the specific OSPFv3 instance on the interface, which ranges from 0 to 255.

Defaults No neighbor is defined;

Neighbor polling interval: 120 seconds;

Priority value of non-broadcast network neighbor: 0.

Command Mode Interface configuration mode.

Usage Guide You can set relevant parameters for the neighbors depending on the actual network type.

Configuration Examples The following example shows how to configure the OSPFv3 neighbor as follows: IPv6 address: 2001:DB8:4::1, priority value: 1, polling interval: 150 seconds.

```
Ruijie(config)# interface fastEthernet 0/1
```

```
Ruijie(config-if)# ipv6 ospf neighbor 2001:DB8:4::1 priority 1 poll-interval
150
```

Related Commands

Command	Description
Ipv6 ospf priority	Sets the priority value of an interface.
Ipv6 ospf network	Sets the network type of an interface.

Platform Description N/A

6.26 ipv6 ospf network

Use this command to set the network type of the interface. Use the **no** form of this command to restore the default settings.

ipv6 ospf network { **broadcast** | **non-broadcast** | **point-to-point** | **point-to-multipoint** [**non-broadcast**] } [**instance** *instance-id*]

no ipv6 ospf network [**broadcast** | **non-broadcast** | **point-to-point** | **point-to-multipoint** [**non-broadcast**]] [**instance** *instance-id*]

Parameter Description

Parameter	Description
broadcast	Specifies the broadcast network type.
non-broadcast	Specifies the non-broadcast network type.

point-to-point	Specifies the point-to-point network type.
point-to-multipoint	Specifies the point-to-multipoint network type.
point-to-multipoint non-broadcast	Specifies the point-to-multipoint non-broadcast network type.
instance instance-id	Configures the specific OSPFv3 instance on the interface with the valid id range from 0 to 255.

Defaults

Point-to-point network type: PPP, SLIP, frame relay point-to-point sub-interface and X.25 point-to-point sub-interface encapsulation.

NBMA network type: frame relay(except for the point-to-point sub-interface) and X.25 encapsulation (except for the point-to-point sub-interface)

Broadcast network type: Ethernet encapsulation.

The point-to-multipoint network type is not the default type.

Command Mode

Interface configuration mode.

Usage Guide

You can set the network type of the interface according to the actual link type applied and the topology.

Configuration Examples

The following example sets the network type of the interface that participates in the OSPFv3 to point-to-point.

```
ipv6 ospf network point-to-point
```

Related Commands

Command	Description
ipv6 ospf priority	Sets the interface priority.
show ipv6 ospf interface	Displays the OSPFv3 interface information.
ipv6 ospf area	Sets the interface to participate in the OSPFv3 routing process.

Platform Description N/A

6.27 ipv6 ospf priority

Use this command to set the interface priority. Use the **no** form of this command to restore the default settings.

ipv6 ospf priority *number-value* [**instance** *instance-id*]

no ipv6 ospf priority [**instance** *instance-id*]

Parameter Description

Parameter	Description
number-value	The priority of the interface. Its range is from 0 to 255.

instance *instance-id*	Configures the specific OSPFv3 instance on the interface. Its range is from 0 to 255.

Defaults The default priority is 1.

Command Mode Interface configuration mode.

Usage Guide In the broadcast network type, it is necessary to elect the DR/BDR. In electing the DR/BDR, the device of a higher priority is preferred. If several devices are of the same priority, the one with the largest router-ID is preferred.

The device with the priority level of 0 does not participate in the election of DR/BDR.

Configuration Examples The following example disables the interface from being elected as the DR/BDR.

```
ipv6 ospf priority 0
```

Related Commands

Command	Description
ipv6 ospf network	Sets the network type of an interface.
router-id	Sets the ID of a router.
show ipv6 ospf interface	Displays the OSPFv3 interface information.

instance *instance-id*	Configures the specific OSPFv3 instance on the interface.

Platform Description N/A

6.28 ipv6 ospf retransmit-interval

Use this command to set the interval for the interface to retransmit the LSA. Use the **no** form of this command to restore the default settings.

ipv6 ospf retransmit-interval *seconds* [**instance** *instance-id*]

no ipv6 ospf retransmit-interval [**instance** *instance-id*]

Parameter Description

Parameter	Description
seconds	Interval for retransmitting the LSA. Its range is from 1 to 65535 in the unit of seconds.
instance *instance-id*	Configures the specific OSPFv3 instance on the interface.

Defaults The default is five seconds.

Command Interface configuration mode.

Mode

Usage Guide To ensure the reliability of the routing information transmission, the LSA sent to the neighbor shall be acknowledged by the neighbor. You can use this command to set the interval for the acknowledgement by the neighbor. If no acknowledgement is received within the specified period, the LSA information will be retransmitted.

Configuration Examples The following example sets the interval for retransmitting the LSA to 10 seconds.

```
ipv6 ospf retransmit-interval 10
```

Related Commands

Command	Description
show ipv6 ospf interface	Displays the OSPFv3 interface information.
ipv6 ospf area	Sets the interface to participate in the OSPFv3 routing process.

Platform Description N/A

6.29 ipv6 ospf transmit-delay

Use this command to set the delay on the interface in sending the LSA. Use the **no** form of this command to restore the default settings.

ipv6 ospf transmit-delay *seconds* [**instance** *instance-id*]

no ipv6 ospf transmit-delay [**instance** *instance-id*]

Parameter Description

Parameter	Description
seconds	The delay in sending LSA. Its range is from 1 to 65535 in the unit of seconds.
instance *instance-id*	Configures the ID of a specific OSPFv3 instance on the interface, in the range from 0 to 255.

Defaults The default is one.

Command Mode Interface configuration mode.

Usage Guide Use this command to set the delay on the interface in transmitting the LSA.

Configuration Examples The following example sets the delay on the interface in transmitting the LSA.

```
ipv6 ospf transmit-delay 2
```

Related Commands

Command	Description

show ipv6 ospf interface	Displays the OSPFv3 interface information.

Platform Description N/A

6.30 ipv6 router ospf

Use this command to start the OSPFv3 routing process. Use the **no** form of this command to restore the default settings.

ipv6 router ospf

ipv6 router ospf *process-id* [**vrf** *vrf-name*]

no ipv6 router ospf *process-id*

Parameter Description

Parameter	Description
process-id	OSPFv3 process ID number. Without the process number configured, it indicates that process 1 is started.
vrf-name	Specifies the VRF that OSPFv3 process belongs to.

Defaults No OSPFv3 routing process is started.

Command Mode Global configuration mode.

Usage Guide After the OSPFv3 process is started, the routing process configuration mode is entered.

At present, our products support up to 32 OSPFv3 processes.

Configuration Examples The following example starts OSPFv3 process in the specified VRF VPN1.

```
Ruijie(config)# ipv6 router ospf 1 vrf vpn_1
```

Related Commands

Command	Description
ipv6 ospf area	Configures an interface to participate in the OSPFv3 routing process.
show ipv6 ospf	Displays the OSPFv3 routing process information.

Platform Description N/A

6.31 ipv6 router ospf max-concurrent-dd

Use this command to set the maximum concurrent interacting neighbors allowed in all OSPFv3 routing processes. Use the **no** form of this command to restore the default settings.

ipv6 router ospf max-concurrent-dd *number*

no ipv6 router ospf max-concurrent-dd

Parameter Description

Parameter	Description
number	Maximum concurrent interacting neighbors, in the range from 1 to 65535.

Defaults The default is 5.

Command Mode Global configuration mode

Usage Guide When a router is exchanging data with multiple neighbors at the same time which affects its performance, by configuring this command, the maximum concurrent interacting neighbors allowed in all OSPFv3 routing processes can be restricted.

Configuration Examples The following example sets the maximum concurrent interacting neighbors allowed in all OSPFv3 routing processes to 4. The result is that in the interaction between a large number of neighbors, interactions with up to 4 neighbors are allowed to be initiated on this device concurrently, and interactions initiated by up to 4 neighbors are allowed to be received concurrently. That is, interaction with up to 8 neighbors is allowed on this device.

```
Ruijie#conf terminal
Ruijie(config)#ipv6 router ospf max-concurrent-dd 4
```

Related Commands

Command	Description
max-concurrent-dd	Sets the maximum concurrent interacting neighbors in the OSPFv3 processes

Platform Description N/A

6.32 log-adj-changes

Use this command to enable the logging of adjacency changes. Use the **no** form of this command to restore the default settings.

log-adj-changes

no log-adj-changes

Parameter Description

Parameter	Description
detail	Displays details of adjacency changes

Defaults By default, the adjacency state log on the entry of or exit from the FULL state is output.

Command Mode Routing process configuration mode

Usage Guide N/A

Configuration Examples The following example turns on the log of adjacency state change.

```
Ruijie(config)# router ospf 1
Ruijie(config)# log-adj-changes detail
```

Related Commands

Command	Description
show ipv6 ospf	Displays the OSPF global configuration information

Platform Description N/A

6.33 max-concurrent-dd

Use this command to set the maximum number of DD packets that can be processed concurrently in the OSPFv3 routing process. Use the **no** form of this command to restore the default settings.

max-concurrent-dd *number*

no max-concurrent-dd

Parameter Description

Parameter	Description
number	Maximum number of DD packets that can be processed concurrently, in the range from 1 to 65535.

Defaults The default is 5.

Command Mode Routing process configuration mode.

Usage Guide When a router is exchanging data with multiple neighbors at the same time which affects its performance, by configuring this command, the maximum concurrent interacting neighbors allowed in each OSPFv3 instance can be restricted.

Configuration Examples The following example sets the maximum concurrent interacting neighbors allowed in the current OSPFv3 routing process to 4. The result is that in the interaction between a large number of neighbors, interactions with up to 4 neighbors are allowed to be initiated on this device concurrently, and interactions initiated by up to 4 neighbors are allowed to be received concurrently. That is, interaction with up to 8 neighbors is allowed on this device.

```
router ipv6 ospf 1
max-concurrent-dd 4
```

Related Commands

Command	Description

ipv6 router ospf max-concurrent-dd	Sets the maximum concurrent interacting neighbors allowed in the OSPFv3 processes.

Platform Description N/A

6.34 passive-interface

Use this command to set the passive interface. Use the **no** form of this command to restore the default settings.

passive-interface { **default** | *interface-type interface-number* }

no passive-interface { **default** | *interface-type interface-number* }

Parameter Description

Parameter	Description
default	Sets all the interfaces to passive ones.
interface-type interface-number	Sets the specified interface to a passive one.

Defaults No passive interface is set by default.

Command Mode Routing process configuration mode

Usage Guide After an interface is set to a passive one, it no longer receives or sends the hello message.

This command applies to the interfaces participating in the OSPFv3 but not to the virtual links.

Configuration Examples The following example enables only the VLAN1 interface to participate in the OSPFv3 process.

```
passive-interface default
no passive-interface vlan 1
```

Related Commands

Command	Description
ipv6 ospf area	Configures an interface to participate in the OSPFv3 routing process.
show ipv6 ospf	Displays the OSPFv3 routing process information.
show ipv6 ospf neighbor	Displays the OSPFv3 neighbor information.

Platform Description N/A

6.35 redistribute

Use this command to start the route redistribution in order to import the routing information of other routing protocols to the OSPFv3 routing process. Use the **no** form of this command to restore the default settings.

redistribute { **bgp** | **connected** | **isis** [*area-tag*] | **ospf** *process-id* | **rip** | **static** } [{ **level-1** | **level-1-2** | **level-2** } | **match** { **internal** | **external [1|2**] | **nssa-external** [**1 | 2**] } | **metric** *metric-value* | **metric-type** {*1|2*} | **route-map** *route-map-name* | **tag** *tag-value*]

no redistribute { **bgp** | **connected** | **isis** [*area-tag*] | **ospf** *process-id* | **rip** | **static** } [{ **level-1** | **level-1-2** | **level-2** } | **match** { **internal** | **external** [**1|2**] | **nssa-external** [**1 | 2**] } | **metric** | **metric-type** { *1|2* } | **route-map** *route-map-name* | tag *tag-value*]

Parameter Description

Parameter	Description
bgp	The bgp protocol is redistributed.
connected	The directly connected route is redistributed.
isis*[area-tag]*	The isis is redistributed. The area-tag specifies a particular isis instance.
ospf *process-id*	The ospf is redistributed. The process-id specifies a particular ospf instance within the range of 1-65535.
rip	The rip is redistributed.
static	The static route is redistributed.
level-1| **level-1-2**| **level-2**	It is used in the IS-IS route redistribution only and redistributes the routes at a specified level. .
match	It is used in the OSPFv3 route redistribution only and filters specific routes for redistribution; internal: inter-area and intra-area routes.

	external [1|2]: E1, E2 or all external routes. Nssa-external [1 | 2]: N1, N2 or all external routes of the NSSA area. All sub-type OSPFv3 routes are redistributed by default.
metric *metric-value*	Specifies the metric for the OSPFv3 external 2 LSA with metric-value. Its range is 0 to 16777214.
metric-type *{ 1|2 }*	Set the metric type for the external route to E-1 or E-2.
route-map *map-map-name*	Specifies the routing policy for route redistribution. The name of map-tag can be composed of up to 32 characters. No route-map is associated by default.
tag *tag-value*	Specifies the tag value redistributed to the OSPFv3 inner route, in the range of 0 to 4294967295.

Defaults The function is disabled by default;

Metric-type: 2;

Level-2 routes are redistributed in the ISIS redistribution

OSPFv3 routes of all sub-types are redistributed in the OSPFv3 redistribution

No route-map is associated

Command Mode Routing process configuration mode

Usage Guide

When a device supports multiple routing protocols, the coordination between these protocols becomes an important task. The device can run the protocols at the same time, so it should redistribute the protocols. This is applicable to all IP routing protocols.

The parameters level-1, level-2 or level-1-2 can be configured in the redistribution of the ISIS routes to indicate the level of the routes in the redistribution. By default, the level-2 ISIS routes are redistributed

When redistributing OSPFv3 routes, you can configure *match* to redistribute the routes of the corresponding sub-type among the redistributed OSPFv3 routes. All types of OSPFv3 routes are redistributed by default.

The *match* parameter of route-map is specific to the source of routes. The parameters *tag*, *metric* and *metric-type* of the set rule of route-map take precedence over the ones configured for the redistribute command.

The metric value of the route-map associated should be in the range of 0 to 16777214. If the metric value is not in this range, the route cannot be introduced.

The rules for the **no** form of the **redistribute** command are as follows:

If some parameters are specified in the no command, restore their default settings;

If no parameters are specified in the **no** command, delete the whole command.

For example, if the configuration is made below:

Now modify the configuration with the command no redistribute isis 112 level-2

According to the above rules, the command only restores level-2 to default and level-2 is default per se, so after the above no command is executed, the configuration remains as

redistribute isis 112 level-2

To delete the whole command, use the command below

Configuration Examples

The following example redistributes the direct route and associates route-map test :

```
ipv6 router ospf 1
redistribute connect metric 10 route-map test
```

The associated route-map is configured as follows:

```
route-map test permit 10
match metric 20
set metric 30
```

The effect of the above configuration is to set the metric value which is 20 of the redistributed routes to 30, and that of other routes to 10

Related Commands

Command	Description
default-information originate	Sets the default route to be redistributed.
default-metric	Sets the default metric for the route to be redistributed.
summary-prefix	Sets the converged address range of the external route.
show ipv6 ospf	Displays the OSPFv3 routing process information.
show ipv6 ospf database	Displays the OSPFv3 link state database information.

Platform Description N/A

6.36 router-id

Use this command to set the router ID (device ID). Use the **no** form of this command to restore the default settings.

router-id *router-id*

no router-id

Parameter Description

Parameter	Description
router-id	ID of the device in the IPv4 address format.

Defaults The OSPFv3 routing process, the largest IPv4 address of all loopback interfaces is elected as the router ID; If there is no loopback interface with an IPv4 address, the OSPFv3 process will elect the largest IPv4 of all other interfaces as the router ID

Command Mode Routing process configuration mode

Usage Guide Each device that runs the OSPFv3 process shall be identified with a router ID. Router ID is in the format of IPv4 address.

Any IPv4 address can be set as the router ID, but the router ID of every routers in the AS must be unique. If multiple OSPFv3 processes are running on the same device, the router ID of every process must be unique. Note that the change of the router ID results in considerable processing work in the protocol. Therefore, it is not recommended to change any router ID without proper reason. A prompt will be given to ask whether you are sure to modify the router ID. It is recommended that you specify a router ID once an OSPFv3 process starts before configuring other parameters for the process

Configuration The following example sets the ID of the device that participates in the OSPFv3 process to 1.1.1.1.

Examples

```
router-id 1.1.1.1
```

Related Commands

Command	Description
ipv6 ospf priority	Sets the interface priority.
show ipv6 ospf	Displays the OSPFv3 routing process information.

Platform Description N/A

6.37 summary-prefix

Use this command to configure the converged route outside the OSPFv3 routing domain in the routing process configuration mode. Use the **no** form of this command to restore the default settings.

summary-prefix *ipv6-prefix*/*prefix-length* [**not-advertise** | **tag** < *0-4294967295* >]

no summary-prefix *ipv6-prefix*/*prefix-length* [**not-advertise** | **tag** < *0-4294967295* >]

Parameter Description

Parameter	Description
ipv6-prefix/*prefix-length*	Address range of the converged route
not-advertise	Does not advertise the converged route to neighbors. Absence of this parameter means to advertise.

tag<*0-4294967295*>	Tag value redistributed to the OSPFv3 inner route, in the range from 0 to 4294967295.

Defaults No converged route is configured by default.

Command Mode Routing process configuration mode.

Usage Guide When routes are redistributed by another routing process into the OSPFv3 routing process, every route is advertised to the OSPFv3-enabled device separately in the form of external link state. If the incoming routes are continuous addresses, the autonomous system border device can advertise only one converged route, thus reducing the scale of routing table greatly.

It is different from the **area range** command. The area range involves the convergence of routes between OSPFv3 areas, while the **summary-prefix** involves the convergence of external routes of the OSPFv3 routing domain.

Configuring the **summary-prefix** command on the ASBR can perform convergence for only redistributed routes; while configuring this command on the NSSA ABR translator can perform convergence for the redistributed routes and the Type-5 routes translated from Type-7.

Configuration Examples The following example configures the external route within the 2001:DB8::/64 to the converged route 2001:DB8::/64 to advertise it.

```
summary-prefix 2001 :DB8 : : /64
```

Related Commands

Command	Description

area-range	Configures route convergence between the OSPFv3 areas.
redistribute	Redistributes the routes in other routing process.

Platform Description N/A

6.38 show ipv6 ospf

Use this command to display the information of the OSPFv3 process.

show ipv6 ospf [*process-id*]

Parameter Description

Parameter	Description
process- id	OSPF process ID number.

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide N/A

Configuration Examples The following example displays the information about the OSPFv3 process.

```
Ruijie# show ipv6 ospf
Routing Process "OSPFv3 (1)" with ID 1.1.1.1
Process uptime is 24 minutes
Enable two-way-maintain
SPF schedule delay 5 secs, Hold time between SPFs 10 secs
Initial LSA throttle delay 0 msecs
Minimum hold time for LSA throttle 5000 msecs
Maximum wait time for LSA throttle 5000 msecs
Lsa Transmit Pacing timer 40 msecs, 1 LS-Upd
LSA interval 5 secs, Minimum LSA arrival 1000 msecs
Pacing lsa-group: 30 secs
Number of incomming current DD exchange neighbors 0/5
Number of outgoing current DD exchange neighbors 0/5
Number of external LSA 0. Checksum Sum 0x0000
Number of AS-Scoped Unknown LSA 0
Number of LSA originated 11
Number of LSA received 4
Log Neighbor Adjency Changes : Enabled
Number of areas in this router is 2
Area BACKBONE(0)
Number of interfaces in this area is 1(1)
SPF algorithm executed 4 times
Number of LSA 3.  Checksum Sum 0x1DDF1
Number of Unknown LSA 0
 Area 0.0.0.1 (NSSA)
     Number of interfaces in this area is 1(1)
     SPF algorithm executed 5 times
     Number of LSA 7.  Checksum Sum 0x445FE
     Number of Unknown LSA 0
```

Related Commands

Command	Description

ipv6 router ospf	Starts the OSPFv3 routing process.
default-information originate	Sets the default route to be redistributed.
default-metric	Sets the default metric for the route to be redistributed.
router-id	Sets the OSPFv3 routing process ID
timers spf	Sets the delay and the minimum and maximum intervals for the OSPFv3 to perform SPF calculation after receiving the topology change information.

Platform Description N/A

6.39 show ipv6 ospf database

Use this command to display the database information of the OSPFv3 process

show ipv6 ospf [*process- id*] **database** [**lsa-type** [**adv-router** *router-id*]]

Parameter Description

Parameter	Description
process- id	OSPF process ID number
lsa-type	The LSA types are as follows: NSSA-external-LSA, AS-external-LSAs, Link-LSAs,

	Inter-Area-Prefix-LSAs, Inter-Area-Router-LSAs, Intra-Area-Prefix-LSAs, Network-LSAs, Router-LSAs If this parameter is not specified, all LSA information will be displayed.
adv-router *router-id*	Displays the LSA information generated by the specified router.

Defaults N/A

Command Mode Privileged EXEC mode.

Usage Guide N/A

Configuration Examples The following example displays the information about the OSPFv3 process database.

```
Ruijie# show ipv6 ospf database
OSPFv3 Router with ID (1.1.1.1) (Process 1)
Link-LSA (Interface FastEthernet 1/0)
Link State ID   ADV Router     Age  Seq#      CkSum  Prefix
0.0.0.2        1.1.1.1         197 0x80000001 0x7cd8     0
0.0.0.5        2.2.2.2         206 0x80000001 0x8c86     0
              Link-LSA (Interface Loopback 1)
Link State ID   ADV Router     Age  Seq#      CkSum  Prefix
0.0.64.1       1.1.1.1          82 0x80000001 0xb760     0
              Router-LSA (Area 0.0.0.0)
Link State ID   ADV Router     Age  Seq#      CkSum   Link
0.0.0.0        1.1.1.1      17 0x80000006 0x62a1     1
0.0.0.0        2.2.2.2         156 0x80000003 0x8653     1
              Network-LSA (Area 0.0.0.0)
Link State ID   ADV Router     Age  Seq#      CkSum
```

```
0.0.0.5        2.2.2.2         157 0x80000001 0xf8f6
              Router-LSA (Area 0.0.0.1)
Link State ID   ADV Router     Age  Seq#      CkSum   Link
0.0.0.0        1.1.1.1          17 0x80000002 0x0529     0
              Inter-Area-Prefix-LSA (Area 0.0.0.1)
Link State ID   ADV Router     Age  Seq#      CkSum
0.0.0.1        1.1.1.1          77 0x80000002 0x83b4
AS-external-LSA
Link State ID   ADV Router     Age  Seq#      CkSum
0.0.0.1        1.1.1.1          1 0x80000001 0x6035 E2
```

Related Commands

Command	Description
ipv6 router ospf	Starts the OSPFv3 routing process.

Platform Description N/A

6.40 show ipv6 ospf interface

Use this command to display the OSPFv3 interface information.

show ipv6 ospf [*process- id*] **interface** [*interface-type interface-number* | **brief**]

Parameter Description

Parameter	Description
interface-type interface-number	Specifies the interface type and interface number.

process- id	OSPFv3 process ID
brief	Displays the interface summary.

Defaults N/A

Command Mode Privileged EXEC mode.

Usage Guide N/A

Configuration Examples The following example displays the information about the OSPFv3 interface.

```
Ruijie# show ipv6 ospf interface
FastEthernet 1/0 is up, line protocol is up
Interface ID 2
IPv6 Prefixes
fe80::2d0:22ff:fe22:2223/64 (Link-Local Address)
OSPFv3 Process (1), Area 0.0.0.0, Instance ID 0
Router ID 1.1.1.1, Network Type BROADCAST, Cost: 1
Transmit Delay is 1 sec, State BDR, Priority 1
Designated Router (ID) 2.2.2.2
Interface Address fe80::c800:eff:fe84:1c
Backup Designated Router (ID) 1.1.1.1
Interface Address fe80::2d0:22ff:fe22:2223
Timer interval configured, Hello 10, Dead 40, Wait 40, Retransmit 5
Hello due in 00:00:02
Neighbor Count is 1, Adjacent neighbor count is 1
Hello received 26 sent 26, DD received 5 sent 4
LS-Req received 1 sent 1, LS-Upd received 3 sent 6
LS-Ack received 6 sent 2, Discarded 0
```

If the BFD has been enabled for the neighbor on the interface, the content of “BFD enabled” is also displayed. For example:

```
Ruijie# show ipv6 ospf interface
FastEthernet 1/0 is up, line protocol is up
Interface ID 2
IPv6 Prefixes
fe80::2d0:22ff:fe22:2223/64 (Link-Local Address)
OSPFv3 Process (1), Area 0.0.0.0, Instance ID 0
Router ID 1.1.1.1, Network Type BROADCAST, Cost: 1
Transmit Delay is 1 sec, State BDR, Priority 1, BFD enabled
Designated Router (ID) 2.2.2.2
Interface Address fe80::c800:eff:fe84:1c
Backup Designated Router (ID) 1.1.1.1
Interface Address fe80::2d0:22ff:fe22:2223
Timer interval configured, Hello 10, Dead 40, Wait 40, Retransmit 5
Hello due in 00:00:02
Neighbor Count is 1, Adjacent neighbor count is 1
Hello received 26 sent 26, DD received 5 sent 4
LS-Req received 1 sent 1, LS-Upd received 3 sent 6
LS-Ack received 6 sent 2, Discarded 0
```

Related Commands

Command	Description
ipv6 router ospf	Starts the OSPFv3 routing process.
ipv6 ospf area	Enables the interface to participate in the OSPFv3 process.

Platform Description N/A

6.41 show ipv6 ospf neighbor

Use this command to display the neighbor information of the OSPFv3 process.

show ipv6 ospf [*process- id*] **neighbor** [**interface-type** *interface-number* [**detail**]| *neighbor-id* |**detail**]

Parameter Description

Parameter	Description
process- id	OSPFv3 process ID number
detail	Displays details about the neighbor.
interface-type interface-number	Interface type and interface number
neighbor-id	Neighbor’s router ID

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide N/A

Configuration Examples The following command displays the brief information about the OSPFv3 neighbor.

```
Ruijie# show ipv6 ospf neighbor
OSPFv3 Process (1) , 1 Neighbors, 1 is Full:
Neighbor ID  Pri  State    Dead Time   Interface        Instance ID
2.2.2.2      1    Full/DR  00:00:33    FastEthernet 1/0  0
Ruijie# show ipv6 ospf neighbor detail
Neighbor 2.2.2.2, interface address fe80::c800:eff:fe84:1c
In the area 0.0.0.0 via interface FastEthernet 1/0
Neighbor priority is 1, State is Full, 6 state changes
DR is 2.2.2.2 BDR is 1.1.1.1
Options is 0x000013 (-|R|-|-|E|V6)
Dead timer due in 00:00:36
Database Summary List 0
Link State Request List 0
Link State Retransmission List 0
BFD session state up
```

Related Commands

Command	Description
ipv6 router ospf	Starts the OSPFv3 routing process.
ipv6 ospf area	Enables the interface to participate in the OSPFv3 process.
area virtual-link	Configures the OSPFv3 virtual link.
show ipv6 ospf interface	Displays the OSPFv3 interface information.

