



**Ruijie RG-IS2700G Series Switches**

**RGOS Configuration Guide, Release 10.4(3b16)T2**

## **Copyright Statement**

Ruijie Networks©2017

Ruijie Networks reserves all copyrights of this document. Any reproduction, excerpt, backup, modification, transmission, translation or commercial use of this document or any portion of this document, in any form or by any means, without the prior written consent of Ruijie Networks is prohibited.

## **Exemption Statement**

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

## Preface

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

## Audience

This manual is intended for:

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

## Obtaining Technical Assistance

- Ruijie Networks Website: <http://www.ruijienetworks.com/>
- Service Email: [service\\_rj@ruijienetworks.com](mailto:service_rj@ruijienetworks.com)
- Technical Support: <http://www.ruijienetworks.com/service.aspx>
- Technical Support Hotline: +86-4008-111-000

## Related Documents

Documents	Description
Command Reference	Describes the related configuration commands, including command modes, parameter descriptions, usage guides, and related examples.
Hardware Installation and Reference Guide	Describes the functional and physical features and provides the device installation steps, hardware troubleshooting, module technical specifications, and specifications and usage guidelines for cables and connectors.

## Conventions

This manual uses the following conventions:

Convention	Description
<b>boldface</b> font	Commands, command options, and keywords are in <b>boldface</b> .
<i>italic</i> font	Arguments for which you supply values are in <i>italics</i> .
[ ]	Elements in square brackets are optional.
{ x   y   z }	Alternative keywords are grouped in braces and separated by vertical bars.
[ x   y   z ]	Optional alternative keywords are grouped in brackets and separated by vertical bars.

**Symbols**

---



---

**Note**

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

---



**Caution**

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

---



## System Configuration

---

1. Command Line Interface Configuration
2. Basic Switch Management Configuration
3. HTTP Service Configuration
4. LINE Mode Configuration
5. System Upgrade Configuration
6. File System Configuration
7. Configuration File Management Configuration
8. System Management Configuration
9. System Memory Display Configuration
10. Syslog Configuration
11. Cluster Management Configuration
12. SRM Configuration
13. Redundancy Configuration
14. Hardware Entry Capacity Configuration

# Command Line Interface Configuration

## Command Mode

The management interface of Ruijie network devices falls into multiple modes. The command mode you are working with determines the commands you can use.

To list the usable commands in each mode, enter a question mark (?) at the command prompt.

After setting up a session connection to the network device management interface, you enter in the user EXEC mode first. In the user EXEC mode, only a few commands are usable with limited functions, for example, command **show**. The command results are also not saved.

To use all commands, enter the privileged EXEC mode with the privileged password. Then you can use all privileged commands and enter the global configuration mode.

Using commands in a configuration mode (for instance, global configuration or interface configuration) will influence the current configuration. If you have saved the configuration information, these commands will be saved and executed when the system restarts. To enter any of the configuration modes, first enter the global configuration mode.

The following table lists the command modes, access methods, prompts, and exit methods. Suppose the equipment is named "Ruijie" by default.

Summary of main command modes:

Command mode	Access method	Prompt	Exit or enter the next mode	Remark
User EXEC	Log in.	Ruijie>	Enter command <b>exit</b> to quit this mode. Enter command <b>enable</b> to enter the privileged EXEC mode.	Used for basic test and showing system information
Privileged EXEC	In the user EXEC mode, enter command <b>enable</b> .	Ruijie#	To return to the user EXEC mode, enter command <b>disable</b> . To enter the global configuration mode, enter command <b>configure</b> .	Verify settings. This mode is password-protected.

Command mode	Access method	Prompt	Exit or enter the next mode	Remark
Global configuration	In the privileged EXEC mode, enter command <b>configure terminal</b> .	Ruijie (config)#	To return to the privileged EXEC mode, enter command <b>end</b> or <b>exit</b> or press Ctrl+C. To access the interface configuration mode, enter command <b>interface</b> with an interface specified. To access the VLAN configuration mode, enter command <b>vlan</b> <i>vlan_id</i> .	In this mode, you can execute commands to configure global parameters influencing the whole switch.
Interface configuration	In the global configuration mode, enter command <b>interface</b> .	Ruijie (config-if)#	To return to the privileged EXEC mode, enter command <b>end</b> or press Ctrl+C. To return to the global configuration mode, enter command <b>exit</b> . Moreover, you need specify an interface in the <b>interface</b> command.	Configure various interfaces of the equipment in this mode.
Config-vlan (Vlan Mode)	In the global configuration mode, enter command <b>vlan</b> <i>vlan-id</i> .	Ruijie (config-vlan)#	To return to privileged EXEC mode, enter command <b>end</b> or press Ctrl+C. To return to the global configuration mode, enter command <b>exit</b> .	Configure VLAN parameters in this mode.

## Getting Help

To obtain a list of commands that are available for each command mode, enter a question mark(?) at the command prompt. You can also obtain a list of command keywords beginning with the same character or parameters of each command. See the following table.

Command	Description
<b>Help</b>	Obtain the brief description of the help system under any command mode.
<b>abbreviated-command-entry?</b>	Obtain a list of commands that begin with a particular character string.(Do not leave a space between the keyword and question mark.) For example: Ruijie# di? dir disable

Command	Description
<b>abbreviated-command-entry</b> <b>&lt;Tab&gt;</b>	Complete a partial command name. For example: Ruijie# <b>show conf&lt;Tab&gt;</b> Ruijie# <b>show configuration</b>
<b>Command ?</b>	List a command's associated keywords.(Leave a space between the keyword and question mark.) For example: Ruijie# <b>show ?</b>
<b>command keyword ?</b>	List a command's associated arguments.(Leave a space between the keyword and question mark.) For example: Ruijie(config)# <b>snmp-server</b> <b>community ?</b> WORD SNMP community string

## Abbreviating Commands

To abbreviate a command, simply enter part of the command that can uniquely identify the command.

For example, **show configuration** can be abbreviated as:

```
Ruijie# show config
```

If the entered command cannot be uniquely identified by the system, the system will prompt "Ambiguous command."

For example, when you want to view the information about access lists, the following command is not complete.

```
Ruijie# show access
% Ambiguous command: "show access"
```

## Using no and default Options

Almost all commands have the **no** option generally used to disable a feature or function or perform a reversed action of the command. For example, the **no shutdown** command turns on the interface, the opposite operation of the **shutdown** command. You can use the commands without the **no** option to enable the features that have been disabled or are disabled by default.

Most configuration commands have the **default** option that restores the command setting to its default. Most commands are disabled by default. In this case, the **default** and **no** options generally serve the same purpose. However, some commands are enabled by default. In this case, the **default** and **no** options serve different purposes, where the **default** option enables the command and restores the arguments to the default settings.

## Understanding CLI Error Messages

The following table lists the error prompt messages that may occur when you use the CLI to manage equipments.

Common CLI error messages:

Error message	Meaning	How to obtain help
% Ambiguous command: "show c"	The switch cannot identify the unique command for you input insufficient characters.	Re-input the command with a question mark following the ambiguous word. The possible keywords will be listed.
% Incomplete command.	User has not input the required keywords or arguments.	Re-input the command with a space followed by a question mark. The possible keywords or arguments will be displayed.
% Invalid input detected at '^' marker.	The symbol "^" will indicate the position of the wrong words when user inputs a wrong command.	Input a question mark at the command prompt to show the allowed keywords of the command.

## Using Historical Commands

The system records the commands you have input recently, which is very useful when you input a long and complex command again.

To re-execute the commands you have input from the historical records, perform the following operations.

Operation	Result
Ctrl-P or Up	Allows you to browse the previous command in the historical command records.
Ctrl-N or Down	Allows you to return to a more recent command in the historical command records.



### Note

Standards-based terminals like VT100 series support arrow keys.

## Using Editing Features

### Editing Shortcut Keys

The following table lists the edit shortcut keys.

Function	Shortcut Key	Description
Move cursor in an editing line	Left direction key or Ctrl+B	Move the cursor to left by one character.
	Right direction key or Ctrl+F	Move the cursor to right by one character.
	Ctrl+A	Move the cursor to the beginning of the command line.
	Ctrl+E	Move the cursor to the end of the command line.
Delete the	Backspace	Delete the character to the left of the cursor.

Function	Shortcut Key	Description
entered characters	Delete	Delete the character where the cursor is located.
Scroll up by one line or one page	Return	Scroll up the displayed contents by one line and make the next line appear. This is used only before the end of the output.
	Space	Scroll up the displayed contents by one page and make the next page appear. This is used only before the end of the output.

## Sliding Window of Command Line

You can use the sliding window to edit the commands that exceed the width of one line. When the editing cursor closes to the right border, the whole command line will move to the left by 20 characters. In this case, the cursor can still be moved back to the previous character or the beginning of the command line.

When editing a command line, you can move the cursor using the shortcut keys in the following table:

Function	Shortcut key
Move the cursor to the left by one character	Left direction key or Ctrl+B
Move the cursor to the head of a line	Ctrl+A
Move the cursor to the right by one character	Right direction key or Ctrl+F
Move the cursor to the end of a line	Ctrl+E

For example, the contents of the **mac-address-table static** command may exceed the screen width. When the cursor approaches the line end for the first time, the whole line move left by 20 characters, and the hidden beginning part is replaced by "\$" on the screen. The line moves left by 20 characters when the cursor reaches the right border.

```
mac-address-table static 00d0.f800.0c0c vlan 1 interface
$static 00d0.f800.0c0c vlan 1 interface fastEthernet
$static 00d0.f800.0c0c vlan 1 interface fastEthernet 0/1
```

Now you can press **Ctrl+A** to return to the beginning of the command line. In this case, the hidden ending part is replaced by "\$".

```
-address-table static 00d0.f800.0c0c vlan 1 interface $
```



The default line width on the terminal is 80 characters.

### Note

Combined with historical commands, the sliding window enables you to invoke complicated commands repeatedly. For details about shortcut keys, see Edit Shortcut Keys.

## Filtering and Looking UP CLI Output Information

### Filtering and Looking Up the Information Outputted by the Show Command

To look up the specified message in the information outputted by the **show** command, execute the following command:

Command	Description
Ruijie# <b>show</b> <i>any-command</i>   <b>begin</b> <i>regular-expression</i>	Look up the specified content from the information outputted by the show command and output all information of the first line that contains this content and subsequent lines.

**Caution**

1. You can execute **show** command in any mode.
2. The information to be looked up is case sensitive, and the following is the same.

To filter the specified content in the information outputted by the **show** command, execute the following commands:

Command	Description
Ruijie# <b>show</b> <i>any-command</i>   <b>exclude</b> <i>regular-expression</i>	Filter the content from the information outputted by the show command and output other information excluding the line that includes the specified content.
Ruijie# <b>show</b> <i>any-command</i>   <b>include</b> <i>regular-expression</i>	Filter the content from the information outputted by the show command and output the line that includes the specified content. Other information will be filtered.

**Note**

To look up and filter the contents outputted by the **show** command, it is necessary to input the pipeline sign (vertical line, "|") followed by lookup and filtration rules and contents (characters or strings). The contents to be looked up and filtered are case sensitive.

## Using Command Alias

The system provides the command alias function. Any word can be specified as the alias of a command. For example, you can define the word "mygateway" as the alias of "ip route 0.0.0.0 0.0.0.0 192.1.1.1". Inputting this word is equal to inputting the whole string.

You can use one word to replace one command by configuring an alias for the command. For example, you can define an alias to represent the front part of one command, and then continue to enter the following part.

The command that an alias represents must run under the mode you have defined in the current system. In the global configuration mode, you can enter **alias?** to list all command modes that can configure alias.

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

An alias supports help information. An alias appears with an asterisk (\*) before it in the following format:

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

For example, in the EXEC mode, the alias “s” indicates the **show** command by default. Enter “s?” to obtain the help information on the command and the aliases beginning with ‘s’.

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

If the command that an alias represents has more than one word, the command will be included by the quotation marks. As shown in the following example, configure the alias “sv” to replace the **show version** command in the EXEC mode.

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

An alias must begin with the first character of the command line entered without any blank before it. As shown in the above example, the alias is invalid if you have inputted a blank before the command.

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

An alias can also be used to get the help information on obtaining command parameters. For example, the alias “ia” represents “ip address” in the interface configuration mode.

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

Here lists the parameter information after the command “**ip address**”, and replaces the alias with the actual command.

An alias must be inputted fully for use. Otherwise, it cannot be identified.

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

## Accessing CLI

Before using CLI, you need to use a terminal or PC to connect with the network device. Power on the network device. After the initialization of hardware and software, you can use CLI. If the network device is used for the first time, you can only connect the network device through the serial port (Console), which is referred to as out-band management. In addition, you can connect and manage the network device through Telnet virtual terminal by performing corresponding configurations. In either case, you can access the command line interface.



# Basic Switch Management Configuration

## Command Authorization-based Access Control

### Overview

A simple way to manage the terminals' access to a network is to use passwords and assign privileged levels. Password restricts access to a network or network devices. Privileged levels define the commands users can use after they have logged in to a network device.

From the perspective of security, password is stored in the configuration file. Password must be safe when the configuration file is transmitted, for example, over TFTP, across a network. Password is encrypted before being stored into the configuration file, and the clear text password is changed to the cipher text password. The **enable secret** command uses a private encryption algorithm.

### Configuring Default Password and Privileged Level

No password at any level is configured by default. The default privileged level is 15.

### Configuring/Changing the Passwords at Different Levels

Our products provide the following commands for configuring or changing the passwords at different levels.

Command	Function
Ruijie(config)# <b>enable password</b> [ <b>level level</b> ] { <i>password</i>   <i>encryption-type encrypted-password</i> }	Set a static password. You can only set a level-15 password only when no level-15 security password is configured.  If a non- level -15 password is set, the system will show a prompt and automatically convert it into a security password.  If you have set the same level-15 static password as the level 15 security password, the system will show a warning message.
Ruijie(config)# <b>enable secret</b> [ <b>level level</b> ] { <i>encryption-type encrypted-password</i> }	Set the security password, which has the same function but better password encryption algorithm than the static password. For the purpose of security, it is recommended to use the security password.
Ruijie# <b>enable</b> [ <i>level</i> ], and Ruijie# <b>disable</b> [ <i>level</i> ]	Switch over between user levels. To switch over from a lower level to a higher level, you need to input the password for the higher level.

During the process of setting a password, the keyword "**level**" is used to define the password for a specified privileged level. After setting, it is only applicable for the users who are at that level.

## Configuring Multiple Privileged Levels

By default, the system has only two password-protected levels: normal user (level 1) and privileged user (level 15). You can configure up to 16 hierarchical levels of commands for each mode. By configuring different passwords at different levels, you can use different sets of commands by different levels.

When no password is set for the privileged user level, you can enter the privileged EXEC mode without password authentication. For security, you are recommended to set the password for the privileged user level.

### Configuring Command Authorization

To expand the usage range of a command, you can assign it to the users at lower level. On contrary, to narrow the usage range of a command, you can assign it to the users at higher level.

You can use the following commands to authorize users to use a command:

Command	Function
Ruijie# <b>configure terminal</b>	Enter the global configuration mode.
Ruijie(config)# <b>privilege mode [all] {level level   reset} command-string</b>	<p>Set the privileged level for a command.</p> <p><b>mode</b> – The CLI command mode at which you are authorizing the command. For example, <b>config</b> indicates the global configuration mode, <b>exec</b> indicates the privileged command mode, and <b>interface</b> indicates the interface configuration mode.</p> <p><b>all</b> – Change the privileges of all the sub-commands of the specified commands into the same level.</p> <p><b>level level</b> – Authorization level in the range from 0 to 15. <b>Level 1</b> is for the normal user level. <b>Level 15</b> is for the privileged user level. You can switch over between various levels by using the <b>enable/disable</b> command.</p> <p><b>command-string</b> - The command to be authorized.</p>

To restore the configuration for a specified command, use the **no privilege mode [all] level level command** in the global configuration mode.

### Example of Command Authorization Configuration

The following is the configuration process that sets the **reload** command and all its sub-commands to be level 1, and brings level 1 into effective (by setting the command as “**test**”):

```
Ruijie# configure terminal
Ruijie(config)# privilege exec all level 1 reload
Ruijie(config)# enable secret level 1 0 test
Ruijie(config)# end
```

Enter the level 1, you can see the command and its subcommands:

```
Ruijie# disable 1
Ruijie> reload ?
at                reload at a specific time/date
```

```
cancel                cancel pending reload scheme
in                    reload after a time interval
<cr>
```

The following is the configuration process that restores the privilege settings of the **reload** command and all its sub-commands to the default value:

```
Ruijie# configure terminal
Ruijie(config)# privilege exec all reset reload
Ruijie(config)# end
```

Enter the level 1, the privilege setting for the command is removed.

```
Ruijie# disable 1
Ruijie> reload ?
% Unrecognized command.
```

## Configuring Line Password Protection

Our products offer password authentication for remote logons (such as Telnet). A password is required for the protection purpose. Execute the following command in the line configuration mode:

Command	Function
Ruijie(config-line)# <b>password</b> <i>password</i>	Specify a line password.
Ruijie(config-line)# <b>login</b>	Enable the line password protection.



### Note

If no logon authentication is configured, the password authentication on line layer will be ignored even when the line password is configured. The logon authentication will be described in the next section.

## Supporting Session Locking

Our products allow you to lock the session terminal temporarily using the **lock** command, so as to prevent access. To this end, enable the terminal locking function in the line configuration mode, and lock the terminal using the **lock** command in the EXEC mode of the terminal:

Command	Function
Ruijie(config-line)# <b>lockable</b>	Enable the function of locking the line terminal
Ruijie# <b>lock</b>	Lock the current line terminal

## Logon Authentication Control

### Overview

In the previous section, we have described how to control the access to network devices by configuring the locally stored password. In addition to line password protection and local authentication, in AAA mode, we can authenticate users' management privilege based on their usernames and passwords on some servers when they log on to the switch, take RADIUS server for example.

With RADIUS server, the network device sends the encrypted user information to the RADIUS server for authentication rather than authenticates them with the locally stored credentials. The RADIUS server configures user information consistently like user name, password, shared key, and access policy to facilitate the management and control of user access and enhance the security of user information.

## Configuring Local Users

Our products support local database-based identify authentication system used for local authentication of the method list in AAA mode and local authentication of line login management in non-AAA mode.

To enable the username identity authentication, run the following specific commands in the global configuration mode:

Command	Function
Ruijie(config)# <b>username</b> <i>name</i> [ <b>password</b> <i>password</i>   <b>password</b> <i>encryption-type encrypted password</i> ]	Enable the username identity authentication with encrypted password.
Ruijie(config)# <b>username</b> <i>name</i> [ <b>privilege</b> <i>level</i> ]	Set the privilege level for the user (optional).

## Configuring Line Logon Authentication

To enable the line logon identity authentication, run the following specific commands in the line configuration mode:

Command	Function
Ruijie(config-line)# <b>login local</b>	Set local authentication for line logon in non-AAA mode.
Ruijie(config-line)# <b>login</b> <b>authentication</b> { <b>default</b>   <i>list-name</i> }	Set AAA authentication for line logon in AAA mode. The authentication methods in the AAA method list will be used for authentication, including Radius authentication, local authentication and no authentication.



### Note

For more information on how to set AAA mode, configure Radius service and configure the method list, see the sections for AAA configuration.

## System Time Configuration

### Overview

Every switch has its system clock, which provides date (year, month, day) and time (hour, minute, second) and week. When you use a switch for the first time, you must configure the system clock manually. Of course, you can adjust the system clock when necessary. System clock is used for such functions as system logging that need recording the time when an event occurs.

## Setting System Time and Date

You can configure the system time on the network device manually. Once configured, the clock will be running continuously even if the network device is powered off. Therefore, unless you need to modify the time of device, it is not necessary to configure the time again.

However, for the network devices that don't provide the hardware clock, manually setting time actually configures software clock, which only takes effect for this operation. When the network devices are powered off, the manually set time will not be valid.

Command	Function
Ruijie# <b>clock set</b> <i>hh:mm:ss month</i> <i>date day year</i>	Set system date and time.

For example, change the system time to 10:10:12, 2003-6-20:

```
Ruijie# clock set 10:10:12 6 20 2003           //Set system time and date.
Ruijie# show clock                             //Confirm the modification takes effect.
clock: 2003-6-20 10:10:54
```

## Showing System Time and Date

You can show system time and date by using the **show clock** command in the privileged EXEC mode. The following is the format:

```
Ruijie# sh clock           //Show the current system time and date.
clock: 2003-5-20 11:11:34
```

## Updating Hardware Clock

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

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

In the privileged EXEC mode, execute **clock update-calendar** command to make software clock overwrite the value of hardware clock.

Command	Function
Ruijie# <b>clock update-calendar</b>	Update hardware clock via software clock.

Execute the command below to copy current date and time of software clock to hardware clock.

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

## Scheduled Restart

### Overview

This section describes how to use the **reload** [*modifiers*] command to schedule a restart scheme to restart the system at the specified time. This function facilitates user's operation in some circumstance (for the purpose of test, for example). *Modifiers* is a set of options provided by the **reload** command, making the command more flexible. The optional *modifiers* includes **in**, **at** and **cancel**. The following are the details:

```
reload in mmm | hhh:mm [string]
```

This command sets the system restart in fixed intervals in the format of *mmm* or *hhh:mm*. *string* is a help prompt. You can give the scheme a memorable name by the string to indicate its purpose. string is a prompt. For example, to reload the system at the interval of 10 minutes for test, type **reload in 10 test**.

```
reload at hh:mm day month year [string]
```

This command sets the system restart at the specified time in the future, which must not be more than 200 days from the current system time. The usage of *string* is just like above. For example, if the current system time is 14:31 on January 10, 2005, and you want the system to reload tomorrow, you can input **reload at 08:30 11 1 2005 newday**. If the current system time is 14:31 on December 10, 2005, and you want the system to reload at 12:00 a.m. on January 1, 2006, you can input **reload at 12:00 1 1 2006 newyear**.

```
reload cancel
```

This command deletes the restart scheme specified by the user. As mentioned above, you have specified the system to reload at 8:30 a.m. tomorrow, the setting will be removed after you input **reload cancel**.



#### Note

Only if the system supports clock function can users use option **at**. Before the use, it is recommended to configure the system clock according to your needs. If a restart scheme has been set before, the subsequent settings will overwrite the previous settings. If the user has set a restart scheme and then restarts the system before the scheme takes effect, the scheme will be lost.

The span from the time in the restart scheme to the current time shall be within 200 days and must be greater than the current system time. Besides, after you set reload, you should not set the system clock. Otherwise, your setting may fail to take effect, such as setting system time after reload time.

### Specifying the System to Restart at the Specified Time

In the privileged EXEC mode, you can configure the system reload at the specified time using the following commands:

Command	Function
Ruijie# <b>reload at</b> <i>hh:mm day month year</i> [reload-reason]	The system will reload at <i>hh:mm,month day,year</i> . reload-reason (if any) indicates the reason that the system reloads.

The following is an example specifying the system reload at 12:00 a.m. January 11, 2005 (suppose the current system clock is 8:30 a.m. January 11,2005):

```
Ruijie# reload at 12:00 1 11 2005 midday //Set the reload time and date.
```

```
Ruijie# show reload //Confirm the modification takes effect.
Reload scheduled for 2005-01-11 12:00 (in 3 hours 29 minutes)16581 seconds.
At 2005-01-11 12:00
Reload reason: midday
```

## Specifying the System to Restart after a Period of Time

In the privileged EXEC mode, you can configure the system reload in the specified time with the following commands:

Command	Function
Ruijie# reload in <i>mmm</i> [ <i>reload-reason</i> ]	Configure the system reload in <i>mmm</i> minutes, where the reload reason is described in <i>reload-reason</i> (if inputted)
Ruijie# reload in <i>hhh:mm</i> [ <i>reload-reason</i> ]	Configure the system reload in <i>hhh</i> hours and <i>mm</i> minutes, where the reload reason is described in <i>reload-reason</i> (if inputted)

The following example shows how to reload the system in 125 minutes (assumes that the current system time is 12:00 a.m. January 10, 2005):

```
Ruijie# reload in 125 test //Set the system reload time
```

Or

```
Ruijie# reload in 2:5 test //Set the system reload time
Ruijie# show reload //Confirm whether the restart time change takes effect
Reload scheduled System will reload in 2 hours and 4 minutes7485 seconds.
```

## Immediate Restart

The **reload** command without any parameters will restart the device immediately. In the privileged EXEC mode, the user can restart the system immediately by typing the **reload** command.

## Deleting the Configured Restart Scheme

In the privileged EXEC mode, use the following command to delete the configured restart scheme:

Command	Function
Ruijie# reload cancel	Delete the configured restart scheme.

If no reload scheme is configured, you will see an error message for the operation.

## Configuring a System Name and Prompt

### Overview

For easy management, you can configure a system name for the switch to identify it. If you configure a system name of more than 32 characters, the first 32 characters are used as the system prompt. The prompt varies with the system name. By default, the system name and command prompt are specific device names, for example "S2924G" or "R2692".

## Configuring a System Name

Our products provide the following commands to configure a system name in the global configuration mode:

Command	Function
Ruijie(Config)# <b>hostname</b> <i>name</i>	Configure a system name with printable characters less than 255 bytes.

To restore the name to the default value, use the **no hostname** command in the global configuration mode. The following example changes the equipment name to RGOS:

```
Ruijie# configure terminal           //Enter the global configuration mode.
Ruijie(config)# hostname RGOS         //Set the equipment name to RGOS
RGOS(config)#                          //The name has been modified successfully.
```

## Configuring a Command Prompt

System name will be the default prompt if you have not configured command prompt. (If the system name exceeds 32 characters, intercept the first 32 characters) The prompt varies with the system name. You can use the **prompt** command to configure the command prompt in the global configuration mode, and the command prompt is only valid in the EXEC mode.

Command	Function
Ruijie# <b>prompt</b> <i>string</i>	Set the command prompt with printable characters. If the name exceeds 32 characters, intercept the first 32 characters.

To restore the prompt to the default value, use the **no prompt** command in the global configuration mode.

## Banner Configuration

### Overview

When the user logs in the switch, you may need to tell the user some useful information by configuring a banner. There are two kinds of banners: message-of-the-day (MOTD) and login banner. The MOTD is specific for all users who connect with switches. And when users log in the switch, the notification message will appear on the terminal. MOTD allows you send some urgent messages (for example, the system is to be shut down) to network users. The login banner also appears on all connected terminals. It provides some common login messages. By default, the MOTD and login banner are not configured.

### Configuring a Message-of-the-Day

You can create a notification of single or multi-line messages that appears when a user logs in the switch. To configure the message of the day, execute the following commands in the global configuration mode:

Command	Function
---------	----------



<pre>Ruijie(Config)# banner motd c message c</pre>	Specify the message of the day, with c being the delimiter, for example, a pound sign (&). After inputting the delimiter, press the <b>Enter</b> key. Now, you can start to type text. You need to input the delimiter and then press <b>Enter</b> to complete the type. Note that if you type additional characters after the end delimiter, these characters will be discarded by the system. Also note that you cannot use the delimiter in the message and the message length should be no more than 255 bytes.
--	---

To delete the MOTD, use the **no banner motd** command in the global configuration mode. The following example describes how to configure a MOTD. The # symbol is used as the delimiter, and the text is “Notice: system will shut down on July 6th.”

```
Ruijie(config)# banner motd # //Start delimiter.
Enter TEXT message. End with the character '#'.
Notice: system will shutdown on July 6th.# //End delimiter.
Ruijie(config)#
```

Configuring a Login Banner

To configure a login banner, executing the following commands in the global configuration mode:

Command	Function
<pre>Ruijie(Config)# banner login c message c</pre>	Specify the text of the login banner, with c being the delimiter, for example, a pound sign (&). After inputting the delimiter, press the <b>Enter</b> key. Now, you can start to type text. You need to input the delimiter and then press <b>Enter</b> to complete the type. Note that if you type additional characters after the end delimiter, these characters will be discarded by the system. Also note that you cannot use the delimiter in the text of the login banner and the text length should be no more than 255 bytes.

To delete the login banner, use the **no banner login** command in the global configuration mode.

The following example shows how to configure a login banner. The pound sign (#) is used as the starting and end delimiters and the text of the login banner is "Access for authorized users only. Please enter your password."

```
Ruijie(config)# banner login # //Start delimiter
Enter TEXT message. End with the character '#'.
Access for authorized users only. Please enter your password.
# //End delimiter
Ruijie(config)#
```

Displaying a Banner

A banner is displayed when you log in the network device. See the following example:

```
C:\>telnet 192.168.65.236
Notice: system will shutdown on July 6th.
Access for authorized users only. Please enter your password.
User Access Verification
Password:
```

As you can see, "Notice: system will shutdown on July 6th." is a MOTD banner and "Access for authorized users only. Please enter your password." is a login banner.

## Viewing System Information

### Overview

You can view some system information with the **show** command on the command-line interface, such as version, device information, and so on.

### Viewing System Information and Version

System information consists of description, power-on time, hardware version, software version, BOOT-layer software version, CTRL-layer software version, and so on. System information helps you know the system. You can show the system information with the following commands in the privileged EXEC mode.

Command	Function
Ruijie# <b>show version</b>	Show system information.



#### Note

For sequence number ,run the **show version** command on the main program interface to view SYSTEMUPTIME in the form of DD:HH:MM:SS.



#### Note

During upgrading, the running software version may be different from the version in the file system. In this case, the main program version shown by running the **show version** command is the one running in the memory, but the Boot/Ctrl version is the one saved in Flash.

## Viewing Hardware Entity Information

Hardware information refers to the information on physical devices as well as slots and modules assembled in a device. The information on a device itself includes description, number of slots, slot information, slot number, description of the module on the slot (empty description if no module is plugged on the slot), number of physical ports of the module on the slot, and maximum number of ports possibly supported on the slot (number of ports of the module plugged). You may use the following commands to show the information of the device and slots in the privileged EXEC mode:

Command	Function
---------	----------

Ruijie# <b>show version devices</b>	Show device information.
Ruijie# <b>show version slots</b>	Show the information about slots and modules.

## Setting Console Rate

### Overview

The switch comes with a console interface for management. When using the switch for the first time, you need to execute configuration through the console interface. You can change the console rate on the equipment if necessary. Note that the rate of the terminal used to managing the switch must be the same as that of the console interface on the switch.

### Setting Console Rate

In the line configuration mode, execute the following command to set the console rate:

Command	Function
Ruijie(config-line)# <b>speed</b> <i>speed</i>	Set transmission rate in bps on the console interface. For a serial interface, you can only set the transmission rate to one of 9600, 19200, 38400, 57600 and 115200 bps, with 9600 bps by default.

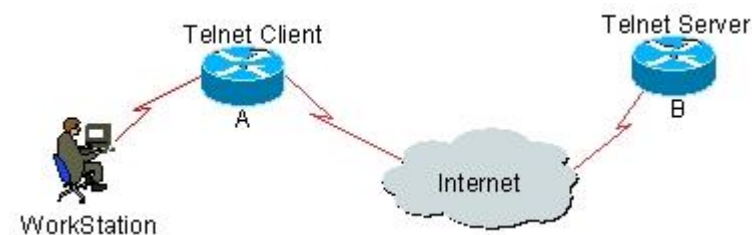
This example shows how to configure the baud rate of the serial interface to 57600 bps:

```
Ruijie# configure terminal //Enter the global configuration mode.
Ruijie(config)# line console 0 //Enter the console line configuration mode
Ruijie(config-line)# speed 57600 //Set the console rate to 57600bps
Ruijie(config-line)# end //Return to the privileged EXEC mode
Ruijie# show line console 0 //View the console configuration
CON      Type      speed  Overruns
* 0      CON      57600    0
Line 0, Location: "", Type: "vt100"
Length: 25 lines, Width: 80 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: 22 bytes
Total output: 115 bytes
Data overflow: 0 bytes
stop rx interrupt: 0 times
Modem: READY
```

## Configuring Telnet

### Overview

Telnet, an application layer protocol in the TCP/IP protocol suite, provides the specifications of remote logon and virtual terminal communication functions. The **Telnet Client** service is used by the local or remote user who has logged onto the local network device to work with the Telnet Client program to access other remote system resources on the network. As shown below, after setting up a connection with Switch A through the terminal emulation program or Telnet, users can log on the Switch B for management and configuration with the **telnet** command.



### Using Telnet Client

You can log in to a remote device by using the **telnet** command on the switch.

Command	Function
Ruijie# <b>telnet</b> <i>host</i> [ <i>port</i> ] [/source { <b>ip</b> <i>A.B.C.D</i> <b>ipv6</b> <i>X:X:X::X</i>   <b>interface</b> <i>interface-name</i> }]	Log on to a remote device via Telnet. <i>host</i> may be an IPv4 or IPv6 host name or an IPv4 or IPv6 address. For supported optional parameters, refer to relevant Telnet command section in <i>Basic Configuration Management Command</i> .