Platform Description N/A

6.42 show ipv6 ospf restart

Use this command to display the OSPFv3 graceful restart configuration.

show ipv6 ospf [*process- id*] **restart**

Parameter Description

Parameter	Description
process- id	OSPFv3 process ID number.

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide N/A

Configuration Examples The following example displays the restarter status.

```
Ruijie# show ipv6 ospf restart
Routing Process is ospf 1
Graceful-restart enabled
Restart grace period 120 secs
Current Restart status is plannedRestart
Current Restart remaining time 50 secs
Graceful-restart helper support enabled
```

The following example displays the helper status.

```
Ruijie# show ipv6 ospf restart
Routing Process is ospf 1
Neighbor 10.1.1.2, interface addr 10.1.1.2
In the area 0.0.0.0 via interface GigabitEthernet 6/0/0
Graceful-restart helper enabled
Current helper status is helping
Current helper remaining time 50 secs
```

Related Commands

Command	Description
ipv6 router ospf	Starts the OSPFv3 routing process.

Platform Description N/A

6.43 show ipv6 ospf route

Use this command to display the OSPFv3 route information.

show ipv6 ospf [*process- id*] **route** [**count**]

Parameter Description

Parameter	Description
process- id	OSPFv3 process ID number.
count	Total number of OSPFv3 routes

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide N/A

Configuration Examples The following example displays the information about OSPFv3 routes.

```
Ruijie# show ipv6 ospf route
OSPFv3 Process (1)
Codes: C - connected, D - Discard, O - OSPF, IA - OSPF inter area
      N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
      E1 - OSPF external type 1, E2 - OSPF external type 2Destination
Metric   Next-hop
E2 2001:DB8:1::/64   1/20    via fe80::c800:eff:fe84:1c, FastEthernet 1/0
O  2001:DB8:2::/64   11      via fe80::c800:eff:fe84:1c, FastEthernet 1/0,
Area 0.0.0.0
```

Related Commands

Command	Description
ipv6 router ospf	Starts the OSPFv3 routing process.

Platform Description N/A

6.44 show ipv6 ospf summary-prefix

Use this command to display the external route convergence information of OSPFv3

show ipv6 ospf [*process- id*] **summary-prefix**

Parameter Description

Parameter	Description
process- id	OSPFv3 process ID number

Defaults N/A

Command Mode Privileged EXEC mode.

Usage Guide N/A

Configuration Examples The following example displays the external route convergence information of OSPFv3.

```
Ruijie# show ipv6 ospf summary-prefix
OSPFv3 Process 1, Summary-prefix:
2001:db8::/64,Metric 16777215,Type0,Tag0,Match count0,advertise
```

Related Commands

Command	Description
ipv6 router ospf	Starts the OSPFv3 routing process.
summary-prefix	Configures the converge route outside the OSPFv3 routing domain.

Platform Description N/A

6.45 show ipv6 ospf topology

Use this command to display the topology information about each area of OSPFv3.

show ipv6 ospf [*process- id*] **topology** [**area** *area-id*]

Parameter Description

Parameter	Description
process- id	OSPFv3 process ID number
area-id	Area ID

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide N/A

Configuration Examples The following command displays the topology information about each area of OSPFv3.

```
Ruijie# show ipv6 ospf topology
OSPFv3 Process (1)
OSPFv3 paths to Area (0.0.0.0) routers
Router ID       Bits  Metric    Next-Hop
Interface
1.1.1.1          EB  --
2.2.2.2          E   1         2.2.2.2
FastEthernet 1/0

OSPFv3 paths to Area (0.0.0.1) routers
Router ID       Bits  Metric    Next-Hop
Interface
1.1.1.1          B   --
```

Related Commands

Command	Description
ipv6 router ospf	Starts the OSPFv3 routing process.
area range	Configures the address range of the OSPF area.

Platform Description N/A

6.46 show ipv6 ospf virtual-links

Use this command to display the virtual link information of the OSPFv3 process

show ipv6 ospf [*process- id*] **virtual-links**

Parameter Description

Parameter	Description
process- id	OSPFv3 process ID number

Defaults N/A

Command Mode Privileged EXEC mode.

Usage Guide N/A

Configuration Examples The following command displays the information about the OSPFv3 virtual link.

```
Ruijie# show ipv6 ospf virtual-links
Virtual Link VLINK1 to router 2.2.2.2 is down
  Transit area 0.0.0.1 via interface FastEthernet 1/0, instance ID 0
  Local address *
  Remote address 3333::1/128
  Transmit Delay is 1 sec, State Down,
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
```

```
Hello due in inactive
Adjacency state Down
```

Related Commands

Command	Description
ipv6 router ospf	Starts the OSPFv3 routing process.
area virtual-link	Configures the OSPFv3 virtual link.
show ipv6 ospf neighbor	Displays the OSPFv3 neighbor information.

Platform Description N/A

6.47 timers lsa arrival

Use this command to configure a delay for receiving repeated LSAs. Use the **no** form of this command to restore the default settings.

timers lsa arrival *arrival-time*

no timers lsa arrival

Parameter Description

Parameter	Description
arrival-time	Specifies the delay for receiving repeated LSAs. The range is from 0 to 600000 in the unit of milliseconds.

Defaults The default is 1000.

Command Mode Routing process configuration mode

Usage Guide Configure the device not to process repeated LSAs received within the specific delay.

Configuration Examples The following example sets the delay for receiving repeated LSAs to 2 seconds.

```
Ruijie(config)# ipv6 router ospf 1
Ruijie(config-router)# timers lsa arrival 2000
```

Related Commands

Command	Description
show ipv6 ospf	Displays OSPFv3 process information, including identifiers of routing devices.

Platform Description N/A

6.48 timers pacing lsa-group

Use this command to set an LSA group pace interval. Use the **no** form of this command to restore the

default settings.

timers pacing lsa-group *seconds*

no timers pacing lsa-group

Parameter Description

Parameter	Description
seconds	Specifies the LSA group pace interval. The range is from 10 to 1800 in the unit of seconds. The default value is 30.

Defaults The default is 30.

Command Mode Routing process configuration mode

Usage Guide Each LSA has its own lifetime, that is, LSA aging time. An LSA existing for 1800s will be refreshed so that the living time of the LSA will not exceed its aging time. This ensures that normal LSAs are not cleared due to timeout of aging time. If update and aging operations of each LSA are separately computed, a large number of CPU resources will be consumed.

To effectively utilize CPU resources, configure the device to group LSAs for uniform refreshment. The time for refreshing a group of LSAs is called an LSA group pace interval. Grouping refreshment is to put the LSAs to be refreshed within an LSA group pace interval into a group and refresh them uniformly.

When the number of LSAs is fixed, a longer LSA group pace interval will allow the CPU to process more LSAs when the timer expires for one time. To keep the stability of the CPU, you are recommended not to set an over long LSA group pace interval. This prevents the CPU from processing excessive LSAs when the timer expires each time. If the CPU processes a large number

of LSAs each time, it is recommended to shorten the LSA group pace interval. For example, if the database has 10000 LSAs, you need to reduce the LSA group pace interval. If it has only 40 to 100 LSAs, you can adjust the group pace interval to 10 through 20 minutes.

Configuration Examples The following example sets the LSA group pace interval to 120 seconds.

```
Ruijie(config)# ipv6 router ospf 1
Ruijie(config-router)#timers pacing lsa-group 120
```

Related Commands

Command	Description
show ipv6 ospf	Displays OSPFv3 configuration information.

Platform Description N/A

6.49 timers pacing lsa-transmit

Use this command to set an interval for sending LSA groups. Use the **no** form of this command to restore the default settings.

timers pacing lsa-transmit *transmit-time transmit-count*

no timers pacing lsa-transmit

Parameter Description

Parameter	Description

transmit-time	Specifies the interval for sending LSA groups. The range is from 10 to 1000 in the unit of milliseconds.
transmit-count	Specifies the number of LS-UPD packets in an LSA group. The range is from 1 to 200.

Defaults The default transmit-time is 40 and the transmit-count is 1.

Command Mode Routing process configuration mode

Usage Guide There are usually a lot of LSAs on a network; therefore, the load of the device is very high. Setting proper **transimit-time** and **transimit-count** values can restrict flooding of LS-UPD packets on the network.

When the CPU load is not high and network bandwidth usage is not large, you can reduce the **transimit-time** value and increase the **transimit-count** value to accelerate route convergence.

Configuration Examples The following example sets the interval for sending LS-UPDs to 50 milliseconds and the specified 20 packets to be sent each time.

```
Ruijie(config)# ipv6 router ospf 1
Ruijie(config-router)# timers pacing lsa-transmit 50 20
```

Related Commands

Command	Description
show ipv6 ospf	Displays OSPFv3 process information.

Platform Description N/A

6.50 timers spf

Use this command to set the delay and interval for the OSPFv3 to calculate SPF after receiving the topology change. Use the **no** format of this command to restore the default settings.

timers spf *delay holdtime*

no timers spf

Parameter Description

Parameter	Description
spf-delay	Defines the waiting time for the SPF calculation, which ranges from 0 to 2147483647 seconds. After receiving the topology change information, the OSPF routing process has to waiting for a given period before making the SPF calculation.
spf-holdtime	Defines the interval between two SPF calculations, which ranges from 0 to 2147483647 seconds. If the interval has not passed even if the waiting time has elapsed, no SPF calculation can be made yet.

Defaults There are two default situations: 1. The versions earlier than RGOS 10.4 do not support the command **timers throttle spf**. The system default is timers spf 5 10. 2. The RGOS 10.4 and the later versions do support the command **timers throttle spf**, where **timer spf** takes no effect by default. The delay for SPF calculation is subject to the default settings of the command **timers throttle spf**. Refer to the description of the command.

Command Mode Routing process configuration mode

Usage Guide The smaller the *spf-delay* and *spf-holdtime*, the shorter time the OSPF takes to adapt to the topology change, but the more CPU time will be used of the router.

The **timer spf** configuration and the **timers throttle spf** configuration will overwrite each other.

Configuration Examples The following example sets the delay and holdtime of the OSPFv3 to 3 seconds and 9 seconds respectively.

```
Ruijie(config)# ipv6 router ospf 20
Ruijie(config-router)# timers spf 3 9
```

Related Commands

Command	Description
clear ipv6 ospf	Restarts part of the function of the OSPFv3.
show ipv6 ospf	Displays the OSPFv3 routing process information.
timers throttle spf	Configures the exponential backoff delay of the SPF calculation

Platform Description N/A

6.51 timers throttle lsa all

Use this command to configure an exponential backoff algorithm for generating LSAs. Use the **no** form of this command to restore the default settings.

timers throttle lsa all *delay-time hold-time max-wait-time*

no timers throttle lsa all

Parameter Description

Parameter	Description
delay-time	Specifies a shortest LSA generation delay, in milliseconds (the first batch of LSAs is usually generated immediately). The range is from 0 to 600000 in the unit of milliseconds.
hold-time	Specifies a shortest interval between the first two times of LSA refreshment, in milliseconds. The range is from 1 to 600000 in the unit of milliseconds
max-wait-time	Specifies a longest interval for consecutive two times of LSA refreshment, in milliseconds. The value is used to determine whether LSAs are refreshed consecutively. The range is from 1 to 600000 in the unit of milliseconds.

Defaults The default *delay-time* is 0, *hold-time* is 5000 and *max-wait-time* is 5000.

Command Routing process configuration mode

Mode

Usage Guide If high route convergence capability is needed when links are changed, set a small *delay-time* value.

To reduce CPU consumption, you can properly increase the values of the parameters.

The *hold-time* value cannot be smaller than the *delay-time* value and must be smaller than or equal to the *max-wait-time* value.

Configuration Examples The following example sets *delay-time* to 10 milliseconds, *hold-time* to one second, and *max-wait-time* to five seconds.

```
Ruijie(config)# ipv6 router ospf 1
Ruijie(config-router)# timers throttle lsa all 10 1000 5000
```

Related Commands

Command	Description
show ipv6 ospf	Displays OSPFv3 process information.

Platform Description N/A

6.52 timers throttle route

Use this command to configure the delay time of route calculation on receiving the ASBR summary LSA and the external summary LSA. Use the **no** form of this command to restore the default settings.

timers throttle route { **inter-area** *ia-delay* | **ase** *ase-delay* }

no timers throttle route { **inter-area** | **ase** }

Parameter Description

Parameter	Description
inter-area	Calculates the inter area routes.
ia-delay	Sets the delay time of the inter-area route calculation, in the range from 0 to 600000 in the unit of milliseconds. On receiving the ASBR summary LSA, the router will not calculate the inter-area routes until the ia-delay time runs out.
ase	Calculates the external routes.
ase-delay	Sets the delay time of the external route calculation, in the range from 0 to 600000 in the unit of milliseconds. On receiving the external summary LSA, the router will not calculate the external routes until the ase-delay time runs out.

Defaults The default *ia-delay* is 0 and *ase-delay* is 0.

Command Mode Routing process configuration mode

Usage Guide The default settings are recommended if the network needs to be fast converged. For the instable network where multiple inter-area and external routes exist, if you want to optimize the route calculation and save the CPU resources, increase the delay time.

Configuration Examples The following example sets the delay time of the inter-area route calculation to one second.

```
Ruijie(config)# ipv6 router ospf 1
Ruijie(config-router)# timers throttle route inter-area 1000
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

6.53 timers throttle spf

Use this command to configure, the delay for SPF calculation as well as the minimum and maximum intervals between two SPF calculations after receiving the topology change information for OSPFv3 in the routing process configuration mode. Use the **no** form of this command to restore the default settings.

timers throttle spf *spf-delay spf-holdtime spf-max-waittime*

no timers throttle spf

Parameter Description

Parameter	Description
spf-delay	Specifies an SPF calculation delay after the topology change

	information is received. The range is from 1 to 600000 in the unit of milliseconds.
spf-holdtime	Specifies a shortest interval between two SPF calculations. The range is from 1 to 600000 in the unit of milliseconds.
spf-max-waittime	Specifies a longest interval between two SPF calculations. The range is from 1 to 600000 in the unit of milliseconds.

Defaults The default *spf-delay* is 1000. *spf-holdtime* is 5000 and *spf-max-waittime* is 10000.

Command Mode Routing process configuration mode.

Usage Guide *Spf-delay* refers to the delay from the topology change to the SPF calculation. *Spf-holdtime* refers to the minimum interval between the first and the second SPF calculations. Then, the interval of the consecutive SPF calculations is at least twice as the last interval till it reaches to *spf-max-waittime*. If the interval between two SPF calculations has exceeded the required minimum value, the interval of SPF calculation will re-start from *spf-holdtime*.

Smaller *spf-delay* and *spf-holdtime* value can make the topology convergence faster. Greater *spf-max-waittime* value can reduce the SPF calculations. Those configuration are flexible according to the actual stability of the network topology.

Compared with the timers spf command, this command is more flexible. It not only speeds up the SPF convergence calculation, but also reduces the system resources consumption of SPF calculation as the topology changes continuously. Therefore, the timers throttle spf command is recommended.

- The spf-holdtime cannot be smaller than spf-delay, or the spf-holdtime will be set to be equal to spf-delay;
- The spf-max-waitime cannot be smaller than spf-holdtime, or the spf-max-waittime will be set

to be equal to spf-holdtime automatically;

The configuration of the timers spf command and of the timers throttle spf command are overwritten each other.

With neither timers spf command nor timers throttle spf command configured, the default value refers to the default of the timers throttle spf command

Configuration Examples

The following example configures the delay and holdtime and the maximum time interval of the OSPFv3 as 5ms, 1000ms and 90000ms respectively. If the topology changes consecutively, the time for SPF calculation is: five milliseconds, one second, three seconds, seven seconds, 15 seconds, 31 seconds, 63 seconds, 89 seconds, 179 seconds, 179+90 seconds……

```
Ruijie(config)# ipv6 router ospf 20
Ruijie(config-router)# timers spf 5 1000 90000
```

Related Commands

Command	Description
clear ipv6 ospf	Restarts part of the OSPFv3 function.
show ipv6 ospf	Displays the routing process information of the OSFPv3
timers spf	Configures the SPF calculation delay .

Platform Description

N/A

6.54 two-way-maintain

Use this command to enable two-way OSPFv3 maintenance. Use the **no** form of this command to disable this function.

two-way-maintain

no two-way-maintain

Parameter Description

Parameter	Description
N/A	N/A

Defaults Two-way OSPFv3 maintenance is enabled by default.

Command Mode Routing process configuration mode

Usage Guide Sometimes, there are a lot of sent and received packets on a network, occupying large CPU and memory resources. As a result, some packets cannot be processed immediately or are directly lost. If hello packets from a neighbor cannot be processed within the dead interval of neighbors, the connection with the neighbor will be interrupted due to connection timeout. If two-way OSPFv3 maintenance is enabled and a large number of packets exist on the network, besides hello packets, the two-way neighboring relationship between the device and the neighbor can also be maintained by DD, LSU, LSR, and LSAck packets from the neighbor. This prevents the neighboring relationship from failing due to receiving delay or discarding of hello packets.

Configuration Examples The following example disables two-way OSPFv3 maintenance.

```
Ruijie(config)# ipv6 router ospf 1
Ruijie(config-router)# no two-way-maintain
```

Related Commands

Command	Description
show ipv6 ospf	Displays global OSPFv3 configuration information.

Platform Description N/A

7 NSM Commands

7.1 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

7.2 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.

7.3 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*.

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 Commands

7.4 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

7.5 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

7.6 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

7.7 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

7.8 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

7.9 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. The actual range varies from products.

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.

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
```

7.10 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.

The following example displays the configuration of the IP routing table.

```
Ruijie# show ip route

Codes:  C - Connected, L - Local, S - Static
       R - RIP, O - OSPF, B - BGP, I - IS-IS, V - Overflow route
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       SU - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       IA - Inter area, * - candidate default
Gateway of last resort is no set
S    20.0.0.0/8 is directly connected, VLAN 1
S    22.0.0.0/8 [1/0] via 20.0.0.1
O E2 30.0.0.0/8 [110/20] via 192.1.1.1, 00:00:06, VLAN 1
R    40.0.0.0/8 [120/20] via 192.1.1.2, 00:00:23, VLAN 1
B    50.0.0.0/8 [120/0] via 192.1.1.3, 00:00:41
C    192.1.1.0/24 is directly connected, VLAN 1
C    192.1.1.254/32 is local host.
```

Examples

Field	Description
O	Source routing protocol, which may be: C: directly connected route S: static route R: RIP route B: BGP route O: OSPF route I: IS-IS route
E2	Route type, which may be: E1: OSPF external route type 1 E2: OSPF external route type 2 N1: OSPF NSSA external type 1 N2: OSPF NSSA external type 2 IA: OSPF area internal route SU: IS-IS summary route L1: IS-IS level-1 route L2: IS-IS level-2 route IA: IS-IS area internal route
20.0.0.0/8	Network address and mask of the destination network
[1/0]	Administrative distance/metric

```
Ruijie# show ip route 30.0.0.0
Routing entry for 30.0.0.0/8
Distance 110, metric 20
Routing Descriptor Blocks:
192.1.1.1, 00:01:11 ago, via VLAN 1, generated by OSPF, extern 2
```

Field	Description
Routing Descriptor Blocks	Next hop IP address, source, update time, forwarding interface, source routing protocol and type of route information

```
Ruijie# show ip route count
--------- route info ----------
the num of active route: 5
```

```
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
```

7.11 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: NORMAL: common routes (not ECMP or FRR); ECMP: equivalent route; FRR: fast reroute; TOTAL: total
Memory	Memory occupied by the table.
Entries	Number of entries (based on prefix, not next-hop)
Connected	Protocol type. Value: Connected: direct connection; Static: static; RIP: RIP; OSPF: OSPF; ISIS: ISIS; BGP: BGP; TOTAL: total

7.12 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: E1: OSPF external route type 1 E2: OSPF external route type 2 N1: OSPF NSSA external type 1 N2: OSPF NSSA external type 2 IA: OSPF area internal route SU: IS-IS summary route L1: IS-IS level-1 route L2: IS-IS level-2 route IA: IS-IS area internal route
20::/64	Network address and mask of the destination network
[20/0]	Administrative distance/metric

Related Commands	Command	Description
	ipv6 route	Configures the IPv6 static route.

Platform Description

7.13 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;

	Connected: Connected route entry. Static: Static route entry. RIP: RIP route entry. OSPF: OSPF route entry. ISIS: ISIS route entry. BGP: BGP route entry. TOTAL: Total number of all protocol entries.
IPv6 routing table count	The number of the routing tables.
Global	The name of the current routing table. The field can be: Global : Global (The default VRF) VRF1: VRF name. TOTAL: All VRF routing table summaries.

Related Commands

Command	Description
N/A	N/A

Platform Description

8 FPM Commands

8.1 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

8.2 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

8.3 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

8.4 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

Parameter	Description

Description		
	N/A	N/A

Defaults By default, the loose TCP status check function is enabled.

Command Mode Global configuration mode

Usage Guide N/A

Configuration Examples The following example enables the loose TCP status transition check function.

```
Ruijie(config)# ip session 1 2 tcp-loose
```

Platform Description N/A

8.5 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

8.6 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

8.7 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 sessiontimeout tcp-established 600
```

Platform Description N/A

8.8 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

8.9 show ip fpm counters

Use this command to displays the counters about the IPv4 packets.

show ip fpm 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 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

8.10 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 Mode Privileged EXEC 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.
vfw_id	Virtual FW ID (only on devices with FW cards).
ctrl_flag	Flows control flag.

Platform Description N/A

8.11 show ip fpm flows filter

Use this command to display IPv4 packet flow information except specific IPv4 packet flows.

show ip fpmflows 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

8.12 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

8.13 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

8.14 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

8.15 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

8.16 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

17. Password-Policy Commands
18. SSH Commands
19. GSN Commands
20. SUMNG

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 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

1.9 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

1.10 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. But it is mandatory in senarios of hot backup and VAC.

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.

1.11 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

1.12 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

1.13 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 N/A

Description

1.14 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.
A maximum of 10 different destination port numbers can be configured, not including default ports 80 and 443.

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

1.15 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 Commands

Command	Description
show http redirect	Displays the HTTP redirection configuration.

Platform Description N/A

1.16 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

1.17 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

1.18 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 N/A

Description

1.19 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

1.20 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

1.21 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

1.22 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

Parameter	Description

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

1.23 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 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 pre-login popup advertisement.

```
Ruijie(config.tmplt.iportal)#login-popup http://www.ruijie.com.cn
```

Platform Description N/A

1.24 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

1.25 nas-port-id

Use this command to configure the port ID of the NAS on a single AP.

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

nas-port-id *string*

no nas-port-id

Parameter Description

Parameter	Description
string	Port ID

Defaults No port ID is configure for the NAS by default.

Command Mode	AP configuration mode
Usage Guide	Make sure this configuration is operated on a single AP

Configuration Examples	The following example configures the port ID of the NAS on a single AP.
	`Ruijie(config)# ap-config ap740`
	`Ruijie(config-ap)# nas-port-id guangdongyidong`

Platform Description	N/A

1.26 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 Description

Parameter	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

1.27 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

1.28 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

1.29 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

1.30 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

1.31 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

1.32 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

1.33 show web-auth control

Use this command to display the authentication configuration.

show web-auth control

Parameter Description

Parameter	Description
N/A	N/A

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide N/A

Configuration Examples The following example displays the authentication configuration and statistics information on the interface.

```
Ruijie(config)#show web-auth control
 Port                   Control  Server Name          Online User Count
 ------------------------ -------- -------------------- -----------------
 GigabitEthernet 0/1      On      <not configured>     0
Ruijie(config)#
```

Field	Description
Port	Name of the authentication port.
Control	Displays whether the Web authentication is enabled on the port or not.
Server Name	The customized server name on the port. **<not configured>** indicates the server name has not been configured.
Online User Count	The number of online users on this port.

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

1.34 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

1.35 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

1.36 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

1.37 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

1.38 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

1.39 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

1.40 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

1.41 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

1.42 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** | **by-ap** *ap-name* | **by-ap-group** *ap-group-name*}

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.
ap-name	AP name.
ap-group-name	AP group name.

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

1.43 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

1.44 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

1.45 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

1.46 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

1.47 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

Parameter	Description

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

1.48 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

1.49 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

1.50 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 (config-wlansec)# web-auth bind-portal eportalv2
```

Platform Description N/A

1.51 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

1.52 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

Parameter	Description

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

1.53 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 Mode Global configuration 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

1.54 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

1.55 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

1.56 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

1.57 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

1.58 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 The default is 1 minute.
times	Ping retries in the range from 0 to 65,535 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

1.59 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

1.60 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

1.61 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

1.62 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

1.63 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

1.64 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

1.65 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

1.66 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

1.67 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

1.68 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

1.69 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

1.70 web-auth update-interval

Use this command to set the interval at which the online user information is updated.
Use the **no** form of this command to restore the default setting.
web-auth update-interval {*seconds*}
no web-auth update-interval

Parameter Description

Parameter	Description
seconds	Update interval in seconds, in the range from 30 to 3,600 in the unit of seconds.

Defaults The default is 180 seconds.

Command Mode Global configuration mode

Usage Guide N/A

Configuration The following example sets the interval at which the online user information is updated to 60 seconds.

Examples

```
Ruijie(config)# web-auth update-interval 60
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

1.71 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

1.72 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 escape. Run the **web-auth wechat-escape** 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

1.73 web-auth wechat-escape

Use this command to enable escape of the authentication server for WeChat access.
web-auth wechat-escape interval *minutes*
Use the **no** form of this command to disable escape.
no web-auth wechat-escape

Use this command to cancel escape. As a trigger, it is not displayed when the **show running-config** command is executed.
web-auth wechat-escape recover

Parameter Description

Parameter	Description
minutes	Escape interval. By default, it is 60minutes.

Defaults Collective escape is disabled by default.

Command Mode Global configuration mode and WLANSEC configuration mode

Usage Guide After the **web-auth wechat-escape recover** command is run, if the server remains unreachable, escape will be resumed.

Configuration Examples The following example configures the parameters for escape.