The following example shows how to establish a Telnet session and manage the remote device with the IP address 192.168.65.119:

```

Ruijie# telnet 192.168.65.119 //Establish the telnet session to the remote device
Trying 192.168.65.119 ... Open
User Access Verification //Enter into the logon interface of the remote device
Password:
  
```

The following example shows how to establish a Telnet session and manage the remote device with the IPv6 address 2AAA:BBBB::CCCC:

```

Ruijie# telnet 2AAA:BBBB::CCCC //Establish the telnet session to the remote device
Trying 2AAA:BBBB::CCCC ... Open
User Access Verification //Enter into the logon interface of the remote device
Password:
  
```

## Setting Connection Timeout

### Overview

You can control the connections that a device has set up (including the accepted connections and the session between the device and a remote terminal) by configuring the connection timeout time for the device. When the idle time exceeds the set value and there is no input or output, this connection will be interrupted.

### Connection Timeout

When there is no information traveling through an accepted connection within a specified time, the server will interrupt this connection.

Our products provide commands to configure the connection timeout in the line configuration mode.

Command	Function
Ruijie(Config-line)# <b>exec-timeout</b> 20	Configure the timeout for the accepted connection. When the configured time is due and there is no input, this connection will be interrupted.

The connection timeout setting can be removed by using the **no exec-timeout** command in the line configuration mode.

```
Ruijie# configure terminal //Enter the global configuration mode.
Ruijie# line vty 0 //Enter the line configuration mode
Ruijie(config-line)#exec-timeout 20 //Set the timeout to 20min
```

### Session Timeout

When there is no input for the session established with a remote terminal over the current line within the specified time, the session will be interrupted and the remote terminal becomes idle.

RGOS provides commands in the line configuration mode to configure the timeout for the session set up with the remote terminal.

Command	Function
Ruijie(Config-line)# <b>session-timeout</b> 20	Configure the timeout for the session set up with the remote terminal over the line. If there is no input within the specified time, this session will be interrupted.

The timeout setting for the session set up with the remote terminal over the line can be removed by using the **no exec-timeout** command in the line configuration mode.

```
Ruijie# configure terminal //Enter the global configuration mode.
Ruijie(config)# line vty 0 //Enter the line configuration mode
Ruijie(config-line)# session-timeout 20 //Set the session timeout to 20min
```

## Executing the Commands in the Executable File in Batch

In system management, sometimes it is necessary to enter multiple configuration commands to manage a function. It takes a long period of time to enter all the commands on CLI, causing error or mission. To resolve this problem, you can encapsulate all the commands in a batch file according to configuration steps. Then, you can execute the batch file for configuration when necessary.

Command	Function
Ruijie# <b>execute</b> { [ <b>flash:</b> ] <i>filename</i> }	Execute a batch file.

For example, the batch file line\_rcms\_script.text enables the reversed Telnet function on all the asynchronous interfaces as shown below:

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

Result:

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



### Note

The file name and contents of a batch file can be specified. Once edited, users send the batch file to the FLASH of the network device in TFTP. The contents of the batch file will simulate the input completely. Hence, it is necessary to edit the contents of the batch file by the sequence that CIL commands are configured. Furthermore, for some interactive commands, it is necessary to write corresponding response information in the batch file, guaranteeing that the commands can be executed normally.

## Setting Service Switch

During operation, you can adjust services dynamically, enabling or disabling specified services (SNMP Server/SSH Server/Telnet Server/Web Server).

Command	Function
Ruijie(Config)# <b>enable service snmp-agent</b>	Enable SNMP Server.
Ruijie(Config)# <b>enable service ssh-server</b>	Enable SSH Server.
Ruijie(Config)# <b>enable service telnet-server</b>	Enable Telnet Server
Ruijie(Config)# <b>enable service web-server</b>	Enable Http Server.

In the configuration mode, you can use the **no enable service** command to disable corresponding services.

```
Ruijie# configure terminal           //Enter the global configuration mode.
Ruijie(config)# enable service ssh-server //Enable SSH Server
```

## Setting HTTP Parameters

When using the integrated Web for management, you can adjust HTTP parameters, and specify service port or login authentication method.

Command	Function
Ruijie(Config)# <b>ip http port</b> <i>number</i>	Specify HTTP service port, 80 by default.
Ruijie(Config)# <b>ip http authentication</b> { <b>enable</b>   <b>local</b> }	Set Web login authentication method, enable by default. <b>enable</b> : Use the password set by the enable password or enable secret command for authentication, where the password must be 15 levels. <b>local</b> : Use the username and password set by the username command for authentication, where the user must be bound with 15-level right.

In the configuration mode, you can use the **no** form of the command to restore the setting to the default value. The following example enables the HTTP Server, sets the service port to 8080, and uses the local username for login authentication.

```
Ruijie# configure terminal           //Enter the global configuration mode.
Ruijie(config)# enable service web-server http //Enable http Server
Ruijie(config)# username name password pass //Set local user
Ruijie(config)# username name privilege 15 //Bind user right
Ruijie(config)# ip http port 8080 //Set service port
Ruijie(config)# ip http authentication local //Set authentication method
```

Use the following command to configure HTTPS service port.

Command	Function
Ruijie(Config)# <b>ip http secure-port</b> <i>number</i>	Specify the HTTP service port. (default:443)

In the configuration mode, you can use the **no** form of the command to restore the setting to the default value. The following example enables the HTTP Server, sets the service port to 4443.

```
Ruijie# configure terminal           //Enter the global configuration mode.
Ruijie(config)# enable service web-server https //Enable https Server
Ruijie(config)# ip http secure-port 4443
```

Use the following command to verify the status of WEB server.

```
Ruijie# show web-server status
http server status : enabled
http server port : 8080
https server status: enabled
```

```
https server port: 4443
```

**Caution**

Avoid configuring http service port and https service port to the same value. If https service is enabled after http service has been enabled, and the port is accidentally configured to the same port used by http service, then the user can only access https service through this port, and http service will be blocked temporarily until https service port is changed or the service is disabled.



# HTTP Service Configuration

## Overview

### Understanding HTTP

The Hypertext Transfer Protocol (HTTP) is used to deliver Web page information over the Internet. HTTP is located at the application layer of the TCP/IP protocol stack and uses connection-oriented TCP as the transport protocol.

The Hypertext Transfer Protocol Secure (HTTPS) is an HTTP protocol that supports the Secure Sockets Layer (SSL) protocol. Its main idea is to create a secure channel on an unsecure network to prevent information from being monitored and Man-in-the-Middle Attacks. HTTPS is now widely used in communication sensitive to Internet safety, such as electronic payment.

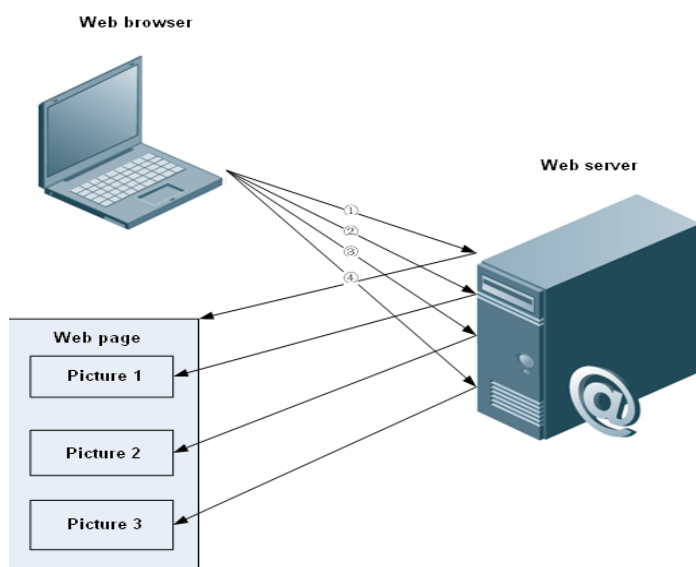
### Basic Concepts

#### HTTP Service

HTTP service uses the HTTP protocol to deliver Web page information on the Internet. HTTP/1.0 is the HTTP protocol version in common use. As a Web server may be accessed for tens of thousands or millions of times a day, HTTP/1.0 adopts the short connection mode to facilitate connection management. A TCP connection is created for a request. After the request completes, the connection will be released. The server does not need to record or track previous requests. Despite that HTTP/1.0 simplifies the connection management, it has weakness in its performance.

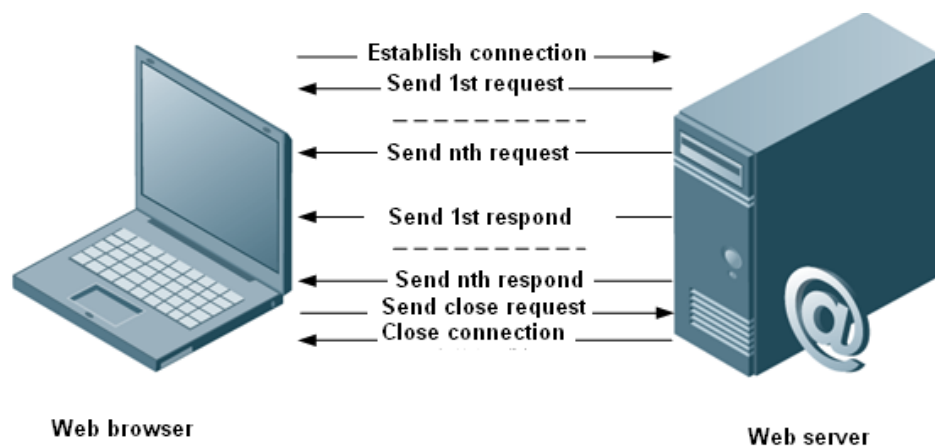
For example, a page may contain many images. In fact, the page contains their URL connection addresses rather than the images themselves. Therefore, a browser will send multiple requests during the access process. A separate connection will be created for each request and every connection is completely isolated. Moreover, the process of establishment and release of connection will substantially affect the performance of clients and the server. See Figure 1-1.

Figure 1-1 HTTP/1.0 protocol packet interaction



HTTP/1.1 solves the weakness. The version supports persistent connection which can transmit multiple requests and responses so that clients do not need to wait for completion of the last request to send the second request. Therefore, network delay is reduced and performance is improved. See Figure 1-2.

Figure 1-2 HTTP/1.1 protocol packet interaction



Currently, Ruijie switches support HTTP/1.0 and HTTP/1.1.

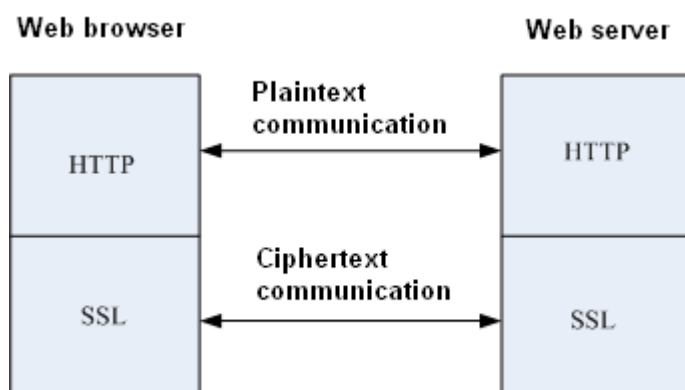
Which protocol version is used by the switch is determined by the Web browser.

## HTTPS Service

HTTPS service adds a SSL layer based on the HTTP to enhance safety. To make the protocol effective, the server must have a Public Key Infrastructure (PKI) certificate, which is unnecessary for clients. The SSL protocol provides the following services:

- Authenticating users and servers to ensure that data is sent to the right clients and servers;
- Encrypting data to prevent interception during transmission;
- Protecting integrity of data and preventing modification of data during transmission.

Figure 1-3 HTTPS service



## HTTP Upgrade Service

HTTP upgrade includes local and remote HTTP upgrade modes.

- During local upgrade, the device serves as the HTTP server and users log in to the device through a Web browser and upload the files to be upgraded to the device and realize the upgrade.
- During remote upgrade, the device serves as the client, connects to the remote HTTP server and acquires the files on the server to upgrade the local files.

## Working Principle

### HTTP Working Process

The HTTP provides services for Web management. Users can log in to devices through the Web interface for configuration and management. Web management includes the Web client and server, and the HTTP service can adopt the client or server mode. The HTTP client is embedded in the Web browser of the Web management client and can send HTTP packets and receive and process HTTP response packets. The Web server (HTTP server) is embedded in the device. The information interaction process between the client and server is described as follows:

- TCP connection is established between the client and server. The default port number of the HTTP service and HTTPS service is 80 and 443 respectively.
- The client sends a request to the server.
- After processing the client's request, the server responds to the client.
- After the HTTP service processes a request, the TCP connection between the client and server is cancelled; the HTTPS can process multiple requests until the client sends a termination request or the connection is cancelled as the server is overtime.

The process of the remote HTTP upgrade service can be summarized as follows:

- Connect to the server. During the connection, prioritize the server address configured by the user. If connection to the address fails, connect to the server address in the local upgrade record.
- Send version numbers of all programs to the server.
- After analysis, the server provides a list of files to be downloaded.
- The device connects to the file server downloads necessary files according to the list. Users can connect to different servers to download different files.
- Prepare for file upgrade.

## Protocol Specification

RFC1945 - Hypertext Transfer Protocol -- HTTP/1.0

RFC2616 - Hypertext Transfer Protocol -- HTTP/1.1

RFC2818 - Hypertext Transfer Protocol Over TLS -- HTTPS

## Typical Application

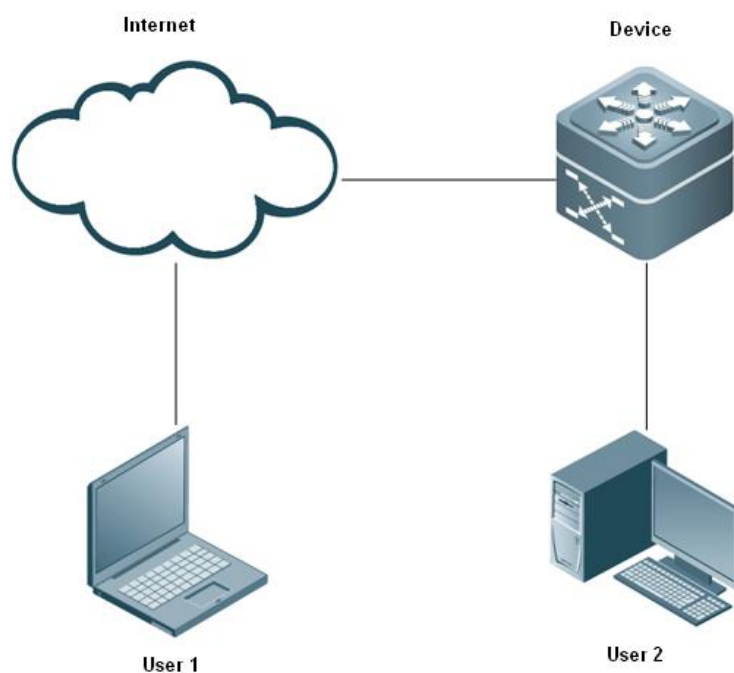
### HTTP Application Service

Web network management remains one of the main methods for users to manage and maintain devices currently. Ruijie's network devices also provide the Web management function. After the HTTP service is enabled on a device, the user only needs to enter `http://` and IP address of the device on the PC's browser to enter the Web management interface after authentication. On the Web interface, the user can monitor device status information, configure the device, and upload and download files.

The ordinary HTTP service is insecure. For security-sensitive communication, Ruijie's devices also provide the safer HTTPS service, which can encrypt the communication between users and devices so that the information cannot be monitored or altered by third parties. Users only need to enter `https://` and the IP address of the device on the browser to enter the Web management interface after authentication.

Figure 1-4 describes a typical application scenario of Web management. The user can access the device remotely over the Internet, also log in to the Web server in LAN to configure and manage the device. The user can choose to enable the HTTPS or HTTP service on the device or enable both at the same time. The user can set the browser to use the HTTP/1.0 or HTTP/1.1 protocol to access the HTTP service of the device.

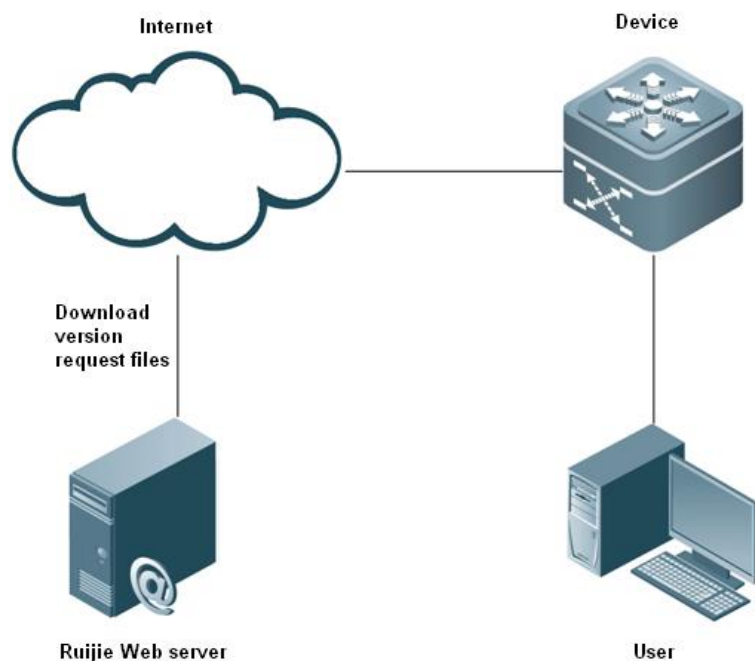
Figure 1-4 HTTP application scenario



### Remote HTTP Upgrade Service

During the remote upgrade, the device serves as the client, connects to the remote HTTP server and acquires the files on the server to upgrade the local files. The default domain name of the Web server provided by Ruijie is `rgos.ruijie.com.cn`. Figure 1-5 shows a typical application scenario.

Figure 1-5 Remote HTTP upgrade



## Configuring HTTP

### Default Configuration

Feature	Default setting
Enabling HTTP service	It is disabled by default.
HTTP Verification mode	By default, the authentication mode of ordinary HTTP service is <b>enable</b> .
HTTP service port	The default port number of the ordinary HTTP service and HTTPS service is 80 and 443 respectively.
HTTP upgrade server	The default server address is 0.0.0.0 and port number is 80.
HTTP upgrade mode	By default, the mode is manual upgrade.
HTTP upgrade auto detect time	By default, it is random.

### Configuration Preconditions

If the authentication mode of the ordinary HTTP service is **enable**, users need to configure the **enable secret** or **enable password** password with the authority level of 15.

If the authentication mode of ordinary HTTP service is **local**, users need to configure the local database's identity information with **username** with the authority level of 15.

Before configuring the domain name of the HTTP upgrade server, users need to enable the DNS function and configure the DNS server address.

### Configuration Steps

Step	Task	Description
1	Enabling HTTP service	"Required"
2	Configuring HTTP verification information	"Optional"; users can configure it when necessary to alter the authentication mode.

Step	Task	Description
3	Configuring HTTP service port	"Optional"; users can configure it when necessary to alter the HTTP service port.
4	Configuring HTTP upgrade server	"Optional"; users can configure it when necessary to specify the server address.
5	Configuring HTTP upgrade mode	"Optional"; users can configure it when necessary to alter the upgrade mode.
6	Configuring HTTP upgrade auto detect time	"Optional"; users can configure it when necessary to alter the auto detect time.
7	HTTP manual upgrade file	"Required"

## Enabling HTTP service

The HTTP service includes the ordinary HTTP and HTTPS service. The HTTPS adds SLL based on the HTTP protocol to improve the safety of information.

Please use the following commands in configuration mode to enable the HTTP service.

Command	Function
Ruijie# <b>configure terminal</b>	Enters global configuration mode.
Ruijie(config)# <b>enable service web-server http</b>	"Required"; enables the ordinary HTTP service.
Ruijie(config)# <b>enable service web-server https</b>	"Required"; enables the HTTPS service.
Ruijie(config)# <b>enable service web-server [all]</b>	"Required"; enables both HTTP and HTTPS services.

Configuration examples:

The following example enables the HTTP and HTTPS services on a Ruijie device.

```
Ruijie# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Ruijie(config)# enable service web-server
```

## Configuring HTTP Authentication Information

To use the HTTP service, users need to pass the login authentication to enter the Web page. Ruijie provides two authentication setting methods.

### ■ Method 1: using **ip http authentication** command

Command	Function
Ruijie# <b>configure terminal</b>	Enters global configuration mode.
Ruijie(config)# <b>ip http authentication { enable   local }</b>	"Optional"; configures the login authentication mode. The default authentication mode is <b>enable</b> .

If the user chooses the **enable** mode, the username is null and password should be set with the **enable password** or **enable secret** command.

If the user chooses the **local** mode, the username and password should be set with the local **username** command.



No matter which mode is adopted, the authentication password has an authority level of 15.


Configuration examples:

The following example configures using local model for Web page authentication on a Ruijie device.

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

■ Method 2: using the **webmaster level** command

Command	Function
Ruijie# <b>configure terminal</b>	Enters global configuration mode.
Ruijie(config)# <b>webmaster level</b> <i>privilege-level</i> <b>username</b> <i>name</i> <b>password</b> { <i>password</i>   [ 0   7 ] <i>encrypted-password</i> }	"Required"; configures login authentication mode, not configured by default.

 Username and password have three authority levels; each authority level can configure 20 usernames and passwords at most.

Configuration examples:

The following example configures using username admin, plaintext password ruijie and authority level 1 for Web authentication.

```
Ruijie# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Ruijie(config)# webmaster level 1 username admin password ruijie
```

## Configuring HTTP Service Port

Configuring the port number can reduce illegal users' attack on the HTTP service. Ruijie's devices support HTTP and HTTPS services.

■ Configuring HTTP port number

Command	Function
Ruijie# <b>configure terminal</b>	Enters global configuration mode.
Ruijie(config)# <b>ip http port</b> <i>port-number</i>	"Optional"; configures the HTTP service port number, which is 80 by default.

Configuration examples:

The following example configures the HTTP service port of the device Ruijie as 8080.

```
Ruijie# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Ruijie(config)# ip http port 8080
```

■ Configuring HTTPS port number

Command	Function
Ruijie# <b>configure terminal</b>	Enters global configuration mode.

Ruijie(config)# <b>ip http secure-port</b> <i>port-number</i>	"Optional"; configures the HTTPS service port number, which is 443 by default.
---	--

Configuration examples:


The following example configures the HTTPS service port of the device Ruijie as 4430.


```
Ruijie# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Ruijie(config)# ip http secure-port 4430
```

## Configuring HTTP Upgrade Server

By default, the server address configured for remote HTTP upgrade is 0.0.0.0 and the port number is 80. Follow the steps to configure the server address:

Command	Function
Ruijie# <b>configure terminal</b>	Enters global configuration mode.
Ruijie(config)# <b>http update server</b> { <i>host-name</i>   <i>ip-address</i> } [ <b>port</b> <i>port-number</i> ]	"Optional"; configures the upgrade server address.

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

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

Server address does not support IPV6.

Configuration examples:

The following example configures the domain name of the HTTP upgrade server as rgos.ruijie.com.cn and the port number as 85.

```
Ruijie# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Ruijie(config)# http update server rgos.ruijie.com.cn port 85
```

## Configuring HTTP Upgrade Mode

The default mode is manual upgrade. To enable the HTTP to automatically detect files that can be upgraded in the server, users can change the upgrade mode. Enter configuration mode and follow the steps:

Command	Function
Ruijie# <b>configure terminal</b>	Enters global configuration mode.
Ruijie(config)# <b>http update mode auto-detect</b>	"Optional"; configures the HTTP upgrade mode as auto detect mode; if it is not configured or the <b>no</b> form of the command is used, the default mode is manual upgrade.

In auto detect mode, the device will detect files in the server during upgrade. Users can view which Web version is available for upgrade in the Web interface.



Configuration examples:

The following example configures HTTP upgrade mode as auto upgrade.

```
Ruijie# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Ruijie(config)# http update mode auto-detect
```

## Configuring HTTP Upgrade Auto Detect Time

In the auto detect mode, the remote HTTP auto detect time is random. To modify the auto detect time, enter configuration mode and follow the steps:

Command	Function
Ruijie# <b>configure terminal</b>	Enters global configuration mode.
Ruijie(config)# <b>http update time daily <i>hh:mm</i></b>	"Optional"; configures the HTTP auto detect time, which is random by default.



The auto detect time must be a specific time accurate to minute.



The configuration command is only effective when HTTP upgrade mode is auto detect.

Configuration examples:

The following example configures the HTTP auto detect time at 3:00 AM everyday.

```
Ruijie# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Ruijie(config)# http update time daily 03:00
```

## HTTP Manual File Upgrade

### ■ Remote upgrade

By default, the HTTP only provides the remote auto detect. The system cannot be automatically upgraded. To enable automatic upgrade, enter privilege mode and follow the steps:

Command	Function
Ruijie# <b>http check-version</b>	"Optional"; detects the upgrade version.
Ruijie# <b>http update web [ <i>version string</i> ]</b>	Version information about the upgrade Web package

Configuration examples:

The following example performs remote HTTP file upgrade on a Ruijie device.

```
Ruijie# http check-version
app name:web
sn          version          filename
-----
0           1.2.1(82381)          web1.2.1(145680).upd
1           1.2.1(82380)          web1.2.1(145680).upd
2           1.2.1(82379)          web1.2.1(145680).upd
3           1.2.1(82378)          web1.2.1(145680).upd
```

## ■ Local upgrade

Users can use **copy tftp** to download the latest Web file to the device and follow the steps:

Command	Function
Ruijie# <b>http web-file update</b>	Updates the Web package.



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

The following example performs the Web package upgrade on a Ruijie's device.

```
Ruijie#copy tftp://10.10.10.13/web_management_pack.upd flash:web_management_pack.upd
Ruijie#http web-file update
```

## Monitoring and Maintenance

### Showing HTTP Configuration Information

Command	Function
<b>show web-server status</b>	Shows the Web service configuration information and status.

Configuration examples:

The following example shows the HTTP configuration information of a Ruijie device.

```
Ruijie# show web-server status
http server status : enabled
http server port : 80
https server status: enabled
https server port: 443
http(s) use memory block: 768, create task num: 0
```

## Configuration Examples

### HTTP Service Configuration Example

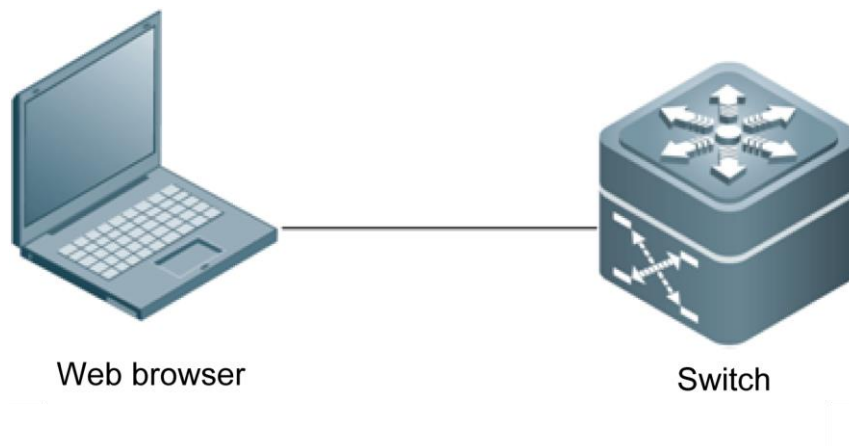
#### Networking Requirements

The network administrator wants to manage a switch through Web management; to log in to the switch through the Web browser and configure related functions.

- Use the local database's identity for authentication.
- Web browser can access the Internet through both the HTTP and HTTPS protocol to improve the security.
- The HTTP service port number is set by the administrative to reduce illegal users' attack on the HTTP.

## Networking Topology

Figure 1-6 HTTP service application topology



## Configuration Tips

The following configuration tips are provided to meet the above-mentioned requirements:

- Use a username to configure the database information to use the local database's identity for authentication.
- Enable both the HTTP and HTTPS services to meet the security requirement.
- Configure the HTTP service port number as 8080; and the HTTPS service port number as 4430.

## Configuration Steps

- 1) Configure the local database's identity information. The username is admin and the plaintext password is ruijie with an authority level of 15.

```
Ruijie#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Ruijie(config)#username admin password ruijie
Ruijie(config)#username admin privilege 15
```

- 2) Enable the HTTP and HTTPS services.

```
Ruijie#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Ruijie(config)#enable service web-server
```

- 3) Configure the HTTP service authentication mode as local.

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

- 4) Configure the HTTP service port as 8080.

```
Ruijie#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Ruijie(config)#ip http port 8080
```

- 5) Configure the HTTPS service port as 4430.

```
Ruijie#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Ruijie(config)#ip http secure-port 4430
```

## Showing Authentication

1) Show HTTP Configuration Information.

```
Ruijie#show web-server status
http server status : enabled
http server port : 8080
https server status: enabled
https server port: 4430
http(s) use memory block: 768, create task num: 0
```

## Remote HTTP Upgrade Configuration Example

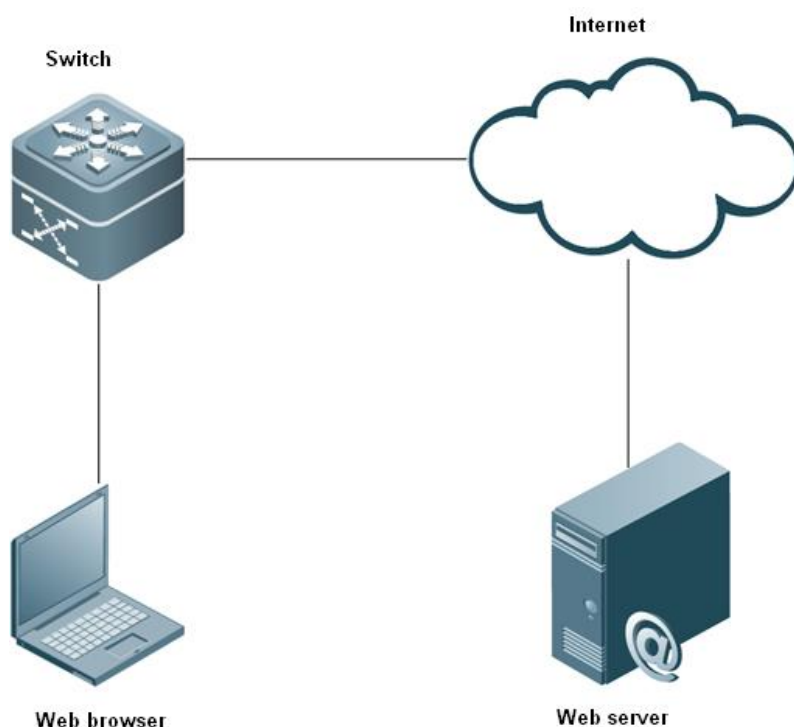
### Networking Requirements

A company purchases a Ruijie's product and intends to use the HTTP upgrade function to upgrade files.

- The device can acquire information about files that can be upgraded remotely from Ruijie's server at a fixed time everyday.
- The device can show files that can be upgraded currently.
- The device can download the latest files from Ruijie's server to upgrade and update the device.

### Networking Topology

Figure 1-7 Remote HTTP upgrade service topology



## Configuration Tips

The following tip is provided to meet the above-mentioned requirements:

- Configure the device to acquire the latest file information at 2:00 AM everyday.

## Configuration Steps

- 2) Configure DNS information.

```
Ruijie#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Ruijie(config)#ip domain-lookup //Enable the device's DNS domain
name analysis function
Ruijie(config)#ip name-server 192.168.5.134 // Configure the DNS server
address
```

- 3) Configure the upgrade server address.

```
Ruijie#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Ruijie(config)# http update server rgos.ruijie.com.cn
```

- 4) Enable auto detect mode and configure the remote monitoring time at 2:00 AM everyday.

```
Ruijie#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Ruijie(config)#http update mode auto-detect
Ruijie(config)#http update time daily 02:00
```

- 5) Acquire the latest information about files that can be upgraded from the remote server.

```
Ruijie#http check-version
app name:web
sn          version          filename
--  -
0          1.2.1(82381)       web1.2.1(145680).upd
1          1.2.1(82380)       web1.2.1(145680).upd
2          1.2.1(82379)       web1.2.1(145680).upd
3          1.2.1(82378)       web1.2.1(145680).upd
```

- 6) Down the files and update the device.

```
Ruijie#http update web
```

## Showing Authentication

The server version information is shown on the Web online upgrade interface.

## Local HTTP Upgrade Configuration Example

### Networking Requirements

- Users can acquire the latest Web package from Ruijie's website and the device can run the latest Web package.

## Networking Topology

Figure 1-8 Local HTTP upgrade service topology



## Configuration Tips

The following tips are provided to meet the above-mentioned requirements:

- Connect the device to the local PC whose IP address is 10.10.10.13; configure the IP address of the device as 10.10.10.131 in the same network segment.
- Download the latest Web package to the device.
- Run the Web package on the device.

## Configuration Steps

- 7) Create VLAN 1 and configure an IP address for the device.

```
Ruijie#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Ruijie(config)#vlan 1
Ruijie(config-vlan)#exit
Ruijie(config)#interface vlan 1
Ruijie(config-VLAN 1)#ip address 10.10.10.131 255.255.255.0
```

- 8) Enable the tftp server on PC and use **copy tftp** command on the device to download the Web package.

```
Ruijie#copy tftp://10.10.10.13/web_management_pack.upd flash:web_management_pack.upd
```

- 9) Update the Web package.

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

## Showing Authentication

Log in to Web management interface again on the PC and detect whether the page is updated.

# LINE Mode Configuration

## Configuring LINE Mode

### Entering the LINE mode

After entering the specific LINE mode, you can configure the specified line. Execute the following commands to enter the specified LINE mode:

Command	Function
Ruijie(config)# <b>line</b> [ <b>console</b>   <b>vty</b> ] <i>first-line</i> <i>[last-line]</i>	Enter the specified LINE mode.

### Increasing/Decreasing LINE VTY

By default, the number of line vty is 5. You can execute the following commands to increase or decrease line vty, up to 36 line vty is supported.

Command	Function
Ruijie(config)# <b>line vty</b> <i>line-number</i>	Increase the number of LINE VTY to the specified value.
Ruijie(config)# <b>no line vty</b> <i>line-number</i>	Decrease the number of LINE VTY to the specified value.

### Configuring the Protocols to Communicate on the Line

To restrain the communication protocol type supported on the line, you can use this command. By default, a VTY supports the communication of all protocols while a TTY do not support the communication of any protocol.

Command	Description
<b>configure terminal</b>	Enter the configuration mode.
<b>line vty</b> <i>line number</i>	Enter the line configuration mode.
<b>transport input</b> { <b>all</b>   <b>ssh</b>   <b>telnet</b>   <b>none</b> }	Configure the protocol to communicate on the line.
<b>no transport input</b>	Disable the communication of any protocol on the line.
<b>default transport input</b>	Restore the setting to the default value.

### Configuring the Access Control List on the Line

To configure the access control list on the line, you can use the command. By default, no access control list is configured on the line. That is, all incoming and outgoing connections are permitted.

Command	Description
<b>configure terminal</b>	Enter the configuration mode.
<b>line vty</b> <i>line number</i>	Enter the line configuration mode.
<b>access-class</b> <i>access-list-number</i> { <b>in</b>   <b>out</b> }	Configure the access control list on the line.
<b>no access-class</b> <i>access-list-number</i> { <b>in</b>   <b>out</b> }	Remove the configuration.



# System Upgrade Configuration

## Understanding Program Image in the System

The system image contains RGOS software. All Ruijie network devices are embedded with specific version of images before distribution. The user may upgrade such images to upgrade the device to the latest version. Use "show version" command to find out the version of images running on the device and the name of various main programs.

RGOS software involves the following types of images:

**Main program:** Also called MAIN, it is a complete image software package. It may contain such images as boot program, line card program and etc. It will be loaded and implement various services when device starts up. Users are generally using and operating on the main program.

**BOOT:** The most fundamental device initialization and boot program. This image is first image run on the device, and generally cannot be upgraded to ensure the system can always be initialized, guided and upgraded (CTRL) correctly. This image only exists in switching devices and line cards of the switch.

**CTRL:** This is a boot program provided with network functions. This program image is initialized by BOOT, and features network communication function and main program booting and upgrading function.

**Bootloader:** Device initialization, network communication and main program booting and upgrading function. This is the first image loaded when the device is powered on, and can boot the main program after device initialization. Routing devices only have Bootloader and Main program. Bootloader has all functions of BOOT and CTRL.

Among the aforementioned program images, only the main program can be viewed, upgraded and modified through file system commands. BOOT/CTRL/Bootloader programs are generally stored in the parallel flash and cannot be managed directly by user. For chassis devices, all line cards have BOOT and CTRL programs, while some line cards may have the main program for line card. Generally, to have new features of a device, you will need to upgrade the main program of the device. In order to maintain the compatibility of BOOT, CTRL and Main programs, as well as the compatibility of the Main program of management board and line card, the upgrade function provides the guarantee to automatic compatibility. Incompatible parts will be upgraded automatically without the need to download upgrade image separately. During the upgrade process, images incompatible with the new-version software will be upgraded automatically. Therefore, the upgrade information of such images will be shown during the upgrade process.

## Overview of Upgrade Function

### Upgrading Image Set

Users generally expect to obtain a more reliable software version and more software features through upgrade. In most cases, these features are related to the main program. The device may contain multiple program images with different functions (such as BOOT/CTRL for booting), and these program images will only work in coordination. Therefore, the upgrade function not only provides the support to main program upgrade, but also allows the automatic synchronized upgrade of respective program images on the device, so that the overall device can maintain good compatibility.

Therefore, the upgrade file contains not only the main program for rendering primary services, but also the BOOT/CTRL images used in conjunction with the main program. When implementing upgrade, these images will be extracted from the upgrade file and upgrade the corresponding images on the device.

### Auto-Installation

If the embedded image version of linecard plugged is incompatible with that of the device, the system will automatically upgrade the image of this linecard before it can work. Some versions of line cards can automatically download image to run from the master management board. This function avoids the need to consider the compatibility between different linecards and the device. The system can well guarantee image compatibility and consistency without the intervention of user.

### Operating Principle

The RGOS program image release for Ruijie devices is a self-extracting executable program. The RGOS program image carries the main program image for the device. For box devices, the RGOS program image contains main program and boot program; for chassis devices, the RGOS program image contains the main program and boot program for respective linecards.

During the upgrade process, the user will first need to operate in the file system to copy the new-version RGOS program image to the device. The user can use this new program image to install the device. During the installation process, the system will automatically search for image to be upgraded and upgrade them one by one. The system will automatically guarantee the compatibility of respective images after the upgrade. No further identification by the user is needed.

As for the upgrade of stacked devices, when the main programs of member devices are different in version, the automatic installation process will start as well. The RGOS program image on the master device will be synchronized to slave devices having the inconsistent version of image, and installation will commence on these devices. After the installation, the entire stack of devices will be reset. When all devices enter into ready state, they will be running the identical main program.

During system upgrade, the user may choose two different means: automatic installation and manual installation. The corresponding processes are shown below:

Automatic installation: The new-version file is copied to the device -> reset device -> wait until device installation is completed

Manual installation: The new-version file is copied to the device -> input install command -> reset device

The advantage of manual installation is that the system services will not be affected during installation. If any accident incurs during the installation, as long as the device is powered on, the installation operation can be repeated without

leading to any risk. Once the installation is completed successfully, the device can function immediately after restart. The manual installation is featured by shorter offline time and higher security.

Automatic installation is easy to operate, and no intervention by user is needed once the upgrade process commences.

## Protocol Specification

N/A

## Default Configurations

N/A

## Upgrade Steps

Device upgrade will require the following steps:

- Preparation before upgrade
- Copy image file to the device
- Device installation and upgrade
- Verify device installation



### Note

Do not carry out upgrade or hot-plug/reset the line card when the device is extremely busy (with CPU utilization rate > 70%). This may lead to unsuccessful upgrade or boot failure of line card, including:

1. Reset line card or dynamically plug in the line card. If the CPU utilization rate is excessively high, the automatic upgrade of this line card or image distribution may fail. Please try to reset the line card again after the CPU utilization rate goes down, until the line card is successfully upgraded or booted.
2. During the process of manual upgrade, high CPU utilization rate will lead to the failure of upgrade. By this time, the user will need to retry manual upgrade after the CPU utilization rate goes down.

## Preparation Before Upgrade

Make the following preparations before implementing device upgrade:

Backup configuration file

Confirm the space of file system

Confirm the method of file download

**Caution**

The upgrade may fail if implemented when the device is busy or being attacked. Please use "show cpu" command to verify whether the system is busy or not, and implement upgrade when the CPU utilization rate is lower than 20%.

## Backup Configuration File

Backup of configuration files is needed before the upgrade. Since different versions of software may contain different default configurations, the newly added default configurations may conflict with the current configurations. In order to ensure successful upgrade, please backup the original configuration file before the upgrade. After successful upgrade, verify whether there is any conflict in configurations.

## Confirm the Space of File System

The user may use "show file system" or "dir" command to learn the space and its usage of the existing file system.

If the target file system has sufficient space to store both new and old program images, then during the upgrade process, the original boot/main program will be renamed as "original filename.bak". When the CTRL version is 10.4 or above, this file will be used as the backup image of new program image. When the new program image fails, the system will boot with this back image. This can save the rollback operation required in the case of upgrade failure.

When the system has hardly any residual space, the user will need to clean up the file system in order to make sure the upgrade is successful. Unnecessary files can be deleted using "del" command. While upgrading the chassis device with dual management boards, the file system space of the slave board shall also be verified. The URL prefix of file system space of the slave board is "slave:".

**Caution**

When file system space is insufficient to store two program images, the backup file of original program image will not be generated.

**Caution**

Timely cleanup of file system will facilitate quick completion of upgrade. When the number and size of files in the file system are comparatively large, the booting speed of device will be subject to great influence. Before upgrade, delete unnecessary files as far as possible.

Installation of software with version older than 10.4(2) will leave such files as install\_xxxx.bin on the management board of chassis device. After the software is upgraded to 10.4(2) or higher version, these files will become useless and shall be deleted manually in order not to slow down booting speed of system.

## Confirm the Method of file Download

There are following means to download RGOS program image to the device:

- Transfer the file via TFTP server

This is the most commonly used method, which allows remote upgrade.

One way is to download the upgrade file from the host to the device, and the other way is to upload the file from the device to the host.

In CLI command mode, download the file by performing the following steps:

Before downloading the file, enable TFTP Server software on the local host, and then select the directory for the file to be downloaded, and then log in to the device and use the following command in privileged mode to download the file. Enter the IP address of the TFTP Server if the parameter location is not specified.

Command	Function
Ruijie# <b>copy tftp: //location / filename flash: filename</b>	Download the file <i>filename</i> specified by URL of the host to the device.

In CLI command mode, upload the file by performing the following steps:

Before uploading the file, enable TFTP Server software on the local host, and then select the directory for saving the file to be uploaded on the host, and use the following command in the privileged mode to upload the file.

Command	Function
Ruijie# <b>copy flash: filename tftp: //location / filename</b>	Upload the file <i>filename</i> from the device to the directory specified by URL of the host. The file name can be reset.



If the name of a source file contains a space, it is required to add quotation marks to the tftp link, as shown as follows:

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

Similarly, if the name of a destination file contains a space, it is also required to add quotation marks to the file name, as shown as follows:

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

#### ■ Transfer the file via TFTP IPv6

One way is to download the upgrade file from the host to the device, and the other way is to upload the file from the device to the host.

In CLI command mode, download the file by performing the following steps:

Before downloading the file, enable TFTP Server first, and the log in to the device and use the following command in the privileged mode to download the file.

Command	Function
Ruijie# <b>copy tftp: //location/filename flash: filename</b>	Download the file <i>filename</i> under the directory specified by the TFTP server of the host to the device.

In CLI command mode, upload the file by performing the following steps:

Before uploading the file, enable the TFTP Server software on the local host, and then select the directory for saving the file to be uploaded on the host, and use the following command in the privileged mode to upload the file.

Command	Function
---------	----------

Ruijie# <b>copy flash: filename tftp: //location/filename</b>	Upload the file <i>filename</i> from the device to the directory specified by TFTP server of the host. The file name can be reset.
---	--

- ⚡ If the parameter location is the local address of the link, it is required to specify an egress. Use the following extended commands to specify one.

```
Ruijie# copy tftp: flash:
Address of remote host []?fe80::5efe:192.168.195.90
Output Interface: loopback 0
Source filename []?rgos.bin
Extended commands [n]:
Destination filename [rgos.bin]?
```

- ☑ This command is supported by all products in release 10.X.

When user uses "copy tftp" command to download upgrade file from tftp server to the device (master management board) and at the same time overwrites the boot/main program, the system will check the validity of the upgrade file downloaded (i.e., whether inappropriate upgrade file is downloaded, or whether the upgrade file is corrupted). Upgrading of boot/main program via other means (such as ftp, xmodem and other file system commands) will not result in validity check. In addition, using "copy tftp" command to overwrite the boot image of slave board won't lead to the corresponding check as well. Therefore, when selecting the download method, it is generally recommended to use "copy tftp" command to overwrite the boot image (master management board) of the device, as it is the safest upgrade method.

- 📖 If the user doesn't want to use this download method, we recommend you to adopt manual installation ("upgrade system" installation command) after copying the upgrade file to the device. Manual installation is safer, and allows the user to quickly discover image problems and timely correct such problems.

- ⚡ TFTP only supports the transfer of files with size below 32 M. If the file size is larger than 32 M, the file will have to be downloaded via FTP or flash disk.

#### ■ Transfer the file via xmodem

Xmodem download is applicable to some exceptional cases, such as the failure in network connection. Before using xmodem download, make sure the device is linked to console with serial line. In order to obtain faster download speed, the baud rate of connection can be increased. At the same time, make sure the terminal software supports xmodem transmission.

One way is to download the upgrade file from the host to the device, and the other way is to upload the file from the device to the host.

In CLI command mode, download the file by performing the following steps:

Before downloading the file, log in to the out-of-band management interface of the device via Windows hyper terminal, and then use the following command in the privileged mode to download the file, and then in the page of Windows hyper terminal on the local host, select Send the file in Transmit menu.

In the pop-up dialog box, select the file to be downloaded by the local host for the file name and **Xmodem** for protocol and click **Send**. The Windows hyper terminal displays sending progress and packets.

Command	Function
Ruijie# <b>copy xmodem flash:filename</b>	Download the file from the host to the device and name it <i>filename</i> .

In CLI command mode, upload the file by performing the following steps:

Before uploading the file, log in to the out-of-band management interface of the device via Windows hyper terminal, and then use the following command in the privileged mode to upload the file, and then in the page of Windows hyper terminal on the local host, select **Receive the file** in **Transmit** menu.

In the pop-up dialog box, select the directory for saving the file to be uploaded and select **Xmodem** for protocol and then click **Receive**. The hyper terminal will prompt the name of the file saved locally to the user again. Click **Yes** to receive the file.

Command	Function
Ruijie# <b>copy flash:filename xmodem</b>	Upload the file <i>filename</i> from the device to the host.

⚡ If the file name contains a space, it is required to add quotation marks to the file name, as shown as follows:

copy xmodem flash:"*filename*" or copy flash:"*filename*" xmodem

⚡ Using this method to copy the upgrade file will not lead to validity check. In addition, this method cannot be used when there are two management boards.

#### ■ Copy via flash disk

Plug the flash disk stored with RGOS program image to the USB port. Make sure the device has found this USB apparatus.



Supported by all devices provided with USB port.



#### Caution

Using this method to copy upgrade file will not lead to validity check. In addition, this method cannot be used when there are two management boards.

#### ■ Download via FTP

Set the device as FTP server, and use FTP client to download upgrade file.



### Caution

Using this method to copy upgrade file will not lead to validity check. In addition, this method cannot be used when there are two management boards.

## Typical Upgrade Process

## Upgrade of Box Device

- Copy the new-version software to the device:

```
Ruijie#copy tftp://192.168.201.98/rgos.bin flash:rgos.bin
Accessing tftp://192.168.201.98/ rgos.bin...
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Checking file, please wait for a few minutes ....
Check file success.

Transmission finished, file length 7243040

THE PROGRAM VERSION: RGOS 10.4.*, Release(64047)
Upgrade Master CM main program OK.

CURRENT PRODUCT INFORMATION :
    PRODUCT ID: 0x20110010
    PRODUCT DESCRIPTION: Ruijie Gigabit Security & Intelligence Access Switch (S2628G) By Ruijie
Network

SUCCESS: UPGRADING OK.
```

- Reset the device:

```
Ruijie# reload
```

Wait for device installation after device reboot:

In most cases, when upgrading older version to 10.4(2) or higher version, the device will become usable at once without any installation after device reset. The installation process will only show up in very few cases, and the system will display the following prompt of BOOT or CTRL image upgrade:

```
Upgrading CTRL...
DO NOT POWER OFF!
Erasing device...eeeeeeeeeeeeeeeeeeeeeeeeeeeeeeee [ok]
Writing flash ##### [OK - 1,215,488 bytes]
*Apr  1 07:32:44: %UPGRADE-5-LOCAL FIN: New software image installed in flash.
```





## Caution

When the system prompts any flash operation (such as "Erasing device" or "Writing flash" as shown above), never turn the device off. Any power failure during flash operation will lead to boot failure of device, and such failure cannot be recovered.

- Degrade to 10.4(1) or older version

The degrading steps are exactly same as the upgrading steps. Only the interface of installation waiting process is different.

Copy the new-version software to the device:

```
Ruijie#copy tftp://192.168.201.98/rgos.bin flash:rgos.bin
Accessing tftp://192.168.201.98/rgos.bin...
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Transmission finished, file length 6128032 bytes.
Verify the system boot image .[ok]

CURRENT PRODUCT INFORMATION :
    PRODUCT ID: 0x20110010
    PRODUCT DESCRIPTION: Ruijie Gigabit Security & Intelligence Access Switch (S2628G) By Ruijie Networks

SUCCESS: UPGRADING OK.
```

- Reset the device:

Ruijie#reload

Wait for device installation after device reboot:

After reboot, the device will automatically commence local image installation. For example:

[illegible]

```
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Checking file, please wait for a few minutes ....
Check file success.
Upgrade main succeed.
Installation process finished successfully ...
```

Upon completion of automatic installation, the system will reset the device automatically.

```
SYS-5-RESTART: The device is restarting. Reason: Upgrade product !.
```

After the reset, the device will enter into ready state.

## Dynamic Linecard Plug-in

When linecard is dynamically inserted in the device, the system will automatically check the software version of this linecard. If its software version is incompatible with that of master management board, then this card will be automatically upgraded by the system before operation.

The following is an example of dynamically inserting a line card with incompatible software version in the device (running 10.4(1) or older version):

```
*Apr 1 06:17:31: %7: MODULE-6-INSTALL: Install Module M8600-24GT/12SFP in slot 5.
*Apr 1 06:17:33: %OIR-6-INSCARD: Card inserted in slot 5, interfaces are now online.
*Apr 1 06:17:33: %7: Card in slot [5] CPU 0 need to do version synchronization ...Current
software version :
*Apr 1 06:17:33: %7: BOOT VERSION: 10.4.59831
*Apr 1 06:17:33: %7: CTRL VERSION: 10.4.64046
*Apr 1 06:17:33: %7: MAIN VERSION: 10.4.63967
*Apr 1 06:17:33: %7: Need update to software version :
*Apr 1 06:17:33: %7: BOOT VERSION: 10.4.59831
*Apr 1 06:17:33: %7: CTRL VERSION: 10.4.59831
*Apr 1 06:17:33: %7: MAIN VERSION: 10.4.61477
*Apr 1 06:17:33: %7: Install package transmission begin, wait please ...
*Apr 1 06:17:33: %7: Transmitting install package file to slot [5] ...
*Apr 1 06:17:33: %7: Transmitting file install_lc_20070010.bin;
*Apr 1 06:17:59: %7: Transmitting install package file to slot [5] OK ...
*Apr 1 06:17:59: %7: Install package transmission finished, system will reset cards ...
*Apr 1 06:17:59: %7: Reset card in slot [5]
*Apr 1 06:17:59: %7: Software installation is in process, wait please ...
*Apr 1 06:17:59: %7: Installing, wait please !
*Apr 1 06:18:01: %OIR-6-REMCARD: Card removed from slot 5, interfaces disabled.
*Apr 1 06:18:09: %7: Installing, wait please !
*Apr 1 06:19:29: %7: Installing, wait please !
*Apr 1 06:19:39: %7: Installing, wait please !
*Apr 1 06:19:49: %7: Installing, wait please !
*Apr 1 06:19:59: %7: Installing, wait please !
```

```
*Apr  1 06:20:08: %OIR-6-INSCARD: Card inserted in slot 5, interfaces are now online.
*Apr  1 06:20:08: %AUTO_UPGRADE-6-VER_SYNC_SUCCEED: Version synchronization for line card in
slot [5] has been succeeded.
```

The following is an example of dynamically inserting a line card with incompatible software version in the device (running 10.4(2) or higher version):

These images in linecard will be updated:

Slot	image	linecard
3	MAIN	M8600-24GT/12SFP

```
*Aug  7 07:46:25: %UPGRADE-5-SLOT_BEG: (Slot 3): Installing MAIN
(Slot 3): Download image
*Aug  7 07:47:21: %UPGRADE-5-SLOT_SUCC: (Slot 3): MAIN installed.
*Aug  7 07:47:21: %UPGRADE-5-SLOT_FIN: (Slot 3): All images is installed.
*Aug  7 07:47:21: %UPGRADE-5-RESET CARD: (Slot 3): Reset.
```

The following is an example of dynamically inserting a line card with compatible software version (only when the master management board is running 10.4(2) or higher version):

```
*Apr  2 07:39:06: %UPGRADE-5-DISPATCH_BEGIN: Dispatch image to slot 3.
Download image to slot 3: !!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!![OK - 8,007,680 bytes]
```

Waiting for image installed....Complete



### Caution

When line card inserted cannot be supported by the existing master management board, the system will prompt:

```
UPGRADE-4-CARDNOTSUPPORT: The linecard in slot 1/4 is not
supported by current version.
```

## Verify Device Installation

After the system installation, the user may use the **show version** command to verify the conditions of device upgrade, and make sure the version of main program is same as the anticipated version. It is normal that the versions of BOOT, CTRL and Bootloader programs and the image of line card may be different from the version of the main program package.

The displayed main program version indicates the version number of main program being run in the system. Therefore, in the case of manual installation, the displayed version number of main program is not the version number of software newly installed, but the version number of software run currently.

For chassis device, if the line card automatic installation process begins, the line card will be reset and execute the new program. The user needs to wait until the line card enters into UP state and then uses **show version** command to verify its version number.

The following is an example of executing **show version** command on the device with two management boards and two line cards:

```
Ruijie#sh version
System description      : Ruijie High-density IPv6 10G Core Routing Switch(S8614) By Ruijie
Networks
System start time      : 2008-01-04 3:20:23
System uptime          : 0:15:35:55
System hardware version : 1.0
System software version : RGOS 10.4(2) Release(64533)
System BOOT version    : 10.4 Release(59831)
System CTRL version    : 10.4(2) Release(64533)
Module information:
  Slot-8 : M8600-48GT/4SFP
    Hardware version : 1.0
    Software version : RGOS 10.4(2) Release(64533)
    BOOT version    : 10.4 Release(59831)
    CTRL version    : 10.4(2) Release(64533)
  Slot-9 : M8600-24SFP-E
    Hardware version : 2.0
    Software version : RGOS 10.4(2) Release(64533)
    BOOT version    : 10.4 Release(59831)
    CTRL version    : 10.4(2) Release(64533)
  Slot-M1 : M8614-CM II
    Hardware version : 1.0
    Software version : RGOS 10.4(2) Release(64533)
    BOOT version    : 10.4 Release(59831)
    CTRL version    : 10.4(2) Release(64533)
  Slot-M2 : M8614-CM II
    Hardware version : 1.0
    Software version : RGOS 10.4(2) Release(64533)
    BOOT version    : 10.4 Release(59831)
CTRL version          : 10.4(2) Release(64533)
```

**Note**

When using "show version" command to show the version number of image with version older than 10.4(2), the system cannot display the release version marking of this image. The release version marking indicates the release time of this image, and is shown in the brackets after the version number. For example, in the version number of 10.4(2), "2" is the release version marking.

For instance, when using "show version" command, versions older than 10.4(2) will display the version number of 10.4 Release (59831) or 10.4.59831, while the versions higher than 10.4(2) will display the version number of 10.4(2) release (59381).

**Caution**

For versions higher than 10.4(2), no reset operation will be needed after the installation. To verify whether the automatic installation process of chassis device is completed, check if the installation list information shown during the installation process indicates the end of operation, or use "show version" command to check whether each card on the device is ready.

## Other Upgrade Processing


After the system completed the preceding upgrade installation, part of the products and systems need some additional processing. For example, in VSU stack scenario, to ensure the certainty of start-up configuration of the system, it is recommended to synchronize the configuration file.


### Synchronizing the Configuration File

In some products systems, for example, in VSU stack scenario, when users use the **rename** command or commands in the format like **copy tftp://172.18.2.65/config.text startup-config** to update the start-up configuration file on the master device, the start-up configuration file will not be synchronized to slave and candidate devices immediately (some product systems only support configuration synchronization and timed synchronization triggered by the **write** command). At this time, if the system is reset and the master device changes after system reset, the start-up configuration of the system is not the same as expected.

To avoid the preceding problem, after updating the configuration file on the master device, you can use the **synchronize filename** command to synchronize the file to each non-master devices, for example:

```
Ruijie#synchronize flash:rgos.bin
Synchornize file /rgos.bin to slave:/
Device(6): download
file!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!![OK
- 10,414,752 bytes]
Synchornize file to slave devices successfully!
```

 The **synchronize filename** command can be used to synchronize any file (not only the configuration file) on the master device to each non-master devices in the same name and under the same path.

 Since establishing the communication check requires processes and topological environment may change, confirm whether the file is already synchronized to all non-master devices successfully as expected according to prompt information. If it does not, retry the command.

 The preceding prompt and functions are supported only by products in v10.4 (3b16) and later.

## Common Upgrade Problems

### Loss of Main Program of Master Management Board

The user may accidentally delete the boot/main program of the file system, and the system will give the following warning information:

Warning: System boot file rgos.bin is missing.

### Insufficient File System Space

Insufficient file system space may take place during download or file copying. The system will prompt:

Insufficient file system space.

By this time, useless files on the file system shall be cleaned up. For device with smaller file system space, the current boot/main program can be deleted as long as the device is powered on, and then use "copy tftp" command to copy the new upgrade file to the device as the new boot/main program.

### Boot/main Program not Overwritten during Upgrade

If the boot/main program is not upgraded during the upgrade, the new program will not run after system reboot.

As for the slave board, please verify the name of boot/main program before upgrade. If the boot/main program is not upgraded, the software versions of master and slave boards may be inconsistent after system reboot.

### Boot/main Program Name Error

The user may use the **boot system** command to set a nonexistent boot/main program.

Warning: System boot file xxx is missing.

By this time, the user needs to verify whether the configured filename is correct, and shall especially pay attention to the case-sensitive problem.

### Timeout Failure Displayed during Upgrade

The timeout failure may be displayed during the upgrade.

\*Feb 10 15:47:12: %UPGRADE-4-PROTO\_TIMEOUT: Server is busy and ack timeout.

By this time, the following solutions can be used:

Ensure whether the boardcards to be upgraded are plugged or reset.

Ensure whether the boardcards to be upgraded are busy (with high CPU utilization rate)

Ensure whether the boardcards to be upgraded are using large file system space, if so, remove some useless files, and retry the upgrade after freeing the file system space.

# File System Configuration

## Overview

The file system offers a unified management of file crossing platforms, no matter what kinds of devices, storages and file transmission protocol are used.

Locally, there are many kinds of storage medias, for instance, USB and FLASH, which can be distributed on different boards like primary control module and secondary module. Users can exchange files with remote devices through xModem and TFTP protocols under file management commands.

Not all types of devices and all types of file systems support all file system commands described in this chapter, because they support different types of file operations. The Help command shows the storage medias and protocols supported by the file operation commands.

## Basic Features of File System

### Using URL to Locate A File

The file system uses URL to uniformly locate the files and directories in the storage medias of local device or remote device. For example, you can copy a file by using the **copy** *source-url destination-url* command, which can be local or remote.

URL representation varies by commands.

#### Locate the file on the server

To locate the file on the server, use the following command:

**tftp:***[[//location]/directory]/filename*

*location*: IP address or host name

*/directory*: position for file transmission. For instance, the file transmission directory specified by the TFTP server is C:\download, the file path specified by the device is the one under C:\download. *tftp://192.168.0.1/binary/rgos.bin* refers to the *c:\download\binary\rgos.bin* file on the TFTP server of the IP address of 192.168.0.1.

For software versions earlier than 10.4(3), TFTP can only transfer a file whose size is smaller than 32 MB. You need to use FTP to transfer a file whose size is greater than 32 MB. Use the device as the FTP server to upload or download files to the device. For software versions later than 10.4(3), TFTP can transfer a file of any size.



#### Note

TFTP transmits only the files in the size of less than 32M. To transmit the files in the size of larger than 32M, use the FTP protocol.

#### Locate the local file

To locate the local file from FLASH, USB and the FLASH of the control module of the device, use the *[prefix]:[directory]/filename* syntax. For example:



flash:/config.text: the configuration on the local FLASH

usb0:/backup/rgos.bin.bak: the file on the first USB

slave:/rgos.bin: the file under the root directory of the secondary control module



#### Note

Without prefix, the syntax refers to the file system type in the current path, for instance, usb0 under the root directory of USB0.



#### Note

When you use prefix to specify a local file, the path after ":" must be absolute path.

## Description of URL prefix

URL prefix is used to specify a file system. Different devices and file operation commands can run different file systems. You can show the file system supported on the device by the **show file system** command.

The following table shows the URL prefixes:

Prefix	Description
<b>flash:</b>	FLASH, which can be used on all devices. The startup program is generally stored in the FLASH of a device when delivery.
<b>tftp:</b>	TFTP server
<b>xmodem:</b>	Receive and send files through xModem
slave:	FLASH on the secondary control module of the rack-mounted device
usb0:	The first USB device
usb1:	The second USB device
sd0:	First SD card
sw1-m1-disk0:	Management module in slot M1 on the cabinet whose switch ID is 1 in the VSU mode
sw1-m2-disk0:	Management module in slot M2 on the cabinet whose switch ID is 1
sw2-m1-disk0:	Management module in slot M1 on the cabinet whose switch ID is 2
sw2-m2-disk0:	Management module in slot M2 on the cabinet whose switch ID is 2



Different file system commands and product platforms support different types of file systems. In addition, it varies in the support for file system operation prefix combination. Therefore, you need to use them according to the actual situations. To understand current commands support which types of file system services, view the help information in command lines. For example (this example is only for your reference, and it varies in the actual situation):

**Note**

Different file system commands and different platforms support different types of file system. For details, use the help information in the command line, for example:

```
WORD          Copy from current file system
flash:        Copy from flash: file system
running-config Copy from current system configuration
slave:        Copy from slave: file system
startup-config Copy from startup configuration
tftp:         Copy from tftp: file system
usb0:         Copy from usb0: file system
usb1:         Copy from usb1: file system
sd0:          Copy from sd0: file system
xmodem:       Copy from xmodem: file system
```

**Note**

Given the limit of xModem, the size of the files transmitted through xModem will be slightly larger than the real file size.

## Showing the File System Information

This command shows all the file systems supported on the device and their available spaces.

In the privileged EXEC mode, use the following command:

```
Ruijie#show file systems
```

File Systems:

	Size (b)	Free (b)	Type	Flags	Prefixes
	-----	-----	-----	-----	-----
*	33488896	16191488	flash	rw	flash:
	-	-	flash	rw	usb0:
	-	-	flash	rw	usb1:
	-	-	flash	rw	sd0:
	-	-	flash	rw	slave:
	-	-	network	rw	tftp:
	-	-	network	rw	xmodem:

In this information, “\*” means the active file system, size means the space of the file system and free means the available space.

**Note**

Free means the available space of the file system, not the size of the file to be stored. Since the file system has its own management overhead, the size of the files that the system finally can store is slightly less than the free space.

## Managing Local Files

Local files refer to the ones storing in various storage medias on the device, for instance, FLASH, and USB. The system files such as main program, configuration, file, logs and web files are stored generally in FLASH. Some devices come with USB interface. The files on the U-shaped disc are also local files. For each-mounted device with dual control modules, you can manage the files in the FLASH of the secondary control module by the slave prefix of URL.

For local files, you can:

- Copy files
- Move files
- Delete files
- Create directory
- Delete directory
- Show directory
- Show the current working path
- Modify the working path

These operations apply to slave-, USB-, or FLASH-type file systems.



### Note

File name is case sensitive on the FLASH- and slave- file systems. For example, abc.txt and Abc.txt are different documents. On USB-type file system, however, file name is not case sensitive, namely abc.txt and Abc.txt are considered to be one document.



### Note

Number and size of files will influence the startup speed and operation speed of files at a certain extent. Too many large files stored in FLASH will slow down the startup and update of devices. When the device starts for the first time, the waiting time of the **dir** command is longer. Generally, it is recommended to use the file system of less than 128M. When it is necessary to store a lot number of files, it is recommended to store them on U-shaped disc. After using the file system for a long period of time, clear some old and useless files by hand.

Some files are important for normal operation. Deleting these files will cause malfunction. These important system files include:

- RCMS configuration file (/rcms\_config.ini)
- Web management package (/web\_management\_pack.upd)
- Main program (for multi-boot-supported devices, the main program includes all the files in the boot system configuration)

**Note**

The system will automatically recognize these files and trigger an alarm before you execute deletion operation. If you need to delete system files, the system will print WARN-level logs as below:

```
Ruijie# delete rgos.bin
```

File [rgos.bin] is a system file. System may not work properly without it.

Are you sure you want to delete it? [no] yes

```
0:1:1:38 Ruijie: FS-4-SYSTEM_FILE_DELETED: System file [rgos.bin] deleted!
```

**Note**

The file name with path should be no more than 4096 bytes. Wildcard is not supported for file name and path.

## Transmitting Files through Communication Protocols

### Transmit files through TFTP:

You are allowed to upload and download files to the TFTP server.