```
Ruijie (config)# web-auth wechat-escape interval 30

Ruijie (config-wlansec)# web-auth wechat-escape interval 30
```

Platform Description

1.74 web-auth wechat-template wlan-range portal-ip nas-ip

Use this command to enable the one-click configuration via WeChat.
web-auth wechat-template *name* **wlan-range** *wlanid-start wlanid-end* **portal-ip** *portal-ip-addr* **nas-ip** *nas-ip-addr* [**nas-id** *nas-id-str*] **[ios-adapter | perception]**

Use the **no** form of this command to disable the one-click 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.
nas-id-str	Configures the NAS ID of the device. Mandatory in scenarios of hot backup and VAC.
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 of the *nas-id-str* field is mandatory in scenarios of hot backup and VAC. It requires no configuration in standalone mode.

Configuration Examples The following example enables the one-click 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

1.75 web-auth wifidog-template wlan-range portal-ip nas-ip url

Use this command to enable the one-click 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* [**gateway-id** *gwid-str*] **[perception]**

Use the **no** form of this command to disable the one-click 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.
gwid-str	Gateway ID
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.
- The configuration of the *gateway-id* field is mandatory in scenarios of hot backup and VAC. In standalone mode, you do not need to configure it.

Configuration Examples The following example enables the one-click 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.

1.76 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

1.77 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 N/A

Description

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 Mode Global configuration mode

Usage Guide If the AAA security service is not enabled, the accounting update function cannot be used. This command is used to set the accounting interval if the AAA security service has been enabled.

Configuration Examples The following example sets the interval of accounting update to 1 minute.

```
Ruijie(config)# aaa new-model
Ruijie(config)# aaa accounting update
Ruijie(config)# aaa accounting update periodic 1
```

Related Commands

Command	Description
aaa new-model	Enables the AAA security service.
aaa accounting network	Defines a network accounting method list.

Platform Description N/A

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 Global configuration mode

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 Examples The following example enables the configuration command authorization function.

```
Ruijie(config)# aaa authorization config-commands
```

Related Commands

Command	Description
aaa new-model	Enables the AAA security service.
aaa authorization commands	Defines the AAA command authorization.

Platform Description N/A

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 N/A

Description

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

Parameter	Description

Description	N/A	N/A

Defaults This function is disabled by default.

Command Mode Global configuration mode

Usage Guide To perform the domain-name-based AAA service configuration, enable this service.

Configuration 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 N/A

Description

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 43200 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 Global configuration mode

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 Examples The following example allows the local account (username or subs) to be shared by multiple terminals 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. 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 Description N/A

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 Description N/A

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 Privileged EXEC mode/Global configuration mode/Interface configuration mode

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	mgmt	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

Command	Description

Commands		
	N/A	N/A

Platform Description N/A

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** [**tries**] **| tries** }

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-number	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. 0: no encryption; 7: Simply-encrypted.

Defaults No shared password is specified by default.

Command Mode Global configuration mode.

Usage Guide A shared password is the basis for communications between the device and the RADIUS security server. In order to allow the device to communicate with the RADIUS security server, you must define the same shared password on the device and the RADIUS security server.

Configuration Examples The following example defines the shared password **aaa** for the RADIUS security server:

```
Ruijie(config)# radius-server key aaa
```

Related Commands

Command	Description
radius-server host	Defines the RADIUS security server.
radius-server retransmit	Defines the number of RADIUS packet retransmissions.
radius-server timeout	Defines the timeout for the RADIUS packet.

Platform Description N/A

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 The following example displays RADIUS accounting statistics.

Examples

```
Ruijie#show radius acct statistics
Accounting Servers:

Server Index..................................... 1
Server Address................................... 192.168.1.1
Server Port...................................... 1813
Msg Round Trip Time.............................. 0 (msec)
First Requests................................... 1
Retry Requests................................... 1
Accounting Responses............................. 0
Malformed Msgs................................... 0
Bad Authenticator Msgs........................... 0
Pending Requests........
```

Related Commands

Command	Description
N/A	N/A

Platform 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.
Configuration in WLAN security configuration mode is prior to that in global configuration mode.

Configuration Examples The following example configures the accounting list.

```
Ruijie(config)# dot1x accounting dot1x-acct
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

4.7 dot1x 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.

```
Ruijie(config)# dot1x acct-update base-on first-time server
```

Platform N/A

Description

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 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 Examples The following example enables uppercase letters in MAB user names.

```
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 N/A

Description

4.19 dot1x max-req

Use this command to set the maximum attempts of authentication requests.

dot1x max-req *num*

Parameter Description	**Parameter**	**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 The default is 15 minutes.
num	Traffic threshold in the unit of KB 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 0 to 65,535 in the unit of seconds.

Defaults The default is 10 seconds.

Command Mode Global configuration mode

Usage Guide When authentication fails, the supplicant must wait for a period of time before re-authentication.

Configuration Examples The following example sets the quiet period after authentication failure to 60 seconds.

```
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 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 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 Examples The following example enables IP address-triggered accounting.

```
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 N/A

Description

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 Privileged EXEC mode/Global configuration mode/Interface configuration mode

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 summary by-ap

Use this command to display the AP-based 802.1X authentication summary.

show dot1x summary by-ap *ap-name*

Parameter Description

Parameter	Description
ap-name	Name of the AP.

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 AP name.

Configuration Examples The following example displays the AP-based summary of 802.1X authentication.

```
Ruijie#show dot1x summary by-ap ap1
AP-NAME:ap1
ID      User      MAC           Interface VLAN INNER-VLAN Auth-State
Backend-State Port-Status User-Type Time
-------- ---------- --------------  --------- ---- ---------- ---------------
------------- ----------- --------- ------------------
1        a03be38... a03b.e38e.0565 wlan 1    1    Authenticated   Idle
Authed     static    0days 0h 0m 4s
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

4.44 show dot1x summary by-ap-group

Use this command to display the AP-group-based 802.1X authentication summary.

show dot1x summary by-ap-group *ap-group-name*

Parameter Description

Parameter	Description
ap-group-name	Name of the AP group.

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 AP group name.

Configuration Examples The following example displays the AP-group-based summary of 802.1X authentication.

```
Ruijie#show dot1x summary by-ap-group apgroup1
AP-GROUP-NAME:apgroup1
ID       User       MAC             Interface VLAN INNER-VLAN Auth-State
Backend-State Port-Status User-Type Time
-------- ---------- --------------  --------- ---- ---------- --------------- -------------
---------- --------- ------------------
1        a03be38... a03b.e38e.0565 wlan 1    1    Authenticated   Idle
Authed     static    0days 0h 0m 4s
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

4.45 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

4.46 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

4.47 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

4.48 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

4.49 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

4.50 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

4.51 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 N/A

Description

4.52 show dot1x user name

Use this command to display information about 802.1X authentication users based on usernames.

show dot1x user name *name*

Parameter Description	**Parameter**	**Description**
	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/ ap-config all 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 ipv6-mode

This command is used to set the IPv6 address binding mode. Use the **no** form of this command to restore the default setting.

This command is also used to set the compatible mode.

address-bind ipv6-mode { **compatible** | **loose** | **strict** }

no address-bind ipv6-mode

Parameter Description

Parameter	Description
compatible	Compatible mode
loose	Loose mode
strict	Strict mode

Defaults The default is strict mode.

Command Mode Global configuration mode.

Usage Guide N/A

Configuration Examples The following example configures the IPv6 address binding mode.

```
Ruijie# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Ruijie(config)# address-bind ipv6-mode compatible
```

Related Commands

Command	Description
show address-bind uplink	Displays the exceptional port of the address binding.

Platform Description N/A

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 N/A

Description

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

Command	Description

Commands

show ip dhcp snooping	Displays the configuration information of the DHCP Snooping.

Platform Description N/A

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. STA information is not wrotten into flash.

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

Command	Description

Commands		
	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 Description N/A

8.17 renew ip dhcp snooping database

Use this command to import the information in the backup file 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 backup 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 backup 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 the backup file periodically.
ip dhcp snooping information option	Adds option82 to the DHCP request message.
ip dhcp snooping bootp-bind	Enables the DHCP Snooping bootp bind function.
ip dhcp snooping trust	Sets the port as a trust port.

Platform N/A

Description

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 Description

N/A

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/WLAN ap-config all 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.
Enabling IP Source Guard in WLAN ap-config all mode means enabling it on wired ports of all APs.

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 Port Security Commands

11.1 switchport port-security

Use this command to configure port security and the way to deal with violation.
Use the **no** form of this command to restore the default setting.
switchport port-security [violation { protect | restrict | shutdown }]
no switchport port-security [**violation**]

Parameter Description

Parameter	Description
protect	Discards the packets breaching security.
restrict	Discards the packets breaching security and sends the Trap message.
shutdown	Discards the packets breaching the security, sends the Trap message and disables the interface.

Defaults This function is disabled by default.

Command Mode Interface configuration mode

Usage Guide With port security, you can strictly control the input on a specific port by restricting access to the MAC address and IP address (optional) of the port on the switch. After you configure some secure addresses for the port security-enabled port, only the packets from these addresses can be forwarded. In addition, you can also restrict the maximum number of secure addresses on a port. If you set the maximum value to 1 and configure one secure address for this port, the workstation (whose address is the configured secure Mac address) connected to this port will occupy all the bandwidth of this port exclusively.

- If the violation handling mode is changed after violation occurs, the new mode takes effect only after the violation mode is restarted.
- When the port security and 802.1x are configured at the same time, secure ports do not generate dynamic secure address entries.

Configuration Examples The following example enables port security on interface gigabitethernet 1/1, and the way to deal with violation is **shutdown**:

```
Ruijie(config)#interface gigabitethernet 1/1
Ruijie(config-if)# switchport port-security
Ruijie(config-if)# switchport port-security violation shutdown
```

Related

Command	Description

Commands		
	show port-security	Displays port security settings.

Platform Description N/A

11.2 switchport port-security aging

Use this command to set the aging time for all secure addresses on an interface.
Use the **no** form of this command to restore the default setting.
switchport port-security aging {**static** | **time** *time* }
no switchport port-security aging {**static** | **time** }

Parameter Description

Parameter	Description
static	Applies the aging time to both manually configured secure addresses and automatically learned addresses. Otherwise, apply it to only the automatically learned secure addresses.
time *time*	Specifies the aging time for the secure address on this port. Its range is 0-1,440 in minutes. If you set it to 0, the aging function is disabled actually.

Defaults No secure address is aged by default.

Command Mode Interface configuration mode

Usage Guide In interface configuration mode, use the **no switchport port-security aging time command** to disable the aging for security addresses on the port. Use the **no switchport port-security aging static** command to apply the aging time to only the dynamically learned security address.
Use the **show port-security** command to display configuration.
When both port security and 802.1X authentication functions are enabled, 802.1X clients must get re-authenticated for network access once the secure addresses are aged.

To enable this function, you need to set the maximum number of secure addresses. In this way, you can make the switch automatically add or delete the secure addresses on the interface.

Configuration Examples The following example sets the aging time for all secure addresses on interface gigabitethernet 1/1 to eight minutes.

```
Ruijie# configure terminal
Ruijie(config)# interface gigabitethernet 1/1
Ruijie(config-if)# switchport port-security aging time 8
Ruijie(config-if)# switchport port-security aging static
```

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

Related Commands

Command	Description
show port-security	Displays port security settings.

Platform Description N/A

11.3 switchport port-security binding

Use these commands to configure secure address binding manually in the interface configuration mode through performing the source IP address plus source MAC address binding or only the source IP address binding. With this binding configured, only the packets match the binding secure address could enter the switch, others will be discarded.

Use the **no** form of these commands to remove the binding addresses.

switchport port-security binding [*mac-address* **vlan** *vlan_id*] { *ipv4-address* | *ipv6-address* }

switchport port-security binding { *ipv4-address* | *ipv6-address* }

no switchport port-security binding [*mac-address* **vlan** *vlan_id*] { *ipv4-address* | *ipv6-address* }

no switchport port-security binding { *ipv4-address* | *ipv6-address* }

Parameter Description

Parameter	Description
mac-address	The source MAC addresses to be bound
vlan_id	VLAN ID of the binding source MAC address
ipv4-address	Binds IPv4 addresses.
ipv6-address	Binds IPv6 addresses.

Defaults N/A

Command Mode Interface configuration mode

Usage Guide 1. For packets complying with IP/IP-MAC binding, they can be forwarded only if MAC addresses are secure addresses.

2. For dynamic secure addresses, packets cannot be forwarded before bound even if their addresses comply with the binding list.

Network is often accessible to static users with secure addresses without authorization. If authorization is configured, these users must comply with it.

Configuration Examples The following example binds the IP address 192.168.1.100 on interface g 0/10:

```
Ruijie# configure terminal
Ruijie(config)#interface gigabitethernet 0/10
Ruijie(config-if)# switchport port-security binding 192.168.1.100
```

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

The following example binds the IP address 192.168.1.100 and MAC address 00d0.f800.5555 with VLAN ID 1 on interface g 0/10.

```
Ruijie# configure terminal
Ruijie(config)#interface gigabitethernet 0/10
Ruijie(config-if)# switchport port-security binding 00d0.f800.5555 vlan 1
192.168.1.100
Ruijie(config-if)# end
```

Related Commands

Command	Description
show port-security	Displays port security settings.
switchport port-security	Enables the port-security.
switchport port-security binding interface	Configures the secure address binding in privileged EXEC mode.
switchport port-security mac-address	Sets the static secure address.
switchport port-security aging	Sets the aging time for secure address.

Platform Description N/A

11.4 switchport port-security interface binding

Use these commands to configure secure address binding manually in the privileged EXEC mode through performing the source IP address plus source MAC address binding or only the source IP address binding. With this binding configured, only the packets match the binding secure address could enter the switch, others will be discarded.

Use the **no** form of these commands to remove the binding addresses.

switchport port-security interface i*nterface-id* **binding** [*mac-address* **vlan** *vlan_id*] {*ipv4-address* | *ipv6-address* }

switchport port-security interface *interface-id* **binding**{ *ipv4-address* | *ipv6-address* }

no switchport port-security interface i*nterface-id* **binding** [*mac-address* **vlan** *vlan_id*] { *ipv4-address* | *ipv6-address* }

no switchport port-security interface *interface-id* **binding**{ *ipv4-address* | *ipv6-address* }

Parameter Description

Parameter	Description
interface-id	**Binds interface ID.**
mac-address	Binds source MAC address.
vlan_id	VLAN ID of the binding source MAC address
ipv4-address	Binds IPv4 address.
ipv6-address	Binds IPv6 address .

Defaults N/A

Command Mode Global configuration mode

Usage Guide 1. For packets complying with IP/IP-MAC binding, they can be forwarded only if MAC addresses are secure addresses.
2. For dynamic secure addresses, packets cannot be forwarded before bound even if their addresses comply with the binding list.

Configuration Examples The following example binds the IP address 192.168.1.100 on the interface g 0/10.

```
Ruijie# configure terminal
Ruijie(config)# switchport port-security binding interface g0/10  binding
192.168.1.100
Ruijie(config)# end
```

The following example binds the IP address 192.168.1.100 and MAC address 00d0.f800.5555 with VLAN ID 1 on the interface g 0/10.

```
Ruijie# configure terminal
Ruijie(config)# switchport port-security binding interface g0/10 binding
00d0.f800.5555 vlan 1 192.168.1.100
Ruijie(config)# end
```

Related Commands

Command	Description
show port-security	Displays port security settings.
switchport port-security	Enables the port-security.
switchport port-security binding	Configures the secure address binding in interface configuration mode.
switchport port-security mac-address	Sets the static secure address.
switchport port-security aging	Sets the aging time for secure address.

Platform Description N/A

11.5 switchport port-security mac-address

Use this command to configure the static secure address.
Use the **no** form of this command to remove the configuration.
switchport port-security mac-address *mac-address* [vlan *vlan-id*]
no switchport port-security mac-address *mac-address* [vlan *vlan-id*]

Parameter

Parameter	Description

Description

mac-address	Static secure MAC address
vlan-id	VLAN ID of the MAC address The configuration of vlan-id is only supported on the TRUNK port.

Defaults N/A

Command Mode Interface configuration mode

Usage Guide N/A

Configuration Examples The following example sets the static secure address and VLAN ID of TRUNK port 10 to 00d0.f800.5555 and 2 respectively.

```
Ruijie# configure terminal
Ruijie(config)#interface gigabitethernet 0/10
Ruijie(config-if)# switchport port-security mac-address 00d0.f800.5555 vlan 2
Ruijie(config-if)# end
```

Related Commands

Command	Description
show port-security	Displays port security settings.
switchport port-security	Enables the port-security.
switchport port-security binding	Configures the secure address binding.
switchport port-security mac-address interface	Sets the static secure address in privileged EXEC mode.
switchport port-security aging	Sets the aging time for the secure address.

Platform Description N/A

11.6 switchport port-security interface mac-address

Use this command to configure the static secure address.

Use the **no** form of this command to remove the configuration.

switchport port-security interface *interface-id* **mac-address** *mac-address* [**vlan** *vlan-id*]

no switchport port-security interface *interface-id* mac-address *mac-address [vlan vlan-id]*

Parameter Description

Parameter	Description

interface-id	Interface ID
mac-address	Static secure address
vlan-id	VLAN ID of the MAC address The configuration of vlan-id is only supported on the TRUNK port.

Defaults N/A

Command Mode Global configuration mode

Usage Guide N/A

Configuration Examples The following example sets the static secure address and VLAN ID of TRUNK port 10 to 00d0.f800.5555 and 2 respectively.

```
Ruijie# configure terminal
Ruijie(config)# switchport port-security interface g0/10 mac-address
00d0.f800.5555 vlan 2
Ruijie(config)# end
```

Related Commands

Command	Description
show port-security	Displays port security settings.
switchport port-security	Enables the port-security.
switchport port-security binding	Configures the secure address binding.
switchport port-security mac-address	Sets the static secure address in interface configuration mode.
switchport port-security aging	Sets the aging time for the secure address.

Platform Description N/A

11.7 switchport port-security maximum

Use this command to set the maximum number of port secure addresses.

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

switchport port-security maximum *value*

no switchport port-security maximum

Parameter Description

Parameter	Description
value	Maximum number of the secure address, in the range from 1 to 128.

Defaults The default is 128.

Command Mode Interface configuration mode

Usage Guide The number of the secure address contains the sum of static secure address and dynamically learnt secure address, 128 by default.
If the number of the secure address you set is less than current number, it will prompt this setting failure.

Configuration Examples The following example sets the maximum number of the secure address to 2 for interface g 0/10.

```
Ruijie# configure terminal
Ruijie(config)#interface gigabitethernet 0/10
Ruijie(config-if)# switchport port-security maximum 2
Ruijie(config-if)# end
```

Related Commands

Command	Description
show port-security	Displays port security settings.
switchport port-security	Enables the port-security.
switchport port-security binding	Configures the secure address binding.
Switchport port-security mac-address	Sets the static secure address in the interface configuration mode.
switchport port-security aging	Sets the aging time for the port secure address.

Platform Description N/A

11.8 switchport port-security mac-address sticky

Use this command to configure the Sticky MAC secure address.
Use the **no** form of this command to restore the default setting.
switchport port-security mac-address sticky *mac-address* [**vlan** *vlan-id*]
no switchport port-security mac-address sticky *mac-address* [**vlan** *vlan-id*]
Use the command without parameters to enable the Sticky MAC address learning.
Use the **no** form of this command to disable the Sticky MAC address learning.
switchport port-security mac-address sticky
no switchport port-security mac-address sticky

Parameter Description

Parameter	Description
mac-address	Static secure address
vlan-id	Vlan ID of the MAC address

	The configuration of vlan-id is only supported on the TRUNK port.

Defaults This function is disabled by default.

Command Mode Interface configuration mode

Usage Guide Sticky MAC addresses, either static or dynamic, are special addresses free from aging.

Configuration Examples The following example sets the MAC address and VLAN ID of TRUNK port 10 to 00d0.f800.5555 to 2 respectively.

```
Ruijie# configure terminal
Ruijie(config)#interface gigabitethernet 0/10
Ruijie(config-if)# switchport port-security mac-address 00d0.f800.5555 vlan 2
Ruijie(config-if)# end
```

The following example enables the Sticky MAC address learning on interface g0/10.

```
Ruijie# configure terminal
Ruijie(config)#interface gigabitethernet 0/10
Ruijie(config-if)# switchport port-security sticky mac-address
Ruijie(config-if)# end
```

Related Commands

Command	Description
show port-security	Displays port security settings.
switchport port-security	Enables the port-security.
switchport port-security binding	Configures the secure address binding.
switchport port-security mac-address interface	Sets the static secure address in privileged EXEC mode.
switchport port-security mac-address	Sets the static secure address in interface configuration mode.
switchport port-security aging	Sets the aging time for the secure address.

Platform Description N/A

11.9 show port-security

Use this command to display the port security configuration and the secure address.

show port-security [**address** [**interface** *interface-id*] | **binding** [**interface** *interface-id*] | **interface** *interface-id* | **all**]

Parameter Description

Parameter	Description
address	Displays all secure addresses, or the secure address of the specified port.
binding	Displays all port security bindings, or the port security bindings of the specified port.
interface *interface-id*	Displays the port security configuration of the specified port.
all	Displays all valid secure addresses and valid port security bindings.

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide To display all port security configuration and violation management, execute the command without any parameter. To display the security configuration, the secure address, or the port security binding of the specified interface, execute the command with the corresponding parameter.

Configuration Examples The following example displays the port security statistics.

```
Ruijie#show port-security
NO.  SecurePort MaxSecureAddr CurrentAddr CurrentIpBind CurrentIpMacBind
SecurityAction
                (Count)      (Count)      (Count)        (Count)
---- ---------- ------------ ----------- ------------- ----------------
--------------
1    Gi0/1     128          2          2           1              protect
-------------------------------------------------------------------------
------------
Total secure addresses in System : 2
Total secure bindings  in System : 3
```

Field	Description
NO.	Serial number.
Secure Port	Port name
MaxSecureAddr(count)	The maximum number of secure addresses on the port.
CurrentAddr(count)	The current number of secure addresses on the port.
CurrentIpBind (count)	The current number of IP addresses bindings on the port.
CurrentIpMacBind (count)	The current number of IP-MAC address bindings on the port.
Security Action	Violation management.

Total secure addresses in System	The total number of secure addresses on the device.
Total secure bindings in System	The total number of port security bindings on the device,

The following example displays the port security configuration on interface Gigabitethernet 0/1.

```
Ruijie#show port-security interface gigabitEthernet 0/1
Interface                 : GigabitEthernet 0/1
Port status               : down
Port Security             : enabled
SecureStatic address aging   : disabled
Sticky dynamic address      : disabled
Violation mode            : protect
Maximum MAC Addresses       : 128
Total MAC Addresses         : 2
Configured MAC Addresses    : 2
Dynamic MAC Addresses       : 0
Sticky MAC Addresses        : 0
Total security binding      : 3
IPv4-ONLY Binding Addresses  : 1
IPv6-ONLY Binding Addresses  : 1
IPv4-MAC Binding Addresses   : 1
IPv6-MAC Binding Addresses   : 0
Aging time(min)           : 0
```

Field	Description
Interface	Port name.
Port status	Port status.
Port Security	Displays whether the port security is enabled.
SecureStatic address aging	Displays whether the static secure address aging is enabled.
Sticky dynamic address	Displays whether the dynamic secure address is converted to the sticky secure address,
Violation mode	Port violation management.
Maximum MAC Addresses	The maximum number of secure addresses on the port.
Total MAC Addresses	The number of valid secure addresses on the port.
Configured MAC Addresses	The number of static secure addresses.
Dynamic MAC Addresses	The number of dynamic secure addresses.
Sticky MAC Addresses	The number of sticky secure addresses,
Total security binding	The number of valid port security bindings.
IPv4-ONLY Binding Addresses	The number of IPv4 addresses bindings.
IPv6-ONLY Binding Addresses	The number of IPv6 addresses bindings.

IPv4-MAC Binding Addresses	The number of IPv4-MAC address bindings.
IPv6-MAC Binding Addresses	The number of IPv6-MAC address bindings.
Aging time(min)	The aging time of the secure address.

The following example displays all secure addresses on the device.

```
Ruijie#show port-security address
NO.  VLAN  MacAddress     PORT                    TYPE
RemainingAge(mins)  STATUS
---- ----- -------------- ------------------------ ----------
-----------------  ---------
1    1     00d0.f800.073c  GigabitEthernet 0/1      Configured        --
active
2    1     00d0.f800.073d  GigabitEthernet 0/1      Configured        --
active
```

Field	Description
NO.	Serial number.
Vlan	VLAN ID.
Mac Address	MAC address.
Port	Port name.
Type	Secure address type.
Remaining Age(mins)	The aging time of the secure address.
STATUS	The secure address status.

The following example displays all port security bindings on the device.

```
Ruijie#show port-security binding
NO.  VLAN MacAddress    PORT      IpAddress
FilterType FilterStatus
---- ---- -------------- ---------- ---------------------------------------
---------- ------------
1    1    00d0.f800.073c Gi0/1     192.168.12.202
ipv4-mac   active
2     --       --      Gi0/1     192.168.0.1
ipv4-only  active
3     --       --      Gi0/1     ffaa:ddcc::1
ipv6-only  activ
```

Field	Description
NO.	Serial number.
Vlan	VLAN ID.
Mac Address	MAC address.
Port	Port name.
IpAddress	IP address.
FilterType	The filtering type of the port security binding.
FilterStatus	The status of the port security binding.

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

12 VRRP Commands

12.1 show vrrp

Use this command to display the VRRP information.

show [**ipv6**] **vrrp** [**brief** | *group*]

Parameter Description

Parameter	Description
ipv6	(Optional) Applies to IPv6 VRRP.
brief	(Optional) Displays the brief of the VRRP group.
group	Number of the VRRP group to be displayed

Defaults N/A

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

Usage Guide If no optional parameter is used, the information of all VRRP groups is displayed.

Configuration Examples The following example displays the information of all VRRP groups.

```
Ruijie# show vrrp
FastEthernet 0/0 - Group 1
State is Backup
Virtual IP address is 192.168.201.1 configured
Virtual MAC address is 0000.5e00.0101
Advertisement interval is 3 sec
Preemption is enabled
min delay is 0 sec
Priority is 100
Master Device is 192.168.201.213 , pritority is 120
Master Advertisement interval is 3 sec
Master Down interval is 9 sec
FastEthernet 0/0 - Group 2
State is Master
Virtual IP address is 192.168.201.2 configured
Virtual MAC address is 0000.5e00.0102
Advertisement interval is 3 sec
Preemption is enabled
min delay is 0 sec
Priority is 120
Master Device is 192.168.201.217 (local), priority is 120
```

```
Master Advertisement interval is 3 sec
Master Down interval is 9 sec
Ruijie#
```

The following example displays the brief information of the VRRP group.