In the CLI privileged EXEC mode, use the following command to download files:

```
Ruijie# copy tftp:[[/location]/directory]/filename destination-url
```

In the CLI privileged EXEC mode, use the following command to upload files:

```
Ruijie# copy source-url tftp:[[/location]/directory]/filename
```

### Transmit files through xModem:

In the CLI privileged EXEC mode, use the following command to download files:

```
Ruijie# copy xmodem: destination-url
```

In the CLI privileged EXEC mode, use the following command to upload files:

```
Ruijie# copy source-url xmodem:
```

## Typical Configuration Example

### Downloading Files from the TFTP Server

The following example shows how to download a.dat from the c:\download\ of the TFTP server to the local device:

Step 1: Run the TFTP Server on the host and select C:\download where the file to be downloaded locates.

Step 2: Use the ping command to test the connection between the device and the TFTP server.

Step 3: Log on the device, enter the privileged EXEC mode and run the command:

```
Ruijie#copy tftp://192.168.201.54/a.dat flash:
Destination filename [a.dat]?
Accessing tftp://192.168.201.54/a.dat
!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Transmission finished, file length 343040
```

Step 4: Run the dir command to show the files on the device.

```
Ruijie#dir
Directory of flash:/

   Mode Link          Size           MTime Name
-----
      1   343040 2009-01-01 02:02:59 a.dat
      1 10838016 2009-01-01 00:08:38 rgos.bin
      1     399 2009-01-01 00:01:37 config.text
-----
3 Files (Total size 11181455 Bytes), 9 Directories.
Total 33030144 bytes (31MB) in this device, 20492288 bytes (19MB) available.
```

## Uploading Files to the TFTP Server

The following example shows how to upload a.dat to the c:\download\ of the TFTP server:

Step 1: Run the TFTP Server on the host and select C:\download where the file to be uploaded locates.

Step 2: Use the ping command to test the connection between the device and the TFTP server.

Step 3: Log on the device, enter the privileged EXEC mode and run the command:

```
Ruijie#copy flash:/a.dat tftp://192.168.201.54/a.dat
Accessing flash:a.dat...
!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Transmission finished, file length 343040
```

Step 4: Check the result.

## Downloading Files through xModem

The following example shows how to download config.txt from PC through xModem to the local device:

Step 1: Use serial cable to connect the serial interface of PC and the serial interface of the device.

Step 2: Run the hyperterminal of Windows to connect to the console of the device.

Step 3: In the privileged EXEC mode, use the following command to download file:

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

Step 4: In the Windows hyperterminal of local device, select Transmit files of Transmit menu.

Step 5: In the pop-up dialog box, select the file to download and xModem. Click Transmit. The Windows hyperterminal shows the transmission progress and packets.

Step 6: Run the dir command to show the files on the device.

```
Directory of flash:/
  Mode Link          Size           MTime Name
-----
      1   343040 2009-01-01 02:02:59 a.dat
      1 10838016 2009-01-01 00:08:38 rgos.bin
      1     399 2009-01-01 00:01:37 config.text
-----
3 Files (Total size 11181455 Bytes), 0 Directories.
Total 33030144 bytes (31MB) in this device, 20492288 bytes (19MB) available.
```

## Uploading Files through xModem

The following example shows how to upload config.txt from the local device through xModem to C:\Documents and Settings\ju of PC:

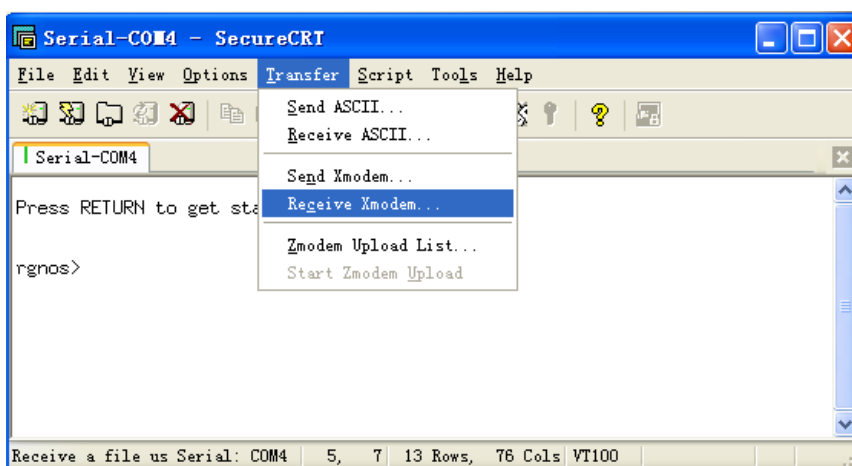
Step 1: Use serial cable to connect the serial interface of PC and the serial interface of the device.

Step 2: Run the hyperterminal of Windows to connect to the console of the device.

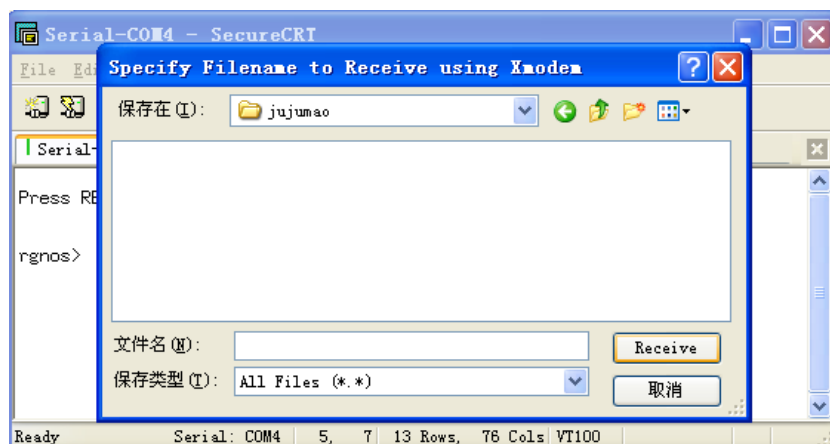
Step 3: In the privileged EXEC mode, use the following command to upload file:

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

Step 4: In the Windows hyperterminal of local device, select Receive files of Transmit menu, as shown below:



Step 5: In the pop-up dialog box, select the place to save the uploaded file and xModem. Click Receive. The Windows hyperterminal prompts to set the name used to store the file. Click OK.



Step 6: Check the configuration.

## Moving Files from FLASH to USB

The following example shows how to move config.txt from FLASH to U-shaped disc inserting USB0 and save it in the backup directory of U-shaped disc:

```
Directory of flash:/
  Mode Link      Size           MTime      Name
-----
      1    343040 2009-01-01 02:02:59   a.dat
      1  10838016 2009-01-01 00:08:38   rgos.bin
      1      399 2009-01-01 00:01:37   config.text
-----
3 Files (Total size 11181455 Bytes), 0 Directories.
Total 33030144 bytes (31MB) in this device, 20492288 bytes (19MB) available.
```

Enter the root directory of U-shaped disc:

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

Confirm the current path:

```
Ruijie#pwd
usb0:/
```

Create backup directory on U-shaped disc:

```
Ruijie#mkdir backup
```

Copy the file to U-shaped disc:

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

Check the result.

```
Ruijie#dir backup
Directory of usb0:/backup
  Mode Link      Size           MTime      Name
-----
```

```
1      399    2009-01-01 00:01:37  config.text
```

```
-----
Total 33030144 bytes (31MB) in this device, 20488192 bytes (19MB) available.
```

Command	Function
Ruijie# <b>rename flash: <i>old_filename</i> flash: <i>new_filename</i></b>	Name the file named as <i>old_filename</i> to <i>new_filename</i> .

## Moving Files from FLASH to SD Card

The following example shows how to move config.txt from FLASH to SD card and save it in the backup directory of SD card:

```
Directory of flash:/
```

Mode	Link	Size	MTime	Name
1		343040	2009-01-01 02:02:59	a.dat
1		10838016	2009-01-01 00:08:38	rgos.bin
1		399	2009-01-01 00:01:37	config.text

```
-----
3 Files (Total size 11181455 Bytes), 0 Directories.
```

```
Total 33030144 bytes (31MB) in this device, 20492288 bytes (19MB) available.
```

Enter the root directory of SD card:

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

Confirm the current path:

```
Ruijie#pwd
sd0:/
```

Create backup directory on the SD card:

```
Ruijie#mkdir backup
```

Make sure that the directory is created successfully:

```
Ruijie#dir
```

```
Directory of sd0:/
```

Mode	Link	Size	MTime	Name
<DIR>	1	343040	2009-01-01 02:02:59	backup

```
-----
3 Files (Total size 11181455 Bytes), 0 Directories.
```

```
Total 33030144 bytes (31MB) in this device, 20492288 bytes (19MB) available.
```

Copy the file to the SD card:

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

Check the result:



```
Ruijie#dir backup
Directory of sd0:/backup
  Mode Link      Size           MTime      Name
-----
      1      399    2009-01-01 00:01:37  config.text
-----
Total 33030144 bytes (31MB) in this device, 20488192 bytes (19MB) available.
```

## Copying Files between USB and SD Card

The following example shows how to copy rgos\_10\_4.bin from U-shaped disc to SD card:

Check the available space on the SD card:

```
Ruijie#dir sd0:/
Directory of sd0:/
  Mode Link      Size           MTime Name
-----
<DIR>    2          0 2035-02-11 23:24:34 backup/
      1 7650112 2035-02-11 23:42:25 rgos.bin
-----
1 Files (Total size 7650112 Bytes), 1 Directories.
Total 528482304 bytes (504MB) in this device, 475058176 bytes (453MB) available.
```

Copy the file from U-shaped disc to SD card:

```
Ruijie#copy usb0:/rgos_10_4.bin sd0:/rgos_10_4.bin
[OK 7,650,112 bytes]
```

Check the result:

```
Ruijie#dir sd0:/
Directory of sd0:/
  Mode Link      Size           MTime Name
-----
<DIR>    2          0 2035-02-11 23:24:34 backup/
      1 7650112 2035-02-11 23:42:25 rgos.bin
      1 7650112 2035-02-11 23:47:36 rgos_10_4.bin
-----
2 Files (Total size 15300224 Bytes), 1 Directories.
Total 528482304 bytes (504MB) in this device, 459571200 bytes (438MB) available.
```

Copy the file from SD card to U-shaped disc:

```
Ruijie#copy sd0:/rgos_10_4.bin usb0:/new_rgos.bin
[OK 7,650,112 bytes]
```

Check the result:

```
Ruijie#dir usb0:/
Directory of usb0:/
  Mode Link      Size           MTime Name
```



```
Ruijie#dir
Directory of flash:/
   Mode Link          Size           MTime          Name
-----
          1          11014633 2006-01-01 08:00:46  rgos.bin
<dir>    1           0          2006-01-01 08:00:00  aaa/
          1           399          2006-01-01 08:01:37  config.text
-----
2Files (Total size 11015032 Bytes), 1 Directories
Total 33030144 bytes (31MB) in this device, 9563693 bytes (9MB) available
```

Check whether there is a file in aaa directory:

```
Ruijie#dir aaa
Directory of flash:/aaa
   Mode Link          Size           MTime          Name
-----
          1           149 2006-01-01 08:01:37  backup.txt
-----
1Files (Total size 149 Bytes), 0 Directories
Total 33030144 bytes (31MB) in this device, 9563693 bytes (9MB) available
```

The aaa directory is not empty. Delete the files first:

```
Ruijie# delete aaa/backup.txt
```

Delete the empty directory:

```
Ruijie# rmdir aaa
```

Check the result:

```
Ruijie#dir
Directory of flash:/
   Mode Link          Size           MTime          Name
-----
          1          11014633 2006-01-01 08:00:46  rgos.bin
          1           399          2006-01-01 08:01:37  config.text
-----
2Files (Total size 11015032 Bytes), 0 Directories
Total 33030144 bytes (31MB) in this device, 9563693 bytes (9MB) available
```

# Configuration File Management Configuration

## Introduction to Configuration File Management

### Overview

Along with the instant development of network, the network environment is getting more and more complicated, resulting more and more configuration information and higher and higher requirements on the network administrator. The change in configuration information may lead to unpredictable impacts on the entire network. Therefore, the monitoring of configuration change is of crucial importance. Currently, we can only determine whether the configurations have been change by copying the current running configuration file (running-config) and start-up configuration file (startup-config) and comparing the difference in command lines of both files. Although such a method can help identify changes in the configuration, there are still many defects. For example: the sequence of configuration changes cannot be identified; the network administrator cannot be notified in a timely manner; the relevant responsible personnel cannot be identified in the event of network failure caused by such configuration change. The configuration file management can remind the administrator of such configuration change through messages or logs.

### Basic Characteristics

Configuration file management involves configuration change messaging and logging.

### Configuration Change Logging

Configuration Change Logging provides a new approach for determining whether the configurations have changed. This approach can track the time of configuration change, configuration contents and the user making such configuration change, and it can also notify the network administrator in a real-time way.

### Working Principle

By tracking each command applied, the system will log the corresponding user name, corresponding time, commands configured, configuration mode and etc, and then send the log to the remote log server through the notification mechanism. By looking up these records, we will understand whether the configurations have been changed, what the changes are and which user made such change.

### Protocol Specification

N/A

### Default Configurations

The following table describes the default configurations of configuration file management.

Function	Default setting
Configuration change logging	Disabled
Configuration change notification	Disabled
Entries reserved in the configuration log	100

## Configuring Configuration Change Logging

### Enabling Configuration Change Logging

By default, the configuration change logging function is disabled. Enter privilege mode and execute the following steps to enable configuration change logging function.

Command	Function
Ruijie# <b>configure terminal</b>	Enter global configuration mode.
Ruijie(config)# <b>archive</b>	Enter archive configuration mode.
Ruijie(config-archive)# <b>log config</b>	Enter archive log configuration mode.
Ruijie(config-archive-log-config)# <b>logging enable</b>	Enable configuration change logging.

To disable configuration change logging, execute the **no logging enable** command in log config configuration mode.

Configuration example:

# Enable configuration change logging.

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

### Specifying the Maximum Number of Entries Reserved in the Configuration Log

By default, the maximum number of entries reserved in the configuration log is 100. Enter privilege mode and execute the following steps to specify the maximum number of entries reserved in the configuration log.

Command	Function
Ruijie# <b>configure terminal</b>	Enter global configuration mode.
Ruijie(config)# <b>archive</b>	Enter archive configuration mode.
Ruijie(config-archive)# <b>log config</b>	Enter archive log configuration mode.
Ruijie(config-archive-log-config)# <b>logging size entries</b>	Specify the maximum number of entries reserved in the configuration log (1-1000). The default value is 100.

To restore to the default setting, execute the **no logging size** command in log config configuration mode.

Configuration example:

# Specify the maximum number of entries reserved in the configuration log to 50.

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

## Enabling Key Hiding

By default, keys are displayed in the configuration log. Enter privilege mode and execute the following steps to hide keys contained in the configuration log.

Command	Function
Ruijie# <b>configure terminal</b>	Enter global configuration mode.
Ruijie(config)# <b>archive</b>	Enter archive configuration mode.
Ruijie(config-archive)# <b>log config</b>	Enter archive log configuration mode.
Ruijie(config-archive-log-config)# <b>hidekeys</b>	Hide keys contained in the configuration log.

To restore to the default setting, execute the **no hidekeys** command in log config configuration mode.

Configuration example:

# Hide keys contained in the configuration log.

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

## Enabling Configuration Change Notification

By default, the configuration change notification function is disabled. Enter privilege mode and execute the following steps to enable configuration change notification function.

Command	Function
Ruijie# <b>configure terminal</b>	Enter global configuration mode.
Ruijie(config)# <b>archive</b>	Enter archive configuration mode.
Ruijie(config-archive)# <b>log config</b>	Enter archive log configuration mode.
Ruijie(config-archive-log-config)# <b>notify syslog</b>	Enable configuration change notification.

To restore to the default setting, execute the **no notify syslog** command in log config configuration mode.

Configuration example:

# Enable configuration change notification.

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

## Viewing Configuration Change Log Information

The following commands are provided to display configuration log information and memory usage status.

Command	Function
---------	----------

Ruijie# <b>show archive log config</b> { { <b>all</b>   <i>start-num</i> [ <i>end-num</i> ] } [ <b>provisioning</b>   <b>contenttype</b> [ <b>plaintext</b> ] ]   <b>statistics</b> }	Display configuration log information and memory usage status.
---	--

## Typical Example of Configuration File Management

### Networking Requirements

To timely track the configuration changes, assuming that the network administrator has the following needs:

Enable configuration change logging;

Specify the maximum number of entries reserved in the configuration log to 1000;

Hide keys contained in the configuration log;

Send configuration change log to the remote log server (IP: 192.168.12.11);

### Network Topology

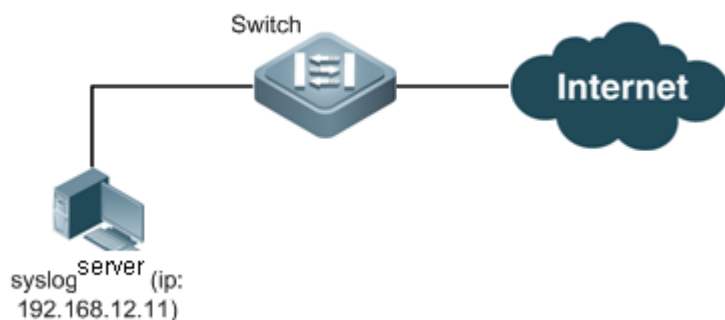


Fig 1 Configuration change log networking diagram

### Configuration Tips

N/A

### Configuration Steps

1) Enable configuration change logging;

# Enable configuration change logging function to track configuration changes

```

Ruijie# configure terminal
Ruijie(config)# archive
Ruijie(config-archive)# log config
Ruijie(config-archive-log-config)# logging enable
  
```

2) Specify the maximum number of entries reserved in the configuration log to 1000;

# Specify the maximum number of entries reserved in the configuration log

```
Ruijie(config-archive-log-config)# logging size 1000
```

3) Hide keys contained in the configuration log

# Hide keys contained in the configuration log

```
Ruijie(config-archive-log-config)# hidekeys
```

4) Send configuration change log to the remote log server (IP: 192.168.12.11)

# Enable the function to send configuration change log to the remote log server

```
Ruijie(config-archive-log-config)# notify syslog
```

# Configure remote log server

```
Ruijie(config-archive-log-config)# exit
```

```
Ruijie(config-archive)# exit
```

```
Ruijie(config)# logging server 192.168.12.11
```

## Verification

# View configuration log information

```
Ruijie(config)# show archive log config all
```

idx	sess	user@line	datetime	logged command
1	1	unknown@console	Mar 21 09:57:22	logging enable
2	1	unknown@console	Mar 21 09:59:42	logging size 1000
3	1	unknown@console	Mar 21 10:02:12	hidekeys
4	1	unknown@console	Mar 21 10:02:26	notify syslog
5	1	unknown@console	Mar 21 10:02:50	exit
6	1	unknown@console	Mar 21 10:03:01	exit

# View configuration log memory usage status

```
Ruijie(config)# show archive log config statistic
```

```
Config Log Session Info:
```

```
Number of sessions being tracked: 1
```

```
Memory being held: 1270 bytes
```

```
Total memory allocated for session tracking: 1270 bytes
```

```
Total memory freed from session tracking: 0 bytes
```

```
Config Log log-queue Info:
```

```
Number of entries in the log-queue: 3
```

```
Memory being held in the log-queue: 671 bytes
```

```
Total memory allocated for log entries: 671 bytes
```

```
Total memory freed from log entries: 0 bytes
```



# System Management Configuration

## CPU Utilization Display

### Showing CPU Utilization

Use the **show cpu** command to show the total CPU utilization and the CPU utilization per process:

Command	Function
Ruijie# <b>show cpu</b>	Show CPU utilization.

By default, the switch name is Ruijie.

Below is the result of executing this command:

```
Ruijie#show cpu
=====
      CPU Using Rate Information
CPU utilization in five seconds: 25%
CPU utilization in one minute  : 20%
CPU utilization in five minutes: 10%
 NO   5Sec  1Min  5Min  Process
  0    0%    0%    0%   LISR INT
  1    7%    2%    1%   HISR INT
  2    0%    0%    0%   ktimer
  3    0%    0%    0%   atimer
  4    0%    0%    0%   printk_task
  5    0%    0%    0%   waitqueue_process
  6    0%    0%    0%   tasklet_task
  7    0%    0%    0%   kevents
  8    0%    0%    0%   snmpd
  9    0%    0%    0%   snmp_trapd
10    0%    0%    0%   mtdblock
11    0%    0%    0%   gc_task
12    0%    0%    0%   Context
13    0%    0%    0%   kswapd
14    0%    0%    0%   bdflush
15    0%    0%    0%   kupdate
16    0%    3%    1%   ll_mt
17    0%    0%    0%   ll main process
18    0%    0%    0%   bridge_relay
19    0%    0%    0%   dlx_task
20    0%    0%    0%   secu_policy_task
21    0%    0%    0%   dhcpa_task
22    0%    0%    0%   dhcpsnp_task
23    0%    0%    0%   igmp_snp
```

24	0%	0%	0%	mstp_event
25	0%	0%	0%	GVRP_EVENT
26	0%	0%	0%	rldp_task
27	0%	2%	1%	rerp_task
28	0%	0%	0%	reup_event_handler
29	0%	0%	0%	tpp_task
30	0%	0%	0%	ip6timer
31	0%	0%	0%	rtadvd
32	0%	0%	0%	tnet6
33	2%	0%	0%	tnet
34	0%	0%	0%	Tarptime
35	0%	0%	0%	gra_arp
36	0%	0%	0%	Ttcptimer
37	8%	1%	0%	ef_res
38	0%	0%	0%	ef_rcv_msg
39	0%	0%	0%	ef_inconsistent_daemon
40	0%	0%	0%	ip6_tunnel_rcv_pkt
41	0%	0%	0%	res6t
42	0%	0%	0%	tunrt6
43	0%	0%	0%	ef6_rcv_msg
44	0%	0%	0%	ef6_inconsistent_daemon
45	0%	0%	0%	imid
46	0%	0%	0%	nsmd
47	0%	0%	0%	ripd
48	0%	0%	0%	ripngd
49	0%	0%	0%	ospfd
50	0%	0%	0%	ospf6d
51	0%	0%	0%	bgpd
52	0%	0%	0%	pimd
53	0%	0%	0%	pim6d
54	0%	0%	0%	pdmd
55	0%	0%	0%	dvmrpd
56	0%	0%	0%	vty_connect
57	0%	0%	0%	aaa_task
58	0%	0%	0%	Tlogtrap
59	0%	0%	0%	dhcp6c
60	0%	0%	0%	sntp_rcv_task
61	0%	0%	0%	ntp_task
62	0%	0%	0%	sla_deamon
63	0%	3%	1%	track_daemon
64	0%	0%	0%	pbr_guard
65	0%	0%	0%	vrrpd
66	0%	0%	0%	psnpsd
67	0%	0%	0%	igsnpsd
68	0%	0%	0%	coa_rcv
69	0%	0%	0%	co_oper

70	0%	0%	0%	co_mac
71	0%	0%	0%	radius_task
72	0%	0%	0%	tac+_acct_task
73	0%	0%	0%	tac+_task
74	0%	0%	0%	dhcpd_task
75	0%	0%	0%	dhcps_task
76	0%	0%	0%	dhcpping_task
77	0%	0%	0%	dhcpc_task
78	0%	0%	0%	uart_debug_file_task
79	0%	0%	0%	ssp_init_task
80	0%	0%	0%	rl_listen
81	0%	0%	0%	ikl_msg_operate_thread
82	0%	0%	0%	bcmDPC
83	0%	0%	0%	bcmL2X.0
84	3%	3%	3%	bcmL2X.0
85	0%	0%	0%	bcmCNTR.0
86	0%	0%	0%	bcmTX
87	0%	0%	0%	bcmXGS3AsyncTX
88	0%	2%	1%	bcmLINK.0
89	0%	0%	0%	bcmRX
90	0%	0%	0%	mngpkt_rcv_thread
91	0%	0%	0%	mngpkt_recycle_thread
92	0%	0%	0%	stack_task
93	0%	0%	0%	stack_disc_task
94	0%	0%	0%	redun_sync_task
95	0%	0%	0%	conf_dispatch_task
96	0%	0%	0%	devprob_task
97	0%	0%	0%	rdp_snd_thread
98	0%	0%	0%	rdp_rcv_thread
99	0%	0%	0%	rdp_slot_change_thread
100	4%	2%	1%	datapkt_rcv_thread
101	0%	0%	0%	keepalive_link_notify
102	0%	0%	0%	rerp_msg_rcv_thread
103	0%	0%	0%	ip_scan_guard_task
104	0%	0%	0%	ssp_ipmc_hit_task
105	0%	0%	0%	ssp_ipmc_trap_task
106	0%	0%	0%	hw_err_snd_task
107	0%	0%	0%	rerp_packet_send_task
108	0%	0%	0%	idle_vlan_proc_thread
109	0%	0%	0%	cmic_pause_detect
110	1%	1%	1%	stat_get_and_send
111	0%	1%	0%	rl_con
112	75%	80%	90%	idle

As shown in the above, the first three lines indicate the total CPU utilization in the last 5 seconds, 1 minute and 5 minutes respectively, including LISR, HISR and task. Below details CPU utilization, where:

- No: number
- 5Sec: CPU utilization in the last 5 seconds
- 1Min: CPU utilization in the last 1 minute
- 5Min: CPU utilization in the last 5 minutes
- Process: process name

The first two lines indicate the CPU utilization of all LISRs and the CPU utilization of all HISRs respectively. All the lines starting the third line indicate the CPU utilization of processes. The last line indicates the CPU utilization of idle process. As with System Idle Process under Windows, it indicates an idle status. The above example shows that the CPU utilization of idle processes in the last 5 seconds is 75%, meaning that 75% CPU is available.

## Configuring CPU Log Limit Threshold

To configure the CPU log limit threshold, execute the following command:

Command	Function
<b>cpu-log log-limit</b> <i>low_num high_num</i>	Configure the CPU log limit threshold.

By default the upper threshold is 100% and the lower threshold is 90%.

The following example sets the lower threshold to 70% and the higher threshold to 80%:

```
Ruijie# configure terminal                // Enter the global configuration mode
Ruijie(config)# cpu-log log-limit 70 80  // Configure the CPU logging trigger threshold
If the CPU utilization is higher than 80%, the system prompts:
Oct 20 15:47:01 %SYSCHECK-5-CPU_USING_RATE: CPU utilization in one minute : 95% ,Using most
cpu's task is ktimer : 94%
If the CPU utilization is lower than 70%, the system prompts:
Oct 20 15:47:01 %SYSCHECK-5-CPU_USING_RATE: CPU utilization in one minute :68% ,Using most
cpu's task is ktimer : 60%
Oct 20 15:47:01 %SYSCHECK-5-CPU_USING_RATE: The CPU using rate has down!
```

## System Memory Display

### Showing the Usage of System Memory

Use the **show memory** command to show the usage and status of system memory:

Command	Function
Ruijie# <b>show memory</b>	Show the usage of system memory.

By default, the switch name is Ruijie.

Below is the result of executing this command:

```
Ruijie#show memory
System Memory Statistic:
  Free pages: 13031
  watermarks : min 378, lower 756, low 1534, high 1912
  System Total Memory : 128MB, Current Free Memory : 54892KB
  Used Rate : 58%
```

The above information includes the following parts:

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

Parameter	Description
min	The memory resources are extremely insufficient. It can only keep the kernel running. All application modules fail to run if the minimum watermark has been reached.
lower	The memory resources are severely insufficient. One route protocol will auto-exit and release the memory if the lower watermark has been reached. For the details, see the <b>memory-lack exit-policy</b> command.
low	The memory resources are insufficient. The route protocol will be in OVERFLOW state if the low watermark has been reached. In the overflow state, the routers do not learn new routes any more. The commands are not allowed to be executed when the memory lacks.
high	A plenty of memory resources. Each route protocol attempts to restore the state from OVERFLOW to normal.

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

### Configuring the memory-lack exit-policy

Use the **memory-lack exit-policy** command to configure the exit policy of the route protocol if the lower watermark has been reached. The route protocol includes BGP, OSPF, RIP, PIM-SM.

**memory-lack exit-policy [bgp|ospf|pim-sm|rip]**

Command	Function
Ruijie(config)# <b>memory-lack exit-policy [ bgp   ospf   pim-sm   rip ]</b>	Configure the exit policy of the route protocol if the lower watermark has been reached.

Use the **no memory-lack exit-policy** command to restore the default configuration. By default, if the memory size reaches the lower watermark, the protocol that occupies the most memory exits.

If the system free memory decreases to the lower watermark, the system will disable one route protocol, releasing the memory resources to ensure the normal operation of other protocols.

You shall know what route protocols support the major network service. If the memory resources lack, you can disable the most unimportant protocol to ensure the normal operation of the major services.

For example, in a user network, the routes BGP learned are irrelevant to the major network service; you can use the **memory-lack exit-policy bgp** command.

Specifying the disabled route protocol as the exit policy cannot help the system obtain enough memory resources.

**Showing the Usage of the protocol memory**

Use the **show memory protocol** command to display the usage of the memory protocol.

Command	Function
<b>show memory protocol</b>	Show the usage of the memory protocol

Below is the result of executing this command:

```
Ruijie# show memory protocols
=====
protocol      |memory(byte)
BGP           102000000
OSPF          24000000
RIP           10000000
PIM           50000000
LDP           20000000
Total         206000000
```

# System Memory Display Configuration

## Showing the Usage of System Memory

Use the **show memory** command to show the usage and status of system memory:

Command	Function
Ruijie# <b>show memory</b>	Show the usage of system memory.

By default, the switch name is Ruijie.

Below is the result of executing this command:

```
Ruijie#show memory
System Memory Statistic:
  Free pages: 13031
  watermarks : min 378, lower 756, low 1534, high 1912
  System Total Memory : 128MB, Current Free Memory : 54892KB
  Used Rate : 58%
```

The above information includes the following parts:

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

Parameter	Description
min	The memory resources are extremely insufficient. It can only keep the kernel running. All application modules fail to run if the minimum watermark has been reached.
lower	The memory resources are severely insufficient. One route protocol will auto-exit and release the memory if the lower watermark has been reached. For the details, see the <b>memory-lack exit-policy</b> command.
low	The memory resources are insufficient. The route protocol will be in OVERFLOW state if the low watermark has been reached. In the overflow state, the routers do not learn new routes any more. The commands are not allowed to be executed when the memory lacks.
high	A plenty of memory resources. Each route protocol attempts to restore the state from OVERFLOW to normal.

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

## Configuring the memory-lack exit-policy

Use the **memory-lack exit-policy** command to configure the exit policy of the route protocol if the lower watermark has been reached. The route protocol includes BGP, OSPF, RIP, PIM-SM.

**memory-lack exit-policy [bgp|ospf|pim-sm|rip]**

Command	Function
Ruijie(config)# <b>memory-lack exit-policy [ bgp   ospf   pim-sm   rip ]</b>	Configure the exit policy of the route protocol if the lower watermark has been reached.

Use the **no memory-lack exit-policy** command to restore the default configuration. By default, if the memory size reaches the lower watermark, the protocol that occupies the most memory exits.

If the system free memory decreases to the lower watermark, the system will disable one route protocol, releasing the memory resources to ensure the normal operation of other protocols.

You shall know what route protocols support the major network service. If the memory resources lack, you can disable the most unimportant protocol to ensure the normal operation of the major services.

For example, in a user network, the routes BGP learned are irrelevant to the major network service, you can use the **memory-lack exit-policy bgp** command.

Specifying the disabled route protocol as the exit policy cannot help the system obtain enough memory resources.

## Showing the usage of the protocol memory

Use the **show memory protocol** command to display the usage of the memory protocol.

Command	Function
<b>show memory protocol</b>	Show the usage of the memory protocol

Below is the result of executing this command:

```
Ruijie# show memory protocols
=====
protocol      |memory(byte)
BGP           102000000
OSPF          24000000
RIP           10000000
PIM           50000000
LDP           20000000
Total        206000000
```



# Syslog Configuration

## Overview

During the operation of a device, there are various state changes, such as the link status up/down, and various events occurring, such as receiving abnormal messages and handling abnormalities. Our product provides a mechanism to generate messages of fixed format (log message) in case of status change or event occurring. These messages can be displayed in related windows (console, VTY, etc.) or recorded in related media (memory buffer, FLASH), or sent to a group of log servers in the network for the administrators to analyze and locate problems. Meanwhile, in order to make it easy for administrators to read and manage log messages, these log messages can be labeled time stamps and serial numbers, and is graded according to the priority of log information.

## Log Message Format

The format of the log message is as follows:

**<priority> seq no: timestamp sysname: %severity**

**%ModuleName-severity-MNEMONIC: description**

They are: <priority> Sequential number timestamp device name module name-severity – information type: abbrev: information contents

Priority value = Device value \*8 + Severity

For example:

```
<189> 226:Mar 5 02:09:10 Ruijie %SYS-5-CONFIG_I: Configured from console by console
```



**Caution**

The priority field is not attached to the log messages that are printed in the user window. It only appears in the log messages that are sent to the syslog server.

## Log Configuration

### Log Switch

The log switch is turned on by default. If it is turned off, the device will not print log information in the user window, or send log information to the syslog server, or record the log information in the related media (memory buffer, flash).