```
Ruijie# show vrrp brief
Interface   Grp Pri timer  Own Pre State   Master addr    Group addr
Gi 0/0    1 100  10.82    -   P  Backup  192.168.201.213 192.168.201.1
Gi 0/0    2 120  10.59    -   P  Master  192.168.201.217 192.168.201.2
Ruijie#show ipv6 vrrp brief
Interface     Grp Pri timer Own Pre State Master addr  Group addr
Gi0/13         1 100 3.60 -  P  Master FE80::1             FE80::2
```

Related Commands

Command	Description
vrrp *group* **ip** *ipaddress* [**secondary**]	Enables the VRRP function and set the IP address for the virtual device.

Platform Description N/A

12.2 show vrrp interface

Use this command to display the information of the VRRP on the interface.

show [**ipv6**] **vrrp interface** *type number* [**brief**]

Parameter Description

Parameter	Description
ipv6	(Optional) Applies to IPv6 VRRP.
type	Interface type
number	Interface number
brief	(Optional) Displays the brief of the VRRP group on the interface.

Defaults N/A

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

Usage Guide N/A

Configuration Examples The following example displays the VRRP information on Ethernet interface E1/0.

```
Ruijie# show vrrp interface fastethernet 0/0
FastEthernet 0/0 - Group 1
State is Backup
Virtual IP address is 192.168.201.1 configured
```

```
Virtual MAC address is 0000.5e00.0101
Advertisement interval is 3 sec
Preemption is enabled
min delay is 0 sec
Priority is 100
Master Device is 192.168.201.213 , pritority is 120
Master Advertisement interval is 3 sec
Master Down interval is 9 sec
FastEthernet 0/0 - Group 2
State is Master
Virtual IP address is 192.168.201.2 configured
Virtual MAC address is 0000.5e00.0102
Advertisement interval is 3 sec
Preemption is enabled
min delay is 0 sec
Priority is 120
Master Device is 192.168.201.217 (local), priority is 120
Master Advertisement interval is 3 sec
Master Down interval is 9 sec
```

Related Commands

Command	Description
vrrp *group* **ip** *ip address* [**secondary**]	Enables the VRRP function and set the IP address for the virtual device

Platform Description N/A

12.3 show vrrp packet statistics

Use this command to display the statistics of the VRRP packet transmission.

show vrrp packet statistics [*interface-type interface-number*]

Parameter Description

Parameter	Description
interface-type interface-number	Interface type and 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 statistics of VRRP packet transmission on all interfaces.

```
Ruijie# show vrrp packet statistics

Total
   InReceives: 966043 packets, InOctets: 38641824, InErrors: 38826
   OutTransmits: 306079, OutOctets: 7798564
GigabitEthernet 3/0/1
   InReceives: 799665 packets, InOctets: 31986600, InErrors: 19657
   OutTransmits: 272931, OutOctets: 6675320
GigabitEthernet 3/0/2
   InReceives: 0 packets, InOctets: 0, InErrors: 0
   OutTransmits: 681, OutOctets: 16344
```

The following example displays the statistics of VRRP packets on the interface gigabitEthernet 3/0/1.

```
Ruijie#show vrrp packet statistics gigabitEthernet 3/0/1
GigabitEthernet 3/0/1
   InReceives: 799911 packets, InOctets: 31996440, InErrors: 19657
   OutTransmits: 273053, OutOctets: 6677760
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

12.4 vrrp accept_mode

Use this command to enable the packet accepting function on the IPv6 VRRP virtual router.
Use the **no** form of this command to disable this function.
vrrp ipv6 *group* **accept_mode**
no vrrp ipv6 *group* **accept_mode**

Parameter Description

Parameter	Description
group	VRRP group number

Defaults The master IPv6 VRRP is not allowed to accept packets whose destination IPv6 address is the IPv6 address of a virtual router. However, the NA and NS packets should be accepted regardless of the configuration of Accept_Mode. Also, the master IPv6 VRRP virtual router in the owner state will accept and process any packets whose destination IPv6 address is the IPv6 address of a virtual router, regardless of the configuration of Accept_Mode.

Command Mode Interface configuration mode

Usage Guide Configuration of the network interface is effective for the master virtual router.

Only IPv6 VRRP has this configuration mode.

Configuration Examples The following example enables the accept mode on the group 1.

```
Ruijie#configure terminal
Ruijie(config)#interface GigabitEthernet 0/0
Ruijie(config-if-GigabitEthernet 0/0)#no switchport //used on the switch.
Ruijie(config-if-GigabitEthernet 0/0)#ipv6 enable
Ruijie(config-if-GigabitEthernet 0/0)#ipv6 address 2001::2/64
Ruijie(config-if-GigabitEthernet 0/0)#vrrp 1 ipv6 FE80::1
Ruijie(config-if-GigabitEthernet 0/0)#vrrp 1 ipv6 2001::1
Ruijie(config-if-GigabitEthernet 0/0)# vrrp ipv6 1 accept_mode
```

Platform Description N/A

12.5 vrrp authentication

Use this command to enable VRRP authentication.
Use the **no** form of this command to disable this function.
vrrp *group* **authentication** *string*
no vrrp *group* **authentication**

Parameter Description

Parameter	Description
group	VRRP group number
string	String for the VRRP group authentication (within 8 bytes, plaintext password)

Defaults This function is disabled by default. Even if the VRRP function is enabled, no authentication password is configured by default.

Command Mode Interface configuration mode

Usage Guide The devices in the same VRRP group must have the same authentication password configured. The plaintext authentication password cannot provide security. It aims only to prevent/prompt the incorrect VRRP configuration.

Configuration Examples The following example sets the authentication password for VRRP group 1.

```
Ruijie#configure terminal
```

```
Ruijie(config)#interface GigabitEthernet 0/0
Ruijie(config-if-GigabitEthernet 0/0)#no switchport //used on the switch.
Ruijie(config-if-GigabitEthernet 0/0)#ip address 10.0.1.1 255.255.255.0
Ruijie(config-if-GigabitEthernet 0/0)#vrrp 1 ip 10.0.1.20
Ruijie(config-if-GigabitEthernet 0/0)# vrrp 1 authentication x30dn78k
```

Platform Description N/A

12.6 vrrp delay

Use this command to set the reload latency of the VRRP group on the interface.
Use the **no** form of this command to restore the default setting.
vrrp delay { **minimum** *min-seconds* | **reload** *reload-seconds* }
no vrrp delay

Parameter Description

Parameter	Description
minimum *min-seconds*	When the interface is up, VRRP group shall be reloaded after at least min-seconds.
reload *reload-seconds*	The reload latency of the VRRP group. If the configured *min-seconds* is more than *reload-seconds*, the actual reload latency of the VRRP group will be min-seconds.

Defaults This function is disabled by default.

Command Mode Interface configuration mode

Usage Guide Use this command to set the reload latency of the VRRP group on the interface, when it is required that the VRRP group shall not be reloaded immediately after the system reloads or the interface is up. The reload latency range is 0 to 60 seconds.

Configuration Examples The following example sets the VRRP reload latency on E0 to 10 seconds. When E0 is up, VRRP group 1 shall be reloaded in 10 seconds.

```
Ruijie#configure terminal
Ruijie(config)#interface GigabitEthernet 0/0
Ruijie(config-if-GigabitEthernet 0/0)#no switchport //used on the switch.
Ruijie(config-if-GigabitEthernet 0/0)#vrrp delay minimum 10 reload 10
Ruijie(config-if-GigabitEthernet 0/0)#ip address 10.0.1.1 255.255.255.0
Ruijie(config-if-GigabitEthernet 0/0)#vrrp 1 ip 10.0.1.20
```

Related

Command	Description

Commands	N/A	N/A

Platform Description N/A

12.7 vrrp description

Use this command to specify a descriptor for the VRRP.
Use the **no** form of this command to restore the default setting.
vrrp [**ipv6**] *group* **description** *text*
no vrrp [**ipv6**] *group* **description**

Parameter Description

Parameter	Description
ipv6	Applies to IPv6 VRRP.
group	VRRP group number
text	VRRP group descriptor

Defaults This function is disabled by default. Even if the VRRP function is enabled, no VRRP group descriptor is configured by default.

Command Mode Interface configuration mode

Usage Guide This command will set the descriptor for the VRRP group to facilitate the identification of the VRRP group.

Configuration Examples The following example labels the VRRP group 1 on Ethernet interface E0 as Building A – Marketing and Administration.

```
Ruijie#configure terminal
Ruijie(config)#interface GigabitEthernet 0/0
Ruijie(config-if-GigabitEthernet 0/0)#ip address 10.0.1.1 255.255.255.0
Ruijie(config-if-GigabitEthernet 0/0)#vrrp 1 ip 10.0.1.20
Ruijie(config-if-GigabitEthernet 0/0)#vrrp 1 description "Building A -
Marketing and Administration"
Ruijie(config-if-GigabitEthernet 0/0)#vrrp 1 ipv6 fe80::1
Ruijie(config-if-GigabitEthernet 0/0)#vrrp ipv6 1 description "Building B -
Marketing and Administration"
```

Related Commands

Command	Description
vrrp *group* **ip** *ip-address* [**secondary**]	Enables the VRRP function and set the IP address for the virtual device

Platform N/A

Description

12.8 vrrp detection-vlan

Use this command to enable IPv4 VRRP packets to be sent to only the first in a Super VLAN interface.

Use the **no** form of this command to enable IPv4 VRRP packets to be sent to all the Sub VLANs in a Super VLAN interface.

vrrp detection-vlan first-subvlan

no vrrp detection-vlan

Parameter Description

Parameter	Description
first-subvlan	IPv4 VRRP packets are sent to only the first Sub VLAN in a Super VLAN interface.

Defaults By default, IPv4 VRRP packets are sent to only the first Sub VLAN in a Super VLAN interface.

Command Mode Interface configuration mode

Usage Guide Use this command to configure the mode in which IPv4 VRRP packets are sent to a Super VLAN interface. There are two modes in which IPv4 VRRP packets are sent to a Super VLAN interface: to only the first Sub VLAN or all Sub VLANs.


This command is configured on a VLAN interface and applies only to Super VLAN interfaces.

Configuration Examples The following example enables IPv4 VRRP packets to be sent to all Sub VLANs in Super VLAN 3.

```
Ruijie#configure terminal
Ruijie(config)# vlan 3
Ruijie(config-vlan)# supervlan
Ruijie(config-vlan)# subvlan 5-10
Ruijie(config-vlan)#exit
Ruijie(config)#interface vlan 3
Ruijie(config-if)# no vrrp detection-vlan
```

Related Commands

Command	Description
vrrp ip	Enables the VRRP function and set the IP address of the VRRP.

Platform Description N/A

12.9 vrrp ip

Use this command to enable VRRP on the interface and specify the related virtual IP address.
Use the **no** form of this command to restore the default setting.
vrrp *group* **ip** *ipaddress* [**secondary**]
no vrrp *group* **ip** *ipaddress* [**secondary**]

Parameter Description

Parameter	Description
group	VRRP group number of the virtual device
ipaddress	IP address of the virtual device
secondary	Specifies the secondary IP address of the virtual device.

Defaults This function is disabled by default.

Command Mode Interface configuration mode

Usage Guide If the **secondary** parameter is not used, the IP address set here will become the master IP address of the virtual device.

Configuration Examples The following example enables the VRRP function on Ethernet interface 0. The VRRP group number is 1, primary IP address of the virtual device is 10.0.1.20 and secondary IP address is 10.0.2.20.

```
Ruijie#configure terminal
Ruijie(config)#interface GigabitEthernet 0/0
Ruijie(config-if-GigabitEthernet 0/0)#no switchport //used on the switch.
Ruijie(config-if-GigabitEthernet 0/0)#ip address 10.0.1.1 255.255.255.0
Ruijie(config-if-GigabitEthernet 0/0)#ip address 10.0.2.1 255.255.255.0
secondary
Ruijie(config-if-GigabitEthernet 0/0)#vrrp 1 ip 10.0.1.20
Ruijie(config-if-GigabitEthernet 0/0)#vrrp 1 ip 10.0.2.20 secondary
```

Related Commands

Command	Description
show vrrp [**brief** | **group**]	Displays the VRRP configuration.

Platform Description N/A

12.10 vrrp ipv6

Use this command to enable IPv6 VRRP on the interface and specify the related virtual IPv6 address.
Use the **no** form of the command to restore the default setting.
vrrp *group* **ipv6** *ipv6-address*

no vrrp *group* **ip** *ipv6-address*

Parameter Description

Parameter	Description
group	VRRP group number of the virtual device
ipv6-address	IPv6 address of the virtual device

Defaults This function is disabled by default.

Command Mode Interface configuration mode

Usage Guide IPv6 VRRP and IPv4 VRRP share group numbers ranging from 1 to 255. One VRRP group number of an interface is applicable to both IPv4 VRRP and IPv6 VRRP at the same time. The first configured address should be the link's local address, which cannot be deleted until the other virtual addresses are deleted.

Configuration Examples The following example enables the IPv6 VRRP function on Ethernet interface FastEthernet 0/0 with VRRP group number 1and virtual IPv6 address FE80::1 and 2001::1.

```
Ruijie#configure terminal
Ruijie(config)#interface GigabitEthernet 0/0
Ruijie(config-if-GigabitEthernet 0/0)#no switchport //used on the switch.
Ruijie(config-if-GigabitEthernet 0/0)#ipv6 enable
Ruijie(config-if-GigabitEthernet 0/0)#ipv6 address 2001::2/64
Ruijie(config-if-GigabitEthernet 0/0)#vrrp 1 ipv6 FE80::1
Ruijie(config-if-GigabitEthernet 0/0)#vrrp 1 ipv6 2001::1
```

Related Commands

Command	Description
show ipv6 vrrp [**brief | group**]	Displays the IPv6 VRRP configuration.

Platform Description N/A

12.11 vrrp preempt

Use this command to set the preemption mode of the VRRP group.

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

vrrp [**ipv6**] *group* **preempt** [**delay** *seconds*]

no vrrp [**ipv6**] *group* **preempt** [**delay**]

Parameter Description

Parameter	Description
ipv6	Applies to IPv6 VRRP.
group	VRRP group number
delay *seconds*	(Optional)Specifies the delay before a device declares itself master.

	The default value is 0.

Defaults This function is disabled by default. Once the VRRP function is enabled, the VRRP group will work in the preemption mode by default.

Command Mode Interface configuration mode

Usage Guide If the VRRP group is working in the preemption mode, once a device finds its priority is higher than the priority of the master, it will become the master device of the VRRP group. If the VRRP group is not working in the preemption mode, even if a device finds its priority is higher than the master's priority, it will not become the master device of the VRRP group. In case the VRRP group is using the Ethernet interface IP address, the setting of the preemption mode does not make sense, because that VRRP group has the highest priority and thus automatically becomes the master device in the VRRP group.

Configuration Examples The following example enables IPv4 VRRP on interface GigabitEthernet 0/0.When VRRP group 1 finds its priority (200) is higher than that of the current master device, it will declare its preemption of master after a delay of 15 seconds.

```
Ruijie#configure terminal
Ruijie(config)#interface GigabitEthernet 0/0
Ruijie(config-if-GigabitEthernet 0/0)#no switchport //used on the switch.
Ruijie(config-if-GigabitEthernet 0/0)#ip address 10.0.1.1 255.255.255.0
Ruijie(config-if-GigabitEthernet 0/0)#vrrp 1 ip 10.0.1.20
Ruijie(config-if-GigabitEthernet 0/0)#vrrp 1 preempt delay 15
Ruijie(config-if-GigabitEthernet 0/0)#vrrp 1 priority 200
```

The following example enables IPv4 VRRP on interface GigabitEthernet 0/0. When VRRP group 1 finds its priority (200) is higher than that of the current master device, it will declare its preemption of master after a delay of 15 seconds.

```
Ruijie#configure terminal
Ruijie(config)#interface GigabitEthernet 0/0
Ruijie(config-if-GigabitEthernet 0/0)#no switchport //used on the switch.
Ruijie(config-if-GigabitEthernet 0/0)#ipv6 enable
Ruijie(config-if-GigabitEthernet 0/0)#ipv6 address 2001::2/64
Ruijie(config-if-GigabitEthernet 0/0)#vrrp 1 ipv6 FE80::1
Ruijie(config-if-GigabitEthernet 0/0)#vrrp 1 ipv6 2001::1
Ruijie(config-if-GigabitEthernet 0/0)#vrrp ipv6 1 preempt delay 15
Ruijie(config-if-GigabitEthernet 0/0)#vrrp ipv6 1 priority 200
```

Related Commands

Command	Description
vrrp *group* **ip** *ipaddress* [**secondary**]	Enables the VRRP function and set the IP address for the virtual device.
vrrp *group* **priority** *level*	Sets the VRRP group priority.

Platform Description N/A

12.12 vrrp priority

Use this command to specify the priority of the VRRP group.

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

vrrp [**ipv6**] *group* **priority** *level*

no vrrp [**ipv6**] *group* **priority**

Parameter Description

Parameter	Description
ipv6	Specifies the priority of the IPv6 VRRP group.
group	VRRP group number
level	VRRP group priority

Defaults This function is disabled by default. Once the VRRP function is enabled, the default priority of the VRRP group is 100.

Command Mode Interface configuration mode

Usage Guide N/A

Configuration Examples The following example sets the priority of IPv4 VRRP group 1 as 254.

```
Ruijie#configure terminal
Ruijie(config)#interface GigabitEthernet 0/0
Ruijie(config-if-GigabitEthernet 0/0)#no switchport //used on the switch.
Ruijie(config-if-GigabitEthernet 0/0)#ip address 10.0.1.1 255.255.255.0
Ruijie(config-if-GigabitEthernet 0/0)#vrrp 1 ip 10.0.1.20
Ruijie(config-if-GigabitEthernet 0/0)#vrrp 1 priority 254
```

The following example sets the priority of IPv6 VRRP group 1 as 254.

```
Ruijie#configure terminal
Ruijie(config)#interface GigabitEthernet 0/0
Ruijie(config-if-GigabitEthernet 0/0)#no switchport //used on the switch.
Ruijie(config-if-GigabitEthernet 0/0)#ipv6 enable
Ruijie(config-if-GigabitEthernet 0/0)#ipv6 address 2001::2/64
Ruijie(config-if-GigabitEthernet 0/0)#vrrp 1 ipv6 FE80::1
Ruijie(config-if-GigabitEthernet 0/0)#vrrp 1 ipv6 2001::1
Ruijie(config-if-GigabitEthernet 0/0)#vrrp ipv6 1 priority 254
```

Related

Command	Description

Commands		
	vrrp *group* **ip** *ipaddress* [**secondary**]	Enables the VRRP function and set the IP address for the virtual device.
	vrrp *group* **preempt** [**delay** *seconds*]	Sets the VRRP in the preemption mode.

Platform Description N/A

12.13 vrrp timers advertise

Use this command to specify the interval for the master device to send the VRRP advertisement.
Use the **no** form of this command to restore the default setting.
vrrp [**ipv6**] *group* **timers advertise** { *advertise-interval* | **csec** *centisecond-interval* }
no vrrp [**ipv6**] *group* **timers advertise**

Parameter Description

Parameter	Description
ipv6	Applies to IPv6 VRRP.
group	VRRP group number
advertise-interval	Sets the interval time in seconds between sending VRRP advertisement.
csec *centisecond-interval*	Sets the interval time in milliseconds between sending advertisement frames from the master VRRP router in the backup group. The range is from 50 to 99. This value is not set by default. This parameter takes effect only for VRRPv3.

Defaults This function is disabled by default. Once the VRRP function is enabled, the default advertisement interval of the master device is one second.

Command Mode Interface configuration mode

Usage Guide If the current device becomes the master device in the VRRP group, it will notify its VRRP status, priority and other information by sending the VRRP advertisement in the set interval.
Based on the RFC specification, the maximum advertisement interval of the IPv4/IPv6 VRRPv3 group is 40 seconds. The advertisement interval can be configured larger than 40 seconds, but the effective advertisement interval is 40 seconds.

Configuration Examples The following example sets the IPv4 VRRP advertisement interval as 4 seconds.

```
Ruijie#configure terminal
Ruijie(config)#interface GigabitEthernet 0/0
Ruijie(config-if-GigabitEthernet 0/0)#no switchport //used on the switch.
Ruijie(config-if-GigabitEthernet 0/0)#ip address 10.0.1.1 255.255.255.0
Ruijie(config-if-GigabitEthernet 0/0)#vrrp 1 ip 10.0.1.20
Ruijie(config-if-GigabitEthernet 0/0)#vrrp 1 timers advertise 4
```

The following example sets the IPv6 VRRP advertisement interval as 4 seconds.

```
Ruijie#configure terminal
Ruijie(config)#interface GigabitEthernet 0/0
Ruijie(config-if-GigabitEthernet 0/0)#no switchport //used on the switch.
Ruijie(config-if-GigabitEthernet 0/0)#ipv6 enable
Ruijie(config-if-GigabitEthernet 0/0)#ipv6 address 2001::2/64
Ruijie(config-if-GigabitEthernet 0/0)#vrrp 1 ipv6 FE80::1
Ruijie(config-if-GigabitEthernet 0/0)#vrrp 1 ipv6 2001::1
Ruijie(config-if-GigabitEthernet 0/0)#vrrp ipv6 1 timers advertise 4
```

The following example sets the IPv4 VRRP advertisement interval as 50 centi-seconds.

```
Ruijie#configure terminal
Ruijie(config)#interface GigabitEthernet 0/0
Ruijie(config-if-GigabitEthernet 0/0)#no switchport //used on the switch.
Ruijie(config-if-GigabitEthernet 0/0)#ip address 10.0.1.1 255.255.255.0
Ruijie(config-if-GigabitEthernet 0/0)#vrrp 1 ip 10.0.1.20
Ruijie(config-if-GigabitEthernet 0/0)#vrrp 1 timers advertise csec 50
```

The following example sets the IPv6 VRRP advertisement interval as 50 centi-seconds.

```
Ruijie#configure terminal
Ruijie(config)#interface GigabitEthernet 0/0
Ruijie(config-if-GigabitEthernet 0/0)#no switchport //used on the switch.
Ruijie(config-if-GigabitEthernet 0/0)#ipv6 enable
Ruijie(config-if-GigabitEthernet 0/0)#ipv6 address 2001::2/64
Ruijie(config-if-GigabitEthernet 0/0)#vrrp 1 ipv6 FE80::1
Ruijie(config-if-GigabitEthernet 0/0)#vrrp 1 ipv6 2001::1
Ruijie(config-if-GigabitEthernet 0/0)#vrrp ipv6 1 timers advertise csec 50
```

Related Commands

Command	Description
vrrp *group* **ip** *ipaddress* [**secondary**]	Enables the VRRP function and set the IP address for the virtual device.
vrrp group timers learn	Enables the timer learning function.

Platform Description N/A

12.14 vrrp timers learn

Use this command to enable the timer learning function.

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

vrrp [**ipv6**] *group* **timers learn**

no vrrp [**ipv6**] *group* **timers learn**

Parameter Description

Parameter	Description
ipv6	Applies to IPv6 VRRP.

group	VRRP group number

Defaults This function is disabled by default. Even if the VRRP function is enabled, the timer learning function is disabled by default.

Command Mode Interface configuration mode

Usage Guide Once the timer learning function is enabled, if the current device is a VRRP backup device, it will learn the VRRP advertisement interval from the VRRP advertisement of the master device, with which it calculates the master device's failure interval instead of the VRRP advertisement interval configured locally. This command may synchronize the VRRP advertisement timer with the master device.

Configuration Examples The following example enables the timer learning function on the IPv4 VRRP group 1.

```
Ruijie#configure terminal
Ruijie(config)#interface GigabitEthernet 0/0
Ruijie(config-if-GigabitEthernet 0/0)#no switchport //used on the switch.
Ruijie(config-if-GigabitEthernet 0/0)#ip address 10.0.1.1 255.255.255.0
Ruijie(config-if-GigabitEthernet 0/0)#vrrp 1 ip 10.0.1.20
Ruijie(config-if-GigabitEthernet 0/0)#vrrp 1 timers learn
```

The following example to enables the timer learning function on the IPv6 VRRP group 1.

```
vrrp ipv6 1 timers learn
Ruijie#configure terminal
Ruijie(config)#interface GigabitEthernet 0/0
Ruijie(config-if-GigabitEthernet 0/0)#no switchport //used on the switch.
Ruijie(config-if-GigabitEthernet 0/0)#ipv6 enable
Ruijie(config-if-GigabitEthernet 0/0)#ipv6 address 2001::2/64
Ruijie(config-if-GigabitEthernet 0/0)#vrrp 1 ipv6 FE80::1
Ruijie(config-if-GigabitEthernet 0/0)#vrrp 1 ipv6 2001::1
Ruijie(config-if-GigabitEthernet 0/0)#vrrp ipv6 1 timers learn
```

Related Commands

Command	Description
vrrp *group* **ip** *ipaddress* [**secondary**]	Enables the VRRP function and set the IP address for the virtual device.
vrrp *group* **ipv6** *ipaddress*	Enables the VRRP function and set the IPv6 address for the virtual device.
vrrp *group* **timers advertise** *interval*	Sets the IPv4 VRRP advertising interval.
vrrp ipv6 *group* **timers advertise** *interval*	Sets the IPv6 VRRP advertising interval.

Platform Description N/A

12.15 vrrp track

Use these commands to enable the IPv4/IPv6 VRRP track in the interface configuration mode. Use the no form of these commands to restore the default setting.

vrrp *group* **track** *interface-type interface-number* [*priority*]

vrrp ipv6 *group* **track** *interface-type interface-number* [*priority*]

no vrrp [**ipv6**] *group* **track** *interface-type interface-number*

Use these commands to enable VRRP IPv4/IPv6 address track. Use the **no** form of these commands to restore the default setting.

vrrp *group* **track** *ipv4-address* [**interval** *interval-value*] [**timeout** *timeout-value*] [**retry** *retry-value*] [*priority*]

vrrp ipv6 *group* **track** { *ipv6-global-address* | *ipv6-linklocal-address interface-type interface-number* } [**interval** *interval-value*] [**timeout** *timeout-value*] [**retry** *retry-value*] [*priority*]

no vrrp *group* **track** *ipv4-address*

no vrrp ipv6 *group* **track** { *ipv6-global-address* | *ipv6-linklocal-address interface-type interface-number* }

Parameter Description

Parameter	Description
group	VRRP group number
interface-type interface-number	Type of monitored interface
priority	VRRP priority change range when the interface or ip address reachability status changes. If this parameter is not selected, the default value is 10.
ipv6	Applies to IPv6 VRRP.
ipv4-address	Monitored IPv4 address. With BFD configured, it refers to the neighbor IP address.
interval *interval-value*	The interval of time to probe whether the monitored ip address is reachable or not. If this parameter is not selected, the default value is 3 seconds.
timeout *timeout-value*	The timeout time of the unreachable monitored ip address. If this parameter is not selected, the default value is 1 seconds.
retry *retry-value*	Track retries. If the value is reached, the link is thought unreachable. If this parameter is not configured, the default value is 3.
ipv6-global-address	Global unicast IPv6 address
ipv6-linklocal-address	Local link IPv6 address

Defaults This function is disabled by default. Even if the VRRP function is enabled, no interface or IP address is specified.

Command Interface configuration mode

Mode

Usage Guide

- This command can be used to monitor the outlet links. Note that layer-3 routable logical interfaces can be monitored (such as Routed Port, SVI, Loopback and Tunnel).
- If a host is monitored, specify the IPv4 address for the IPv4 VRRP router or the IPv6 address for the IPv6 VRRP router.
- If the host IP address is link-local, an interface must be specified.
- If a VRRP router owns the IP address of the physical interface, the priority is 255. No monitored IP addresses or monitored interfaces can be configured.

Configuration Examples

The following example enables the VRRP group 1 to monitor the routed port Fa1/1. If the Fa1/1 link is disconnected, the priority of the VRRP group decreases by 30. When the Fa1/1 link recovers, the priority of VRRP group 1 is restored.

```
Ruijie#configure terminal
Ruijie(config)#interface  GigabitEthernet 0/0
Ruijie(config-if-GigabitEthernet 0/0)#no switchport //used on the switch.
Ruijie(config-if-GigabitEthernet 0/0)#ip address 10.0.1.1 255.255.255.0
Ruijie(config-if-GigabitEthernet 0/0)#vrrp 1 ip 10.0.1.20
Ruijie(config-if-GigabitEthernet 0/0)#vrrp 1 priority 254
Ruijie(config-if-GigabitEthernet 0/0)#vrrp 1 track GigabitEthernet 1/1 30
```

The following example enables IPv6 VRRP on the interface GigabitEthernet 0/0. The VRRP group 1 monitors reachability of the host 1000::1.

```
Ruijie#configure terminal
Ruijie(config)#interface GigabitEthernet 0/0
Ruijie(config-if-GigabitEthernet 0/0)#no switchport //used on the switch.
Ruijie(config-if-GigabitEthernet 0/0)#no switchport
Ruijie(config-if-GigabitEthernet 0/0)#ipv6 enable
Ruijie(config-if-GigabitEthernet 0/0)#ipv6 address 2001::2/64
Ruijie(config-if-GigabitEthernet 0/0)#vrrp 1 ipv6 FE80::1
Ruijie(config-if-GigabitEthernet 0/0)#vrrp 1 ipv6 2001::1
Ruijie(config-if-GigabitEthernet 0/0)#vrrp ipv6 1 priority 254
Ruijie(config-if-GigabitEthernet 0/0)#vrrp ipv6 1 track 1000::1
```

The following example enables IPv6 VRRP on the interface GigabitEthernet 0/0. The VRRP group 1 monitors reachability of the host `FE80::2` on VLAN 1. Note that a network interface should be specified.

```
Ruijie#configure terminal
Ruijie(config)#interface GigabitEthernet 0/0
Ruijie(config-if-GigabitEthernet 0/0)#no switchport //used on the switch.
Ruijie(config-if-GigabitEthernet 0/0)#no switchport
Ruijie(config-if-GigabitEthernet 0/0)#ipv6 enable
```

```
Ruijie(config-if-GigabitEthernet 0/0)#ipv6 address 2001::2/64
Ruijie(config-if-GigabitEthernet 0/0)#vrrp 1 ipv6 FE80::1
Ruijie(config-if-GigabitEthernet 0/0)#vrrp 1 ipv6 2001::1
Ruijie(config-if-GigabitEthernet 0/0)#vrrp ipv6 1 priority 254
Ruijie(config-if-GigabitEthernet 0/0)#vrrp ipv6 1 track FE80::2 vlan 1
```

Related Commands

Command	Description
vrrp *group* **ip** *ipaddress* [**secondary**]	Enables the VRRP function and set the IP address for the virtual device.
vrrp *group* **priority** *level*	Sets the VRRP group priority.

Platform Description N/A

12.16 vrrp version

Use this command to configure the version of sending the IPv4 VRRP multicast packets.
For the IPv4 VRRP, there are two versions: VRRPv2 and VRRPv3.
Use the **no** form of this command to restore the default setting.
vrrp *group* **version** { **2** | **3** }
no vrrp *group* **version**

Parameter Description

Parameter	Description
2	Uses the VRRPv2 version to send the packets.
3	Uses the VRRPv3 version to send the packets.

Defaults The default is VRRPv2.

Command Mode Interface configuration mode

Usage Guide Considering the compatibility of VRRPv2 and VRRPv3 for the IPv4 VRRP, you can choose the version of VRRP packets based on the actual network environment. VRRPv2 is based on RFC3768 and VRRPv3 is based on RFC 5798.

This command is applicable to IPv4 VRRP only.

Configuration Examples The following example configures the version of sending the IPv4 VRRP packets on the interface gi0/0.

```
Ruijie#configure terminal
Ruijie(config)#interface GigabitEthernet 0/0
Ruijie(config-if-GigabitEthernet 0/0)#no switchport //used on the switch.
Ruijie(config-if-GigabitEthernet 0/0)#ip address 10.0.1.1 255.255.255.0
```

```
Ruijie(config-if-GigabitEthernet 0/0)#vrrp 1 ip 10.0.1.20
Ruijie(config-if-GigabitEthernet 0/0)# vrrp 1 version 3
```

Related Commands

Command	Description
vrrp *group* **ip** *ipaddress* [**secondary**]	Enables the VRRP function and set the IP address for the virtual device.
vrrp *group* **timers advertise** *interval*	Sets the interval of sending the VRRP advertisement.

Platform Description N/A

13 IGMP Snooping Commands

13.1 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

13.2 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

13.3 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 N/A

Description

13.4 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

13.5 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

13.6 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

13.7 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

13.8 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

13.9 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

13.10 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 Mode Global configuration mode

Usage Guide After globally enabling the IGMP querier, you must enable the IGMP querier function in VLAN to activate this function.
If the IGMP querier function is disabled globally, the IGMP querier will be disabled in all VLANs.

Configuration Examples The following example enables the IGMP querier function in VLAN 2.

```
Ruijie(config)# ip igmp snooping querier
Ruijie(config)# ip igmp snooping vlan 2 querier
```

Platform Description N/A

13.11 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

13.12 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

13.13 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

13.14 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

13.15 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 N/A

Description

13.16 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

13.17 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

13.18 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

13.19 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

13.20 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

13.21 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

13.22 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

13.23 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

14 ACL

14.1 command ID table

For IDs used in the following commands, refer to the command ID table below:

ID	Meaning
ID	Number of access list. Range: Standard IP ACL: 1 to 99, 1300 to 1999 Extended IP ACL: 100 to 199,2000 to 2699 Extended MAC ACL: 700 to 799 Extended expert ACL: 2700 to 2899
name	ACL name
sn	ACL SN (products can be set according to the priority)
start-sn	Start sequence number
inc-sn	Sequence number increment
deny	If matched, access is denied.
permit	If matched, access is permitted.
port	Protocol number. For IPv6, this field can be IPv6, ICMP, TCP, UDP and numbers 0 to 255. For IPv4, it can be one of EIGRP, GRE, IPINIP, IGMP, NOS, OSPF, ICMP, UDP, TCP,AHP, ESP, PCP, PIM and IP, or it can be numbers 0 to 255 that represent the IP protocol. It is described when some important protocols, such as ICMP, TCP and UDP, are listed individually.
interface *idx*	Interface index
src	Packet source IP address (host address or network address)
src-wildcard	Source IP address wildcard. It can be discontinuous, for example, 0.255.0.32.
src-ipv6-pfix	Source IPv6 network address or network type
dst-ipv6-pfix	Destination IPv6 network address or network type
pfix-len	Prefix mask length
src-ipv6-addr	Source IPv6 address
dst-ipv6-addr	Destination IPv6 address
dscp	Differential service code point, and code point value. Range: 0 to 63
flow-label	Flow label in the range 0 to 1048575
dst	Packet destination IP address (host address or network address)
dst-wildcard	Destination IP address wildcard. It can be discontinuous, such as 0.255.0.32
fragment	Packet fragment filtering. (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) *port* indicates the port number. Dyadic operation needs two port numbers, while other operators only need one port number
src-mac-addr	Physical address of the source host
dst-mac-addr	Physical address of the destination host
VID vid	VLAN ID
VID inner vid	VID of the tag
ethernet-type	Ethernet protocol type. 0x value can be entered.
match-all *tcpf*	Match all bits of the TCP flag.
established	Match the RST or ACK bit of the TCP flag.
text	Remark text
in	Filter the incoming packets of the interface
out	Filter the outgoing packets of the interface
{rule mask offset}$^{+}$	rule: Hexadecimal value field; mask: Hexadecimal mask field offset: Refer to the offset table "+" sign indicates at least one group
log	Output the matching syslog when the packet matches the ACL rule.

The fields in the packet are as follows:

AA AA AA AA AA AA BB BB BB BB BB BB CC CC DD DD

DD DD EE FF GG HH HH HH II II JJ KK LL LL MM MM

NN NN OO PP QQ QQ RR RR RR RR SS SS SS SS TT TT

UU UU VV VV VV VV WW WW WW WW XY ZZ aa aa bb bb

The corresponding offset table is as follows:

Letter	Meaning	Offset	Letter	Meaning	Offset
A	Destination MAC	0	O	TTL field	34
B	Source MAC	6	P	Protocol number	35

C	Data frame length field	12	Q	IP check sum	36
D	VLAN tag field	14	R	Source IP address	38
E	DSAP (Destination Service Access Point) field	18	S	Destination IP address	42
F	SSAP (Source Service Access Point) field	19	T	TCP source port	46
G	Ctrl field	20	U	TCP destination port	48
H	Org Code field	21	V	Sequence number	50
I	Encapsulated data type	24	W	Confirmation field	54
J	IP version number	26	XY	IP header length and reserved bits	58
K	TOS field	27	Z	Resrved bits and flags bit	59
L	Length of IP packet	28	a	Windows size field	60
M	ID	30	b	Others	62
N	Flags field	32			

The offsets of fields in the above table are their offsets in 802.3 data frames of SNAP+tag.

14.2 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

14.3 access-list list-remark

Use this command to write a helpful comment (remark) for an access list. Use the **no** form of this command to remove the remark.

access-list *id* **list-remark** *text*

no access-list *id* **list-remark**

Parameter Description

Parameter	Description
id	Access list number. Standard IP ACL: 1 to 99, 1300 to 1999. Extended IP ACL: 100 to 199. 2000 to 2699. Extended MAC ACL: 700 to 799. Extended Expert ACL: 2700 to 2899.
text	Comment that describes the access list.

Defaults The access lists have no remarks by default.

Command Mode Global configuration mode

Usage Guide You can use this command to write a helpful comment for a specified access list. If the specified access list does not exist, the command will create the access list, then add remarks for the access list.

Configuration Examples The following example writes a comment of “this acl is to filter the host 192.168.4.12” for ACL100.

```
Ruijie(config)# ip access-list extended 100
Ruijie(config)# access-list 100 list-remark this acl is to filter the host
192.168.4.12
```

Related Commands

Command	Description
show access- lists	Displays all access lists, including the remarks for the access lists.

show access-lists *id*	Displays the access list of a specified number, including the remarks for the access list.
show access-lists *name*	Displays the access list of a specified name, including the remarks for the access list.

Platform Description

14.4 access-list remark

Use this command to write a helpful comment (remark) for an entry in a numbered access list. Use the **no** form of this command to remove the remark.

access-list *id* **remark** *text*

no access-list *id* **remark** *text*

Parameter Description

Parameter	Description
id	Access list number. Standard IP ACL: 1 to 99, 1300 to 1999. Extended IP ACL: 100 to 199. 2000 to 2699. Extended MAC ACL: 700 to 799. Extended Expert ACL: 2700 to 2899.
text	Comment that describes the access list entry.

Defaults The access list entries have no remarks by default.

Command Mode Global configuration mode

Usage Guide You can use this command to write a helpful comment for an entry in a specified access list. If the specified access list does not exist, the command will create the access list, then add remarks for the access entry.

Configuration Examples The following example writes a comment for an entry in ACL102.

```
Ruijie(config)# access-list 102 remark deny-host-10.1.1.1
```

Related Commands

Command	Description
show access-lists	Displays all access lists, including the remarks for the access list entries.
show access-lists *id*	Displays the access list of a specified number, including the remarks for the access list entry.
show access-lists *name*	Displays the access list of a specified name,

	including the remarks for the access list entry.

Platform

Description

14.5 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

14.6 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 The following example applies the expert ACL named **accept_00d0f8xxxxxx_only** to Gigabit

Examples 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

14.7 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

14.8 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 Description N/A

14.9 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: 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

14.10 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: Standard: 1 to 99, 1300 to 1999; 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

14.11 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: Standard IP access list: 1 to 99, 1300 to 1999; Extended IP access list: 100 to 199, 2000 to 2699.
name	Name of the standard or extended IP access list
start-sn	Start sequence number. Range: 1 to 2147483647
inc-sn	Increment of the sequence number. Range: 1 to 2147483647

Defaults

start-sn: 10

inc-sn: 10

Command mode

Global configuration mode

Usage Guide

Use this command to change the order of the access entries.

Configuration Examples

The following example resequences entries of ACL1:

Before the configuration:

```
Ruijie# show access-lists
ip access-list standard 1
10 permit host 192.168.4.12
20 deny any any
```

After the configuration:

```
Ruijie# config
Ruijie(config)# ip access-list resequence 1 21 43
Ruijie(config)# exit
Ruijie# show access-lists
ip access-list standard 1
21 permit host 192.168.4.12
64 deny any any
```

Related Commands

Command	Description
show access-lists	Displays all access lists..

Platform Description N/A

14.12 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

14.13 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

14.14 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

14.15 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

14.16 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 Commands

Command	Description
show access-group	Displays the ACL configuration on the interface.

Platform Description N/A

14.17 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

14.18 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 Description N/A

14.19 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

14.20 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

Command	Description

Commands

show access-lists	Displays all access lists.
ip access-list	Defines an IP access list.

Platform Description N/A

14.21 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

14.22 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

14.23 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

14.24 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

14.25 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

14.26 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

14.27 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

14.28 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

14.29 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 Privileged EXEC mode

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

14.30 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 N/A

Description

15 TACACS+ Commands

15.1 aaa group server tacacs+

Use this command to configure different groups of TACACS+ server hosts.
Use the **no** form of this command to remove a specified TACACS server group.
aaa group server tacacs+ *group_name*
no aaa group server tacacs+ *group_name*

Parameter Description

Parameter	Description
group_name	TACACS+ server group name, which cannot be **radius** or **tacacs+** The two names are the built-in group name.

Defaults No TACACS+ server group is configured.

Command Mode Global configuration mode

Usage Guide After you group different TACACS+ servers, the tasks of authentication, authorization and accounting can be implemented by different server groups.

Configuration Examples The following example configures a TACACS+ server group named tac1, and configures a TACACS+ server with IP address 1.1.1.1 in this group:

```
Ruijie(config)#aaa group server tacacs+ tac1
Ruijie(config-gs-tacacs+)# server 1.1.1.1
```

Related Commands

Command	Description
server	Configures server list of TACACS+ server group.
ip vrf forwarding	Configures VRF name supported by TACACS+ server group.

Platform Description N/A

15.2 ip tacacs source-interface

Use this command to use the IP address of a specified interface for all outgoing TACACS+ packets.

Use the **no** form of this command to disable use of the specified interface IP address.

ip tacacs source-interface *interface-name*

no ip tacacs source-interface *interface-name*

Parameter Description

Parameter	Description
interface-name	Interface for the outgoing TACACS+ packets

Defaults The source IP address of TACACS+ packets is set on the network layer.

Command Mode Global configuration mode

Usage Guide To decrease the work of maintaining massive NAS messages in TACACS+ server, use this command to use the IP address of a specified interface for all outgoing TACACS+ packets.
This command specifies the primary IP address of the specified interface as the source address of TACACS+ packets on Layer 3 devices. If the specified interface is in a VRF instance, the route of this VRF instance is used for packet transmission.

Configuration Examples The following example specifies the IP address of GigabitEthernet 0/0 for the outgoing TACACS+ packets.

```
Ruijie(config)# ip tacacs source-interface gigabitEthernet 0/0
```

Related Commands

Command	Description
tacacs-server host	Defines a TACACS+ server.
ip address	Configures the IP address of an interface.

Platform Description N/A

15.3 ip oob

Use this command to specify the MGMT port used in the TACACS+ server group.
Use the **no** form of this command to restore the default setting.

ip oob [**via** *mgmt_name*]

no ip oob

Parameter Description

Parameter	Description
mgmt_name	MGMT port name

Defaults N/A

Command Mode TACACS+ server group configuration mode

Usage Guide Use the **aaa group server tacacs+** command to enter TACACS+ server group configuration mode. No MGMT port is specified by default.

Configuration Examples The following example specifies MGMT port 1 used in the TACACS+ server group.

```
Ruijie(config)# aaa group server tacacs+ ss
Ruijie(config-gs-tacacs+)# server 1.1.1.1
Ruijie(config-gs-tacacs+)# ip oob via mgmt 1
```

Platform Description N/A

15.4 server

Use this command to configure the IP address of the TACACS+ server for the group server.
Use the **no** form of this command to remove the TACACS+ server.
server { *ipv4-address* | *ipv6-address* }
no server { *ipv4-address* | *ipv6-address* }

Parameter Description

Parameter	Description
ipv4-address	IPv4 address of the TACACS+ server
ipv6-address	IPv6 address of the TACACS+ server

Defaults No TACACS+ server is configured by default.

Command Mode TACACS+ server group configuration mode

Usage Guide You must configure the **aaa group server tacacs+** command before configuring this command.
To configure server address in TACACS+ group server, you must use the **tacacs-server host** command in global configuration mode.
If there is no response from the first host entry, the next host entry is tried.

Configuration Examples The following example configures a TACACS+ server group named tac1 and a TACACS+ server address 1.1.1.1 in this group.

```
Ruijie(config)#aaa group server tacacs+ tac1
Ruijie(config-gs-tacacs+)# server 1.1.1.1
```

Related

Command	Description

Commands		
	aaa group server tacacs+	Configures a TACACS+ server group.

Platform Description N/A

15.5 show tacacs

Use this command to display the TACACS+ server configuration.

show tacacs

Parameter Description

Parameter	Description
N/A	N/A

Defaults N/A

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

Usage Guide N/A

Configuration Examples The following example displays the TACACS+ server configuration.

```
Ruijie# show tacacs
Tacacs+ Server : 172.19.192.80/49
Socket Opens: 0
Socket Closes: 0
Total Packets Sent: 0
Total Packets Recv: 0
Reference Count: 0
```

Related Commands

Command	Description
tacacs-server host	Defines a TACACS+ secure server host.

Platform Description N/A

15.6 tacacs-server host

Use this command to configure a TACACS+ host.

Use the **no** form of this command to remove the TACACS+ host.

tacacs-server host {*ipv4-address* | *ipv6-address*} [**port** *integer*] [**timeout** *integer*] [**key** [**0** | **7**] *text-string*]

no tacacs-server host { *ip-address* | *ipv6-address* }

Parameter Description

Parameter	Description
ip-address	IPv4 address of the TACACS+ host
ipv6-address	IPv6 address of the TACACS+ host
port *integer*	Port number of the server. The range is from 1 to 65,535. The default is 49.
timeout *integer*	Timeout time of TACACS+ host. The range is from 1 to 1,000.
key *string*	Configures an authentication and encryption key. The value can be 0 or 7. 0 indicates no encryption, while 7 indicates simple encryption. The default is 0.

Defaults No TACACS+ host is specified by default.

Command Mode Global configuration mode

Usage Guide The TACACS+ host must be configured to implement AAA security service You can use this command to configure one or multiple TACACS+ hosts.

Configuration Examples The following example configures a TACACS+ host.

```
Ruijie(config)# tacacs-server host 192.168.12.1
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

15.7 tacacs-server key

Use this command to configure the authentication encryption key used for TACACS+

communications between the access server and the TACACS+ server.

Use the **no** form of this command to remove the authentication encryption key.

tacacs-server key [**0** | **7**] *string*

no tacacs-server key

Parameter Description

Parameter	Description
string	Key string
**0	7**	Encryption type of key 0 indicates no encryption; 7 indicate simple encryption.

Defaults No authentication encryption key is configured by default.

Command Mode Global configuration mode

Usage Guide Use command to configure a global authentication and encryption key for TACACS+ communication.

Use the **key** parameter in the **tacacs-server host** command to configure a server-based key.

Configuration Examples The following example defines the authentication encryption key of TACACS+ server as aaa:

```
Ruijie(config)# tacacs-server key aaa
```

Related Commands

Command	Description
tacacs-server host	Defines a TACACS+ host.

Platform Description N/A

15.8 tacacs-server timeout

Use this command to set the interval for which the server waits for a server host to reply. Use the **no** form of this command to restore the default timeout interval.

tacacs-server timeout *seconds*

no tacacs-server timeout

Parameter Description

Parameter	Description
seconds	Timeout interval in the range from 1 to 1,000 in the unit of seconds

Defaults The default is 5 seconds.

Command Mode Global configuration mode

Usage Guide Use command to configure a global timeout interval. Use the **timeout** parameter in the **tacacs-server host** command to configure a server-based interval.

Configuration Examples The following example configures the timeout interval to 10 seconds.

```
Ruijie(config)# tacacs-server timeout 10
```

Related Commands

Command	Description
tacacs-server host	Defines a TACACS+ secure server host.

Platform Description N/A

16 SCC Commands

16.1 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

16.2 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

16.3 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

16.4 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

16.5 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

16.6 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

16.7 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

16.8 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

Parameter	Description

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

16.9 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

16.10 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	

17 Password-Policy Commands

17.1 password policy life-cycle

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

password policy life-cycle days

no password policy life-cycle

Parameter Description

Parameter	Description
days	Sets the password lifecycle, in the range from 1 to 65535 in the unit of days.

Defaults No password lifecycle is set by default.

Command Mode Global configuration mode

Usage Guide This command is used to set the password lifecycle. After the password lifecycle expires, the system reminds you to change the password when you login next time.

This function is valid for the global password (the **enable password** and the **enable secret** commands) and the local user password (the **username** *name* **password** *password* command) while not valid for the password in line mode.

Configuration Examples The following example sets the password lifecycle to 90 days.

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

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

17.2 password policy min-size

Use this command to set the minimum length of the password. Use the **no** form of this command to restore the default setting.

password policy min-size *length*

no password policy min-size

Parameter Description

Parameter	Description
length	Sets the minimum length of the password, in the range from 1 to 31.

Defaults No minimum length of the password is set by default.

Command Mode Privileged EXEC mode

Usage Guide This command is used to set the minimum length of the password,

> This function is valid for the global password (the **enable password** and the **enable secret** commands) and the local user password (the **username** *name* **password** *password* command) while not valid for the password in line mode.

Configuration Examples The following example sets the minimum length of the password to 8.

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

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

17.3 password policy no-repeat-times

Use this command to ban the use of passwords used in the past several times. Use the no form of this command to restore the default setting.

password policy no-repeat-times *times*

no password policy no-repeat-times

Parameter Description

Parameter	Description
times	The past several times when passwords are configured, in the range from 1 to 31.

Defaults This function is disabled by default.

Command Mode Global configuration mode

Usage Guide After this function is enabled, passwords used in the past several times are recorded. If the new password has been used, the alarm message is displayed and password configuration fails.
This command is used to set the maximum number of password entries. When the actual number of password entries exceeds the configured number, the new password overwrites the oldest password.

> This function is valid for the global password (the **enable password** and the **enable secret** commands) and the local user password (the **username** *name* **password** *password* command) while not valid for the password in line mode.

Configuration Examples The following example bans the use of passwords used in the past five times.

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

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

password policy secret-dictionary

Use this command to configure the week password. Use the **no** form of this command to restore the default.

password policy secret-dictionary weak *password*
no password policy secret-dictionary weak [*password*]

Parameter Description

Parameter	Description
password	Configures the weak password.

Defaults No weak password is configured.

Command Mode Global configuration mode

Usage Guide If you set a password consistent with the weak password, the password is considered invalid and a prompt is displayed to inform setting failure.
This command is is configured for only global passwords (configurd by the **enable password** and **enable secret** commands) and local user passwords (configurd by the commands).

Configuration The following example configures weak password “admin”.

Examples

```
Ruijie(config)# password policy secret-dictionary weak admin
```

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

17.4 password policy strong

Use this command to enable strong password check.

password policy strong

no password policy strong

Parameter Description

Parameter	Description
N/A	N/A

Defaults

This function is disabled by default.

Command Mode

Global configuration mode

Usage Guide

If the following two kinds of passwords are set not matching the strength policy, the alarm message is displayed.

1. The password the same as the username.
2. The simple password containing only characters or numbers.

This function is valid for the global password (the **enable password** and the **enable secret** commands) and the local user password (the **username** *name* **password** *password* command) while not valid for the password in line mode.

Configuration Examples

The following example configures the strong password check.

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

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

17.5 service password-encryption

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

service password-encryption

no service password-encryption

Parameter Description

Parameter	Description
N/A	N/A

Defaults This function is disabled by default.

Command Mode Global configuration mode

Usage Guide This command is disabled by default. Various passwords are displayed in plain text, unless they are encrypted. After you run the **service password-encryption** and **show running** or **write** command to save your configuration, the password changes into cipher text. If you disable the command, the password in cipher text cannot be restored to plain text.

Configuration Examples The following example encrypts the password:

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

Related Commands

Command	Description
enable password	Sets passwords of different privileges.

Platform Description N/A

17.6 show password policy

Use this command to display the password security policy set by the user.

show password policy

Parameter Description

Parameter	Description
N/A	N/A

Defaults N/A

Command Privileged EXEC mode

Mode

Usage Guide This command is used to display the password security policy set by the user.

Configuration Examples The following example displays the password security policy set by the user.