To turn on or off the log switch, run the following command in the global configuration mode:

Command	Function
Ruijie(config)# <b>logging on</b>	Turn on the log switch
Ruijie(config)# <b>no logging on</b>	Turn off the log switch

**Caution**

Do not turn off the log switch in general case. If it prints too much information, you can reduce it by setting different displaying levels for device log information.

## Log Redirection Switch

In the VSU environment, the log redirection switch is on by default. The log information on the secondary or standby device can not only be displayed on the CONSOLE box on the secondary or standby device, but also redirected to the primary device for output to the CONSOLE and VTY boxes on the primary device, or for record in the memory buffer, extended FLASH memory and Syslog Server of the primary device.

Execute the following commands in the global configuration mode of the host to enable or disable the log redirection.

Command	Function
Ruijie(config)# <b>logging rd on</b>	Switch on the Log redirection
Ruijie(config)# <b>no logging rd on</b>	Switch off the Log redirection

With the log redirection enabled, the log information on the secondary or standby device is redirected to the primary device for output. When it is output, a corresponding role mark string ("device number") will be added to the very front of the log content to identify the log information as the redirected log information. In the VSU environment, assuming four devices exist at the same time, the primary device is numbered 1, the secondary device is number 2, and the standby devices are numbered 3 and 4 respectively, no role mark string will be added to the log generated by the primary device; role mark string (\*2) will be added to the log redirected from the secondary device to the primary device; and role mark strings (\*3) and (\*4) will be added to the logs redirected from the standby devices to the primary device respectively.

## Configuring the Device Displaying the Log Information

When the log switch is turned on, the log information will be displayed on the console and also sent to different displaying devices. To configure different displaying devices for receiving logs, run the following commands in the global configuration mode or privileged level:

Command	Function
Ruijie(config)# <b>buffered</b> [ <i>buffer-size</i> ] [ <i>level</i> ]	Record log in memory buffer
Ruijie# <b>terminal monitor</b>	Allow log to be displayed on VTY window
Ruijie(config)# <b>logging server</b> <i>host</i>	Send log information to the syslog sever in the network
Ruijie(config)# <b>logging file</b> <i>flash:filename</i> [ <i>max-file-size</i> ] [ <i>level</i> ]	Record log on extended FLASH

Logging Buffered will record log information in the memory buffer. The memory buffer for log is used in recycled manner. That is, when it is full, the oldest information will be overwritten. To show the log information in the memory buffer, run **show logging** at the privileged user level. To clear the log information in the memory buffer, run **clear logging** at the privileged user level.

Terminal Monitor allows log information to be displayed on the current VTY (such as the telnet window).

Logging Host specifies the address of the syslog server that will receive the log information. Our product allows the configuration of at most 5 syslog servers. The log information will be sent to all the syslog servers at the same time.

**Caution**

To send the log information to the syslog server, it is required to turn on the timestamp switch or sequential number switch of the log information. Otherwise, log information will not be sent to the syslog server.

Logging File Flash: Record log information in FLASH. The filename for log shall not have any extension to indicate the file type. The extension of the log file is fixed as txt. Any configuration of extension for the filename will be refused.

More flash: filename command shows the contents of the log file in the flash.

**Caution**

Some devices support extended FLASH. If the device has extended FLASH, the log information will be recorded there. If the device has no extended FLASH, the log information will be recorded in the serial FLASH.

## Enabling the Log Timestamp Switch of Log Information

To add or delete timestamp in log information, run the following command in the global configuration mode:

Command	Function
Ruijie(config)# <b>service timestamps</b> [ <i>message-type</i> [ <b>uptime</b>   <b>datetime</b> [ <b>msec</b> ] [ <b>year</b> ] ]	Enable the timestamp in the log information
Ruijie(config)# <b>no service timestamps</b> [ <i>message-type</i> ]	Disable the timestamp in the log information

The timestamp are available in two formats: device uptime and device datetime. Select the type of timestamp appropriately.

Message type: log or debug. The "log" type means the log information with severity levels 0-6. The "debug" type means that with severity level 7.

**Caution**

If the current device has no RTC, the configured time is invalid, and the device automatically uses the startup time as the timestamp for the log information.

## Enabling Switches in Log System

By default, the system name is not included in the log information. To add or remove the system name in the log information, perform the following commands in the global configuration mode.

Command	Function
Ruijie(config)# <b>no service sysname</b>	Cancel the system name in the log message.

Command	Function
Ruijie(config)# <b>service sysname</b>	Add the system name to the log message.

## Enabling the Show Switch of Standard Log Format

By default, in the log format, there is a "\*" and a "." in front of and behind the timestamp respectively, and a "%" in front of the mark string. Execute the following commands in the global configuration mode to display the log in the standard format, i.e. without the "\*" and "." in front of and behind the timestamp of the log format:

Command	Function
Ruijie(config)# <b>service standard-syslog</b>	Enable the show switch of standard log format
Ruijie(config)# <b>no service standard-syslog</b>	Disable the show switch of standard log format

By default, the log information on the device is shown in the following format:

\*timestamp: %facility-severity-mnemonic: description

In order: \*timestamp: %module name-severity level-Mnemonic information: Log details

Example: **\*May 31 23:25:21: %SYS-5-CONFIG\_I: Configured from console by console**

With the standard log format show enabled, the log information on the device is shown in the following format:

timestamp %facility-severity-mnemonic: description

In order, timestamp %module name-severity level-Mnemonic information: Log details

Example: **May 31 23:31:28 %SYS-5-CONFIG\_I: Configured from console by console**

The standard log format differs from the default log format in the timestamp. There is neither "\*" or "." in front of or behind the timestamp in the standard log format.

## Enabling the Show Switch of Private Log Format

By default, in the log format, there is a "\*" and a "." in front of and behind the timestamp respectively, and a "%" in front of the mark string. Execute the following commands in the global configuration mode to display the log in the private mode, that is, without the "\*" and "." in front of and behind the timestamp, and the "%" in front of the mark string in the log format:

Command	Function
Ruijie(config)# <b>service private-syslog</b>	Enable the show switch of private log format
Ruijie(config)# <b>no service private-syslog</b>	Disable the show switch of private log format

By default, the log information on the device is shown in the following format:

\*timestamp: %facility-severity-mnemonic: description

In order: \*timestamp: %module name-severity level-Mnemonic information: Log details

Example: **\*May 31 23:25:21: %SYS-5-CONFIG\_I: Configured from console by console**

With the private log format show enabled, the log information on the device is shown in the following format:

timestamp facility-severity-mnemonic: description

In order, timestamp module name-severity level-Mnemonic information: Log details

Example: **May 31 23:31:28 SYS-5-CONFIG\_I: Configured from console by console**

The private log format differs from the default log format in the timestamp. There is neither “\*” or “.” in front of or behind the timestamp and no “%” in front of the mark string in the standard log format.

## Enabling Log Statistics

By default, the log statistics function is disabled. To enable or disable the log statistics function, perform the following commands in the global configuration mode.

Command	Function
Ruijie(config)# <b>no logging count</b>	Disable the log statistics function and delete the statistics information
Ruijie(config)# <b>logging count</b>	Enable the log statistics function

## Enabling the Sequential Number Switch of Log Information

By default, the log information has no sequential number. To add or delete sequential number in log information, run the following command in the global configuration mode:

Command	Function
Ruijie(config)# <b>no service sequence-numbers</b>	Delete sequential number in the log messages
Ruijie(config)# <b>service sequence-numbers</b>	Add sequential number to the log messages

## Configuring Synchronization Between User Input and Log Output

By default, user input is asynchronous with log output. User input is interrupted if the log is output when the user is keying in characters. Use this command to configure synchronization between user input and log output in the line configuration mode:

Command	Function
Ruijie(config-line)# <b>logging synchronous</b>	Set synchronization between user input and log output.
Ruijie(config)# <b>no logging synchronous</b>	Delete synchronization between user input and log output.

## Configuring Log Rate Limit

By default, log rate is not limited. Use this command to configure log rate limit in the global configuration mode:

Command	Function
---------	----------

Ruijie(config)# <b>logging rate-limit</b> <i>number</i>	Set log rate limit.
Ruijie(config)# <b>no logging rate-limit</b>	Delete the setting of log rate limit.

## Configuring Log Redirecting Rate Limit

In the VSU environment, neither the secondary nor standby device generates much log information in general. To prevent the secondary or standby device from generating much log information, you need to limit the rate of redirecting log information to the primary device, otherwise this will cause much load on the system. By default, the rate for redirecting log information to the primary device is no more than 200 logs per second.

Execute the following commands in the global configuration mode of the primary device to modify the log redirecting rate limit:

Command	Function
Ruijie(config)# <b>logging rd rate-limit</b> <i>number</i> [ <b>except</b> [ <i>severity</i> ] ]	Configure the log redirecting rate limit.
Ruijie(config)# <b>no logging rate-limit</b>	Remove the log redirecting rate limit.

## Configuring the Log Information Displaying Level

To limit the number of log messages displayed on different devices, it is possible to set the severity level of log information that is allowed to be displayed on those devices.

To configure the log information displaying level, run the following command in the global configuration mode:

Command	Function
Ruijie(config)# <b>logging console</b> [ <i>level</i> ]	Set the level of log information that is allowed to be displayed on the console
Ruijie(config)# <b>logging monitor</b> [ <i>level</i> ]	Set the level of log information that is allowed to be displayed on the VTY window (such as telnet window)
Ruijie(config)# <b>logging buffered</b> [ <i>buffer-size</i> ] [ <i>level</i> ]	Set the level of log information that is allowed to be recorded in memory buffer
Ruijie(config)# <b>logging file</b> <b>flash:filename</b> [ <i>max-file-size</i> ] [ <i>level</i> ]	Set the level of log information that is allowed to be recorded in extended flash
Ruijie(config)# <b>logging trap</b> [ <i>level</i> ]	Set the level of log information that is allowed to be sent to syslog server

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

Level Keyword	Level	Description
<b>Emergencies</b>	0	Emergency case, system cannot run normally
<b>Alerts</b>	1	Problems that need immediate remedy

Level Keyword	Level	Description
<b>Critical</b>	2	Critical conditions
<b>Errors</b>	3	Error message
<b>Warnings</b>	4	Alarm information
<b>Notifications</b>	5	Information that is normal but needs attention
<b>Informational</b>	6	Descriptive information
<b>Debugging</b>	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 that can be displayed is set for the specified device, the log information that is at or below the set level will be displayed. For example, after the command `logging console 6` is executed, all log information at or below level 6 will be displayed on the console.

By default, the log information that is allowed to be displayed on the console is at level 7.

By default, the log information that is allowed to be displayed on the VTY window is at level 7.

By default, the log information that is allowed to be sent to the syslog server is at level 6.

By default, the log information that is allowed to be recorded in the memory buffer is at level 7.

By default, the log information that is allowed to be recorded in the extended flash is at level 6.

The privileged command `show logging` can be used to show the level of log information allowed to be displayed on different devices.

## Configuring the log information device value

The device value is one of the parts that form the priority field in the messages sent to the syslog server, indicating the type of device that generates the information.

To configure the log information device value, run the following command in the global configuration mode:

Command	Function
<code>Ruijie(config)# logging facility facility-type</code>	Configure the log information device value
<code>Ruijie(config)# no logging facility</code>	Restore the default of the log information device value

The meanings of various device values are described as below:

Numerical Code	Facility
0	kernel messages
1	user-level messages
2	mail system
3	system daemons
4	security/authorization messages

5	messages generated internally by syslogd
6	line printer subsystem
7	network news subsystem
8	UUCP subsystem
9	clock daemon
10	security/authorization messages
11	FTP daemon
12	NTP subsystem
13	log audit
14	log alert
15	clock daemon
16	local use 0 (local0)
17	local use 1 (local1)
18	local use 2 (local2)
19	local use 3 (local3)
20	local use 4 (local4)
21	local use 5 (local5)
22	local use 6 (local6)
23	local use 7 (local7)

The default device value of our products is 23.

## Configuring the Source Address of Log Messages

By default, the source address of the log messages sent to the syslog server is the address of the port that sends the messages. It is possible to fix the source address for all log messages through commands.

It is possible to directly set the source IP address of the log messages or the remote port of the log messages.

To configure the source address of the log messages, run the following command in the global configuration mode:

Command	Function
Ruijie(config)# <b>logging source interface</b> <i>interface-type interface-number</i>	Configure the source port of log information
Ruijie(config)# <b>logging source {ip ip-address   ipv6 ipv6-address}</b>	Configure the source IP address of log messages

## Setting and Sending User Log

By default, no log is output when a user logs in or out and executes configuration commands. To output user login/logoff logs or configuration command logs, execute the following commands in the global configuration mode:

Command	Function
Ruijie(config)# <b>logging userinfo</b>	Set user login/logoff log.



Command	Function
Ruijie(config)# <b>logging userinfo</b> <b>command-log</b>	Send a log when a configuration command is executed

## Log Monitoring

To monitor log information, run the following commands in the privileged user mode:

Command	Function
Ruijie# <b>show logging</b>	View the log messages in memory buffer as well as the statistical information of logs
Ruijie# <b>show logging count</b>	View the statistical information of logs in every modules
Ruijie# <b>clear logging</b>	Clear the log messages in the memory buffer
Ruijie# <b>more flash:filename</b>	View the log files in the extended flash



### Caution

The format of the timestamp in the output result of **show logging count** is the format in the latest log output.

## Examples of Log Configurations

Here is a typical example to enable the logging function:

```
Ruijie(config)# interface gigabitEthernet 0/1
Ruijie(config-if)# ip address 192.168.200.42 255.255.255.0
Ruijie(config-if)# exit
Ruijie(config)# service sequence-numbers           //Enable sequence number
Ruijie(config)# service timestamps debug datetime //Enable debug information timestamp, in
date format
Ruijie(config)# service timestamps log datetime    //Enable log information timestamp, in
date format
Ruijie(config)# logging 192.168.200.2             //Specify the syslog server address
logging trap debugging                             //The log information of all levels will be sent to syslog
server
Ruijie(config)# end
```

# Cluster Management Configuration

## Overview

With the development of network technology, the size of the network as well as the number of devices are growing, which brings network management difficulties. Numerous devices require unique network addresses, and each manageable device can meet application requirements only after configuration. As the device quantity grows, the demand for network addresses and management capability is unbearable.

For these problems, cluster management provides perfect solutions. A cluster consists of a group of interconnected devices and can be managed as an entire entity. A cluster holds a maximum of 240 devices. Among these devices, one device is assigned as the administrator, while all others are members. All devices of a cluster are configured and managed on the administrator, and a member can belong to only one cluster.

Cluster management simplifies network management by enabling you to configure and manage cluster members universally on the administrator despite the concrete locations of members. In addition, only the administrator needs an IP address, and members do not need IP addresses, thereby saving the IP address space and benefiting users particularly.

## Device Role

In cluster management, devices are classified into three roles: Administrator (command device), Member Candidate In a cluster, only the administrator and members exist. Candidates do not belong to any clusters. An assigned candidate will join the cluster of the specified administrator, while an unassigned candidate can join any cluster.

## Administrator

Each cluster has a unique administrator, which configures and manages the cluster. The administrator meets the following conditions:

- Run the cluster support software.
- Run the Link Layer Discovery Protocol (LLDP) software.
- Do not belong to another cluster.

## Member

Members are cluster devices other than the administrator. They are managed by the administrator. Only candidates of a cluster can join the cluster and become members. The members meet the following conditions:

- Run the cluster support software.
- Run the LLDP software.
- Do not belong to another cluster.

## Candidate

Candidates are devices that the administrator can discover but have not joined the cluster. The candidates meet the following conditions:

- Run the cluster support software.

- Run the LLDP software.
- Do not belong to another cluster.

## Cluster Management Scope

### Device Support for LLDP

Cluster discovery uses LLDP that runs on the data link layer. LLDP enables a device to obtain information about another device that is directly connected to the device. The device running LLDP regularly sends packets to a multicast address, thereby advertising its information to other devices.

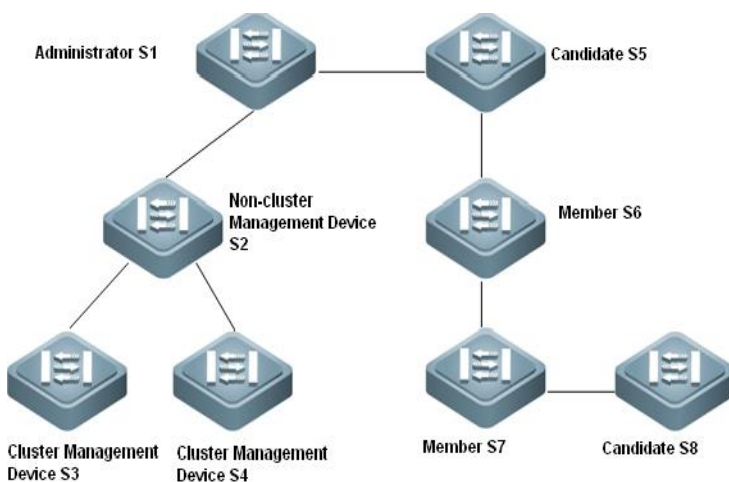
Upon receiving advertisement, each receiver advertises to neighbors except the original sender. In this way, the network management system can discover neighbors of existing devices, making cluster management feasible.

The administrator uses LLDP to discover other devices. Therefore, the administrator cannot discover: Devices that do not support LLDP Devices that have LLDP disabled Devices connected to preceding devices

### Discovered Hop Count

Topology hop count refers to the number of devices between a member and the administrator. The administrator only can discover and manage members within the topology hop count range, which is also called the cluster range. By default, the cluster range is five hops. Here, assume that the administrator can find devices within 16 hops during topology collection. See the following figure.

Figure 1-1 Topology discovered hop count



If the currently discovered hop count is three, S5, S6, and S7 can be discovered because they are within three hops, but S8 cannot be discovered because it is beyond three hops. S2 does not support the cluster function, and fails to be discovered by the administrator. As S3 and S4 are connected to S2, they also fail to be discovered, although they are within three hops and support the cluster function.

### Lately Installed Devices

By default, LLDP and the cluster function are enabled on newly installed devices that support the cluster function. Therefore, the administrator can discover newly installed devices and no configuration is required.

### Cluster Maintenance

To distinguish a cluster, a cluster prefix `ClusterName_N` is added to the command prompt of the administrator and members. A running cluster is also configured with **service sysname** and the prefix `ClusterName_N` is added to the device host name when system logs are recorded. In both cases, N indicates the cluster SN of a device.

## Cluster Access

### Logging In to a Member

Run the **cluster login** command on the administrator to log in to the command line interface (CLI) of a member device, or run the command on a member to log in to the administrator CLI. In the first situation, you enter the privileged EXEC mode. In the second situation, you enter the user mode by default. To enter the privileged EXEC mode, enter the administrator CLI password and pass the authentication.

### Accessing a Member Through SNMP

If the Simple Network Management Protocol (SNMP) agent is configured on the administrator, the network management workstation can use the administrator IP address to access the entire cluster through SNMP, even when SNMP is not configured on all members. The management workstation sends the SNMP request to the administrator. Upon receiving the request, the administrator recognizes and forwards the request to corresponding members, and then forwards member responses to the management workstation. The administrator differentiates members through the community character string or user name added with a suffix.

- When using SNMPv1 or SNMPv2, the management workstation adds the suffix `@esN` (N indicates the cluster SN of a member) to the community character string in the SNMP packet for specifying the member to be accessed.
- When using SNMPv3, the management workstation adds the suffix `@esN` (N indicates the cluster SN of a member) to the user name in the SNMP packet for specifying the member to be accessed.



For details about the SNMP Agent configuration, see the related sections in "SNMP Configuration".

---

### Trap Agent

If the Trap-packet receiving host (the management workstation) is set on the administrator, a member can send a Trap packet to the management workstation through the administrator.

- When using SNMPv1 or SNMPv2, the member adds the suffix `@esN` (N indicates the cluster SN of a member) to the community character string in the Trap packet.
- When using SNMPv3, the member adds the suffix `@esN` (N indicates the cluster SN of a member) to the user name in the Trap packet for specifying the member to be accessed.



For details about the SNMP Trap configuration, see the related sections in "SNMP Configuration".

---

### Syslog Agent

If the log receiving host (Syslog server) is set on the administrator, a member can send a log to the management workstation through the administrator.



For details about the Syslog configuration, see the related sections in "System Log Configuration".

---

## TFTP Agent

If the shared Trivial File Transfer Protocol (TFTP) server is set on the administrator, a member can use the TFTP to download files from the TFTP server or upload files to the TFTP server through the administrator agent.



For details about the TFTP configuration, see the section "Using TFTP to Transfer Files" in "System Upgrade Maintenance Configuration".



The administrator provides the TFTP transfer agent service for only one member at a time. Other members shall wait until the current member finishes using the service.

## Working Principles

The device, who supports cluster management and runs LLDP, regularly sends packets to a multicast address, thereby advertising its information to other devices. In this way, other devices can "discover" it upon receiving the multicast packet. This multicast packet includes the device MAC address, port, and other information.

By default, the cluster function is enabled. However, the device is a "single node" when it does not belong to any cluster. In this case, the device regularly receives topology collection requests sent from the administrator, responds to the request, and becomes a candidate. Once the administrator discovers the candidate, the administrator automatically adds the candidate to the cluster.

Since a cluster can have only one administrator, a cluster is created if you set a "single node" as the administrator. Then, the administrator does not advertise its information any more. Instead, it receives information about other "single nodes" and treats them as its candidates.

The administrator can require a candidate to join the cluster. Then, the candidate becomes a member if the candidate is a "single node". Upon joining the cluster, the member establishes the communication channel to the administrator, enabling the administrator to manage the member remotely. By default, the member assigns the highest priority to the administrator. That is, the member does not authenticate the connection from the administrator.

The administrator can join another cluster only after the administrator exits the current cluster and becomes a "single node". The member stops sending information to other clusters.

The administrator regularly sends advertisements to all its members, and the members also regularly send advertisements to the administrator. If the administrator fails to receive advertisements from a member for a specified period, the administrator considers the member as lost and therefore stops managing the member. Similarly, if a member fails to receive advertisements from the administrator for a specified period, the member considers the cluster as lost. The member will exit the cluster and become a "single node", so that another cluster can manage it.

## Protocols and Specifications

Cluster management depends on LLDP, and LLDP complies with IEEE 802.1AB-2005.

## Configuring Cluster Management

### Default Settings

The following table lists default settings of cluster management.

Feature	Default
---------	---------

Cluster management function	Enabled
Status of a cluster member	No cluster is created, and a device belongs to no cluster.
Cluster auto-addition function	Enabled
Topology collection range	Five hops
Cluster timer value	60 seconds
Cluster timer-hello value	30 seconds
Cluster timer-hold value	90 seconds

## Enabling or Disabling the Cluster Function

By default, the cluster function is enabled. To disable the cluster function, run the commands listed in the following table.

Command	Function
Ruijie# <b>configure terminal</b>	Enter global configuration mode.
Ruijie(config)# <b>no cluster enable</b>	Disable the cluster management function.
Ruijie(config)# <b>end</b>	Return to privileged EXEC mode.
Ruijie# <b>show run</b>	Verify the configuration.

If you run the command on the administrator to disable the cluster function, the cluster and its configurations will be deleted. If you run the command on a member to disable the cluster function, the cluster function of the member is disabled and the member exits the cluster.

If you run the command on a candidate to disable the cluster function, the cluster function of the candidate is disabled and the candidate cannot join any cluster.

To re-enable the cluster function, run the **cluster enable** command in the global configuration mode:

Configuration Example:

# Disable the cluster management function for the device.

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

## Creating or Deleting a Cluster

A cluster can have only one administrator. When creating a cluster on a device, the device becomes the administrator of the cluster at the same time. To create a cluster, run the commands listed in the following table.

Command	Function
Ruijie# <b>configure terminal</b>	Enter the global configuration mode.
Ruijie(config)# <b>cluster</b> [ <i>name</i> ]	Create a cluster on a device, set the device as the administrator, assign the cluster SN 1 to the administrator, and enter the cluster configuration mode. <i>name</i> : indicates the name of the cluster. The default value is CLUSTER.
<i>name_1</i> .Ruijie(config-cluster)# <b>exit</b>	Return to configuration mode.
<i>name_1</i> .Ruijie(config)# <b>exit</b>	Return to privileged EXEC mode.
<i>name_1</i> .Ruijie# <b>show cluster</b>	Verify the configuration.

To delete the cluster after creation, run the **no cluster** command in the global configuration mode. Only the administrator can delete the cluster.

Configuration Example:

# Create a cluster and name it clus0.

```
Ruijie# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Ruijie(config)# cluster clus0
```

## Adding or Deleting a Member

The administrator of a cluster can add a member and assign a cluster SN to the member, under the prerequisite that the device must be a candidate of the cluster. To add a member, run the commands listed in the following table.

Command	Function
Ruijie# <b>configure terminal</b>	Enter global configuration mode.
Ruijie(config)# <b>cluster</b> clus	Enter cluster configuration mode.
clus_1.Ruijie(config-cluster)# <b>member add</b> [ <i>member-id</i> ] <b>mac-address</b> <i>H.H.H</i>	Add a candidate as a member. A cluster SN can be assigned to the member. <i>member-id</i> : indicates the cluster SN of the member. The cluster assigns an idle SN to the member if it is not configured with a cluster SN. When the subnet mask of the cluster management IP address contains no more than 24 digits, the cluster SN range is 2–240. When the subnet mask of the cluster management IP address contains more than 24 digits, for example 255.255.255.128: The allocable IP host number range is 2–126, excluding IP host numbers consists of only zeros or all ones, and the one assigned to the administrator; The allocable cluster SN range is 2–126. <i>H.H.H</i> : indicates the MAC address of the device to be added.
clus_1.Ruijie(config-cluster)# <b>exit</b>	Return to the configuration mode.
clus_1.Ruijie(config)# <b>exit</b>	Return to privileged EXEC mode.
clus_1.Ruijie# <b>show cluster members</b>	View the cluster member and verify the configuration.

To delete a static member, run the **no member add** *member-id* command in the global configuration mode. The command can be run only on the administrator.

Configuration Example:

# Add the device with the MAC address 00d0.f8fe.1007 to the cluster and specify the cluster SN to 2.

```
Ruijie# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Ruijie(config)# cluster clus
clus_1.Ruijie(config-cluster)# member add 2 mac-address 00d0.f8fe.1007
```

## Specifying a Cluster for Managing a Device

This section describes how to specify a cluster for managing a member or candidate. To achieve this, run the commands listed in the following table.

Command	Function
Ruijie# <b>configure terminal</b>	Enter global configuration mode.
Ruijie(config)# <b>cluster member</b> { <b>cluster-name</b> <i>name</i>   <b>admin-address</b> <i>H.H.H</i> }	Specify the name or the MAC address of the cluster that manages the device. <i>name</i> : indicates the cluster name. <i>H.H.H</i> : indicates the MAC address of the administrator.
Ruijie(config)# <b>end</b>	Return to privileged EXEC mode.
Ruijie# <b>show run</b>	Verify the configuration.

You can run this command to configure the cluster that manages the device.

You can run the **no cluster member** command to delete the related information, so that the device can join any cluster.

After the command is run for a candidate, the candidate can join a specified cluster.

If the command is run for a member, the member exits the cluster and becomes a candidate if the current cluster is different from the specified cluster.

Configuration Example:

# Specify "cluster" as the name of the cluster that manages the device.

```
Ruijie# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Ruijie#cluster member cluster-name cluster
```

## Logging In to a Device

You can run the **cluster login** command on the administrator to log in to a member device for configuration, or run the command on a member device to log in to the administrator as described in the following table.

Command	Function
clus_1.Ruijie# <b>cluster login</b> { <b>administrator</b>   <b>member</b> { <i>member-id</i>   <i>H.H.H</i> } }	Run the command on the administrator to log in to a member device, or run the command on a member device to log in to the administrator. <i>member-id</i> : indicates the cluster SN of a member. <b>administrator</b> : logs in to the administrator from a member. <i>H.H.H</i> : indicates the MAC address of the member to be logged in to.

Run the command on the administrator to log in to a member for management.

To exit the member, run the **exit** command in the privileged EXEC mode.

Configuration Example:

# Run the following command to log in to member 2 from the administrator.



```
clus_1.Ruijie# cluster login member 2
CLUS_2.Ruijie# //Access the command line interface (CLI) of the member.
```

## Configuring the Cluster Timer

To configure the cluster timer value, run the commands listed in the following table.

Command	Function
clus_1.Ruijie# <b>configure terminal</b>	Enter global configuration mode.
clus_1.Ruijie(config)# <b>cluster</b>	Enter cluster configuration mode.
clus_1.Ruijie(config-cluster)# <b>timer topo-seconds</b>	Set the cluster topology collection timer. The range is 10–300 and the unit is second. The default value is 60 seconds.
clus_1.Ruijie(config-cluster)# <b>timer hold hold-seconds</b>	Set the timer-hold value of the topology request packet. The range is 10–300 and the unit is second. The default value is 90 seconds.
clus_1.Ruijie(config-cluster)# <b>timer hello hello-seconds</b>	Set the update time, namely the timer-hello value, of the member status. The range is 10–300 and the unit is second. The default value is 30 seconds.
clus_1.Ruijie(config-cluster)# <b>exit</b>	Return to the configuration mode.
clus_1.Ruijie (config)# <b>end</b>	Return to privileged EXEC mode.
clus_1.Ruijie # <b>show cluster</b>	Verify the configuration.

Run the command for configuring the cluster timer only on the administrator. Use the **no** form of the command to restore the default value.

Configuration Example:

# Configure the cluster timer value on the administrator.

```
clus_1.Ruijie#configure terminal //Run the command on the administrator CLI.
Enter configuration commands, one per line. End with CNTL/Z.
clus_1.Ruijie(config)# cluster
clus_1.Ruijie(config-cluster)# timer 65 //Set the topology collection time to 65.
clus_1.Ruijie(config-cluster)# timer hold 95 //Set the timer-hold value to 95 seconds.
clus_1.Ruijie(config-cluster)# timer hello 30 //Set the timer-hello value to 30 seconds.
```

## Configuring the Cluster Blacklist

This section describes how to add a device to the blacklist. That is, prohibit the device from joining the cluster. To achieve this, run the commands listed in the following table.

Command	Function
clus_1.Ruijie# <b>configure terminal</b>	Enter global configuration mode.

clus_1.Ruijie(config)# <b>cluster</b>	Enter cluster configuration mode.
clus_1.Ruijie(config-cluster)# <b>member black-list</b> <i>H.H.H</i>	Add a specified device to the cluster blacklist. <i>H.H.H</i> : indicates the MAC address of the device to be blacklisted.
clus_1.Ruijie(config-cluster)# <b>exit</b>	Return to configuration mode.
clus_1.Ruijie (config)# <b>end</b>	Return to privileged EXEC mode.
clus_1.Ruijie # <b>show cluster black-list</b>	Verify the configuration.

Run the command for blacklisting a device only on the administrator. If the specified device is in the cluster topology table, the device and its associated devices will exit the cluster and the device is blacklisted after the command is run.

Use the **no** form of the command to delete a device from the blacklist. If *H.H.H* is set, the device specified by *H.H.H* is deleted. If *H.H.H* is not set, all devices in the blacklist are deleted. After the device is deleted from the blacklist, it can join a cluster and become a member.

Configuration Example:

# Configure the cluster blacklist on the administrator. Add the device with the MAC address 0010-3500-e001 to the blacklist.

```
clus_1.Ruijie#configure terminal          //Run the command on the administrator CLI.
Enter configuration commands, one per line. End with CNTL/Z.
clus_1.Ruijie(config)# cluster
clus_1.Ruijie(config-cluster)#member black-list 0010-3500-e001
```

# Release all devices in the current cluster blacklist.

```
clus_1.Ruijie#configure terminal          //Run the command on the administrator CLI.
Enter configuration commands, one per line. End with CNTL/Z.
clus_1.Ruijie(config)# cluster
clus_1.Ruijie(config-cluster) # no member black-list
```

## Restarting a Member

Run the command listed in the following table to make a member restart.

Command	Function
clus_1.Ruijie# <b>cluster reload member</b> { <i>member-id</i>   <i>H.H.H</i> }	Restart a member. <i>member-id</i> : indicates the cluster SN of the member to be restarted. <i>H.H.H</i> : indicates the MAC address of the member to be restarted.

Run the command only on the administrator in privileged EXEC mode.

Configuration Example:

# Run the following command to make member 2 restart:

```
clus_1.Ruijie# cluster reload member 2
```

## Configuring the Topology Collection Hop Count of the Administrator

The allowed hop count indicates the topology collection range, within which devices can be discovered by the administrator and become candidates of the cluster. Run the command listed in following table to set the allowed hop count in topology collection from the farthest device to the administrator and use the **no** form of the command to restore the default value **5**.

Command	Function
clus_1.Ruijie# <b>configure terminal</b>	Enter global configuration mode.
clus_1.Ruijie(config)# <b>cluster</b>	Enter cluster configuration mode.
clus_1.Ruijie(config-cluster)# <b>hops-limit</b> <i>hop-number</i>	Set the allowed hop count in topology collection from the farthest device to the administrator. <i>hop-number</i> : indicates the hop count range for the cluster to discover candidates. The range is 1–16 and the default value is <b>5</b> .
clus_1.Ruijie(config-cluster)# <b>exit</b>	Return to the configuration mode.
clus_1.Ruijie (config)# <b>end</b>	Return to privileged EXEC mode.
clus_1.Ruijie # <b>show cluster</b>	Verify the configuration.

Run the command only on the administrator.

Configuration Example:

# Run the following command to set the allowed hop count to **4** in topology collection from the farthest device to the administrator:

```
clus_1.Ruijie#configure terminal          //Run the command on the administrator CLI.
Enter configuration commands, one per line. End with CNTL/Z.
clus_1.Ruijie(config)# cluster
clus_1.Ruijie(config-cluster)# hops-limit 4
```

## Configuring Cluster Management Resources

By default, when a cluster is created on a device, the device automatically configures management resources for the cluster. The cluster automatically obtains the idle management VLAN within VLAN 2049–3000 and the idle management IP address pool within 192.168.168.0/24–192.168.254.0/24. After the cluster is creation, run the command listed in the following table to manually configure new cluster management resources for the administrator, or run the **no** form of the command to restore the default settings.

Command	Function
clus_1.Ruijie# <b>configure terminal</b>	Enter global configuration mode.
clus_1.Ruijie(config)# <b>cluster</b>	Enter cluster configuration mode.
clus_1.Ruijie(config-cluster)# <b>management</b> { <b>vlan</b> <i>vlan-id</i>   <b>ip-pool</b> <i>ip-address ip-mask</i>   <b>vlan</b> <i>vlan-id</i> <b>ip-pool</b> <i>ip-address ip-mask</i> }	Configure cluster management resources. <i>lan-id</i> : indicates the cluster management VLAN ID. The range is 1–4094, <i>ip-address</i> : indicates the cluster management IP address. <i>ip-mask</i> : indicates the mask of the cluster management IP address pool.
clus_1.Ruijie(config-cluster)# <b>exit</b>	Return to configuration mode.

clus_1.Ruijie (config)# <b>end</b>	Return to privileged EXEC mode.
clus_1.Ruijie # <b>show cluster</b>	Verify the configuration.

Run the command only on the administrator.

Configuration Example:

# Run the following command to set 3333 as the cluster management VLAN and 10.10.10.0 255.255.255.128 as the cluster management IP address pool:

```
clus_1.Ruijie#configure terminal //Run the command on the administrator CLI.
Enter configuration commands, one per line. End with CNTL/Z.
clus_1.Ruijie(config)# cluster
clus_1.Ruijie(config-cluster)# management vlan 3333 ip-pool 10.10.10.0 255.255.255.128
```

## Configuring the Cluster Authentication Password

Run the commands listed in the following table to configure the authentication password of privileged EXEC mode for the management device or configure the authentication password for a specified device.

Command	Function
clus_1.Ruijie# <b>configure terminal</b>	Enter global configuration mode.
clus_1.Ruijie(config)# <b>cluster</b>	Enter cluster configuration mode.
clus_1.Ruijie(config-cluster)# <b>member password</b> { <i>password-id</i>   <i>H.H.H</i> } { <i>password</i>   <i>encryption-type</i> <i>encrypted-password</i> }	Configure the authentication password. <i>password-id</i> : indicates the ID of the cluster management password. <i>H.H.H</i> : indicates the MAC address of a device. <i>Password</i> : indicates a plain text password. <i>encryption-type</i> : indicates the encryption mode of the authentication password. <b>0</b> : not encrypted; <b>7</b> : encrypted. <i>encrypted-password</i> : indicates the authentication password after the encryption mode is specified.
clus_1.Ruijie(config-cluster)# <b>exit</b>	Return to configuration mode.
clus_1.Ruijie (config)# <b>end</b>	Return to privileged EXEC mode.
clus_1.Ruijie # <b>show run</b>	Verify the configuration.

Configuration Example:

# Configure the plain text password aaa for the device with the MAC address 00d0.f8fe.1007.

```
clus_1.Ruijie#configure terminal //Run the command on the administrator CLI.
Enter configuration commands, one per line. End with CNTL/Z.
clus_1.Ruijie(config)# cluster
clus_1.Ruijie(config-cluster)# member password 00d0.f8fe.1007 aaa
```

# Add the plain text password bbb to the cluster authentication password pool and specify the password pool SN to 12:

```
clus_1.Ruijie#configure terminal //Run the command on the administrator CLI.
Enter configuration commands, one per line. End with CNTL/Z.
clus_1.Ruijie(config)# cluster
clus_1.Ruijie(config-cluster)# member password 12 bbb
```

## Using the TFTP Agent

A member can use the administrator TFTP agent to download files from the TFTP server or upload files to the TFTP server. The administrator uses the **proxy tftp-server** command to set the TFTP server shared by clusters, and a member uses the administrator TFTP agent to implement the TFTP function. To achieve these, run the commands listed in the following table.

Command	Function
clus_1.Ruijie# <b>configure terminal</b>	Enter global configuration mode.
clus_1.Ruijie(config)# <b>cluster</b>	Enter cluster configuration mode.
clus_1.Ruijie(config-cluster)# <b>proxy tftp-server</b> <i>ip-address</i>	Set the TFTP server shared by clusters. <i>ip-address</i> : indicates the address of the TFTP servers shared by clusters (IPv4).
clus_1.Ruijie(config-cluster)# <b>exit</b>	Return to configuration mode.
clus_1.Ruijie (config)# <b>exit</b>	Return to privileged EXEC mode.
clus_1.Ruijie# <b>cluster login member 2</b>	Log in to member 2.
clus_2.Ruijie# <b>cluster tftp server: source-file flash:</b> [ <i>destination-file</i> ]	Member 2 downloads files from the TFTP server to a local host. <i>source-file</i> : indicates the source file to be transferred. The source file can be located on a remote TFTP server. <i>destination-file</i> : indicates the destination file to be transferred to. The destination file can be located on the local FLASH. If the destination file is not specified, the source file name is used the destination file name.
clus_2.Ruijie# <b>cluster tftp flash:source-file server:</b> [ <i>destination-file</i> ]	Member 2 uploads files from a local host to the TFTP server. <i>source-file</i> : indicates the source file to be transferred. The source file can be located on the local FLASH. <i>destination-file</i> : indicates the destination file to be transferred to. The destination file can be located on a remote TFTP server. If the destination file is not specified, the source file name is used the destination file name.

Run the command only on the administrator for configuring the TFTP server shared by cluster.

Configuration Example:

# Run the command on the administrator to set the TFTP server 172.10.1.1 to be the one shared by clusters. Then, access member 2, and use the TFTP server shared by clusters to transfer the **config.text** file to a local host.

```
clus_1.Ruijie#configure terminal           //Run the command on the administrator CLI.
Enter configuration commands, one per line. End with CNTL/Z.
clus_1.Ruijie(config)# cluster
clus_1.Ruijie(config-cluster)# proxy tftp-server 172.10.1.1
clus_1.Ruijie(config-cluster)#exit
clus_1.Ruijie(config)#exit
clus_1.Ruijie# cluster login member 2      //Access the CLI of member 2.
clus_2.Ruijie# cluster tftp server://config.text flash:config.text //Use the cluster TFTP
agent.
```

## Viewing the Cluster Configuration and Status

Run the commands listed in the following table in privileged EXEC mode to view information about the cluster.

Command	Function
<b>show cluster</b>	Show the basic information about the cluster of the device.
<b>show cluster members</b> [ <i>member-id</i>   <b>detail</b> ]	Show the member information, specifically all member information on the administrator, but only the administrator information and its own information on a member. <i>member-id</i> : indicates the cluster SN of a member.
<b>show cluster candidates</b> [ <b>detail</b>   <i>H.H.H</i> ]	Show candidate information only on the administrator. <i>H.H.H</i> : indicates the MAC address of a candidate.
<b>show cluster topology</b> [ <i>H.H.H</i>   <i>member-id</i> ]	Show the topology information about the cluster. <i>H.H.H</i> : indicates the MAC address of a cluster device. <i>member-id</i> : indicates the cluster SN of a member.
<b>show cluster black-list</b>	Show all the blacklist information.

Configuration Example:

# Show the basic information about the cluster of the device.

```
clus_1.Ruijie#show cluster
Cluster:                CLUSTER <Administrator>
Member-id:              1
Administrator mac address: 00d0.f822.33ac
Administrator name:      ruijie
Management vlan:         2056
Management ip:           192.168.176.1
Management ip-pool:       192.168.176.0/24
Total number of members:  2
Status:                  0 members are unreachable
Run time:                 0 days, 1 hours, 5 minutes, 37 seconds
Timer:                    60 seconds
Timer hello:              30 seconds
Timer hold:               90 seconds
Hops-limit:               5
Proxy tftp-server:        Not configured!
```

# Show information about a member.

```
clus_1.Ruijie# show cluster member
SN      MAC      Name      Hops State  LcPort  UpSN    UpMAC    UpPort
-----
1       00d0.f8fe.1007 switch-1    0    <Admin>
2       00d0.f8fe.43d2 switch-2    1    up      Fa0/2    1    00d0.f8fe.1007 Fa0/3
3       00d0.f8fe.a861 switch-3    2    up      Fa0/5    2    00d0.f8fe.43d2 Fa0/12
```

# Show information about a candidate.

```
clus_1.Ruijie# show cluster candidates
MAC      Hops LcPort   UpSN    UpMAC    UpPort   STATUS
-----
00d0.f8fe.43d2 1   Fa0/2    1    00d0.f8fe.1007 Fa0/3    ready
00d0.f8fe.a861 2   Fa0/5    -    00d0.f8fe.43d2 Fa0/12   ready
```

# Show the topology information about the cluster.

```
clus_1.Ruijie#show cluster topology
-----
      (PeerPort) ConnectFlag (LocalPort) [HostName:DeviceMac]
-----
ConnectFlag:
  <--> normal connect   **** cluster unenable -||- in blacklist
  ??? status down
-----
[CLUSTER_1.Ruijie:00d0.f822.33c8]
  |
  +-- (Fa0/11) <--> (Fa0/13) [CLUSTER_3.Ruijie:001a.a97b.d3ac]
  |  |
  |  +-- (Fa0/23) <--> (Fa0/21) [CLUSTER_4.ruijie:001a.a97e.043b]
  |      (Fa0/7) <--> (Fa0/7)
```

# Show all the blacklist information.

```
clus_1.Ruijie#show cluster black-list
MAC      Hops LcPort   UpSN    UpMAC    UpPort
-----
00d0.f8fe.43d2 1   Fa0/2    1    00d0.f8fe.1007 Fa0/3
00d0.f8fe.a861 -   -        -    -          -
```

## Example of Configuring Cluster Management

### Networking Requirements

The network has devices such as S0–S6 and these devices are directly interconnected through the network. Specifically: S0 has the IP address of the public network. The management workstation is a PC that can use Telnet or SNMP to access S0 through the network. Other devices are lately installed and require no configuration. S0–S5 support cluster management, but S6 does not.

MAC addresses of S0–S5 are as follows:

S0: 00d0.f800.0a10

S1: 00d0.f800.0ab1

S2: 00d0.f800.0ab2

S3: 00d0.f800.0ab3

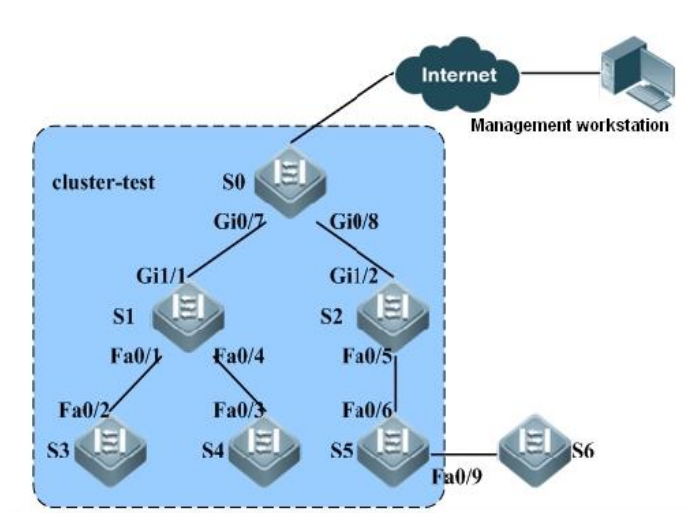
S4: 00d0.f800.0ab4

S5: 00d0.f800.0ab5

## Networking Topology

The following figure shows the networking topology.

Figure 1-2 Network topology



As shown in the preceding figure:

- S0 is directly connected to S1 and S2. S1 is directly connected to S0, S3, and S4. S2 is directly connected to S0 and S5. S5 is directly connected to S2 and S6. The figure shows the physical interfaces of these devices.
- The management workstation can directly access S0 through the IP address, involving using Telnet and SNMP. Other devices have no IP address and therefore cannot be accessed by the management workstation.

## Key Points

Since S0 is the only device that has the IP address of the public network, S0 is selected as the administrator and a cluster can be created on S0.

When topology collection is initiated on S0, the administrator can discover S1–S5 on the network that also support cluster management. S6 cannot be discovered because it does not support cluster management.

You can find that S1–S5 join the cluster on S0. Thus, the management workstation can access these devices.

## Configuration Procedure

Create a cluster on S0 and specify clus as the cluster name. S0 becomes the administrator, and its cluster SN is 1.

```
Ruijie# config
Enter configuration commands, one per line. End with CNTL/Z.
Ruijie(config)# cluster clus
```

The allowed cluster hop count, timer, timer-hold value, and timer value retain the default values. The cluster auto-addition function is disabled.



After creating the cluster on S0, S0 starts topology collection on S0, which takes some time. You can run the **show cluster candidates** command on S0 to view all discovered candidates.

Add discovered S1–S5 to the cluster. S6 cannot join the cluster because it cannot be discovered. Add devices by MAC address. Assign cluster SNs 2–6 to S1–S6 (if you do not assign the cluster SNs, the cluster automatically assigns the cluster SNs). Since S1–S5 are not configured with passwords of the enable 15 level, you do not need to specify the passwords.

```
clus_1.Ruijie(config-cluster)# member add 2 mac-address 00d0.f800.0ab1
clus_1.Ruijie(config-cluster)# member add 3 mac-address 00d0.f800.0ab2
clus_1.Ruijie(config-cluster)# member add 4 mac-address 00d0.f800.0ab3
clus_1.Ruijie(config-cluster)# member add 5 mac-address 00d0.f800.0ab4
clus_1.Ruijie(config-cluster)# member add 6 mac-address 00d0.f800.0ab5
```

Run the **show cluster member** command on S0 to view all discovered candidates after members are added.

Run the **cluster login** command on S0 to log in to every member. To exit the member, run the **exit** command on the member CLI in privileged EXEC mode. For example: Log in to the CLI of S2.

```
clus_1.Ruijie# cluster login member 3
clus_3.Ruijie-3#
```

Enable the SNMP Server function on S0. The community character string needs to be configured for SNMPv1/v2. For example, configure a read-only community character string as public.

```
clus_1.Ruijie# config
Enter configuration commands, one per line. End with CNTL/Z.
Ruijie(config)# enable services snmp-agent
clus_1.Ruijie(config)# snmp-server community public ro
```

Use SNMP to directly access a member on the management workstation. During usage, set the destination IP address to the public network IP address of S0, and add the member suffix in the community character string of S0. For example, use public@es3 as the community character string for accessing S2.

## Verifying the Configuration

Show the basic information about the cluster of the device.

```
clus_1.Ruijie# show cluster
Cluster:                               clus<Administrator>
Member -id:                            1
Administrator mac address:             00d0.f800.0a10
Administrator name:                    Ruijie
Management vlan:                       2049
Management ip:                         192.168.176.1
Management ip-pool:                    192.168.176.0/24
Total number of members:                6
Status:                                0 members are unreachable
Run time:                              0 days, 0 hours, 15 minutes, 8 seconds
Timer:                                 60 seconds
Timer hello:                           30 seconds
```

```

Timer hold:          90 seconds
Hops-limit:          5
Proxy tftp-server:    Not configured!

```

Show information about a candidate before the candidate is added as a member.

```

Ruijie# show cluster candidate

```

MAC	Hops	LcPort	UpSN	UpMAC	UpPort	STATUS
00d0.f800.0ab1	1	Gi1/1	1	00d0.f800.0a10	Gi0/7	READY
00d0.f800.0ab2	1	Gi1/2	1	00d0.f800.0a10	Gi0/8	READY
00d0.f800.0ab3	2	Fa0/2	-	00d0.f800.0ab1	Fa0/1	READY
00d0.f800.0ab4	2	Fa0/3	-	00d0.f800.0ab1	Fa0/4	READY
00d0.f800.0ab5	2	Fa0/6	-	00d0.f800.0ab2	Fa0/5	READY

Show information about a member.

```

clus_0.Ruijie# show cluster member

```

SN	MAC	Name	Hops	State	LcPort	UpSN	UpMAC	UpPort
1	00d0.f800.0a10	Ruijie	0	<Admin>				
2	00d0.f800.0ab1	Ruijie-1	1	up	Gi1/1	1	00d0.f800.0a10	Gi0/7
3	00d0.f800.0ab2	Ruijie-2	1	up	Gi1/2	1	00d0.f800.0a10	Gi0/8
4	00d0.f800.0ab3	Ruijie-3	2	up	Fa0/2	2	00d0.f800.0ab1	Fa0/1
5	00d0.f800.0ab4	Ruijie-4	2	up	Fa0/3	2	00d0.f800.0ab1	Fa0/4
6	00d0.f800.0ab5	Ruijie-5	2	up	Fa0/6	3	00d0.f800.0ab2	Fa0/5

```

clus_1.Ruijie# show cluster member detail

```

```

Device 'Ruijie-1' with member id 2 (Member)
  Device type:          S2628G
  MAC address:          00d0.f800.0ab1
  Serial Number:        1234942570112
  Upstream MAC address: 00d0.f800.0a10
  Local port:           Gi1/1
  Upstream port:        Gi0/7
  Hops from Administrator: 1
  Last topo update:     37 seconds ago
  Last udp update:      7 seconds ago
  Management ip:        192.168.176.2
  State:                up (Active)
  no receive topo response: 0 times
  no receive udp response: 0 times
  add method:           Manually add
Device 'Ruijie-2' with member id 3 (Member)
  Device type:          S2628G
  MAC address:          00d0.f800.0ab2
  Serial Number:        1234942579121
  Upstream MAC address: 00d0.f800.0a10

```

Local port: Gi1/2  
Upstream port: Gi0/8  
Hops from Administrator: 1  
Last topo update: 37 seconds ago  
Last udp update: 7 seconds ago  
Management ip: 192.168.176.2  
State: up (Active)  
no receive topo response: 0 times  
no receive udp response: 0 times  
add method: Manually add

Device 'Ruijie-3' with member id 4 (Member)

Device type: S2628G  
MAC address: 00d0.f800.0ab3  
Serial Number: 1234942579801  
Upstream MAC address: 00d0.f800.0ab1  
Local port: Fa0/2  
Upstream port: Fa0/1  
Hops from Administrator: 2  
Last topo update: 37 seconds ago  
Last udp update: 7 seconds ago  
Management ip: 192.168.176.2  
State: up (Active)  
no receive topo response: 0 times  
no receive udp response: 0 times  
add method: Manually add

Device 'Ruijie-4' with member id 5 (Member)

Device type: S2628G  
MAC address: 00d0.f800.0ab4  
Serial Number: 1234942570108  
Upstream MAC address: 00d0.f800.0ab1  
Local port: Fa0/3  
Upstream port: Fa0/4  
Hops from Administrator: 2  
Last topo update: 37 seconds ago  
Last udp update: 7 seconds ago  
Management ip: 192.168.176.2  
State: up (Active)  
no receive topo response: 0 times  
no receive udp response: 0 times  
add method: Manually add

Device 'Ruijie-5' with member id 6 (Member)

Device type: S2628G  
MAC address: 00d0.f800.0ab5  
Serial Number: 1234942570019  
Upstream MAC address: 00d0.f800.0ab2 (Cluster member 2)  
Local port: Fa0/6

```
Upstream port:          Fa0/5
Hops from Administrator: 2
Last topo update:       37 seconds ago
Last udp update:        7 seconds ago
Cluster ip:             192.168.176.2
State:                  up (Active)
no receive topo response: 0 times
no receive udp response: 0 times
add method:             Manually add
```

# SRM Configuration

## Introduction to SRM

### Overview

The System Resource Manager (SRM) feature allows you to monitor the utilization of limited resources in the embedded system. Through analysis of monitoring information, the network administrator can have a comprehensive understanding of device operation status and more accurate measurement of system performance, through which the administrator can take the corresponding measures to improve serviceability.

SRM mainly provides two functions: statistics and monitoring

**Statistics:** By querying the statistical information about resource usage, the user can understand the current resource distribution and historic records, providing strong reference for system optimization and troubleshooting.

**Monitoring:** Through reasonable configuration, the user can timely understand the changes in system status, and the system can also take specified actions according to such changes in order to maintain system stability and reliability.

The RGOS SRM architecture is shown below: SRM regards all system resources as Resource Owners (RO) and modules using these resources as Resource Users (RU). SRM framework is a bridge connecting resource owner, resource user and outside users; it is also the core of SRM architecture.

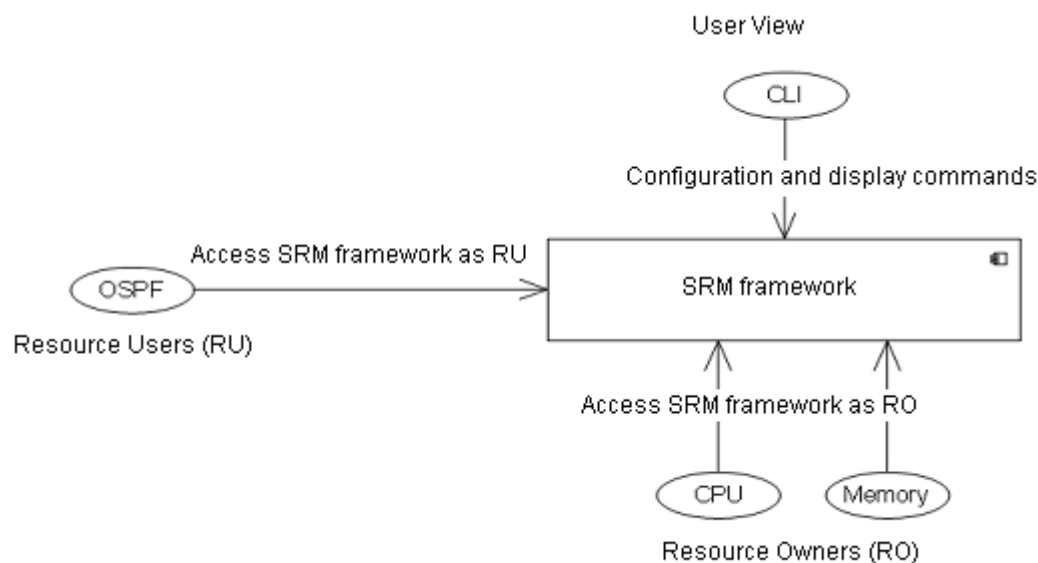


Fig 1 SRM architecture

### Basic concepts

#### Resource user

Resource User (RU) accesses the SRM framework in order to monitor resource usage and receive event notifications sent by the SRM framework.

RGOS only supports Task-type RU, namely RU and Task are in a one-to-one correspondence.

## Resource owner

Resource Owner (RO) corresponds to the existing resource management modules in RGOS and accesses the SRM framework to provide statistical information about resource allocation. When monitor event incurs, the SRM framework will notify RO, which will then execute the corresponding action.

Currently, RO only includes two resources: CPU and memory.

## SRM framework

SRM framework is built on basis of specific ROs and is responsible for the maintenance of RU, RO and policy related information and monitoring of resource utilization. The purpose of introducing SRM framework is to eliminate the difference between resource management modules and offer unified SRM configuration commands for users.

SRM framework mainly consists of three parts: RU group management, policy management and monitor instance. The relationship between SRM framework, RU and RO is shown below:

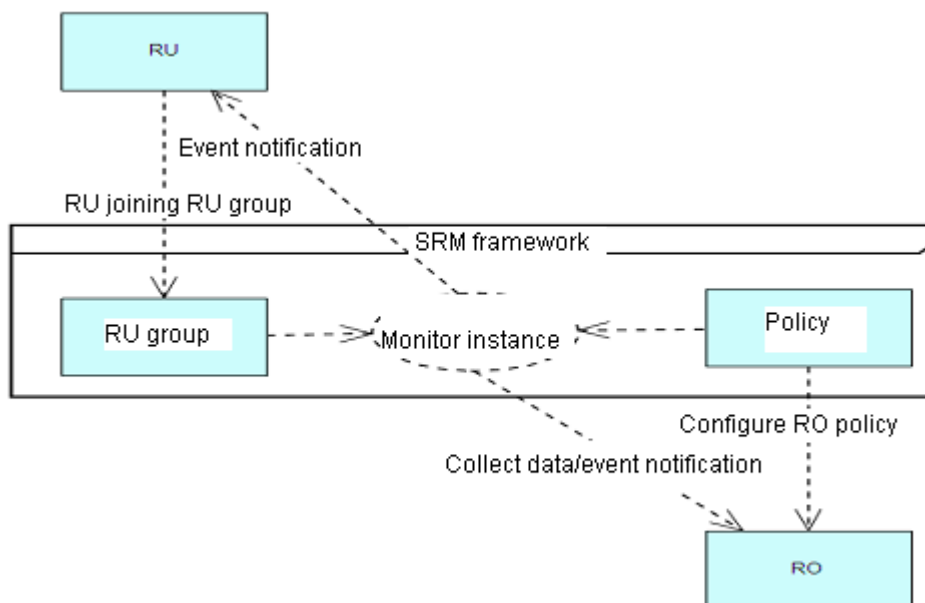


Fig 2 SRM framework

## RU group

To allow unified monitoring of similar RUs, the concept of "group" is introduced on the basis of RU, and the user can freely include multiple RUs into one RU group. When a monitor event incurs, the SRM framework will send the notification to all members in the RU group.

SRM contains the following three types of RU groups:

**Global group:** It the default RU group in the system, representing the monitoring of RO's global occupancy rate. There can be only one global group in the system.

**Unit group:** The group only contains a single RU. When the user monitors a single RU, SRM will automatically generate a unit group with the same name as RU. This unit group will replace RU and become the subject of monitoring.

Multi-member group: Such group contains multiple RUs. The user can define this group and add/delete RU members according to its own needs.

One RU can only belong to one RU group instead of multiple RU groups, or else one RU may be using multiple policies, which is not allowed in policy association.

## Policy

Policy is used to specify the subject and behavior of monitoring. One policy consists of one or more RO rules, while each RO rule consists of one or more thresholds of different levels.

One policy can be applied to multiple RU groups. When the policy is applied to RU group, we can say that the policy has associated with RU group, and a monitor instance will then be generated to monitor the usage of corresponding resource.

Policies can be divided into:

Global policy: The threshold monitoring in global policy will monitor the global occupancy rate of RO. Therefore, the global policy can only associate with global group, and the global group can only be applied with global policy.

User policy: The threshold monitoring in user policy will monitor the total resource occupancy rate of RUs specified by the user. The user policy can only associate with the unit group or multi-member group.

## Threshold

Threshold involves the following attributes:

Level: threshold level, which is used to indicate the degree of urgency: critical, major and minor. Different levels of thresholds will create different event notifications. The user can view historical information of such notification to learn about system operation status.

Rising value: rising threshold value (1-100). When the resource occupancy rate rises from a value lower than rising value to a value higher than the rising value, an UP event will incur.

Falling value: falling threshold value (1-100), which must be less than or equal to the rising value. When the resource occupancy rate falls from a value higher than falling value to a value lower than the falling value, a DOWN event will incur.

Interval: holding time, with unit being second, minimal value being 5s and maximal value being 86400s. When the occupancy rate exceeds the threshold and remains stable on one side of the threshold for a time exceeding the interval, a monitor event will incur. This will avoid that excessive null event notifications are created while the resource occupancy rate is fluctuating around the threshold.

## Working principle

As shown in Fig 2, the SRM framework monitors RU/RO resource utilization through the monitor instance created upon the association of policy and RU group. The monitor instance will periodically monitor RU/RO resource utilization and compare with the threshold indicated in the policy. When the resource occupancy rate is found to exceed the threshold and remains stable on one side of the threshold for a time exceeding the interval, the corresponding monitor event will be triggered.

When a monitor event incurs, SRM framework will notify RO and RU, and RO will usually generate the corresponding log.

## Protocol specification

N/A

## Configure SRM

### Default configurations

There is no default configuration for SRM.

### Configure monitor policy

Command	Function
Ruijie>enable	Enter privilege mode.
Ruijie#configure terminal	Enter global configuration mode.
Ruijie(config)#resource manager [[device device-num] mboard {M1   M2}   slot slot-num]]	Enter SRM configuration mode. Enter SRM configuration mode of this board. <b>device device-num</b> : Specify the device to be configured (only effective for stacked and VSU devices); <b>mboard { M1   M2 }</b> : Specify the management board to be configured (M1 or M2, only effective for chassis or VSU devices); <b>slot slot-num</b> : Specify the line card to be configured (only effective for chassis or VSU devices).
Ruijie(config-srm)#policy policy-name [global] or Ruijie(config-srm-slave)#policy policy-name [global] or Ruijie(config-srm-slot-slotnum)#policy policy-name [global]	Configure the policy and enter SRM-policy configuration mode. <i>policy-name</i> : Name of monitor policy. <b>Global</b> : If you add the global parameter, it will become a global policy; otherwise, it is a user policy.
Ruijie(config-srm-policy)#{memory   cpu}	Enter owner configuration mode. Currently, two ROs are supported: memory and cpu.
Ruijie(config-owner-memory)#{critical   major   minor} rising rising-waterline-value [interval interval-value] [falling falling-waterline-value [interval interval-value]]	Configure threshold. The unit of threshold is percent (1-100). Note: The rising threshold of major must be greater than that of minor, and the rising threshold of critical must be greater than that of major.

To delete the policy configuration, execute "**no policy policy-name**" command in the SRM mode.

Configuration example:

# Configure a global policy named rgos\_policy and configure the memory option of this policy.

```
Ruijie#configure terminal
Ruijie(config)#resource manager
Ruijie(config-srm)#policy rgos_policy global
```



```
Ruijie(config-srm-policy)#memory
Ruijie(config-owner-memory)#major rising 30 falling 15 interval 10
```

## Apply monitor policy

Command	Function
Ruijie> <b>enable</b>	Enter privilege mode.
Ruijie# <b>configure terminal</b>	Enter global configuration mode.
Ruijie(config)# <b>resource manager</b>	Enter SRM configuration mode.
Ruijie(config-srm)# <b>user global</b> <i>global-policy-name</i>	Apply global policy to the global group.
Ruijie(config-srm)# <b>user</b> <i>resource-user-name</i> <i>resource-policy-name</i>	Apply user policy to a resource user.

Configuration example:

# Configure a global policy named rgos\_policy and apply to the global group.

```
Ruijie#configure terminal
Ruijie(config)#resource manager
Ruijie(config-srm)#policy rgos_policy global
Ruijie(config-srm-policy)#exit
Ruijie(config-srm)#user global rgos_policy
# Configure an user policy named rgos_policy and apply to ospf.
Ruijie#configure terminal
Ruijie(config)#resource manager
Ruijie(config-srm)#policy rgos_policy
Ruijie(config-srm-policy)#exit
Ruijie(config-srm)#user ospf rgos_policy
```

# Please refer to "Configure RU group" to learn how to apply policy to the group.

## Configure RU group

Command	Function
Ruijie> <b>enable</b>	Enter privilege mode
Ruijie# <b>configure terminal</b>	Enter global configuration mode
Ruijie(config)# <b>resource manager</b>	Enter SRM configuration mode.
Ruijie(config-srm)# <b>user group</b> <i>resource-group-name</i>	Configure RU group and enter res-group configuration mode <i>resource-group-name</i> : name of RU group
Ruijie(config-res-group)# <b>instance</b> <i>resource-user-name</i>	Add RU. <i>resource-user-name</i> is the name of RU; view all RUs by executing "show resource database".
Ruijie(config-res-group)# <b>policy</b> <i>policy-name</i>	Apply policy. <i>policy-name</i> is the name of policy.