```
Ruijie#show password policy
Global password policy configurations:
 Password encryption:              Enabled
 Password strong-check:            Enabled
 Password min-size:                Enabled (6 characters)
 Password life-cycle:              Enabled (90 days)
 Password no-repeat-times:          Enabled (max history record: 5)
```

Field	Description
Password encryption	Whether to encrypt the password.
Password strong-check	Whether to enable password strong-check.
Password min-size	Whether to set the minimum length of the password.
Password life-cycle	Whether to set the password lifecycle.
Password no-repeat-times	

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

18 SSH Commands

18.1 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

18.2 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

18.3 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

18.4 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

18.5 ip scp server topdir

Use this command to set the path for uploading/downloading files to/from the SCP server.

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

ip scp server topdir {flash:/*path* **| flash2:/***path* **| usb0:/***path* **| usb1:/***path* **| sd0:/***path* **| sata0:/***path* **| tmp:/***path* **}**

no ip scp server topdir

Parameter Description	Parameter	Description
	flash	Selects the file transfer path from the extended flash memory. The file transfer path is **flash:/** by default.
	flash2	Selects the file transfer path from Extended Flash Memory 2. This option is supported only when the device has the data2 partition.
	usb0	Selects the file transfer path from USB Disk 0. This option is supported only when the device has one USB interface and is connected with an extended USB device.
	usb1	Selects the file transfer path from USB Disk 1. This option is supported only when the device has two USB interfaces and is connected with extended USB devices.
	sd0	Selects the file transfer path from the SD card. This option is supported only when the device has an SD card interface and is connected with an extended SD card.
	sata0	Selects the file transfer path from the hard disk. This option is supported only when the device has the SATA partition.
	tmp	Sets the file transfer path to **tmp/vsd/**.

Defaults The file transfer path is **flash:/** by default.

Command Mode Global configuration mode

Default Level 14

Usage Guide This command is used to change the file transfer path for uploading and downloading files.

Configuration The following example changes the file transfer path to **tmp/vsd**.

Examples

```
Ruijie# configure terminal
Ruijie(config)# ip scp server topdir tmp:/
```

18.6 ip ssh authentication-retries

Use this command to set the authentication retry times of the SSH server.
Use the **no** form of this command to restore the default setting.
ip ssh authentication-retries *retry times*
no ip ssh authentication-retries

Parameter 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

18.7 ip ssh cipher-mode

Use this command to set the SSH server encryption mode.
Use the **no** form of this command to restore the default setting.
ip ssh cipher-mode { **cbc** | **ctr** | **others** }
no ip ssh cipher-mode

Parameter Description

Parameter	Description
cbc	Encryption mode: CBC (Cipher Block Chaining) Encryption algorithm: DES-CBC, 3DES-CBC, AES-128-CBC, AES-192-CBC, AES-256-CBC, Blow fish-CBC

ctr	Encryption mode: CTR (Counter) Encryption algorithm: AES128-CTR, AES192-CTR, AES256-CTR
others	Encryption mode: Others Encryption algorithm: RC4

Defaults All encryption modes are supported by default.

Command Mode Global configuration mode

Usage Guide 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

18.8 ip ssh hmac-algorithm

Use this command to set the algorithm for message authentication.
Use the **no** form of this command to restore the default setting.
ip ssh hmac-algorithm { **md5** | **md5-96** | **sha1** | **sha1-96** }
no ip ssh hmac-algorithm

Parameter 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

18.9 ip ssh peer

Use this command to associate the public key file and the user name on the client. During client login authentication, you can specify a public key file based on the user name.
Use the **no** form of this command to restore the default setting.
ip ssh peer *username* **public-key** { **rsa** | **dsa** } *filename*
no ip ssh peer *username* **public-key** { **rsa** | **dsa** } *filename*

Parameter 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

18.10 ip ssh port

Use this command to set a monitoring port ID for the SSH server.
ip ssh port *port*

Use either of the following commands to restore the monitoring port ID of the SSH server to the default value.
no ip ssh port
ip ssh port 22

Parameter Description

Parameter	Description
port	Monitoring port ID of the SSH server. The value ranges from 1025 to 65535.

Defaults N/A

Command Mode Global configuration mode

Default Level 14

Usage Guide N/A

Configuration Examples The following example sets the monitoring port ID of the SSH server to 10000.

```
Ruijie# configure terminal
Ruijie(config)# ip ssh port 10000
```

Verification Run the **show ip ssh** command to display the configured monitoring port ID of the SSH server.

Prompts 1. If the required port ID is the same as the current value, a prompt is displayed, indicating that the current port ID is the required value.

```
Ruijie(config)# ip ssh port 22
% SSH tcp-port has been 22
```

2. If a port in the monitoring state is configured as the monitoring port of the SSH server, a prompt is displayed, indicating that the port is already in the monitoring state and you are required to set another port ID, and the SSH server still uses the previous port ID.

```
Ruijie(config)# ip ssh port 10000
% SSH open tcp-port(10000) failed, please use another tcp-port, otherwise the system
will use the old tcp-port(22)!
```

3. If a monitoring error occurs after a monitoring port ID is configured for the SSH server, a port ID configuration failure prompt is displayed.

```
Ruijie(config)# ip ssh port 10000
```

```
% SSH change to tcp-port(10000) fail!
```

4. If a port ID is configured successfully, a port ID configuration success prompt is displayed.

```
Ruijie(config)# ip ssh port 10000
% SSH change to tcp-port(10000) success!
```

18.11 ip ssh time-out

Use this command to set the authentication timeout for the SSH server.

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

ip ssh time-out *time*

no ip ssh time-out

Parameter Description

Parameter	Description
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

18.12 ip ssh version

Use this command to set the version of the SSH server.

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

ip ssh version { **1** | **2** }

no ip ssh version

Parameter 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

18.13 show crypto key mypubkey

Use this command to display the information about the public key part of the public key to the SSH server.

show crypto key mypubkey { **rsa | dsa** }

Parameter 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

18.14 show ip ssh

Use this command to display the information of the SSH server.

show ip ssh

Parameter Description

Parameter	Description
N/A	N/A

Defaults N/A

Command 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, port number, encryption mode, message authentication algorithm, 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
SSH Port:            22
SSH Cipher Mode:       cbc,ctr,others
SSH HMAC Algorithm:    md5-96,md5,sha1-96,sha1
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
SSH Port:            22
SSH Cipher Mode:       cbc,ctr,others
SSH HMAC Algorithm:    md5-96,md5,sha1-96,sha1
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

18.15 show ssh

Use this command to display the information about the established SSH connection.

show ssh

Parameter Description

Parameter	Description
N/A	N/A

Defaults N/A

Command 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

19 GSN Commands

19.1 gsn address-bind

Use this command to enable GSN address binding in a WLAN.
Use the **no** form of this command to disable this function.
gsn address-bind
no gsn address-bind

Parameter Description

Parameter	Description
N/A	N/A

Defaults GSN address binding is disabled.

Command Mode WLAN security configuration mode

Usage Guide This command takes effect only when the global security network (GSN) function is enabled and the WLAN security mode is WPA or WPA2.
802.1x IP authorization should be disabled when the GSN address binding policy is applied.

Configuration Examples The following example enables GSN address binding on WLAN 100.

```
Ruijie(config)# wlansec 100
Ruijie(config-wlansec)# gsn address-bind
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

19.2 security community

Use this command to configure the security community to communicate with the SMP server.
Use the **no** form of this command to remove the security community setting.
security { [**v1 | v2**] **community** *community* | **v3 user** *username* }
no security { [**v1 | v2**] **community** *community* | **v3 user** *username* }

Parameter

Parameter	Description

Description

community	Community string containing up to 32 characters.
username	V3 security community username, containing up to 32 characters.

Defaults No security community is configured by default.

Command Mode Global configuration mode

Usage Guide When you are configuring the communication between the device and the server, configure an appropriate authentication name of the appropriate protocol version according to the server settings if it is necessary. If you choose v3, use the **snmp-server** command to set the v3 username. For the detailed information, please refer to *SNMP command reference*.

Configuration Examples The following example sets the v1 community:

```
Ruijie(config)# security v1 community public
```

The following example sets the v3 username as start:

```
Ruijie(config)# security v3 user start
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

19.3 security event interval

Use this command to set the sending interval of security events.
Use the **no** form of this command to restore the default value.
security event interval *interval*
no security event interval

Parameter Description

Parameter	Description
interval	Configures the security event interval. The range is from 1 to 65,535 seconds.

Defaults The default interval is 5 seconds.

Command Mode Global configuration mode

Usage Guide Take care to set the sending interval of security events properly. Too small value may cause the drop of security event messages, and too large value may cause that the security event messages cannot be received in a long period.

Configuration Examples The following example configures the sending interval for security events to 10.

```
Ruijie# security event interval 10
```

The following example restores the sending interval for security events to the default setting.

```
Ruijie(config)# no security event interval
```

Related Commands

Command	Description
show security event interval	Displays the interval of security event.

Platform Description N/A

19.4 security gsn enable

Use this command to enable GSN.
Use the **no** form of this command to disable GSN.
security gsn enable
no security gsn enable

Parameter Description

Parameter	Description
N/A	N/A

Defaults GSN is disabled by default.

Command Mode Global configuration mode

Usage Guide Use this command to enable GSN on the device.

Configuration Examples The following example enables GSN.

```
Ruijie(config)# security gsn enable
```

The following example disables GSN.

```
Ruijie(config)# security gsn enable
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

19.5 show security event interval

Use this command to display the sending interval of security events.

show security event interval

Parameter Description

Parameter	Description
N/A*x*	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 sending interval of security events.

```
Ruijie# show security event interval
Event sending interval(seconds): 10
```

Related Commands

Command	Description
security event interval *interval*	Configures the sending interval of security events.

Platform Description N/A

19.6 show smp-server

Use this command to display the IP address of the SMP server.

show smp-server

Parameter Description

Parameter	Description
N/A	N/A

Defaults N/A

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

Usage Guide N/A

Configuration Examples The following example displays the IP address of the SMP server.

```
Ruijie# show smp-server
smp-server IP: 192.168.30.9
```

Related Commands

Command	Description
smp-server host	Configures the IP address for the SMP server.

Platform Description N/A

19.7 smp-server host

Use this command to configure the IP address for the SMP server.

Use the **no** form of this command to remove the IP address of the SMP server.

smp-server host *ip-address*

no smp-server host

Parameter Description

Parameter	Description
ip-address	IP address of the SMP server.

Defaults

Command Mode Global configuration mode

Usage Guide N/A

Configuration Examples The following example configures the IP address of the SMP server to 192.168.30.9.

```
Ruijie(config)# smp-server host 192.168.30.9
```

The following example removes the IP address of the SMP server.

```
Ruijie(config)# smp-server host 192.168.30.9
```

Related Commands

Command	Description
show smp-server	Displays the SMP server configuration.

Platform N/A

Description

20 SUMNG

20.1 sumng username

Use this command to enter a user identity to generate a WiFi key. Use the **no** form of this command to delete all WiFi keys of a user identity.

sumng username *uname*

no sumng username *uname*

Parameter Description	**Parameter**	**Description**
	uname	User identity of a WiFi key

Defaults N/A

Command Mode Global configuration mode

Default Level 14

Usage Guide N/A

Configuration Examples The following example adds a security account and a registered client.

```
Ruijie(config)#sumng username test
```

Verification Run the **show sumng user all** command to display the configurations.

Prompts N/A

Common Errors N/A

Platform Description N/A

20.2 sumng delete wifi-key

Use this command to delete a WiFi key.

sumng delete wifi-key ***key***

Parameter	**Parameter**	**Description**

Description	*key*	WiFi key to be deleted

Defaults N/A

Command Mode Global configuration mode

Default Level 14

Usage Guide N/A

Configuration Examples The following example deletes the WiFi key **23Q92w3AzMUJJ**.

```
Ruijie(config)#sumng delete wifi-key 23Q92w3AzMUJJ
```

Verification Run the **show sumng user all** command to display the configurations.

Prompts N/A

Common Errors N/A

Platform Description N/A

20.3 sumng log enable

Use this command to enable SUMNG to output syslogs. Use the **no** form of this command to disable the output of syslogs.

sumng log enable

no sumng log enable

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

Defaults The output of syslogs is enabled by default.

Command Mode Global configuration mode

Default Level 14

Usage Guide N/A

Configuration Examples The following example disables the output of syslogs.

```
Ruijie(config)#no sumng log enable
```

Verification Run the **show running-config** command to display the configurations.

Prompts N/A

Common Errors N/A

Platform Description N/A

20.4 sumng log rate-limit

Use this command to configure the rate limit of outputting syslogs.

sumng log rate-limit *rate*

Parameter Description

Parameter	Description
rate	Rate limit of outputting syslogs.

Defaults The rate limit is 5 syslogs per second by default.

Command Mode Global configuration mode

Default Level 14

Usage Guide The value **0** indicates no limit.

Configuration Examples The following example configures the rate limit to 10 syslogs per second.

```
Ruijie(config)#sumng log rate-limit 10
```

Verification Run the **show running-config** command to display the configurations.

Prompts N/A

Common Errors N/A

Platform Description N/A

20.5 show sumng user

Use this command to display SUMNG user information.

show sumng user {**all** | **name** *user_name*}

Parameter Description

Parameter	Description
user_name	User name, for which the corresponding account information and bound client information are to be displayed.

Command Mode Global configuration mode, privileged EXEC mode, and interface configuration mode

Default Level 14

Usage Guide N/A

Configuration Examples

```
- Ruijie#show sumng user all
Sumng Total User Num: ..................... 1
Sumng Total Sta Num: ...................... 0

    UserName                    Account-Time                Mac-Address
Reg-Time
------------------      ----------------------------      --------------
------------------------ -----------------
test             Tue Jan  3 17:29:09 2017    -            -
Ruijie#
```

Field Description

Field	Description
UserName	Name of an account
Account-Time	Start time of an account
Mac-Address	MAC address of a bound client
Reg-Time	Binding time

Prompts N/A

Platform Description N/A

System Configuration Commands

17. SPAN-RSPAN Commands
18. TIME Range 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 Privileged EXEC mode

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

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

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

```
Ruijie# disable 10
```

Related Commands

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

Platform Description N/A

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

no enable password [**level** *leve l*]

Parameter Description

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

Defaults N/A

Command Mode Global configuration mode

Usage Guide No encryption is required in general. The encryption type must be specified for copying and pasting a encrypted password for the device.
A valid password is defined as follows:

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

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

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

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

Related Commands

Command	Description
enable secret	Sets the security password

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

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

Parameter Description

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

Defaults N/A

Command Mode Global configuration mode

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

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

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

Related Commands

Command	Description
enable password	Sets passwords for different privilege levels.

Platform Description N/A

2.14 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

Parameter	Description

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 Mode LINE configuration mode

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

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

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

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

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

2.16 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 language character-set

Use this command to set a language character set.

language character-set { **UTF-8** | **GBK** | **default** }

Parameter Description

Parameter	Description
UTF-8	Specifies the UFT-8 character set,
GBK	Specifies the GBK character set.
default	Specifies the default character set.

Defaults Default

Command Mode Global configuration mode

Usage Guide If you want to set a character set in running configuration, please delete the character set configuration different from the target character set first.

Configuration Examples The following example specifies the UFT-8 character set.

```
Ruijie(config)#language character-set UTF-8
This may take some time to build configuration, Continue? (yes[no]): y
Ruijie(config)#
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

2.21 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

2.22 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

2.23 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 Login is disabled for console and enabled for VTY terminals 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 Description N/A

2.24 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 When AAA is enabled, the default authentication method is used.

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

2.25 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

Parameter	Description

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

2.26 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

2.27 password

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

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

no password

Parameter Description

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

Defaults N/A

Command Mode Line configuration mode

Usage Guide

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

2.28 prompt

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

prompt string

Parameter Description

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

Defaults N/A

Command Mode Global configuration mode

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

Configuration Examples The following example sets the prompt string to rgnos.

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

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

2.29 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

2.30 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

2.31 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

2.32 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

2.33 show running-config

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

show running-config

Parameter Description

Parameter	Description
N/A	N/A

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide N/A

Configuration Examples N/A

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

2.34 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

2.35 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

2.36 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.

Configuration Examples N/A

Related Commands

Command	Description
boot config	Sets the name of the boot configuration file.

Platform Description N/A

2.37 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 Any mode

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

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

Configuration 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

2.38 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

2.39 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.

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

2.40 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

2.41 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

2.42 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

2.43 write

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

write [**memory | terminal**]

Parameter Description

Parameter	Description
memory	Writes the system configuration (running-config) into NVRAM, which is equivalent to **copy running-config startup-config**.
terminal	Displays the system configuration, which is equivalent to **show running-config**.

Defaults N/A

Command Mode Privileged EXEC mode

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

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

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

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

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

Related Commands

Command	Description
N/A	N/A

Platform Description	N/A

3 LINE Commands

3.1 access-class

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

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

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

Parameter Description

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

Defaults N/A

Command Mode Line configuration mode

Usage Guide N/A

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

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

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

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

Related Commands

Command	Description
show running	Displays status information

Platform Description N/A

3.2 accounting commands

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

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

no accounting commands *level*

Parameter Description

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

Defaults This function is disabled by default.

Command Mode Line configuration mode

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

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

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

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

3.3 accounting exec

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

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

no accounting exec

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

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 Line configuration mode

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 Commands

Command	Description
N/A	N/A

Platform Description N/A

3.10 history

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

history [**size** *size*]

no history

no history size

Parameter Description

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

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

Command Mode Line configuration mode

Usage Guide N/A

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

```
Ruijie(config)# line vty 0 5
Ruijie(config-line)# history size 20
```

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

```
Ruijie(config)# line vty 0 5
Ruijie(config-line)# no history
```

Related 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	VTY connection number, in the range from 0 to 35.

Defaults

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

Parameter	Description

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

Command	Description

Commands

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

Parameter	Description

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

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

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

3.22 show 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 The following example sets the logout message to “Logout from the ruijie device”.

Examples

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

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

3.33 width

Use this command to set the screen width 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 RMON Commands

4.1 rmon alarm

Use this command to monitor a MIB variable. Use the **no** form of this command to remove the alarm entry.

rmon alarm *number variable interval* {**absolute** | **delta** } **rising-threshold** *value* [*event-number*] **falling-threshold** *value* [*event-number*] [**owner** *ownername*]

no rmon alarm *number*

Parameter description

Parameter	Description
number	Alarm number. The value ranges from 1-65,535.
variable	Alarm variable. The value is a character string consisting of 1 to 255 characters in OID dotted format (the format is entry.integer.instance or a leaf node named .instance, for example. 1.3.6.1.2.1.2.1.10.1).
interval	Sampling interval. The valye ranges from 1 to 2,147,483,647 in the unit of second.
absolute	Absolute sampling. In this mode, when the sampling time arrives, the system directly invokes the variable value.
delta	Delta sampling. In this mode, when the sampling time arrives, the system invokes the delta value of the variable within the sampling interval.
rising-threshold *value*	Rising threshold and the corresponding event number when the threshold is reached. The threshold ranges from -2,147,483,648 to +2,147,483,647.
event-number	The event number ranges from 1 to 65,535.
falling-threshold *value*	Falling threshold and the corresponding event number when the threshold is reached. The threshold ranges from -2,147,483,648 to +2,147,483,647
owner *ownername*	Owner of an entry. The value is a character string consisting of 1 to 63 characters that are case sensitive.

Default N/A.

Command mode Global configuration mode.

Usage guidelines The RGOS allows you to modify the configured history information of the Ethernet network, including variable, absolute/delta, owner, rising-threshold/falling-threshold, and the corresponding events. However, the modification does not take effect immediately until the system triggers the monitoring event at the next time.

Examples The example below monitors the MIB variable instance ifInNUcastPkts.6.

```
Ruijie(config)# rmon alarm 10 1.3.6.1.2.1.2.2.1.12.6 30 delta
```

```
rising-threshold 20 1 falling-threshold 10 1 owner zhangsan
```

Related commands

Command	Description
rmon event *number* [**log**] [**trap** *community*] **description** *string* [**owner** *owner-string*]	Adds an event definition.

4.2 rmon collection history

Use this command to enable history statistics on the Ethernet interface. Use the **no** form of this command to remove the history entry.

rmon collection history *index* [**owner** *ownername*] [**buckets** *bucket-number*] [**interval** *seconds*]

no rmon collection history *index*

Parameter description

Parameter	Description
index	Index of a history entry. The value ranges from 1 to 65,535.
owner *ownername*	Owner of an entry. The value is a character string consisting of 1 to 63 characters that are case sensitive.
buckets *bucket-number*	Capacity of a history entry (that is, the maximum number of history entries). The value ranges from 1 to 65,535. The default value is 10.
interval *seconds*	Statistics period. The unit is second. The value ranges from 1 to 3,600. The default value is 1,800 seconds.

Default N/A.

Command mode Interface configuration mode.

Usage guidelines The configured history control entry parameters cannot be modified. And the history entry can be removed from the interface where the entry configured.

Examples The example below enables log statistics on interface GigabitEthernet 0/1.

```
Ruijie# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Ruijie(config)#interface gigabitEthernet 0/1
Ruijie(config-GigabitEthernet0/1)#rmon history 1 owner UserA buckets 5
interval 60
```

Related commands

Command	Description
rmon collection stats *index* [owner *owner-name*]	Adds a statistical entry on the Ethernet interface.

4.3 rmon collection stats

Use this command to monitor an Ethernet interface. Use the **no** form of this command to remove the configuration.

rmon collection stats *index* [**owner** *owner-string*]

no rmon collection stats *index*

Parameter description

Parameter	Description
index	Index of the statistic table. The value ranges from 1 to 65,535.
owner *ownername*	Owner of an entry. The value is a character string consisting of 1 to 63 characters that are case sensitive and do not contain spaces.

Default N/A.

Command mode Interface configuration mode.

Usage guidelines N/A.

Examples The example below enables monitoring the statistics of interface GigabitEthernet 0/1.

```
Ruijie# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Ruijie(config)#interface gigabitEthernet 0/1
Ruijie(config-GigabitEthernet0/1)# rmon stats 1 owner UserA
```

Related commands

Command	Description
rmon collection history *index* [**owner** *owner-name*] [**buckets** *bucket-number*] [**interval** *seconds*]	Adds a history control entry.

4.4 rmon event

Use this command to define an event. Use the **no** form of this command to remove the event entry.

rmon event *number* [**log**] [**trap** *community*] [**description** *description-string*] [**owner** *owner-name*]

no rmon event *number*

Parameter description

Parameter	Description
number	Event number. The value ranges from 1 to 65,535.
log	(Optional) Log event. When a log event is triggered, the system records a log.
trap *community*	(Optional) Trap event. When a trap event is triggered, the system sends trap with the group named “community”.

description *description-string*	(Optional) Description of the event. The value is a character string consisting of 1 to 127 characters.
owner *owner-name*	(Optional) Owner of an entry. The value is a character string consisting of 1 to 63 characters that are case sensitive.

Default N/A.

Command mode Global configuration mode.

Usage guidelines N/A.

Examples

The example below defines the event actions: log event and send trap message.

```
Ruijie#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Ruijie(config)#rmon event 1 log trap public description "ifInNUcastPkts
is abnormal" owner UserA
```

Related commands

Command	Description
rmon alarm *number variable interval* {**absolute** | **delta** } **rising-threshold** *value* [*event-number*] **falling-threshold** *value* [*event-number*] [**owner** *ownername*]	Adds an alarm entry.

4.5 show rmon

Default Use this command to display the RMON configuration.

show rmo

Default N/A.

Command mode Privileged EXEC mode.

Usage guidelines N/A.

Examples

The example below displays the RMON configuration.

```
Ruijie#show rmon
ether statistic table:
                index = 1
                interface = GigabitEthernet 0/1
                owner = admin
                status = 0
                dropEvents = 61
                octets = 170647461
```

```
                pkts = 580375
                broadcastPkts = 2135
                multiPkts = 3615
                crcAlignErrors = 0
                underSizePkts = 0
                overSizePkts = 0
                fragments = 0
                jabbers = 0
                collisions = 0
                packets64Octets = 3254668
                packets65To127Octets = 1833370
                packets128To255Octets = 2098146
                packets256To511Octets = 126716
                packets512To1023Octets = 363621
                packets1024To1518Octets = 1077865

rmon history control table:
                index = 1
                interface = GigabitEthernet 0/1
                bucketsRequested = 5
                bucketsGranted = 5
                interval = 60
                owner = UserA
                stats = 1

rmon history table:
                index = 1
                sampleIndex = 2485
                intervalStart = 7d:22h:56m:38s
                dropEvents = 0
                octets = 5840
                pkts = 27
                broadcastPkts = 0
                multiPkts = 0
                crcAlignErrors = 0
                underSizePkts = 0
                overSizePkts = 0
                fragments = 0
                jabbers = 0
                collisions = 0
                utilization = 0
rmon alarm table:
                index: 1
                interval: 60
```

```
                oid = 1.3.6.1.2.1.2.2.1.12.6
                sampleType: 2
                alarmValue: 0
                startupAlarm: 3
                risingThreshold: 20
                fallingThreshold: 10
                risingEventIndex: 1
                fallingEventIndex: 1
                owner: UserA
                status: 1

rmon event table:
                index = 1
                description = ifInNUcastPkts is abnormal
                type = 4
                community = public
                lastTimeSent = 0d:0h:0m:0s
                owner =UserA
                status = 1

rmon log table:
                eventIndex = 1
                index = 1
                logTime = 6 d:19 h:21 m:48 s
                logDescription = ifInNUcastPkts is abnormal
```

Related commands	Command	Description
	N/A	N/A

4.6 show rmon alarm

Default Use this command to display the RMON alarm table.

show rmon alarm

Default N/A.

Command mode Privileged EXEC mode.

Usage guidelines N/A.

Examples The example below displays the RMON alarm table.

```
Ruijie#show rmon alarm
rmon alarm table:
```

```
                index: 1
                interval: 60
                oid = 1.3.6.1.2.1.2.2.1.12.6
                sampleType: 2
                alarmValue: 0
                startupAlarm: 3
                risingThreshold: 20
                fallingThreshold: 10
                risingEventIndex: 1
                fallingEventIndex: 1
                owner: UserA
                status: 1
```

Related commands

Command	Description
rmon alarm *number variable interval* {**absolute** | **delta** } **rising-threshold** *value* [*event-number*] **falling-threshold** *value* [*event-number*] [**owner** *ownername*]	Adds an alarm entry.

4.7 show rmon event

Use this command to display the event configuration.

show rmon event

Default N/A.

Command mode Privileged EXEC mode.

Usage guidelines N/A.

Examples

The example below displays the event configuration.

```
Ruijie#show rmon event
rmon event table:
                index = 1
                description = ifInNUcastPkts is abnormal
                type = 4
                community = public
                lastTimeSent = 0d:0h:0m:0s
                owner =UserA
                status = 1
```

```
rmon log table:
                eventIndex = 1
                index = 1
                logTime = 6d:19h:21m:48s
                logDescription = ifInNUcastPkts is abnormal
```

Related commands

Command	Description
rmon event *number* [**log**] [**trap** *community*] [**description** *description-string*] [**owner** *ownername*]	Adds an event entry.

4.8 show rmon history

Use this command to display the history information.

show rmon history

Default N/A.

Command mode Privileged EXEC mode.

Usage guidelines N/A.

Examples The example below displays the history information.