Configuration example:

# Configure a RU group named rgos\_group and add ospf into the group, and finally apply the policy to the group.

```
Ruijie#configure terminal
Ruijie(config)#resource manager
```

```
Ruijie(config-srm)#user group rgos_group
Router(config-res-group)#instance ospf
Router(config-res-group)#policy rgos_policy
```

## Display SRM configurations and status

Command	Function
Ruijie# <b>show resource database</b> [ <b>device</b> <i>device-num</i> ] <b>mboard</b> { <b>M1</b>   <b>M2</b> }   slot <i>slot-num</i> ] ]	View SRM database, including RU information, RO information and policy information.  By default, SRM database information of main board is displayed;  <b>device</b> <i>device-num</i> : Specify the device to view (only effective for stacked and VSU devices);  <b>mboard</b> { <b>M1</b>   <b>M2</b> }: Specify the management board to view (M1 or M2, only effective for chassis or VSU devices);  slot <i>slot-num</i> : Specify the line card to view (only effective for chassis or VSU devices).
Ruijie# <b>show resource notification owner</b> { <b>all</b>   <b>cpu</b>   <b>memory</b> } [ [ <b>device</b> <i>device-num</i> ] <b>mboard</b> { <b>M1</b>   <b>M2</b> }   <b>slot</b> <i>slot-num</i> ] ]	Display statistics of event notifications.  <b>all</b> : Display statistics of all ROs;  <b>cpu</b> : Display statistics related to CPU;  <b>memory</b> : Display statistics related to memory;  By default, event notification statistics of main board will be displayed;  <b>device</b> <i>device-num</i> : Specify the device to view (only effective for stacked and VSU devices);  <b>mboard</b> { <b>M1</b>   <b>M2</b> }: Specify the management board to view (M1 or M2, only effective for chassis or VSU devices);  slot <i>slot-num</i> : Specify the line card to view (only effective for chassis or VSU devices).
Router# <b>show resource owner</b> { <b>all</b>   <b>cpu</b>   <b>memory</b> } [ [ <b>device</b> <i>device-num</i> ] <b>mboard</b> { <b>M1</b>   <b>M2</b> }   slot <i>slot-num</i> ] ]	Display RO utilization.  <b>all</b> : Display all RO resources;  <b>cpu</b> : CPU resource;  <b>memory</b> : Memory resource.  By default, RO utilization of main board is displayed;  <b>device</b> <i>device-num</i> : Specify the device to view (only effective for stacked and VSU devices);  <b>mboard</b> { <b>M1</b>   <b>M2</b> }: Specify the management board to view (M1 or M2, only effective for chassis or VSU devices);  slot <i>slot-num</i> : Specify the line card to view (only effective for chassis or VSU devices).

Router#show resource policy {all   policy-name} [[ <b>device</b> device-num] mboard { M1   M2 }   slot slot-num]]	<p>Display policy information.</p> <p>all: Display all policies;</p> <p>policy-name: Specific name of policy.</p> <p>By default, policy information of main board is displayed;</p> <p><b>device</b> device-num: Specify the device to view (only effective for stacked and VSU devices);</p> <p><b>mboard { M1   M2 }</b>: Specify the management board to view (M1 or M2, only effective for chassis or VSU devices);</p> <p>slot slot-num: Specify the line card to view (only effective for chassis or VSU devices).</p>
Ruijie#show resource relationship [[ <b>device</b> device-num] mboard { M1   M2 }   slot slot-num]]	<p>Display the association between policy and RU group.</p> <p>By default, association information of main board is displayed;</p> <p><b>device</b> device-num: Specify the device to view (only effective for stacked and VSU devices);</p> <p><b>mboard { M1   M2 }</b>: Specify the management board to view (M1 or M2, only effective for chassis or VSU devices);</p> <p><b>slot</b> slot-num: Specify the line card to view (only effective for chassis or VSU devices).</p>
Ruijie#show resource user {all   group { all   group-name }   resource-user-name } [ [ <b>device</b> device-num ] mboard { M1   M2 }   slot slot-num ] ]	<p>Display RU configurations.</p> <p><b>all</b>: All RUs and RU groups;</p> <p><b>group { all   group-name }</b>: RU group; all means all RU groups; group-name means the name of RU group;</p> <p>resource-user-name: Name of RU.</p> <p>By default, RU configurations of main board is displayed;</p> <p>device device-num: Specify the device to view (only effective for stacked and VSU devices);</p> <p><b>mboard { M1   M2 }</b>:Specify the management board to view (M1 or M2, only effective for chassis or VSU devices);</p> <p><b>slot</b> slot-num: Specify the line card to view (only effective for chassis or VSU devices).</p>

## Typical SRM configuration example

### Networking requirements

Monitor memory and CPU usage of entire device; monitor memory and CPU usage of a specific service module (such as OSPF, 802.1X, etc).

### Network topology

Unrelated to topology.

## Configuration tips

N/A

## Configuration steps

Configure a global policy to monitor CPU usage; when system memory usage reaches 60% for more than 10 seconds, major event is triggered, and SRM will record the relevant log (please view SYSLOG file of SRM.txt).

### # Configure a global policy to monitor memory usage

```
Ruijie#configure terminal
Ruijie(config)#resource manager
Ruijie(config-srm)#policy rgos_global_policy global
Ruijie(config-srm-policy)#memory
Ruijie(config-owner-memory)#major rising 60 interval 10
Ruijie(config-owner-memory)#exit
Ruijie(config-srm-policy)# exit
Ruijie(config-srm)#user global rgos_global_policy
```

### # Configure an user policy and apply to ospf.

```
Ruijie#configure terminal
Ruijie(config)#resource manager
Ruijie(config-srm)#policy rgos_user_policy
Ruijie(config-srm-policy)#memory
Ruijie(config-owner-memory)#major rising 30 falling 15 interval 10
Ruijie(config-owner-memory)#exit
Ruijie(config-srm-policy)#exit
Ruijie(config-srm)#user ospf rgos_user_policy
```

Configure RU group and add specific RU into this group, and then apply the policy to this RU group to monitor resource usage of RU.

### # Configure policy and group and associate them.

```
Ruijie#configure terminal
Ruijie(config)#resource manager
Ruijie(config-srm)#policy rgos_grp_policy
Ruijie(config-srm-policy)#memory
Ruijie(config-owner-memory)#major rising 30
Ruijie(config-owner-memory)#exit
Ruijie(config-srm-policy)#exit
Ruijie(config-srm)#user group rgos_group
Router(config-res-group)#instance dlx_task
Ruijie(config-res-group)#policy rgos_grp_policy
```

## Verification

Display SRM database information

```
Router#show resource database
```

Resource Owners	Id
memory	0x1
cpu	0x2

Resource User Groups	Id
ru-group1	0x1000116
ru-group2	0x1000117

Resource User	Id	Priority	Description
aaa	0x1000001	APP_TASK	AAA service
context	0x1000002	HAPP_TASK_TS	Context service
dot1x	0x1000003	APP_TASK	DOT1X service
eim	0x1000004	APP_TASK	EIM service
ftp	0x1000005	APP_TASK	FTP clinet
ntp	0x1000006	APP_TASK	NTP clinet
ntps	0x1000007	APP_TASK	NTP service
printk	0x1000008	APP_TASK	to print log
radius	0x1000009	APP_TASK	RADIUS service
web-auth	0x100000a	APP_TASK	Web auth service

Display statistics of event notifications.

```
Router#show resource notification owner all user all
```

Owner: memory

global Notif.: critical(0/0), major(0/0), minor(0/0)

RU Group	User Notif. (cr (U/D) :ma (U/D) :mi (U/D) )
ru-group1	0/0:0/0:0/0
ru-group2	0/0:0/0:0/0
ru-group3	0/0:0/0:0/0

RU	User Notif. (cr (U/D) :ma (U/D) :mi (U/D) )
aaa	0/0:0/0:0/0
context	0/0:0/0:0/0
dot1x	0/0:0/0:0/0

```

eim          0/0:0/0:0/0
ftp          0/0:0/0:0/0
ntp          0/0:0/0:0/0
ntps         0/0:0/0:0/0
printk       0/0:0/0:0/0
radius       0/0:0/0:0/0
web-auth     0/0:0/0:0/0

```

Owner: cpu

global Notif.: critical(0/0), major(0/0), minor(0/0)

```

RU Group      User Notif. (cr (U/D) :ma (U/D) :mi (U/D) )
-----

```

```

ru-group1     0/0:0/0:0/0
ru-group2     0/0:0/0:0/0
ru-group3     0/0:0/0:0/0

```

```

RU            User Notif. (cr (U/D) :ma (U/D) :mi (U/D) )
-----

```

```

Aaa           0/0:0/0:0/0
Context       0/0:0/0:0/0
dot1x         0/0:0/0:0/0
eim           0/0:0/0:0/0
ftp           0/0:0/0:0/0
ntp           0/0:0/0:0/0
ntps          0/0:0/0:0/0
printk        0/0:0/0:0/0
radius        0/0:0/0:0/0
web-auth      0/0:0/0:0/0

```

## Display RO information

```
Router#show resource owner all
```

Resource Owner: memory

Total Size(B): 134217728

Used Size(B): 63963136

RU Group	Allocated Size(B)	number
ru-group1	10344992	12
ru-group2	12344992	11
ru-group3	10344992	10

RU	Allocated Size(B)	number
aaa	916100	12
context	894240	11

dot1x	719568	10
eim	629100	15
ftp	400488	16
ntp	262152	22
ntps	262148	25
printk	198444	16
radius	196620	25
web-auth	192008	23

Resource Owner: cpu

Total Size(B): 100

Used Size(B): 66

RU Group	Runtime (ms)	uSecs	5Sec	1Min	5Min
ru-group1	16777216	0	0.00%	0.00%	0.00%
ru-group2	16777217	0	0.00%	0.00%	0.00%
ru-group3	16777218	0	0.00%	0.00%	0.00%

RU	Runtime (ms)	uSecs	5Sec	1Min	5Min
aaa	16777494	0	0.00%	0.00%	0.00%
context	16777495	0	0.00%	0.00%	0.00%
dot1x	16777217	0	0.00%	0.00%	0.00%
eim	16777218	0	0.00%	0.00%	0.00%
ftp	16777219	0	0.00%	0.00%	0.00%
ntp	16777220	0	0.00%	0.00%	0.00%
ntps	16777221	0	0.00%	0.00%	0.00%
printk	16777222	0	0.00%	0.00%	0.00%
radius	16777223	0	0.00%	0.00%	0.00%
web-auth	16777224	0	0.00%	0.00%	0.00%

#### Display policy information

```
Router#show resource policy all
```

List of all Configured Policies:

policy Name: g-policy01

Type: global In Use: Yes

RO memory:

critical rising 80 interval 10 falling 75 interval 10

major rising 70 interval 10 falling 65 interval 10

minor rising 60 interval 10 falling 55 interval 10

RO cpu:

critical rising 90

major rising 60

policy Name: g-policy02

```
Type: global          In Use: No
RO memory:
  critical rising 80 interval 10 falling 75 interval 10
  major rising 70 interval 10 falling 65 interval 10
  minor rising 60 interval 10 falling 55 interval 10
RO cpu:
  critical rising 90
  major rising 60
```

policy Name: u-policy01

```
Type: User           In Use: No
RO memory:
  critical rising 80 interval 10 falling 75 interval 10
  major rising 70 interval 10 falling 65 interval 10
  minor rising 60 interval 10 falling 55 interval 10
RO cpu:
  critical rising 90
  major rising 60
```

policy Name: u-policy02

```
Type: User           In Use: No
RO memory:
  critical rising 80 interval 10 falling 75 interval 10
  major rising 70 interval 10 falling 65 interval 10
  minor rising 60 interval 10 falling 55 interval 10
RO cpu:
  critical rising 90
  major rising 60
RU Group /RU :
User: Context
Group: u-grp01
user: snmpd
```

#### Display association information

```
Router#show resource relationship
policy          RU Group /RU
-----
g-policy01      aaa
u-policy01      u-grp01
u-policy01      ftp
u-policy01      eim
```

#### Display RU information

```
Router#show resource user all

Resource User Grp: u-grp01
```



```
policy: u-policy01
User: aaa, dotlx
Resource Owner: memory
    Allocated Size(B): 0 number: 0
Resource Owner: cpu
    Runtime(ms)    5Sec    1Min    5Min
    16777494      0.00%   0.00%   0.00%
```

```
Resource User Grp: u-grp02
policy: u-policy01
User:
Resource Owner: memory
    Allocated Size(B): 0 number: 0
Resource Owner: cpu
    Runtime(ms)    5Sec    1Min    5Min
    0              0.00%   0.00%   0.00%
```

```
Resource User: EDDRI_MAIN
policy: u-policy01
Resource Owner: memory
    Allocated Size(B): 123456 number: 3
Resource Owner: cpu
    Runtime(ms)    5Sec    1Min    5Min
    0              0.00%   0.00%   0.00%
```

```
Resource User: eim
policy: u-policy01
Resource Owner: memory
    Allocated Size(B): 234516 number: 3
Resource Owner: cpu
    Runtime(ms)    5Sec    1Min    5Min
    0              0.00%   0.00%   0.00%
```

## Redundancy Configuration

This chapter describes how to configure the management module redundancy to implement nonstop forwarding(NSF) and the system file management method of the the management module.

This chapter includes:

1. Understanding redundant NSF of the management module
2. NSF configuration method

## Understanding Redundant NSF of Management Module

---

### Overview

---

NSF means that in the network device with the structure of separating control panel from forward panel, the control panel is planned to shut down(such as software upgrade) or not planned to shut down(such as software and hardware defect) while the forward panel goes on forwarding and there is no forward halt or topology fluctuation during the reboot of control side. NSF is an important part of High Availability Architecture

In the machine which is installed with dual the management modules, the the master management module is used normally while the other backup one is the slave management module which is a substitute for the master one when the master one is broken off or requires for the switchover. It not only enlarges exchanging capacity but also offers management redundancy to improve the stability of device. In the running process of the device, if the the master management module does not work well, the device will switch to the slave one automatically without losing user's corresponding configuration, which ensures that the network runs well. Generally, the slave management module does not join in the switch management but monitors the status of master one. These events below will trigger the management module switchover:

- 1) System suspend or reset due to hardware fault of the master management module
- 2) No heartbeat between two management modules
- 3) Manual switchover

When booting dual management modules at the same time or hot-plugging another when one board is enabled, they will do some batch synchronization configuration before they are in Active/Standby Hot status. At this time, if disturbance sources are configured, the slave management module will reboot and both are in Active/Boot Hot status. If all disturbance sources are cleared in Active/Boot Hot status, the slave one will reboot too and both are in Active/Standby Hot status. If new disturbance sources are configured in Active/Boot Hot status, this brings no influence and both are still in Active/Boot Hot status.



Now, the disturbance sources include the following entities:

- PTLVLAN: Protocol VLAN, VLAN classification technology based on package protocol type. It can divide the null VLAN ID of a protocol type to a same VLAN.
- MCAST6: Multicast for ipv6

Postscript: the dual management panels are in Boot Cold/Boot Cold status if the system detects the inconsistency of the software version of the dual ones when starting up. In other words, they can detect the other side respectively, but they are not in Active/Standby Hot status until the automatic upgrade is finished and the slave one is reset. Finally, the software version of the dual management modules is consistent.

---

## NSF Advantages and Limits

---

The advantages of NSF technology implementation in network service are:

- Improving the network availability:

NSF technology maintains the information of data forwarding and user session status in the process of device change.
- Preventing the neighbour from detecting link flap:

The forwarding side does not reboot during the switchover, so the neighbour can not detect the link status change from Down to Up.
- Preventing routing flaps:

The forwarding side maintains to forward and communicate during the switchover and the control side forms new forwarding list quickly without apparent substitution between the new and old forwarding list, thus preventing routing flaps.
- User sessions will not be lost:

User sessions built before the switchover will not be lost due to the synchronization in real time.

The limits of using NSF technology in the switch are:

- NSF works well on the premise that the software and hardware constitution of the dual the management modules are consistent.
- It should synchronizes the master and the slave management modules in batch to make them consistent, before which is the window period when NSF can not take effect.
- Not all the functions related with forwarding are synchronized. The switch function can be classified into the following types according to NSF supporting degree:
  - High availability support function;
  - Real time synchronization of status information between master and the slave management module. For example, it synchronizes the control side function directly related with L2 forwarding in real time.
  - High availability compatibility function
  - These features do not support high availability for the status datas are not synchronized. However, when enabling high availability, these functions that starts to run from initialization can still be used after switching.
  - High availability incompatibility function

**Caution**

These features do not support high availability for the status datas are not synchronized. When enabling high availability, these functions can not be used, or it may lead to system abnormity. When enabling these functions, the system status is changed from Standby Hot to Boot Hot and the system can only synchronize running-config.

## Key Technology of NSF

The key technologies of implementing NSF include:

- **Status synchronization**

The the master management module synchronizes the running status with the slave one in order to enable the slave one to be a substitute for the master one at any time without noticeable changes.

- **Configuration synchronization**

It synchronizes the configurations of the functions that are not associated with NAF directly. The user configuration keeps consistent during the switchover by the synchronization of running-config and startup-config.

Conducting running-config when user configuration returns to the privileged EXEC mode from the global mode, while conducting startup-config synchronization when the user executes command write or copy to save the configuration.

It can not synchronize SNMP configuration automatically until running-config synchronization is triggered by CLI configuration method.

You can configure auto-sync mode as the following steps. In the global configuration mode, execute command **redundancy** first and then **auto-sync { standard | startup-config | running-config }**. To view the current auto-sync mode, use **show redundancy auto-sync** in the privileged EXEC mode. To configure the auto-sync interval in an unit of second, execute command **redundancy** first and then **auto-sync time-period value**.



Auto-sync has three modes:

- a) standard: synchronizes all the system files. In other words, it synchronizes both startup-config and running-config.
- b) startup-config: synchronizes startup configuration file.
- c) running-config: synchronizes configuration file of running time.

The **no** form of the command disables all the modes, making the configuration file out of auto-sync. By default , the mode of auto-sync is standard, which synchronizes both startup-config and running-config.

---

## NSF Configuration Method

---



In the management module redundancy constitution methods, only the master management module supports all CLI commands, while the slave management module supports a few commands in user EXEC and privileged EXEC mode.

---

## Configuring Redundant Management

---

This chapter includes:

- Automatic selection of the master management module
- Manual selection of the master management module

---

### Automatic selection of the master management module

---

You can plug or unplug the the management modules while the switch is working. Based on the current conditions, the switch automatically selects an engine for its operation without normal data switching. In case of any conditions below during you use, the the master management module will be selected

accordingly:

- If only one the management module is plugged when the switch is started up, the switch will select it as the the master management module no matter whether it is in slot M1 or M2.
- If both the management modules are plugged when the switch is started up, by default, the one in slot M1 will be selected as the master and the one in slot M2 as the slave for purpose of redundancy. Related prompt message will be provided.
- If only one the management module is plugged when the switch is started up, and the other the management module is plugged while the switch is in normal operation, the latter will be regarded as the the slave management module for purpose of redundancy, no matter whether it is slot M1 or M2. Related prompt message will be provided.
- If both the management modules are plugged when the switch is started up, and one of them is unplugged while the switch is in normal operation (or one becomes abnormal): if the unplugged the management module is the slave before it is unplugged (or abnormal), the switch only prompts that the the slave management module is unplugged (or becomes abnormal); if the unplugged the management module is the master before it is unplugged (or abnormal), the other the management module will turn from slave to master, and related prompt will be provided.

---

During the normal operation of the switch, the parameters must be saved when the configurations are done; otherwise, the configuration will be lost in case of master/salve switchover.

During the startup of the device inserted with two the management modules, if the main program of any the management module is incomplete or absent, the switch cannot start. The symptom is that the two boards restart repeatedly or suspend during the startup process.

During the startup of the device inserted with one the management module, if the management module with incomplete or absent CTRL program or main program is inserted before the success of the startup, the switch also cannot start.



**Caution**

In the above two case, remove the faulty the management modules. If the device is still abnormal, power off the switch and restart it.

During the batch backup of master and the slave management module, do not unplug the master one, or it will lead to data flow breakoff due to system reset. If the software of dual the management modules are abnormal during the period of batch backup, it will also lead to data flow breakoff due to system reset.

Please unplug one of the dual the management modules quickly if you want to unplug one of them when they are working simultaneously. Slow unplugging may make the management module work abnormally. Please make sure that the management module is plugged tightly and the screw id tightened.

---

### **Manual selection of the master management module**

---

You may select the master and the slave management modules by using the commands available in CLI.

In the privileged user mode, execute the following commands to forcibly switch over the the master management module:

Command	Meaning
<b>redundancy force-switch</b>	This command is executed immediately without the necessity for global configuration mode.

For example, the current the master management module is the one in slot M1. When the following commands are executed, the the management module will be switched over to the the slave management module, and the one in slot M2 becomes the master.

```
Ruijie# redundancy force-switch
```

## Configuring the Synchronization Mode

Run the following commands to configure the configuration files to be synchronized:

Command	Function
Ruijie(config)# <b>redundancy</b>	Enter the redundancy configuration mode
Ruijie(config-red)# <b>auto-sync</b> { <b>standard</b>   <b>running-config</b>   <b>startup-config</b> }	Configure the configuration files to be synchronized.
Ruijie# <b>show running-config</b>	Confirm the hot-backup started.
Ruijie# <b>show redundancy state</b>	Show the current redundancy operation mode.

## Configuring the Heart-beat Check Time

Run the following command to configure the heart-beat check time between the master and the slave management modules.

Command	Function
Ruijie(config)# <b>redundancy</b>	Enter the redundancy configuration mode
Ruijie(config-red)# <b>switchover timeout</b> <i>timeout-period</i>	Control the heart-beat check time between the master and slave boards
Ruijie# <b>show running-config</b>	Confirm the hot-backup started.
Ruijie# <b>show redundancy state</b>	Show the current redundancy operation mode.

## Resetting the Management Module

Run the following command to reset the specified the management module or both the master and slave ones.

Command	Function
Ruijie(config)# <b>redundancy reload</b> { <b>peer</b>   <b>shelf</b> }	peer: reset the slave management module only. shelf: reset both of master and slave management modules.

# Hardware Entry Capacity Configuration

## Overview

Hardware capacity configuration function is provided to flexibly apply hardware entry resources and meet requirements of different business scenarios.

## Configuring Hardware Entry Capacity

Users can configure the maximum route number of the following hardware entry. The maximum IPv4 unicast route number will be auto-calculated by the system.

The maximum number of IPv4 (S, G) multicast routes

The maximum number of IPv6 unicast routes

The maximum number of IPv6 (S, G) multicast routes

The maximum number of policy-based routes

The maximum number of IPv6 tunnel neighbors

The maximum number of IPv6 tunnel interfaces

The maximum number of shared pools

---

The above configurations take effect after being saved and reloading the device.

---

## Configuring the Maximum Number of IPv4 (S, G) Multicast Routes

Command	Function
Ruijie(config)# <b>initialization route ipv4mc</b> <i>max-num</i>	Sets the maximum number of IPv4 (S, G) multicast routes. The default value is 500.
Ruijie(config)# <b>no initialization route IPv4mc</b>	Restores the default value.
Ruijie(config)# <b>initialization route IPv4mc ?</b>	Displays the current permitted maximum value.

## Configuring the Maximum Number of IPv6 (S, G) Multicast Routes

Command	Function
Ruijie(config)# <b>initialization route ipv6mc</b> <i>max-num</i>	Sets the maximum number of IPv6 (S, G) multicast routes. The default value is 0.
Ruijie(config)# <b>no initialization route</b> <b>ipv6mc</b>	Restores the default value.
Ruijie(config)# <b>initialization route ipv6mc ?</b>	Displays the current permitted maximum value.

## Configuring the Maximum Number of IPv6 Unicast Routes

Command	Function
---------	----------



Ruijie(config)# <b>initialization route ipv6uc</b> <i>max-num</i>	Sets the maximum number of IPv6 unicast routes. The default value is 0.
Ruijie(config)# <b>no initialization route ipv6uc</b>	Restores the default value.
Ruijie(config)# <b>initialization route ipv6uc ?</b>	Displays the current permitted maximum value.

## Configuring the Maximum Number of Policy-based Routes

Command	Function
Ruijie(config)# <b>initialization route pbr</b> <i>max-num</i>	Sets the maximum number of policy-based routes. The default value is 64.
Ruijie(config)# <b>no initialization route pbr</b>	Restores the default value.
Ruijie(config)# <b>initialization route pbr ?</b>	Displays the current permitted maximum value.

## Configuring the Maximum Number of IPv6 Tunnel Neighbors

Command	Function
Ruijie(config)# <b>initialization route tunnel-start</b> <i>max-num</i>	Sets the maximum number of IPv6 tunnel neighbors. The default value is 0.
Ruijie(config)# <b>no initialization route tunnel-start</b>	Restores the default value.
Ruijie(config)# <b>initialization route tunnel-start ?</b>	Displays the current permitted maximum value.

## Configuring the Maximum Number of IPv6 Tunnel Interfaces

Command	Function
Ruijie(config)# <b>initialization route tunnel-termination</b> <i>max-num</i>	Sets the maximum number of IPv6 tunnel interfaces. The default value is 32.
Ruijie(config)# <b>no initialization route tunnel-termination</b>	Restores the default value.
Ruijie(config)# <b>initialization route tunnel-termination ?</b>	Displays the current permitted maximum value.

## Configuring the Maximum Number of Shared Pools

Command	Function
Ruijie(config)# <b>initialization route shared-pool</b> <i>max-num</i>	Configures the maximum number of shared pools. The default value is 200. The shared pool provides resources for MPLS, vlan-mapping, mac-vlan, subnet-vlan and qinq-adv functions.
Ruijie(config)# <b>no initialization route shared-pool</b>	Restores the default value.
Ruijie(config)# <b>initialization route shared-pool ?</b>	Displays the current permitted maximum value.

## Displaying the Hardware Entry Capacity

Command	Function
Ruijie# <b>show initialization route</b>	Displays information of the hardware entry capacity.

“config” indicates current invalid settings; “running” indicates current valid running value; “default” indicates the system default value.

```
Ruijie #show initialization route
```

```

                config  running  default
policy-based route entry:   64      64      64
tunnel termination entry:   32      32      32
shared-pool entry:         200     200     200
```



# Ethernet Switching Configuration

---

1. Interface Configuration
2. MAC Address Configuration
3. Aggregate Port Configuration
4. LACP Configuration
5. VLAN Configuration
6. Protocol VLAN Configuration
7. Private VLAN Configuration
8. Share VLAN Configuration
9. Voice VLAN Configuration
10. MSTP Configuration
11. Transparent Transmission of Protocol Frames Configuration
12. GVRP Configuration
13. LLDP Configuration
14. QinQ Configuration
15. MAC VLAN Configuration
16. ERPS Configuration

# Interface Configuration

## Overview of Interface Types

This chapter classifies the interfaces used on Ruijie devices and defines interface types.

- L2 Interfaces

### L2 Interfaces

This section presents the types of L2 interfaces and their definitions. L2 interfaces fall into the following types

- Switch Port
- L2 Aggregate Ports

#### Switch Port

Switch port refers to a single physical port of only layer 2 switching function on the device. This port can either be an Access Port or a Trunk Port. You can configure a port to be an Access Port or a Trunk Port by using the **Switch Port** command in the interface configuration mode. Switch port is used to manage a physical interface and relevant layer 2 protocols rather than handling routing or bridging.

#### Access Port

An access port belongs to only one VLAN that transports only the frames belonging to the same VLAN. Typically, it is used to connect computers.

##### Default VLAN

An access port belongs to only one VLAN. Therefore, its default VLAN is the VLAN where it locates. You do not need to configure it.

##### Receiving and sending frames

An access port sends untagged frames and receives frames in the following three formats only:

Untagged frame

- Untagged frames
- Tagged frames whose VID is the VLAN where the access port locates
- Tagged frames whose VID is 0

##### Untagged frame

An access port receives untagged frames and then adds the tag of the default VLAN to them. The added tag will be removed before the access port sends them out.

##### Tagged frame

An access port handles tagged frames in the following ways:

- When the VID (VLAN ID) of the tag is the same as the default VLAN ID, the access port receives the frame and removes the tag before sending it out.
- When the VID (VLAN ID) of the tag is 0, the access port receives the frame. In the tag, VID=0 is used to prioritize the frame.

- When the VID (VLAN ID) of the tag is different from the default VLAN ID and is not 0, this frame is discarded.

## Trunk Port

A trunk port can belong to multiple VLANs that receives and sends frames belonging to multiple VLANs. Generally, it is used to connect devices or computers.

### Default VLAN

Because a trunk port can belong to multiple VLANs, you need to set a native VLAN as the default VLAN. By default, the trunk port transmits the frames of all VLANs. In order to reduce device load and minimize waste of bandwidth, you can set a VLAN allowance list to specify the frames of which VLANs the trunk port can transmit.



#### Caution

It is recommended to set the native VLAN of the trunk port on the local device to be consistent with that of the trunk port on the remote device. Otherwise, the trunk port cannot forward packets properly.

### Receiving and sending frames

The trunk port can receive untagged frames and the tagged frames of the VLANs permitted by the port. All the frames of non-native VLANs sent by the trunk port are tagged, and the frames of native VLAN are untagged.

### Untagged frame

If a trunk port receives a frame without IEEE802.1Q TAG, this frame will be transmitted in the native VLAN of the port.

### Tagged frame

If a trunk port receives a tagged frame, it handles the frame in the following ways:

- When the trunk port receives a tagged frame whose VID is the same as that of its native VLAN, this frame is accepted. The tag will be removed before it sends the frame.
- When the trunk port receives a tagged frame whose VID is different from that of its native VLAN but is permitted by the port, the frame is accepted. The tag is kept unchanged when it sends the frame.
- When the trunk port receives a tagged frame whose VID is different from that of its native VLAN and is not permitted by the port, the frame is discarded.



#### Note

Untagged packets are ordinary Ethernet packets that can be recognized by the network cards in PCs for communication. Tagging refers to append four bytes of VLAN information, namely the VLAN tag header, at the end of the source MAC address and the destination MAC address.

## Hybrid port

A hybrid port can belong to multiple VLANs that receives and sends packets of multiple VLANs. It can be used to connect devices or computers. The difference between the hybrid port and the trunk port is that the hybrid port sends the untagged frames of multiple VLANs, but the trunk port sends only the untagged frames of the default VLAN. Note that the VLAN that a hybrid port is going to join must already exist.

## L2 Aggregate Port

An aggregate port consists of several physical ports. Multiple physical connections can be bound into a simple logical connection, which is called an aggregate port (hereinafter referred to as AP).

For layer 2 switching, an AP works like a switch port of high bandwidth. It increases link bandwidth by using the bandwidth of multiple ports together. In addition, the frames that pass through the L2 aggregate port will undergo traffic balancing on the member ports of the L2 aggregate port. If one member link of AP fails, the L2 aggregate port automatically transfers the traffic on this link to other working member links, making the connection more reliable.



**Caution**

The member port of the L2 aggregate port can be either access port or trunk port. However, the member ports in one AP must be of the same type, namely, all the ports are either access ports or trunk ports.

## L3 Interfaces

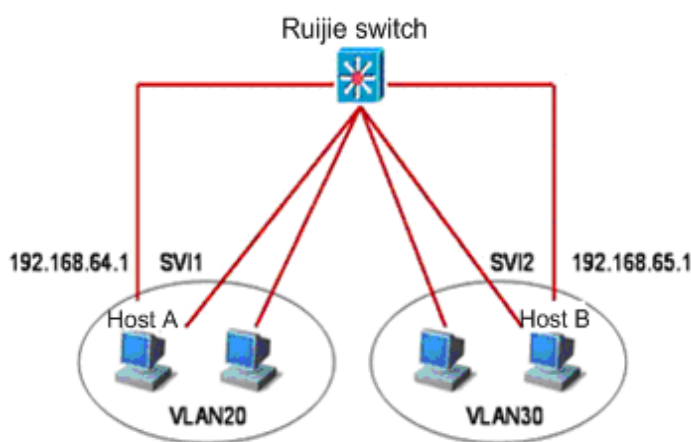
This section discusses the types and definitions of L3 interfaces. L3 interfaces fall into the following categories.

- SVI (Switch virtual interface)
- Routed Port

### SVI (Switch virtual interface)

SVI, short for Switch Virtual Interface, is used to implement the logical interface for layer 3 switching. SVI can work as the local management interface through which administrator can manage devices. You can also create SVI as a gateway interface that serves as the virtual sub-interface of each VLAN. It can be used for inter-VLAN routing on layer 3 device. A SVI can be created simply by using the **interface vlan** command in the interface configuration mode. Then an IP address is assigned to the SVI to establish a route between VLANs.

As the following figure depicts, the hosts of VLAN20 can communicate to each other directly without routing through an L3 device. If host A in VLAN20 wants to communicate with host B in VLAN30, it must route through SVI1 corresponding to VLAN20 and SVI2 corresponding to VLAN30.



### Routed Port

A routed port is a physical port, for example, a port on the layer 3 device. It can be configured by using a layer 3

routing protocol. On the layer 3 device, a single physical port can be set as a routed port that serves as the gateway interface for layer 3 switching. A routed port serves as an access port that is not related to a specific VLAN. A routed port provides no L2 switching function. You may change an L2 switch port into a routed port by using the **no switchport** command and then assign an IP address to it for routing purposes. Note that using the **no switchport** command in the interface configuration mode will close and restart this port and delete all the layer 2 features of this port.

**Caution**

However, when a port is a member port of an L2 aggregate port or an unauthenticated DOT1x authentication port, the **switchport /no switchport** command will not work.

## Configuring Interfaces

This section provides the default setting, guidelines, steps, and examples of configuration.