```
Ruijie#show rmon history
rmon history control table:
                index = 1
                interface = GigabitEthernet 0/1
                bucketsRequested = 5
                bucketsGranted = 5
                interval = 60
                owner = UserA
                stats = 1

rmon history table:
                index = 1
                sampleIndex = 2485
                intervalStart = 7d:22h:56m:38s
                dropEvents = 0
                octets = 5840
                pkts = 27
                broadcastPkts = 0
                multiPkts = 0
                crcAlignErrors = 0
                underSizePkts = 0
```

```
                overSizePkts = 0
                fragments = 0
                jabbers = 0
                collisions = 0
                utilization = 0
```

Related commands	Command	Description
	rmon collection history *index* [owner *ownername*] **[buckets** *bucket-number*] **[interval** *seconds*]	Adds a history control entry.

4.9 show rmon statistics

Use this command to display the RMON statistics.

show rmon statistics

Default N/A.

Command mode Privileged EXEC mode.

Usage guidelines N/A.

Examples The example below displays the RMON statistics.

```
Ruijie#show rmon statistics
ether statistic table:
                index = 1
                interface = GigabitEthernet 0/1
                owner = admin
                status = 0
                dropEvents = 61
                octets = 170647461
                pkts = 580375
                broadcastPkts = 2135
                multiPkts = 3615
                crcAlignErrors = 0
                underSizePkts = 0
                overSizePkts = 0
                fragments = 0
                jabbers = 0
                collisions = 0
                packets64Octets = 3254668
                packets65To127Octets = 1833370
```

```
packets128To255Octets = 2098146
packets256To511Octets = 126716
packets512To1023Octets = 363621
packets1024To1518Octets = 1077865
```

Related commands

Command	Description
rmon collection stats *index* [**owner** *owner-string*]	Adds a statistical entry.

5 File System Commands

5.1 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:** , **usb:**, **sd:** and **tmp:**.
directory	The path name. A file name starts with “/” is an absolute path. Otherwise, it is a relative path.

Defaults The default directory is the flash root directory.

Command Mode Privileged EXEC mode.

Usage Guide

Configuration Examples

Related Commands

Command	Description
pwd	Displays the present word directory.

Platform Description N/A.

5.2 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 Privileged EXEC mode.

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

5.3 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:**, **usb:**, and **tmp:**.
file-url	The file name containing the path. A file name starts with "/" is an absolute path. Otherwise, it is a relative path.

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

Command Mode Privileged EXEC mode.

Usage Guide

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

5.4 dir

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

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

Parameter Description

Parameter	Description
filesystem	The URL of file system, followed by a colon (:). The file system includes **flash:**, **usb:**and **tmp:**.
directory	The path name. A file name starts with “/” is an absolute path. Otherwise, it is a

	relative path.

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

Command Mode Privileged EXEC mode.

Usage Guide

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

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

Field	Description
1, 2, 3…	Index number
-rw-	Permissions on a file include: ● d: directory ● r: read ● w: write ● x: executable
10485760	File size
rpmdb	File name
files	File number
directories	Directory number
total	Total size
free	Available space

Related Commands

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

Platform Description N/A.

5.5 erase

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

erase *filesystem*

Parameter Description

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

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide N/A

Configuration Examples The following example erases the USB filesystem.

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

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

5.6 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:**, **sata:**, **usb:**, **sd:** and **tmp:**.
directory	The path name. A file name starts with “/” is an absolute path. Otherwise, it is a relative path.

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

Command Mode Privileged EXEC mode.

Usage Guide

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

5.7 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:**, **usb:** and **tmp:**.
file-url	The file name containing the path. A file name starts with “/” is an absolute path. Otherwise, it is a relative path.

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

Command Mode Privileged EXEC mode

Usage Guide N/A

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

Examples

```
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

5.8 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

Related Commands

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

Platform Description N/A.

5.9 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 N/A

Description

5.10 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:**, **usb:** and **tmp:**.
directory	The path name. A file name starts with "/" is an absolute path. Otherwise, it is a relative path.

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

Command Mode Privileged EXEC mode.

Usage Guide

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 N/A.

Description

5.11 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

Usage Guide

Configuration Examples The following example displays the file system information:

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

Field	Description
Size(KB)	File system space, in the unit of KB.
Free(KB)	Available file system space, in the unit of KB.
Type	File system type
Flags	Permissions on the file system include: ● ro: read-only ● wo: write-only ● rw: read and write
Prefixes	File system prefix

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

Platform N/A.

Description

5.12 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

5.13 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:**, **usb:** and **tmp:**.
directory	The path name. A file name starts with "/" is an absolute path. Otherwise, it is a relative path.

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

Command Mode Privileged EXEC mode

Usage Guide N/A

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

```
Ruijie#tree flash:/echo
+-- client_module
+-- client_userspace
+-- echo_cli.c
+-- echo_client.c
+-- echo_client.h
+-- echo_client.o
+-- echo_cli.o
+-- echo_flag.h
+-- echo.h
+-- echo.ko
+-- echo_server.h
+-- exec_set_echo.h
+-- exec_show_echo.h
+-- Makefile
+-- module
¦   +-- echo.ko
¦   +-- echo.mod.c
¦   +-- echo.mod.o
¦   +-- echo_module.c
¦   +-- echo_module.o
```

```
¦   +-- echo.o
¦   +-- echo_server.c
¦   +-- echo_server.o
¦   +-- echo_sysfs.c
¦   +-- echo_sysfs.h
¦   +-- echo_sysfs.o
¦   +-- Makefile
¦   +-- modules.order
¦   +-- Module.symvers
¦   +-- msg_fd.c
¦   +-- msg_fd.o
+-- readme
+-- server_module
+-- server_userspace
+-- sys_rgos.ko
+-- user_space
   +-- echo_server.c
   +-- echo_server.o
   +-- Makefile
   +-- msg_fd.c
   +-- msg_fd.o 10,490,132 bytes total (13,192,656 bytes free)
```

Related Commands	Command	Description
	N/A	N/A

Platform Description N/A

5.14 verify

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

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

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

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

Command Privileged EXEC mode.

Mode

Usage Guide N/A

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

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

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

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

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

5.15 show disk

Use this command to display USB/Flash information.

show disk [**usb** | *flash*]

Parameter Description

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

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide N/A

Configuration Examples .The following example displays USB information.

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

The following example displays FLASH information.

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

Related Commands	Command	Description
	N/A	N/A

Platform Description N/A

6 SNMP Commands

6.1 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

6.2 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

6.3 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

6.4 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

6.5 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

6.6 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

6.7 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

6.8 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

6.9 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

6.10 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

6.11 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

6.12 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. snmp: SNMP trap message bridge: Bridge trap message. mac-notification: MAC trap message. ospf: OSPF trap message. urpf: uRPF trap message. vrrp: VRRP trap message. web-auth: Web authentication trap message.

Defaults Sending trap message to the NMS is disabled by default.

Command mode Global configuration mode.

Usage Guide This command must be used together with the **snmp-server host** command to send the trap message. Specifying no trap type indicates all trap messages are sent.

Configuration Examples The following example enables the SNMP agent to send the SNMP trap message.

```
Ruijie(config)# snmp-server enable traps snmp
Ruijie(config)# snmp-server host 192.168.12.219 public snmp
```

Related Commands

Command	Description
snmp-server host	Specifies the SNMP host to send the SNMP trap message.

Platform Description N/A

6.13 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

6.14 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

6.15 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**. 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

6.16 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

6.17 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 Commands

Command	Description

snmp-server contact	Sets the system contact information.

Platform Description N/A

6.18 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

6.19 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

6.20 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.

Configuration Examples The following example specifies the length of message queue as 4.

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

Related Commands

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

Platform Description N/A

6.21 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

6.22 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

6.23 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

6.24 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

6.25 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

6.26 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. In cipher text format, you need to enter continuous hexadecimal numeric characters. Note that the authentication password of MD5 has a length of 16 bytes, while that of SHA has a length of 20 bytes. Two characters make a byte. The encrypted key can be used only by the local SNMP engine on the switch.
auth	Specifies which authentication level should be used.
auth-password	Password string (no more than 32 characters) used by the authentication protocol. The system will change the password to the corresponding authentication key.
priv	Encryption mode. des56 refers to 56-bit DES encryption protocol. *priv-password*: password string (no more than 32 characters) used for encryption. The system will change the password to the corresponding encryption key.
priv-password	Password string (no more than 32 characters) used for encryption. The system will change the password to the corresponding encryption key.
md5	Enables the MD5 authentication protocol. While the **sha** enables the SHA authentication protocol.
aclnumber	Access list number, which specifies the IPV4 addresses that are permitted to access the MIB.
aclname	Name of the access list, which specifies the IPV4 addresses that are permitted to access the MIB.
ipv6_aclname	Name of the IPv6 access list, which specifies the IPv6 addresses that are permitted to access the MIB.

Defaults N/A

Command mode Global configuration mode.

Usage Guide N/A

Configuration Examples The following example configures an SNMPv3 user with MD5 authentication and DES encryption:

```
Ruijie(config)# snmp-server user user-2 mib2user v3 auth md5 authpassstr priv des56 despassstr
```

Related Commands

Command	Description
show snmp user	Displays the SNMP user configuration.

Platform Description N/A

6.27 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

7 HTTP Service Commands

7.1 enable service web-server

Use this command to enable the HTTP service function.

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

enable service web-server [**http** | **https** | **all**]

no enable service web-server [**http** | **https**]

Parameter Description

Parameter	Description
http	Enables the HTTP service.
https	Enables the HTTPS service.
all	Enables both the HTTP service and the HTTPS service.

Defaults By default, the HTTP service function is disabled.

Command mode Global configuration mode.

Usage Guide If run a command ends with the keyword **all** or without keyword, it indicates enabling both the HTTP service and the HTTPS service; if run a command ends with keyword **http**, it indicates enabling the HTTP service; if run a command ends with keyword **https**, it indicates enabling the HTTPS service. Use the command **no enable service web-server** to disable the corresponding HTTP service.

Configuration Examples The following example enables both the HTTP service and the HTTPS service:

```
Ruijie#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Ruijie(config)#enable service web-server
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

7.2 http port

Use this command to configure the HTTP port number.

Use the **no** form of this command to restore the default HTTP port number.

http port *port-number*
no http port

Parameter Description

Parameter	Description
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#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Ruijie(config)#http port 8080
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

7.3 http secure-port

Use this command to configure the HTTPS port number.
Use the **no** form of this command to restore the default HTTPS port number.
http secure-port *port-number*
no http secure-port

Parameter Description

Parameter	Description
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 terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Ruijie(config)#http secure-port 4443
```

Related Commands

Command	Description
enable service web-server	Enables the HTTP service.
show web-server status	Displays the configuration and status of the Web service.

Platform Description N/A

7.4 show web-server status

Use this command to display the configuration and status of the Web service.

show web-server status

Parameter Description

Parameter	Description
N/A	N/A

Defaults N/A

Command mode Privileged EXEC mode

Usage Guide N/A

Configuration 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

7.5 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

7.6 upgrade web download

Use this command to download the Web package from the TFTP server and upgrade the package automatically.

upgrade web download tftp: *path*

Parameter Description

Parameter	Description
tftp: *path*	*path* indicates the storage path of the Web package on the TFTP server.

	tftp indicates the system downloads the Web package from the TFTP server through the physical port and upgrades the Web package automatically.

Defaults N/A

Command mode Global configuration mode.

Usage Guide N/A

Configuration Examples The following example downloads a Web package form the TFTP server and upgrades 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

7.7 webmaster level

Use this command to configure the username and password for Web login authentication. Use the **no** form of this command to restore the default setting.

webmaster level *privilege-level* **username** *name* **password** { *password* | [**0 | 7**] *encrypted-password* }

no webmaster level *privilege-level* [**username** name]

Parameter Description

Parameter	Description
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 1, username of admin and plaintext password of admin.
2. User2 is configured with privilege level 2, username of guest and plaintext password of guest.

Command Global configuration mode.

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

8 Syslog Commands

8. 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

8.2 logging

Use this command to send the log message to the specified syslog server.

logging { *ip-address* | **ipv6** *ipv6-address* } [**udp-prot** *port*]

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

8.3 logging buffered

Use this command to set the memory buffer parameters (log severity, buffer size) for logs at global configuration layer. Use the **no** form of the command to disable recording logs in the memory buffer. Use the **default** form of this command to restore the default setting.

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

no logging buffered

default logging buffered

Parameter Description

Parameter	Description
buffer-size	Size of the buffer is related to the specific device type: 4 K to 128 K Bytes.
level	Severity of logs, from 0 to 7. The name of the severity or the numeral can be used.

Defaults The buffer size is related to the specific device type.
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

8.4 logging console

Use this command to set the severity of logs that are allowed to be displayed on the console in global configuration mode. Use the **no** form of this command to prohibit printing log messages on the console.

logging console [*level*]

no logging console

Parameter Description

Parameter	Description
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

8.5 logging count

Use this command to enable the log statistics function in global configuration mode. Use the **no** form of this command to restore the default setting.

logging count

no logging count

Parameter 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

8.6 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

8.7 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

8.8 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

8.9 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

8.10 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 Mode Global configuration mode

Usage Guide The following table (Table-2) is the possible device values of Syslog:

Numerical Code	Facility
0 (kern)	Kernel messages
1 (user)	User-level messages
2 (mail)	Mail system
3 (daemon)	System daemons
4 (auth1)	security/authorization messages
5 (syslog)	Messages generated internally by syslogd
6 (lpr)	Line printer subsystem
7 (news)	USENET news
8 (uucp)	Unix-to-Unix copy system
9 (clock1)	Clock daemon
10 (auth2)	security/authorization messages
11 (ftp)	FTP daemon
12 (ntp)	NTP subsystem
13 (logaudit)	log audit
14 (logalert)	log alert
15 (clock2)	clock daemon
16 (local0)	Local use
17 (local1)	Local use
18 (local2)	Local use
19 (local3)	Local use
20 (local4)	Local use
21 (local5)	Local use
22 (local6)	Local use
23 (local7)	Local use

The default device value of RGOS is 23 (local 7).

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

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

Related

Command	Description

Commands		
	logging console	Sets the severity of logs that are allowed to be displayed on the console.

Platform Description N/A

8.11 logging file

Use this command to save log messages in the log file, which can be saved in hardware disk, expanded FLASH, USB or SD card. Use the **no** form of this command to restore the default setting,

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

no logging file

Parameter Description

Parameter	Description
flash	Saves the log file in expanded FLASH.
usb0	Saves the log file in USB0. This parameter is supported by the device with one USB connector and the USB extension device.
usb1	Saves the log file in USB1, This parameter is supported by the device with two USB connectors and the USB extension device.
sd0	Saves the log file in the SD card. This parameter is supported by the device with the SD card interface and the SD card 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

8.12 logging flash flush

Use this command to write log messages in the system buffer into the flash file immediately.

logging flash flush

Parameter Description

Parameter	Description
N/A	N/A

Defaults N/A

Command Mode Global configuration mode

Usage Guide In general, the log messages are cached in the log buffer. Only when the buffer is full or the timer expires are log messages written into the flash file. This command is used to write log messages in the system buffer into the flash file immediately.

The **logging flash flush** command takes effect only once for each configuration. The log messages cached in the buffer are written into the flash file immediately after configuration.

Configuration Examples The following example writes log messages in the system buffer into the flash file immediately.

```
Ruijie(config)# logging flash flush
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

8.13 logging flash interval

Use this command to set the interval to write log messages into the flash file, Use the **no** form of this command to restore the default setting.

logging flash interval *seconds*

no logging flash interval

Parameter Description

Parameter	Description
interval *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

8.14 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

8.15 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

1. When too many log messages are printed, the terminal screen keeps being refreshed. If you are not concerned with these log messages, use the “filter-only” filter type to filter the log messages,
2. If you are concerned with certain log messages, use the “contains-only” filter type to print log messages containing the key word of the filter rule, so as to monitor whether certain events happen.

In real operation, the contains-only and the 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

8.16 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

8.17 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

8.18 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 Global configuration mode

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

8.19 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 equipments such as the memory buffer, the expanded FLASH and the Syslog Server. This command is the total log switch. If this switch is turned off, no log will be displayed or recorded unless the severity level is greater than 1.

Configuration Examples The following example disables the log switch on the device.

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

Related

Command	Description

Commands		
	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

8.20 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. 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 Commands

Command	Description
N/A	N/A

Platform Description N/A

8.21 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

8.22 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 an ipv6 address as AAAA:BBBB:FFFF:

```
Ruijie(config)# logging server ipv6 AAAA:BBBB:FFFF
```

Related Commands

Command	Description
logging on	Turns on the log switch.

show logging	Displays log messages and related log configuration parameters in the buffer.
logging trap	Sets the level of logs allowed to be sent to Syslog server.

Platform Description N/A

8.23 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

8.24 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

8.25 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

8.26 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

8.27 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

8.28 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 Print UP-DOWN logs on the port when keying in the command, the input command will be output again:

```
Ruijie# configure terminal
Oct  9 23:40:55 %LINK-5-CHANGED: Interface GigabitEthernet 0/1, changed state
to down
Oct  9 23:40:55 %LINEPROTO-5-UPDOWN: Line protocol on Interface
GigabitEthernet 0/1, changed state to DOWN
Ruijie# configure terminal//----the input command by the user is output
again rather than being intererupted.
```

Related Commands

Command	Description
show running-config	Displays the configuration.

Platform Description N/A

8.29 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 Examples The following example enables logs at severity 6 to be sent to the Syslog Server with the address of 202.101.11.22:

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

Related Commands

Command	Description
logging on	Turns on the log switch.
logging	Sends logs to the Syslog server.
show logging	Displays the log messages and related log configuration parameters in the buffer.

Platform Description N/A

8.30 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

8.31 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

8.32 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

8.33 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

8.34 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

8.35 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

8.36 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

8.37 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

8. 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

8.39 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

8.40 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

8.41 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

8.42 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

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 255 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

9.4 cpe back-up

Use this command to configure the backup and restoration of the main program and configuration file of the CPE.
Use the **no** form of this command to disable this function.
cpe back-up [**delay-time** *seconds*]
no cpe back-up

Parameter Description

Parameter	Description
seconds	Specifies the delay for backup and restoration of the main program and configuration file of the CPE, 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

9.5 cpe inform

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

Parameter Description

Parameter	Description
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 255 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 N/A

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 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

9.12 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 Mode CWMP configuration mode

Usage Guide Use this command to configure the session timeout period of the CPE.
The maximum waiting period that the CPE has when the CPE failed to receive the ACS reply.

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

```
Ruijie#config terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Ruijie(config)#cwmp
Ruijie(config-cwmp)#timer cpe-timeout 50
Ruijie(config-cwmp)#
```

Related Commands

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

Platform Description N/A

10 LED Commands

10.1 led on

Use this command to turn on LEDs for AP location.

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

led on [**slot** *slot-id* [**secondary**]]

no led on [**slot** *slot-id* [**secondary**]]

Parameter Description

Parameter	Description
slot-id	Slot ID corresponding to the RF card
secondary	Secondary device

Defaults This function is disabled by default.

Command Mode AP configuration mode

Usage Guide For rack APs, specify the slot ID for every RF card. For non-rack APs, the *slot-id* parameter is invalid. **Secondary** indicates that this command takes effect for the secondary device. If **secondary** is not configured, this command takes effect for the primary device.

Configuration Examples The following example turns on LEDs for AP location.

```
Ruijie(config)#ap-config 00d0.f822.33bc
Ruijie(config-ap)#led on
```

The following example turns off LEDs for AP location.

```
Ruijie(config)#ap-config 00d0.f822.33bc
Ruijie(config-ap)#no led on
```

Platform Description N/A

10.2 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 LICENSING Commands

11.1 license copy

Use this command to back up a license file.

license { **copy-all** | **copy-file** *filename* } { **flash: | usb0:** } [*target-filename*]

Parameter description

Parameter	Description
copy-all	Copies all permanent license files in the system.
copy-file	Copies the *filename* license file in the system. And ***filename*** can be the name of a license file already installed in the system or the name of a feature. When ***filename*** is a feature name, all license files already installed for this feature are backed up.
filename	The name of a license file already installed in the system or the name of a feature
flash:	Specifies that the license file is installed in the internal flash file system.
usb0:	Specifies that the license file is installed in the USB file system.
target-filename	Specifies the name of the license file.

Command Mode Privileged EXEC mode

Default Level 4

Usage Guide When you back up all license files in the system, a tar file is generated. This command does not require authorization.
Both one license file and all license files of a certain feature can be copied.

Configuration Examples The following example backs up all license files in the system into file-rg-license-lics in a USB flash drive (there must be this path) and name the backup lics.tar.

```
Ruijie#lic copy-all usb0:rg-license-lics/lics.tar
Success to copy all permanent license.
```

Verification You can run the **dir** command to check whether the license file backup is generated. In addition, you can check whether the backup is correct by comparing the output of the **dir** command with the license file name in the **installed license** field of the feature with permanent authorization displayed by running the **show license all_license** command.

Only a multi-instance license file has the **installed license** field. The multi-instance license file backup is named after the ID of the multi-instance license file. At most one single-instance

license file exists in the system at a time; therefore, the single-instance license file backup is named after the feature.

In this example, the IDs 19881021.lic and 19881023.lic are embedded in the license file. License files are stored in different folders based on the features during the packing; therefore, users can still identify the mapping between license files and features.

Prompt Messages

There is not permanent license in the system for backup.

```
Copy failed, there's no permanent license in the system.
```

All license files in the system are successfully backed up.

```
Success to copy all permanent license.
```

The error message is displayed if no feature or license file is specified on the device.

```
Copy failed, there’s no such service or license installed in the system.
```

The error message is displayed if the specified license file is temporary.

```
Copy failed, the license is temporary.
```

The specified license file is backed up successfully.

```
Success to copy license vsd.lic.
```

Common Errors

Specify a license file or a file not in the system.

Specify a temporary license file for backup (a temporary license file cannot be backed up).

11.2 license grace-period

Use this command to set the time of issuing a warning before the validity period of a license file expires. Use the **no** or **default** form of this command to restore the default setting.

license grace-peroid *license days*

no license grace-peroid *filename*

default license grace-peroid *filename*

Parameter Description

Parameter	Description
filename	The name of the license file for a feature
days	The period from the expiry time to the warning time

Defaults

The default value is the smaller one between 120 and half the evaluation license file's validity period.

Command Mode

Privileged EXEC mode

Default Level

4

Usage Guide When the timeout interval of a license file is shorter than the friendly period, the friendly period warning is generated once a day; and the warning is generated once an hour one day before the license file expires. Friendly period warning is issued in log or SNMP TRAP form.

⚠ This command does not require authorization.

⚠ An evaluation license file needs to be configured with friendly period warning. A permanent license file does not need to be configured with friendly period warning.

Configuration Examples The following example installs the temporary license for the VSD feature and sets the friendly period warning time to 100 days.

```
Ruijie#license grace-period LIC-VSD 100
Success to set alarm starting point of license LIC-VSD.
```

Verification When the validity period of the license file for the VSD feature is shorter than 100 days, the friendly period warning is displayed at regular intervals.

Prompt Messages The setting is successful.

```
Success to set alarm starting point of license LIC-VSD.
```

The specified license file is not in the system.

```
There's no license abc in the system
```

Common Errors Specify a license file not in the system.

11.3 license install

Use this command to install a license file.

license install { **flash: | usb0:** } *filename*

Parameter Description

Parameter	Description
flash:	Specifies that the license file is installed in the internal flash file system.
usb0:	Specifies that the license file is installed in the USB file system.
filename	Specifies the name of the license file.

Command Mode Privileged EXEC mode

Default Level 4

Usage Guide The name of the license file can be modified. This command does not require authorization.
In a VSU, run this command on CM, the license is also installed on the other modules; run this

command on a non-CM module, the license is installed locally.

Configuration Examples The following example obtains the host ID of the device, registers at the authorization website, obtains and installs the license file for the VSD feature.

```
Ruijie#show license hostid
8708EH5F00042
Ruijie#license install usb0: vsd.lic
License file install success, service name: LIC-VSD.
```

Verification Run the **show license all_license** command to check the license name. If the license name is displayed, the corresponding license file is installed.

Prompt Messages The specified license file is not in the system.

```
Install failed: no such file or directory.
```

The specified license file is not legal.

```
Install failed: the install license may be wrong.
```

The specified license file is newer than the installed one.

```
Install failed: the system already has a same license which is newer.
```

The license file is reinstalled.

```
Install failed: the license has been installed before.
```

The specified license file is temporary and there is the same permanent one.

```
Install failed: The system already has a same permanent license.
```

The license file is installed successfully (use the license file for LIC-VSD as an example).

```
License file install success, service name: LIC-VSD.
```

The license file is installed successfully and becomes permanent (use the license file for LIC-WLAN-AP-8 as an example).

```
License file install success, service name: LIC-VSD.
The license turns to be permanent.
```

The license file is installed successfully whose expiry date is close (use the license file for LIC-WLAN-AP-8 as an example).

```
License file install success, service name: LIC-VSD.;
The installed license is approaching deadline, less than 30 days.
```

Common Errors Specify a license file not on the device.
Specify a license file illegal.
The SN in the license file does not match the device.
Specify a license file to install older than existing one in the system.

Reinstall the license file.

Replace the permanent license file with the temporary license file.

11.4 license auto-install

Use this command to install a license file through auto-match.

license auto-install { **flash: | usb0:** } *filename*

Parameter Description

Parameter	Description
flash:	The directory for the license file in the internal flash file system
usb0:	The directory for the license file in the USB file system
filename	The name of the license file

Command Mode Privileged EXEC mode

Default Level 4

Usage Guide The *filename* can be modified. This command does not require authorization.

In VSU environment, this command is used for matching devices for installation automatically. The **license install** command is used for installing license on the local device without matching the other devices. In non-VSU environment, the **license auto-install** and the **license install** commands take the same effect.

Configuration Examples The following example obtains the host ID of the device, registers at the authorization website, installs the FC license file.

```
Ruijie#show license dev-hostid

Dev 1: 8708EH5F00042

Dev 2: GH3002893D300

Ruijie#license auto-install usb0:fc.lic

License file install success, dev 2 install it, service name: LIC-FC-BLADE-S.
```

Verification Run the **show license dev_license** command to check the license name. If the license name is displayed, the corresponding license file is installed.

Prompt Messages The specified license file is not in the system.

```
Install failed: no such file or directory.
```

The specified license file is not legal.

```
Install failed: the install license may be wrong.
```

The specified license file is newer than the installed one.

```
Install failed: device 2 already has a same license which is newer.
```

The license file is reinstalled.

```
Install failed: the license has been installed to device 2 before.
```

The specified license file is temporary and there is the same permanent one.

```
Install failed: device 2 already has a same permanent license.
```

The license file is installed successfully (use the license file for FC as an example).

```
License file install success, device 2 installed it, service name:
LIC-FC-BLADE-S.
```

The license file is installed successfully and becomes permanent (use the license file for FC as an example).

```
License file install success, device 2 installed it, service name:
LIC-FC-BLADE-S.

The license turns to be permanent.
```

The license file is installed successfully whose expiry date is close (use the license file for FC as an example).

```
License file install success, device 2 installed it, service name:
LIC-FC-BLADE-S.

The installed license is approaching deadline, less than 30 days.
```

Common Errors

Specify a license file not on the device.
Specify a license file illegal.
No match device.
Specify a license file to install older than existing one in the system.
Reinstall the license file.
Replace the permanent license file with the temporary license file.

11.5 license uninstall

Use this command to remove a license file.

license uninstall { **all |** *license* [*filename*] }

Parameter Description

Parameter	Description
all	Removes all license files in the system.
license	The name of the license to be removed
filename	The name of the file to be removed

Command Mode Privileged EXEC mode

Default Level 4

Usage Guide This command does not require authorization.

After you remove the license file for a feature that is running, the license file removal does not take effect immediately.

A license file cannot be restored after it is removed. It is recommended that you back up the license file before removing it.

Configuration Examples The following example removes the license file for VSD in the system.

```
Ruijie#license uninstall LIC-VSD
Uninstall LIC-VSD success.
```

Verification Run the **show license all_license** command to view the **Service name** filed. If the name of a feature corresponding to a license file already removed is not displayed, the removal is successful.

Prompt Messages The specified license file is not on the device. (it is named after defd in this example).

```
Uninstall failed: there's no license defd in the system.
```

The specified license file of the specified feature is not on the device (The specified feature is LIC-WLAN-AP-32 and the specified license is named 123.lic).

```
Uninstall failed: there's no license 123.lic of service LIC-WLAN-AP-32 in the system.
```

The single instance license does not support license based uninstalling.

```
Uninstall failed: single instance license does not support license based uninstalling.
```

The removing is successful (use VSD feature as an example).

```
Uninstall LIC-VSD success.
```

The removing of a license file is successful (LIC-WLAN-AP-32 is the name of the specified file and AP32_1.lic is a license file in this example).

```
Uninstall license AP32_1.lic of service LIC-WLAN-AP-32 success.
```

Common Errors

The license file has not been installed on the device.
Specify a license file not on the device.
Remove a certain license file for a single-instance feature (One single-instance license does not support the removing of one single file.

11.6 license auto-uninstall

Use this command to remove a license file through auto-match.

license auto-uninstall *devid license* [*filename*]

Parameter Description

Parameter	Description
devid	The ID of the device where the file is
license	The name of the license to be removed
filename	The name of the file to be removed

Command Mode

Privileged EXEC mode

Default Level

4

Usage Guide

This command does not require authorization.

⚠ After you remove the license file for a feature that is running, the license file removal does not take effect immediately.

⚠ A license file cannot be restored after it is removed. It is recommended that you back up the license file before removing it.

Configuration Examples

The following example removes the license file for FC in the system.

```
Ruijie#show license dev-hostid

Dev 1: 8708EH5F00042

Dev 2: GH3002893D300

Ruijie#license auto-install usb0:fc.lic

License file install success, dev 2 install it, service name: LIC-FC-BLADE-S.
```

Verification Run the **show license dev_license** command to view the **Service name** filed. If the name of a feature corresponding to a license file already removed is not displayed, the removal is successful.

Prompt Messages The specified license file is not on the device. (it is named after defd in this example).

```
Uninstall failed: there's no license defd in device 2.
```

The specified license file of the specified feature is not on the device (The specified feature is LIC-WLAN-AP-32 and the specified license is named 123.lic).

```
Uninstall failed: there's no license 123.lic of service LIC-WLAN-AP-32 in device 2.
```

The single instance license does not support license based uninstalling.

```
Uninstall failed: single instance license does not support license based uninstalling.
```

The removing is successful (use FC feature as an example).

```
Uninstall LIC-FC-BLADE-S in device 2 success.
```

The removing of a license file is successful (LIC-WLAN-AP-32 is the name of the specified file and AP32_1.lic is a license file in this example).

```
Uninstall license AP32_1.lic of service LIC-WLAN-AP-32 in device 2 success.
```

Common Errors The license file has not been installed on the device.
Specify a license file not on the device.
Remove a certain license file for a single-instance feature (One single-instance license does not support the removing of one single file.
Specify a device not available.

11.7 license unbind

Use this command to unbind a license.
license unbind *pak*

Parameter Description

Parameter	Description
pak	The license code

Command Privileged EXEC mode

Mode

Default Level 4

Usage Guide This command does not require the license.

⚠ Use this command to unbind a license from the bound device before performing unbinding on the Web page.

⚠ You will get an authenticode after unbinding the license from the device, which is necessary for unbinding operation on the Web page.

Configuration Examples The following example unbinds license code LIC-FCOE00000012268888.

```
Ruijie#license unbind LIC-FCOE00000012268888
Success to unbind license LIC-FCOE00000012268888.
The verification string is
775719468737BA269825589557F558657575B5D5D5D5D785782598859765A8355
855.
```

11.8 license update

Use this command to update a license file.

license update { **flash: | usb0:** } *filename*

Parameter Description

Parameter	Description
flash:	Specifies that the license file is installed in the internal flash file system.
usb0:	Specifies that the license file is installed in the USB file system.
filename	Specifies the name of the license file.

Command Mode Privileged EXEC mode

Default Level 4

Usage Guide This command does not require authorization. The name of a license file can be modified.

Configuration Examples The following example updates the temporary license file for VSD in the system to a permanent license file.

- Purchase the permanent license file vsd_perm.lic for VSD, store the vsd _perm.lic file in a USB flash drive, and connect the USB flash drive to the device.
- Update the license file for VSD.

```
Ruijie#license update usb0:vsd_perm.lic
License file update success, temporary license LIC-VSD changes into permanent.
```

Verification Run the **show license** command to check the **Attribute** field. If the field is displayed as Permanent, the corresponding attribute is updated.

Configuration Examples

```
Ruijie#show license all-license
Searching license in the system...
1.Service name: LIC-VSD
Attribute: Permanent, Releasable
Licensed serial number: LIC-VSD00000012268888
```

Prompt Messages

The specified license file is not in the system.

```
Update failed: No such file or directory.
```

The specified license file is not legal.

```
Update failed: the update license may be wrong.
```

The specified license file is newer than the installed one.

```
Update failed: the new installed license is older than the system one.
```

The license file is reinstalled.

```
Update failed: the license has been installed before.
```

The temporary license file cannot be replaced by a permanent one.

```
Update failed: the period license cannot replace permanent license.
```

The specified license file is not on the device before the corresponding feature of the license file is to be installed first.

```
Update failed: now the system does not have the license.
Try "license install" instead.
```

The license file is updated successfully and the evaluation license file becomes permanent (use the license file for VSD as an example).

```
Update success, temporary license LIC-VSD changes into permanent.
```

Common Errors

Install a license file that does not belong to the present device.
Replace the license file of the new version with the old version.
Reinstall an updated license file.
Replace the permanent license file with the temporary license file.
Start update when the corresponding feature is not licensed for the system.

11.9 show license

Use this command to check a license file for the device.

show license { **all-license | dev-license | file** [*license*] }

Parameter Description

Parameter	Description
all-license	The list of all license files already installed on the device
dev-license	The list of license files on each device.
file *filename*	The name of a specified license file

Command Mode Privileged EXEC mode

Default Level 2

Usage Guide This command does not require authorization. It displays the license information of the system.

Configuration Examples The following example displays the information of a license file for VSD.

```
Ruijie#show license file LIC-VSD
Service name: LIC-VSD
Attribute: Temporary, Releasable
Left days: 362
Licensed serial number: LIC-VSD00000012268888
```

The following example displays the information of all the license files installed in the system.

```
Ruijie#show  license all-license
Searching license in the system...


1. Service name: LIC-AP-64
   Attribute: Releasable
   [Permanent licenses]    [Licensed serial number]
   19880966.lic           LIC-AP-6400000012264966
   19880988.lic           LIC-AP-6400000012264988

   [Temporary license]     [Licensed serial number]
   19880900.lic           LIC-AP-6400000012264900
   (63 days left)
```

```
 2. Service name: LIC-VSD
    Attribute: Temporary, Releasable
    Left days: 362
Licensed serial number: LIC-VSD00000012268888
```

The following example displays the information of all the license files installed in the system on each device.

```
Ruijie#show  license dev-license
Searching license in the system...

Dev 1:
1. Service name: LIC-AP-64
   Attribute: Releasable
   [Permanent licenses]    [Licensed serial number]
   19880966.lic           LIC-AP-6400000012264966
   19880988.lic           LIC-AP-6400000012264988

   [Temporary license]     [Licensed serial number]
   19880900.lic           LIC-AP-6400000012264900
   (63 days left)

 2. Service name: LIC-VSD
Attribute: Temporary, Releasable
Left days: 362
Licensed serial number: LIC-VSD00000012268888

Dev 2:
 1. Service name: LIC-FC-BLADE-S
   Attribute: Temporary, Releasable
   Left days: 99
   Licensed serial number: LIC-FC-BLADE-S 00000001884686

 2. Service name: LIC-AP
   Attribute: Permanent, Releasable
   [Installed licenses]    [Licensed serial number]
   19880921.lic           LIC-AP00000012265001
19880922.lic           LIC-AP00000012265002
```

Field Description:

Field	Description
Service name	The name of the feature of the license file
Attribute	Some features of the license file
Left days	The remaining days of the expiry time of the license file
Installed license	The installed license file

Licensed serial number	License code

11.10 show license hostid

Use this command to display the host ID for the license (one device).

show license hostid

Parameter Description

Parameter	Description
N/A	N/A

Command Mode Privileged EXEC mode

Default Level 2

Usage Guide This command does not require authorization. There is a unique serial number for identifying each device.

Configuration Examples The following example displays the host ID for the license (one device).

```
Ruijie#show license hostid
1234942570021
```

11.11 show license dev-hostid

Use this command to display the host ID for the license (all devices).

show license dev-hostid

Parameter Description

Parameter	Description
N/A	N/A

Command Mode Privileged EXEC mode

Default Level 2

Usage Guide This command does not require authorization.

Configuration Examples The following example displays the host ID for the license (all devices).

```
Ruijie#show license dev-hostid
```

```
Dev 1: 8708EH5F00042

Dev 2: GH3002893D300
```

11.12 show license usage

Use this command to display the status of current license file in the system.

show license usage

Parameter Description

Parameter	Description
N/A	N/A

Command Mode Privileged EXEC mode

Default Level 2

Usage Guide This command does not require authorization.

Configuration Examples The following example displays the status of current license file in the system.

```
Ruijie#show license usage

Searching license in the system...

1. Service name: LIC-AP-64

   Attribute: Releasable

   [Permanent licenses]    [Licensed serial number]

   19880966.lic           LIC-AP-6400000012264966

   19880988.lic           LIC-AP-6400000012264988


   [Temporary license]     [Licensed serial number]

   19880900.lic           LIC-AP-6400000012264900

   (63 days left)


 2. Service name: LIC-VSD

   Attribute: Temporary, Releasable

   Left days: 362

Licensed serial number: LIC-VSD00000012268888
```

Field Description

Field	Description

Service name	The feature name of the license file
Attribute	The attributes of the license file
Left days	The remaining days of the expiry time of the license file

11.13 show license unbind-code

Use this command to display the unbound license code on the current device.

show license unbind-code

Parameter Description

Parameter	Description
N/A	N/A

Command Mode Privileged EXEC mode

Default Level 2

Usage Guide This command does not require license.

Configuration Examples The following example displays unbound license code on the current device.

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

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

11.14 show license dev-unbind-code

Use this command to display the unbound license code on all devices in the system.

show license dev-unbind-code

Parameter Description

Parameter	Description
N/A	N/A

Command Mode Privileged EXEC mode

Default Level 2

Usage Guide This command does not require license.

Configuration Examples The following example displays the unbound license code on all devices in the system.

```
Ruijie#show license unbind-code

Ruijie#show license dev-unbind-code

Searching unbound license in the system...



Dev 1:

LICENSE              UNBINDING-CODE

LIC-FCOE00000012265013
57771FF68737BFF69FF55FF557F55FF57575B5A5556587857FF59FF59765AFF55FF5

LIC-VSD00000012265011
57771FF68737BFF69FF55FF557F55FF57575B5A5556567857FF59FF59765AFF55FF5

Dev 2:

LICENSE              UNBINDING-CODE

LIC-VSD00000012264933
77571FF68737BFF69FF55FF557F55FF57575B595E58587857FF59FF59765AFF55FF5

LIC-TRILL00000012264966
77571FF68737BFF69FF55FF557F55FF57575B595E5B5B7857FF59FF59765AFF55FF5

LIC-FCOE00000012264988
77571FF68737BFF69FF55FF557F55FF57575B595E5D5D7857FF59FF59765AFF55FF5
```

12 USB Commands

12.1 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)

Device: Mass Storage
ID: 1
URL prefix: usb1
Disk Partitions:
usb1(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
ID	Device ID.
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

12.2 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 N/A

Description

13 PKG_MGMT Commands

13.1 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

13.2 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.

13.3 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.

13.4 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.

13.5 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 When this parameter value is N/A, the command is used to display all components already installed on the device and basic information of these components. When this parameter value is not N/A, the command is used to display detailed information of the corresponding component, check whether the component 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
------------------------------------------------------------------
```

13.6 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 When this parameter value is N/A, the command is used to display all components already installed on the device and basic information of these components. When this parameter value is not N/A, the command is used to display detailed information of the corresponding component, check whether the component is intact, and check whether this component works properly.

Command Mode Privileged EXEC mode

Default Level 2

Usage Guide This command is used to check all patches already installed on the device and their information.

Configuration Examples The following example displays all patches already installed on the box device.

```
Ruijie# show patch
patch package patch_install installed in the system, version:pa1
Package : patch_bridge
status:running
Version: pa1      Build time: Mon May 13 09:03:07 2013
Size: 277     Install time: Tue May 21 03:07:17 2013
    Description: a patch for bridge
    Required packages: None
```

This command is used to obtain the basic information of all patches already installed on the device.

Field	Description
Package	Name of the patch
status	Status of the patch
Version	Version of the patch
Build time	Compilation time of the patch on the server
Size	Content size of the patch
Install time	Installation time of the patch
Description	Simple functional description of the patch

The following example displays the information of all patches installed on the chassis device.

```
Ruijie#show patch slot 8
[Slot 8]:
Patch package patch_install installed in the system, version:pa1
Package : patch_test
Status: running
    Version: 1.0.0.05151504
```

```
    Build time: Wed May 15 07:04:28 2013
    Size: 1804
    Install time: Thu Jan  1 00:56:43 1970
    Description: Experimentation
    Required packages: None
-----------------------------------
```

The following example displays the information of particular patches installed on the box device.

```
Ruijie# show 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
```

13.7 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
```

13.8 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

13.9 show upgrade peer

Use this command to display the peer upgrade status.

show upgrade peer { **all** | *ip-address* } **status**

Parameter Description

Parameter	Description
all	All peer devices.
ip-address	Specifies a peer device.

Command Mode Privileged EXEC mode

Default Level 2

Usage Guide N/A

Configuration Examples The following example displays upgrade status.

```
Ruijie#show upgrade peer all status
peer self
       Device type       : ws5708
       Status           : ready
peer 10.1.1.20
       Device type       : ws5708
       Status           : success
peer 10.1.1.30
       Device type       : ws5708
       Status           : transmission
       Upgrade processing : 20%
Ruijie#
```

Prompt Messages N/A

13.10 upgrade

Use this command to install and upgrade an installation package in the local file system.

Upgrade [**patch**] [**peer** { **all** | *ip-address* }] *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
patch	Patch upgrade.
peer	Upgrades peer devices.
all	Upgrades all peer devices.
ip-address	Upgrades a specified device.

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_11S8600E_RGOS11.0(1B2)_20131106_main4)B1_CM_install.bin
[Slot M1]:Upgrade processing is 10%

 [Slot 1]:Upgrade processing is 10%

 [Slot M1]:Upgrade processing is 60%

 [Slot 1]:Upgrade processing is 60%

 [Slot M1]:Upgrade processing is 90%

 [Slot M1]:
 Upgrade info [OK]
```

```
  Kernel version[2.6.32.abb2b41f170c81->2.6.32.abb2b415749f40]
  Rootfs version[1.0.0.d5f0de03->1.0.0.660e0085]

 [Slot M1]:Restart to take effect !

 [Slot M1]:Upgrade processing is 100%
 [Slot 1]:Upgrade processing is 90%

 [Slot 1]:
 Upgrade info [OK]
  Kernel version[2.6.32.9f8b56f1d45ab2 ->2.6.32.0f48cb9f170c81]
  Rootfs version[1.0.0.2ad02537->1.0.0.1bcc12e8]

 [Slot 1]:Restart to take effect !

 [Slot 1]:Upgrade processing is 100%
 [slot: M1]
  device_name: ca-octeon-cm
  status:     SUCCESS
 [slot: 1]
  device_name: ca-octeon-lc
Status:     SUCCESS
```

Verification Run the **show version detail** command to check whether the upgrade of a subsystem component is successful.
Run the **show component** command to check whether the upgrade of a feature component is successful. upgrading a feature component
Run the **show patch** command to check whether the upgrade of a hot patch is successful.

Prompt 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
```

13.11 upgrade download tftp

Use this command to download, install and upgrade installation packages from the tftp server.

upgrade { [**patch**] **|** [**peer** { **all** | *ip-address* }] } **download tftp:***/path* [**force**]

upgrade { [**patch**] | [**peer** { **all** | *ip-address* }] } **download oob_tftp:***/path* [**via mgmt** { *number* }] [**force**]

Parameter Description

Parameter	Description
patch	Patch upgrade.
path	The path of installation packages on the tftp server This command is downloaded and upgraded automatically from the server.
via mgmt *number*	If thetransfer mode is *oob_tftp* and there are multiple MGMT ports, you can select a specific port.
force	Enforces upgrade.
peer	Upgrades peer devices.
all	Upgrades all peer devices.
ip-address	Upgrades a specified peer device.

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
```

13.12 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.

13.13 clear storage

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

Parameter Description

Parameter	Description
url	A local *url* directory or full 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

14 SYS Commands

14.1 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 2099.

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 The following example changes the current hardware time of the system (for example, 2012-02-01

Examples

18:23:06) into 6 o'clock and keeps the values of other parameters.

```
Ruijie# 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

-

14.2 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 -

14.3 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 2099.

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

-

14.4 clock summer-time

Use this command to set the summer time.

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

Use this command to disable the summer time.

no clock summer-time

Parameter Description

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

Defaults -

Command Mode Global configuration mode

Default Level -

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

Configuration Examples 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 -

14.5 clock timezone

Use this command to set the time zone.

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

Use this command to remove the time zone settings.

no clock timezone

Parameter Description

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

Defaults

-

Command Mode

Global configuration mode

Default Level

-

Usage Guide

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

Configuration Examples

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 -

14.6 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 -

14.7 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 [[**up** *up-value*] [**down** *down-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
up *up--value*	Sets the high watermark of the CPU usage. The range is from 1 to 99.
down *down-value*	Sets the watermark fluctuation range. The range is from 1 to 99.

Defaults By default, the range of the CPU usage watermark is from 75% and 85%).

Command Mode Global configuration mode

Default Level -

Usage Guide This command is supported only in VSD0 mode. Multiple VSDs are not supported.
You can use this command to set the high watermark of the CPU usage and enable CPU usage monitoring. When detecting that the CPU usage exceeds the fluctuation range of the highest watermark, the system prints prompts.

Configuration Examples 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 high-watermark up 85%, down 75%
```

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 high-watermark up 85%, down 75%
```

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 up 90 down 70
Open cpu watermark monitor
Set system cpu high-watermark up 90%, down 70%
```

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(91%),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 -

14.8 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-rate*

Use this command to disable the detection of memory low watermark.
no memory low-watermark set

Parameter Description

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

Defaults By default, the memory watermark threshold is 90%.

Command Mode Global configuration mode

Default Level -

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

Configuration Examples The following example sets the low watermark threshold of the memory to 80% and enables detection.

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

Check Method -

Prompt Message

Platform Description -

14.9 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 -

14.10 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 -

14.11 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 -

14.12 show clock

Use this command to display the system software clock.

show clock

Parameter Description

Parameter	Description
-	-

Command Privileged EXEC mode / global configuration mode

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 -

14.13 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 The following example displays the memory usage of each task and the ranking (based on the total

Examples 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 -

14.14 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 -

14.15 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 -

14.16 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. 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 -

14.17 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     :
    Last  5 sec    0.3% (0.6%)
    Last  1 min    0.3% (0.6%)
    Last  5 min    0.3% (0.6%)
    Last 15 min    0.3% (0.6%)
Tty           : ?
```

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

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

Description of the displayed information:

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

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

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

```
Ruijie# show process cpu detailed 1715
Process Id    : 130
Process Name  : crypto
Vsdid         : 0
Process Ppid  : 2

State         : S(sleeping)
On CPU        : 0
Priority      : 0
Age Time      : 03:41:09.9
Run Time      : 00:00.0
Cpu Usage     :
    Last  5 sec    0.0%(  0.0%)
    Last  1 min    0.0%(  0.0%)
    Last  5 min    0.0%(  0.0%)
    Last 15 min    0.0%(  0.0%)
Tty           : ?
Code Usage    : 0.0KB.
```

Prompt Message -

Platform Description -

14.18 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 -

14.19 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 -

14.20 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 -

14.21 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 -

15 NTP Commands

15.1 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 master clock 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

15.2 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

15.3 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

15.4 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. If the key is encrypted, the max length is 64 characters. If

	the key is not encrypted, the max length is 31 characters.
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

15.5 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

15.6 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

15.7 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

15.8 ntp interval

Use this command to set the interval for time synchronization between the NTP client and the NTP server. Use the **no** form of this command to restore the default time synchronization interval.

ntp interval *seconds*

no ntp interval

Parameter Description

Parameter	Description
seconds	Sets the time synchronization interval in seconds. The value ranges from 10 to 2,592,000.

Defaults The default value is 64.

Command Mode Global configuration mode

Default Level 14

Usage Guide

The configuration does not take effect immediately. For immediate validation, enable NTP and then set the interval. If the NTP client has never synchronized the time successfully, it rapidly synchronizes the time at an interval of 5s. Then, it synchronizes time at the preset interval after the first successful time synchronization.

Configuration Examples The following example configures the NTP time synchronization interval to 3,600 seconds.

```
Ruijie(config)# ntp interval 3600
```

15.9 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 No trusted key is set by default.

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

15.10 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

15.11 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

15.12 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

16 SNTP Commands

16.1 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

16.2 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

16.3 sntp server

Use this command to specify an SNTP/NTP 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/NTP server.

Defaults No SNTP/NTP 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

16.4 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

17 SPAN-RSPAN Commands

17.1 monitor session

Use this command to configure the SPAN session and specify the source port (monitored port).
monitor session *session-num* **source interface** *interface-id* [**both** | **rx** | **tx**]

Use this command to configure the SPAN session and specify the destination port (monitoring port).
monitor session *session-num* **destination interface** *interface-id* [**encapsulation replicate** | **switch**]

Use this command to remove the specified SPAN session, or remove the source port or destination port of the specified SPAN session.
no monitor session *session-num* [**source interface** *interface-id* | **destination interface** *interface-id*]

Use this command to remove the specified SPAN session, or remove the source port or destination port of the SPAN session.
default monitor session *session-num* { **source interface** *interface-id* | **destination interface** *interface-id* }

Parameter Description

Parameter	Description
session_number	SPAN session number
interface-id	Interface name
rx	Monitors the only received traffic.
tx	Monitors the only transmitted traffic.
both	Monitors both received and transmitted traffic. This is the default.
encapsulation replicate	Specifies that the destination port replicates the source interface encapsulation method. If not selected, the default is to send packets in native form (untagged).
switch	Enables switching on the destination port. Switching function is disabled by default.

Defaults Port monitoring is disabled by default.

Command mode Global configuration mode.

Usage Guide Use this command to configure SPAN or remote SPAN, and specify the source port or destination port.

If the **both**, **rx** or **tx** is not specified for the source port, the **both** parameter is the default.
The **switch** and **encapsulation replicate** features are disabled on the destination port.

Configuration Examples

The following example configures the source port and destination port of the SPAN session.

```
Ruijie(config)# monitor session 1 source interface gigabitEthernet 0/1
Ruijie(config)# monitor session 1 destination interface gigabitEthernet 0/2
```

The following example removes the SPAN session.

```
Ruijie(config)# no monitor session 1
```

The following example removes the source port and destination port of the SPAN session.

```
Ruijie(config)# no monitor session  1 source interface gigabitEthernet 0/18
Ruijie(config)# no monitor session  1 destination interface gigabitEthernet
0/18
```

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

17.2 show monitor

Use this command to display the SPAN configurations.
show monitor [**session** *session_number*]

Parameter Description

Parameter	Description
session_number	Displays the specified SPAN session.

Defaults

N/A

Command mode

Privileged EXEC mode, global configuration mode and interface configuration mode

Usage Guide

N/A

Configuration Examples

This following example displays all SPAN sessions.

```
Ruijie(config)# show monitor
sess-num: 2
span-type: LOCAL_SPAN
```

```
src-intf:
TenGigabitEthernet 0/5     frame-type Both
dest-intf:
TenGigabitEthernet 0/6
sess-num: 1
span-type: LOCAL_SPAN
src-intf:
TenGigabitEthernet 0/3     frame-type Both
dest-intf:
```

The following example displays SPAN session 1.

```
Ruijie(config)# show monitor session 1
sess-num: 1
span-type: LOCAL_SPAN
src-intf:
TenGigabitEthernet 0/3     frame-type Both
dest-intf:
TenGigabitEthernet 0/4
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

18 Time Range Commands

18.1 absolute

Use this command to configure an absolute time range.
absolute { [**start** *time date*] [**end** *time date*] }

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

Parameter Description

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

Defaults The default absolute time range is the maximum range, which is from 00:00 January 1, 0 to 23:59 December 31, 9999.

Command Mode Time range configuration mode

Default Level 14

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

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 -

18.2 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 -

18.3 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 -

18.4 time-range

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

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

Parameter Description

Parameter	Description
time-range-name	Time range name

Defaults No time range is configured by default.

Command Mode Global configuration mode

Default Level 2

Usage Guide Some applications (such as ACL) may run based on time. For example, an ACL can be effective within certain time ranges of a week. To this end, first you must configure a time range. After the time range is

created, you can configure relevant time control in time range mode.

Configuration Examples

The following example creates a time range.

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

Check Method

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

Prompt Message

-

Platform Description

-