### Interface Numbering Rule

The number of a switch port consists of a slot number and the port number on the slot. For example, the port number is 3 and the slot number is 2, the number of the corresponding interface is 2/3. The slot number ranges from 0 to the total number of slots. The rule of numbering slots is that for panels facing the device, slots are numbered from front to back, from left to right, and from top down starting from 1 and increased in turn. Ports in a slot are numbered from left to right starting from 1 to the number of ports in the slot. For the devices which have a choice of optical or electrical interfaces, in either case, they use the same port number. You can view information on a slot and ports on it by using the **show** command in CLI.

Aggregate ports are numbered from 1 to the number of aggregate ports supported on the device.

A SVI is numbered by the VID of its corresponding VLAN.

**Caution**

The number of the static slot on a device is always 0. However, dynamic slots (pluggable modules or line cards) are numbered starting from 1.

### Using Interface Configuration Commands

Execute the **interface** command to enter interface configuration mode in the global configuration mode.

Command	Function
Ruijie(config)# <b>interface</b> <i>interface ID</i>	Input <b>interface</b> to enter the interface configuration mode in the global configuration mode. You can also configure an interface range by using the <b>interface range</b> or <b>interface range macro</b> command. However, the interfaces in the same range must be of the same type and features.

This example shows how to access Gigabitethernet2/1:

```
Ruijie(config)# interface gigabitethernet 2/1
Ruijie(config-if)#
```

You can configure the related attributes of the interface in the interface configuration mode.



## Using the interface range Command

### Setting an Interface Range

You can configure multiple interfaces at once by using the **interface range** command in the global configuration mode. As a result, the configured parameters apply to all the interfaces within the range.

Command	Function
<b>Ruijie(config)# interface range</b> <b>{port-range   macro</b> <b>macro_name}</b>	<p>Enter an interface range.</p> <p>You can use the <b>interface range</b> command to specify multiple ranges separated by a comma.</p> <p>The <b>macro</b> parameter can use the macro of a range. See the section of <i>Configuring and Using Macro Definition for Interface Range</i>.</p> <p>Be sure that the interfaces of all the ranges specified by a command must be of the same type.</p>

When using the **interface range** command, you should pay attention to the format of **range**.

A valid range format

**vlan** *vlan-ID - vlan-ID*, with VLAN ID in the range of 1–4094;

**Fastethernet** *slot/{the first port} - {the last port}*;

**Gigabitethernet** *slot/{the first port} - {the last port}*;

**TenGigabitethernet** *slot/{the first port} - {the last port}*;

**Aggregate Port Aggregate** *port number*, with *Aggregate port number* in the range of 1 to MAX.

The interfaces in an **interface range** must be of the same type, for example fastethernet, gigabitethernet, aggregate port or SVI.

This example shows how to use the **interface range** command in the global configuration mode:

```
Ruijie# configure terminal
Ruijie(config)# interface range fastethernet 1/1 - 10
Ruijie(config-if-range)# no shutdown
Ruijie(config-if-range)#
```

This example shows how to separate multiple ranges by a comma “,”:

```
Ruijie# configure terminal
Ruijie(config)# interface range fastethernet 1/1-5, 1/7-8
Ruijie(config-if-range)# no shutdown
Ruijie(config-if-range)#
```

### Configuring and Using Macro Definition for Interface Range

You can define a macro instead of inputting port ranges. However, you have to define macros using the **define interface-range** command in the global configuration mode before using the **macro** keyword of the **interface range** command.

Command	Function
---------	----------

Command	Function
Ruijie(config)# <b>define</b> <b>interface-range</b> <i>macro_name</i> <i>interface-range</i>	Define a macro for interface range. Name of the macro, up to 32 characters. A macro can define multiple interface ranges. The interfaces in all ranges in the same macro must be of the same type.
Ruijie(config)# <b>interface range</b> <b>macro</b> <i>macro_name</i>	The string defined by the macro will be saved in the memory. When you use the <b>interface range</b> command, you can use the macro name to replace the interface-range string.

To delete a macro, use the **no define interface-range macro\_name** command in the global configuration mode.

When defining an interface range using the **define interface-range** command, you should pay attention to the range format.

A valid range format is:

- **vlan** *vlan-ID* - *vlan-ID*, with VLAN ID in the range of 1 to 4094;
- **fastethernet** *slot/{the first port}* - { the last port};
- **gigabitethernet** *slot/{the first port}* - { the last port};
- **Aggregate Port Aggregate** *port number*, with *Aggregate port number* in the range of 1 to MAX.

Interfaces contained in an **interface range** must be of the same type, that is, they should be all switch ports, aggregate ports or SVIs.

This example defines a macro for fastethernet1/1-4 by using the **define interface-range** command:

```
Ruijie# configure terminal
Ruijie(config)# define interface-range resource
fastethernet 1/1-4
Ruijie(config)# end
```

This example defines a macro for multiple ranges:

```
Ruijie# configure terminal
Ruijie(config)# define interface-range ports1to2N5to7
fastethernet 1/1-2, 1/5-7
Ruijie(config)# end
```

This example uses the macro ports1to2N5to7 to set the specified range of interfaces:

```
Ruijie# configure terminal
Ruijie(config)# interface range macro ports1to2N5to7
Ruijie(config-if-range)#
```

This example deletes the macro ports1to2N5to7:

```
Ruijie# configure terminal
Ruijie(config)# no define interface-range ports1to2N5to7
Ruijie# end
```

## Selecting Interface Media Type

Some interfaces come with multiple media types for your choice. Once you have selected a media, interface attributes like connection status, speed, duplex, and flow control will be determined. When you change the media, interface attributes will use their default values. Change the default values when necessary.

The interfaces with multiple media types support the interface media auto-select. If the interface media auto-select has been configured, and only one media is connected to the interface, the device will use the media connected

currently; if the two media types are connected to the interface, the device will use the media configured first. The auto-select prefer media is electrical interface by default, use the command **medium-type auto-select prefer fiber** to set the prefer media as optical interface. In the auto-select mode, the interface attributes like speed, duplex, and flow control will use the default values.

This configuration takes effect for only physical ports. Aggregate port and SVI port do not support setting media types.

This configuration command takes effect for only the ports that supports media selection.

The ports configured to be the members of an aggregate port must have the same media type. Otherwise, they cannot be added to the AP. The port type of the members of the aggregate port cannot be changed. The ports configured to be the media auto-select cannot be added to the AP.

Command	Function
Ruijie(config-if)# <b>medium-type</b> { <b>fiber</b>   <b>copper</b> }	Set the media type of a port.

This example sets the media type of gigabitethernet 1/1:

```
Ruijie# config terminal
```

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

```
Ruijie(config)# interface gigabitethernet 1/1  
Ruijie(config-if)# medium-type fiber  
Ruijie(config-if)# end
```

**Caution**

Interface media switching function does not support the 100M fiber module.

## Setting Interface Description and Management Status

You may give an interface a particular name (description) to help you remember its functions. You may name the interface what you want to do with it, for example, if you want to reserve Gigabitethernet 1/1 for the exclusive use of user A, you may set its description to “Port for User A”.

Command	Function
Ruijie(config-if)# <b>description</b> <i>string</i>	Set the interface description in no more than 32 characters.

This example sets the description of Gigabitethernet 1/1:

```
Ruijie# config terminal  
Enter configuration commands, one per line. End with CNTL/Z.  
Ruijie(config)# interface gigabitethernet 1/1  
Ruijie(config-if)# description PortForUser A  
Ruijie(config-if)# end
```

In some circumstances, you may need to disable some interface. You can do this by setting the management status of the interface. Once disabled, no frames can be received and sent through the interface, and all its functions are disabled. You can also restart an disabled interface by setting its management status. The management status of an interface can be **up** or **down**. When a port is disabled, its management status is **down**; otherwise, it is in the status **up**.

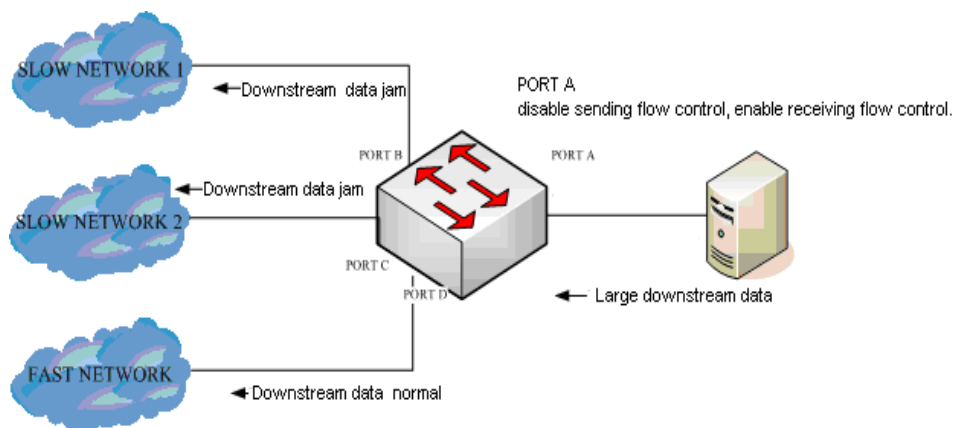
Command	Function
Ruijie(config-if)# <b>shutdown</b>	Disable an interface.

The following example illustrates how to disable Gigabitethernet 1/2.

```
Ruijie# configure terminal
Ruijie(config)# interface gigabitethernet 1/2
Ruijie(config-if)# shutdown
Ruijie(config-if)# end
```

## Setting Speed, Duplexing, and Flow Control for an Interface

The section deals with the setting of speed, duplexing, and flow control for interfaces. The flow control falls into the non-symmetric and symmetric flow control modes. Generally, after enabling the flow control on the interface, the flow control frames received on the interface will be handled, and be sent when the interface jam occurs. The symmetric flow control mode refers to the same handling for the receiving and sending the flow control frames. However, in some conditions, on one hand, the device expects handling the received flow control frame on the interface to avoid the packets being discarded due to the jam; on the other hand, the sending the flow control frame will make the speed of overall network decreased. In this case, the non-symmetric flow control shall be configured to separate the handling pacings of receiving and sending the flow control frames. As shown in Figure 2: the port A is the uplink port, and the ports B-D are the downlink ports, wherein the ports B, C correspond to the slow network. Suppose that the receiving and sending flow control functions are enabled on the port A, the over-large dataflow on the sending port B makes the ports B,C jammed due to the slow network connected, which leads to the ingress jam on the port A, and the flow control frame sent on the port A, if the uplink device responds to this frame, the dataflow sending to the port A will be decreased and network speed on the port D is slowed down indirectly. Then you can disable the sending flow control on the port A to ensure the bandwidth utilization rate in overall network.



The following command takes effect only for switch port and routed port.

Command	Function
---------	----------

Ruijie(config-if)# <b>speed</b> {10   100   1000   <b>auto</b> }	<p>Select a speed or set it to <b>auto</b>.</p> <p>Caution: 1000M applies only to gigabit interfaces</p>
Ruijie(config-if)# <b>duplex</b> {auto / full / half }	Set duplex mode.
Ruijie(config-if)# <b>flowcontrol</b> {auto   on   off }	<p>Set flow control mode.</p> <p>Note: When <b>speed</b>, <b>duplex</b>, and <b>flowcontrol</b> are all set to non-auto, the system will disable auto-negotiation on the interface.</p>
Ruijie(config-if)# <b>flowcontrol</b> {receive   send} {auto   on   off}	<p>Support the setting of non-symmetric flow control mode on the device.</p> <p>Note: if the settings of the receive and send modes are the same, the corresponding <b>flowcontrol</b> command is displayed consistent with it.</p>

In the interface configuration mode, you can restore the settings of speed, duplexing, and flow control to the default values (auto-negotiation) by using the **no speed**, **no duplex**, and **no flowcontrol** commands. The following example shows how to set the speed of Gigabitethernet 1/1 to 1000M, its duplex mode to **full**, and its flow control to **off**.

```
Ruijie# configure terminal
Ruijie(config)# interface gigabitethernet 1/1
Ruijie(config-if)# speed 1000
Ruijie(config-if)# duplex full
Ruijie(config-if)# flowcontrol off
Ruijie(config-if)# end
```

## Configuring Interface MTU

When a heavy throughput of data interchange occurs on a port, there may be a frame beyond the Ethernet standard frame length. This type of frame is called jumbo frame. A user can control the maximum frame length that the port is allowed to receive and send by setting the MTU.

MTU refers to the length of a valid data segment in a frame, excluding the overhead of Ethernet encapsulation. The MTU of a port is checked during input, not output. If the frame received by the port is longer than the set MTU, it will be discarded.

The MTU is in the range from 64 to 9216 bytes with the granularity of 4 bytes. Its default value is 1500 bytes. This configuration command takes effect only for physical ports. The SVI interface currently does not support the MTU setting.

Command	Function
---------	----------

Command	Function
Ruijie(config-if)# <b>Mtu num</b>	Set the MTU for a port. Num: <64 to 9216>

This example shows how to set the MTU for Gigabitethernet 1/1:

```
Ruijie# config terminal
Enter configuration commands, one per line. End with CNTL/Z.
Ruijie(config)# interface gigabitethernet 1/1
Ruijie(config-if)# mtu 64
Ruijie(config-if)# end
```

## Configuring L2 Interfaces

The following table shows the default settings of L2 interfaces. For the configurations of VLAN and ports, please refer to *Configuring VLAN* and *Configuring Port-based Flow Control*.

Attribute	Default Configuration
Working mode	L2 switch mode
Switch port mode	access port
Allowed VLAN range	1 to 4094
Default VLAN (for access port)	VLAN 1
Native VLAN (for trunk port)	VLAN 1
Media Type	copper
Interface management status	Up
Interface Description	Null
Speed	Auto-negotiation
Duplex mode	Auto-negotiation
Flow control	Auto-negotiation
Aggregate port	None
Storm suppression	Off
Port protection	Off
Port Security	Off

## Configuring Switch Ports

### Configuring Access/Trunk Port

This section is devoted to the setting of working modes (access/trunk port) of switch port and the setting in each mode.

To set the related attributes of a switch port, use the **switchport** command or other commands in the interface configuration mode:

Command	Function
Ruijie(config-if)# <b>switchport mode</b> <b>{access   trunk }</b>	Set the operation mode.

The following example shows how to set the operation mode of Gigabitethernet 1/2 to access port.

```
Ruijie# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Ruijie(config)# interface gigabitethernet 1/2
Ruijie(config-if)# switchport mode access
Ruijie(config-if)# end
```

Command	Function
Ruijie(config-if)# <b>switchport access vlan</b> <b>vlan-id</b>	Set the VLAN to which the access port belongs.

The following example shows how to configure the VLAN to which the access port gigabitethernet 2/1 to be 100

```
Ruijie# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Ruijie(config)# interface gigabitethernet 2/1
Ruijie(config-if)# switchport access vlan 100
Ruijie(config-if)# end
```

Set the native VLAN of the trunk port.

Command	Function
Ruijie(config-if)# <b>switchport trunk native</b> <b>vlan vlan-id</b>	Set the Native VLAN of the trunk port.

The following example shows how to set the native VLAN of the trunk port Gigabitethernet 2/1 to be 10.

```
Ruijie# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Ruijie(config)# interface gigabitethernet 2/1
Ruijie(config-if)# switchport trunk native vlan 10
Ruijie(config-if)# end
```

Set port security. For more information about port security, refer to *Port-based Flow Control*:

Command	Function
Ruijie(config-if)# <b>switchport</b> <b>port-security</b>	Set port security.

The following example shows how to enable port security on Gigabitethernet 2/1.

```
Ruijie# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Ruijie(config)# interface gigabitethernet 2/1
Ruijie(config-if)# switchport port-security
Ruijie(config-if)# end
```

For more information on configuring the speed, duplexing, and flow control of an interface, see the section of *Setting Speed, Duplexing, and Flow Control for an Interface*.

The following example shows how to set Gigabitethernet 2/1 to access port, its VLAN to 100, its speed, duplexing, and flow control to self-negotiation and enable port security.

```

Ruijie# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Ruijie (config)# interface gigabitethernet 2/1
Ruijie (config-if)# switchport access vlan 100
Ruijie (config-if)# speed auto
Ruijie (config-if)# duplex auto
Ruijie (config-if)# flowcontrol auto
Ruijie (config-if)# switchport port-security
Ruijie (config-if)# end

```

## Configuring Hybrid Port

You can configure the hybrid port by performing the following steps:

Command	Description
<b>configure terminal</b>	Enter configuration mode
<b>interface &lt;interface&gt;</b>	Enter the interface configuration mode. Megabit, Gigabit, 10 Gigabit
<b>switchport mode hybrid</b>	Configure the port as a hybrid port.
<b>no switchport mode</b>	Delete the port mode.
<b>switchport hybrid native vlan id</b>	Set the default VLAN for the hybrid port.
<b>switchport hybrid allowed vlan</b> [[add] [tagged   untagged]] [remove ] vlist	Set the output rule for the port.

```

Ruijie# configure terminal
Ruijie(config)# interface g 0/1
Ruijie(config-if)# switchport mode hybrid
Ruijie(config-if)# switchport hybrid native vlan 3
Ruijie(config-if)# switchport hybrid allowed vlan untagged 20-30
Ruijie(config-if)# end
Ruijie# show running interface g 0/1

```

## Configuring L2 Aggregate Ports

This section describes how to create an L2 aggregate port and some related settings.

You may create an L2 aggregate port by using the **aggregateport** command in the interface configuration mode. For details, see *Configuring Aggregate Port*.

## Clearing Statistics and Resetting an Interface

In the privileged EXEC mode, you may clear the statistics of an interface and then reset it by using the **clear** command. This command is only applicable for switch port, port members of an L2 aggregate port, and routed port. The **clear** command is shown as follows.

Command	Function
Ruijie# <b>clear counters</b> [interface-id]	Clear interface statistics.



Command	Function
Ruijie# <b>clear interface</b> <i>interface-id</i>	Reset the interface.

In the privileged EXEC mode, use the **show interfaces** command to display interface statistics, or use the **clear counters** command to clear the counters. If no interface is specified, the counters of all layer 2 interfaces will be cleared.

The following example shows how to clear the counter of gigabitethernet 1/1.

```
Ruijie# clear counters gigabitethernet 1/1
```

## Configuring L3 Interfaces

To configure a layer 3 interface, execute the following steps:

Command	Function
Ruijie(config-if)# <b>no switchport</b>	Shut down the interface and change it to L3 mode. This command applies to switch port and L2 aggregate port only.
Ruijie(config-if)# <b>ip address</b> <i>ip_address</i> <i>subnet_mask</i> {[ <b>secondary</b>   <b>tertiary</b>   <b>quartus</b> ][ <b>broadcast</b> ]}	Configure the IP address and subnet mask of the interface.

To delete the IP address of an L3 interface, use the **no ip address** command in the interface configuration mode.

The **no switchport** operation cannot be performed on one member of an L2 aggregate port.

The following example shows how to set an L2 interface to a routed port and assign an IP address to it.

```
Ruijie# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Ruijie(config)# interface gigabitethernet 2/1
Ruijie(config-if)# no switchport
Ruijie(config-if)# ip address 192.20.135.21 255.255.255.0
Ruijie(config-if)# no shutdown
Ruijie(config-if)# end
```

## Configuring SVI

This section describes how to create a SVI and some related configuration.

You may create a SVI or modify an existing one by using the **interface vlan** *vlan-id* command.

To configure a SVI, execute the following command:

Command	Function
Ruijie(config)# <b>interface vlan</b> <i>vlan-id</i>	Enter the SVI interface configuration mode.

Then, you can configure the attributes related to the SVI. For detailed information, refer to *Configuring Single IP Address Route*.

The following example shows how to enter the interface configuration mode and assign an IP address to SVI 100.

```
Ruijie# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Ruijie(config)# interface vlan 100
```

```
Ruijie(config-if) # ip address 192.168.1.1 255.255.255.0
Ruijie(config-if) # end
```

## Configuring Routed Ports

This section deals with how to create and configure a routed port.

You may create a routed port by using the **no switchport** command in the interface configuration command.

To create one routed port and assign an IP address to it, execute the following commands:

Command	Function
Ruijie(config-if)# <b>no switchport</b>	Shut down the interface and then change it to L3 mode.
Ruijie(config-if)# <b>ip address</b> <i>ip_address</i> <i>subnet_mask</i>	Configure the IP address and subnet mask.



### Caution

No layer switching can be performed by using **switchport/ no switchport** when an interface is a member of an L2 Aggregate Port.

The following example shows how to set an L2 interface to a routed port and then assign an IP address to it.

```
Ruijie# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Ruijie(config)# interface fastethernet 1/6
Ruijie(config-if) # no switchport
Ruijie(config-if) # ip address 192.168.1.1 255.255.255.0
Ruijie(config-if) # no shutdown
Ruijie(config-if) # end
```

## Showing Interface Configuration and Status

This section covers interface status display and gives examples. You may view interface status by using the **show** command in the privileged EXEC mode. To show interface status, use the following commands.

Command	Function
Ruijie# <b>show interfaces</b> [ <i>interface-id</i> ]	Show the status and configuration of the specified interface.
Ruijie# <b>show interfaces</b> <i>interface-id</i> <b>status</b>	Show the status of the specified interface.
Ruijie# <b>show interfaces</b> [ <i>interface-id</i> ] <b>switchport</b>	Show the administrative and operational status of a switch interface (non-routing interface).
Ruijie# <b>show interfaces</b> [ <i>interface-id</i> ] <b>description</b>	Show the description and status of the specified interface.

Command	Function
Ruijie# <b>show interfaces</b> [ <i>interface-id</i> ] <b>counters</b>	Show the statistics of the specified port. Where, the rate displayed may have an error of less than 0.5%.

The following example shows how to display the status of GigabitEthernet 0/1.

```
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 shows the status of aggregate port 3.

Ruijie# **show interfaces aggregateport 3:**

```
Interface           : AggregatePort 3
Description         :
AdminStatus         : up
OperStatus          : down
Hardware            : -
Mtu                 : 1500
LastChange          : 0d:0h:0m:0s
AdminDuplex         : Auto
OperDuplex          : Unknown
AdminSpeed          : Auto
```

```

OperSpeed                : Unknown
FlowControlAdminStatus   : Autonego
FlowControlOperStatus    : Disabled
Priority                  : 0

```

This example shows the configuration of GigabitEthernet 1/1:

```

Ruijie# show interfaces gigabitEthernet 1/1 switchport
Interface  Switchport Mode      Access  Native  Protected VLAN lists
-----
gigabitethernet 1/1      Enabled Access    1        1        Enabled All

```

This example shows the description of Gigabitethernet 2/1:

```

Ruijie# show interfaces gigabitethernet 1/2 description
Interface          Status      Administrative  Description
-----
gigabitethernet 2/1  down        down            Gi 2/1

```

This example shows statistics of the interfaces.

```

Ruijie# show interfaces gigabitethernet 1/2 counters
Interface : gigabitethernet 1/2
5 minute input rate      : 9144 bits/sec, 9 packets/sec
5 minute output rate     : 1280 bits/sec, 1 packets/sec
InOctets                 : 17310045
InUcastPkts              : 37488
InMulticastPkts          : 28139
InBroadcastPkts          : 32472
OutOctets                 : 1282535
OutUcastPkts              : 17284
OutMulticastPkts         : 249
OutBroadcastPkts         : 336
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

```

## Showing the Optical Module Information

Use the following commands to show the optical module information in the privileged EXEC mode:

Command	Function
Ruijie# <b>show interfaces</b> [ <i>interface-id</i> ] transceiver	Show the basic information for the optical module on the specified interface.

Ruijie# <b>show interfaces</b> [ <i>interface-id</i> ] <b>transceiver alarm</b>	Show the current alarm information for the optical module on the specified interface. If there is no alarm information, it shows "none".
Ruijie# <b>show interfaces</b> [ <i>interface-id</i> ] <b>transceiver diagnosis</b>	Show the optical module transceiver diagnosis parameter on the specified interface.

The following example shows the optical module information on the interface GigabitEthernet 5/4:

```
Ruijie#show interfaces gigabitEthernet 5/4 transceiver
Transceiver Type : 1000BASE_SX_SFP
Connector Type : LC
Wavelength(nm) : 1310
Transfer Distance:
    SMF fiber
        -- 10km
    EBW 50/125 um fiber
        -- 300m
    50/125 um fiber
        -- 100m
    62.5/125 um fiber
        -- 33m
Digital Diagnostic Monitoring : YES
```

The following example shows the alarm information for the optical module on the interface GigabitEthernet 5/4:

```
Ruijie#show interfaces gigabitEthernet 5/4 transceiver alarm
gigabitEthernet 5/4 transceiver current alarm information:
RX loss of signal
```

The following table shows the alarm information for the SFP optical module:

Field	Description
SFP	
RX loss of signal	Loss of the receiving signal.
RX power high	Alarm of the high receiving power of the optical module.
RX power low	Alarm of the low receiving power of the optical module.
TX fault	Sending fault.
TX bias high	Alarm of the bias high current.
TX bias low	Alarm of the bias low current.

TX power high	Alarm of the high sending power of the optical module.
TX power low	Alarm of the low sending power of the optical module.
Temp high	Alarm of the high temperature.
Temp low	Alarm of the low temperature.
Voltage high	Alarm of the high voltage.
Voltage low	Alarm of the low voltage.
Transceiver info checksum error	Transceiver information checksum error.
Transceiver info I/O error	Transceiver information read&write error
XFP	
RX loss of signal	Loss of the receiving signal.
RX not ready	The receiving state is not ready.
RX CDR loss of lock	RX CDR loss of lock.
RX power high	Alarm of the high receiving power of the optical module.
RX power low	Alarm of the low receiving power of the optical module.
TX fault	Sending fault.
TX CDR loss of lock	TX CDR loss of lock.
TX bias high	Alarm of the bias high current.
TX bias low	Alarm of the bias low current.
TX power high	Alarm of the high sending power of the optical module.
TX power low	Alarm of the low sending power of the optical module.
Module not ready	The module is not ready.
Temp high	Alarm of the high temperature.
Temp low	Alarm of the low temperature.
Voltage high	Alarm of the high voltage.
Voltage low	Alarm of the low voltage.
Transceiver info checksum error	Transceiver information checksum error.
Transceiver info I/O error	Transceiver information

	read&write error
--	------------------

The following example shows the optical module transceiver diagnosis parameter on the interface GigabitEthernet 5/4:

```
Ruijie#show interfaces gigabitEthernet 5/4 transceiver diagnosis
```

Current diagnostic parameters:

```
Temp(°C)   Voltage(V)       Bias(mA)  RX power(dBM)   TX power(dBM)
36(OK)     3.31(OK)      6.13(OK) -35.64(warning) -5.19(alarm)
```

The following table shows the optical module transceiver diagnosis parameter:

Field	Description
diagnostic information	The diagnostic information for the optical module on the interface.
Current diagnostic parameters	Current diagnostic parameters
Temp.(°C)	The diagnostic parameter—temperature, in °C.
Voltage(V)	The diagnostic parameter—voltage, in V.
Bias(mA)	The diagnostic parameter—bias current, in mA.
RX power(dBM)	The diagnostic parameter—RX power, in dBM.
TX power(dBM)	The diagnostic parameter—TX power, in dBM.
OK	The current state is normal.
warning	The current state is warning.
alarm	The current state is alarm.



#### Caution

The alarm and diagnostic parameter can be shown for the optical module supporting the Digital Diagnostic Monitoring function.

## Line Detection

The administrator can use command **line-detect** to detect the work status of lines. Line detection can help the administrator judge the work status of lines correctly when the lines are in abnormal status.

In the interface configuration mode, execute command **line-detect**:

Command	Function
<b>configure terminal</b>	Enter global configuration mode.
Ruijie(config)# <b>interface</b> <i>interface</i>	Enter the Interface configuration mode.
Ruijie(config-if)# <b>line-detect</b>	Detect lines.

**Caution**

1. Only electrical ports can support line detection. Optical and AP ports cannot support line detection.
2. Detecting lines on the normally connected interface may cause temporary disconnection. Then re-create the connection.

The following gives an example to execute the command to detect line:

```
Ruijie(config)#interface gigabitEthernet 0/1
Ruijie(config-if-gigabitEthernet 0/1)#line-detect
start cable-diagnoses,please wait...
cable-daignoses end!this is result:
4 pairs
pair state      length(meters)
-----
A   Ok          2
B   Ok          1
C   Short       1
D   Short       1
```

**Command description:**

Command	Description
pairs	The number of the line pairs. For example, the twisted pair is composed of four line pairs.
State	<p>1.OK; 2.Short; 3.Open; 4. Crosstalk</p> <p>In normal state, two pairs (A,B) of 100M twisted pair are OK, while other two pairs(C,D) are Short. Four pairs (A,B,C,D) of 1000M twisted pair are OK.</p> <p>Crosstalk indicates the line signal is unstable.</p>
Length	The line length, in meter, takes effect only for the pairs in non-Ok state. In addition, some inaccuracy is possible because the line length is calculated according to the signal transferring time. The length of lines in Short or Open states refers to the length from the port to the defective line point.



The administrator can also view the line state of the specified port or all ports by the **show interface** command.

## LinkTrap Policy Configuration

You can determine whether to send the LinkTrap of an interface according to the interface configuration on a device. With this function enabled, when the interface's link status changes, the SNMP protocol will send a LinkTrap message. Otherwise, it will not send a LinkTrap message. By default, this function is enabled.

### Configuration Command

Command	Function
Ruijie(config-if)# <b>[no] snmp trap link-status</b>	Enable or disable the function of sending the LinkTrap function of this interface.

### Configuration Example

The following configuration shows how to configure the interface not to send LinkTrap:

```
Ruijie(config)# interface gigabitEthernet 1/1  
Ruijie(config-if)# no snmp trap link-status
```

## MAC Address Configuration

Using the information in the MAC address table, the Ethernet switch rapidly searches for the address to which the messages in the data link layer are forwarded.

### Understanding the MAC Address Table

#### Overview

Layer-2 forwarding, a major function of the Ethernet Switch, is to forward the messages by identifying the data link layer information. The switch forwards the messages to the corresponding interface through the destination MAC addresses carried by the messages, and stores the information about the relationship between the destination MAC address and the interface in the MAC address table.

All the MAC addresses in the MAC address table are associated with the VLAN. Different MAC addresses are allowed to be in the same VLAN. Each VLAN maintains a MAC address table logically. It is possible that a MAC address learned by a VLAN is unknown to other VLANs and shall be learned again.

The MAC address contains the following information:

State	VLAN	MAC address	Interface
-------	------	-------------	-----------

**Figure-1 MAC Address Entry**

- State: Dynamic,static or filtering address.
- VLAN: VLAN to which the MAC address belongs;
- MAC address: the MAC address information in the entry;
- Interface: the information of the interface with which the MAC address is correspondent.

The MAC address entries are updated and maintained by the following two ways:

- Learning the Dynamic Address
- Configuring the Dynamic Address Manually

The switch searches for the corresponding outgoing forward interface according to the destination MAC address and the VLAN ID for the message in the MAC address table, and then forwards the messages in unicast, multicast and broadcast way.

- Unicast forwarding: if the switch searches for the corresponding entry of the packet destination MAC address and VLAN ID in the MAC address table and the outgoing forward interface is sole, the packets are forwarded through this interface.
- Multicast forwarding: if the switch searches for the corresponding entry of the packet destination MAC address and VLAN ID in the MAC address table and this entry is correspondent with a group of outgoing forward interfaces, the packets are forwarded through the interfaces directly.

- Broadcast forwarding: if the switch receives the packets destined to ffff.ffff.ffff, or it cannot search for the corresponding entry in the MAC address table, the packets are sent to the VLAN to which belongs and forwarded through the outgoing interfaces except for the incoming interface.

**Note**

This chapter describes management of dynamic, static and filtering addresses. For the management of multicast address, please refer to *IGMP Snooping Configurations*.

## Learning the Dynamic Address

### Dynamic Address

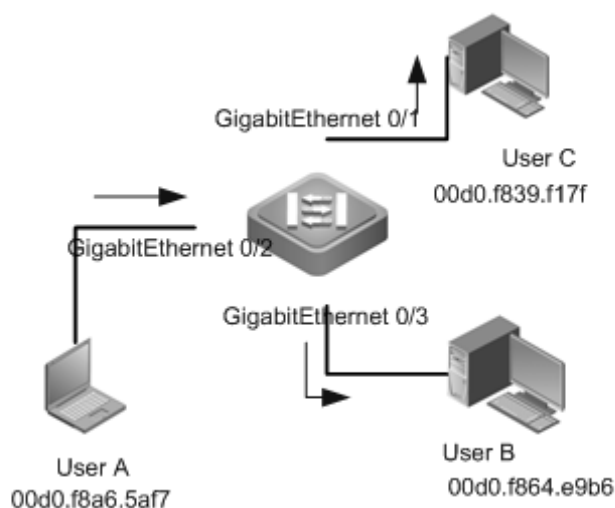
A dynamic address is the MAC address learnt automatically from the packets received by the switch. Only the dynamic address be removed by the aging mechanism of the address table.

### Address Learning Process

In general, it maintains the MAC address table by learning the dynamic address. The operation principle is:

The MAC address table in the switch is null and User A shall communicate with User B. User A sends the packet to interface GigabitEthernet 0/2 and the MAC address for User A is learnt in the MAC address table.

There is no source MAC address for User B in MAC address table. Therefore, the switch sends the packets to all ports except for the ports of User A in broadcast form. User C can receive the packets sent from User A and don't belong to User A.



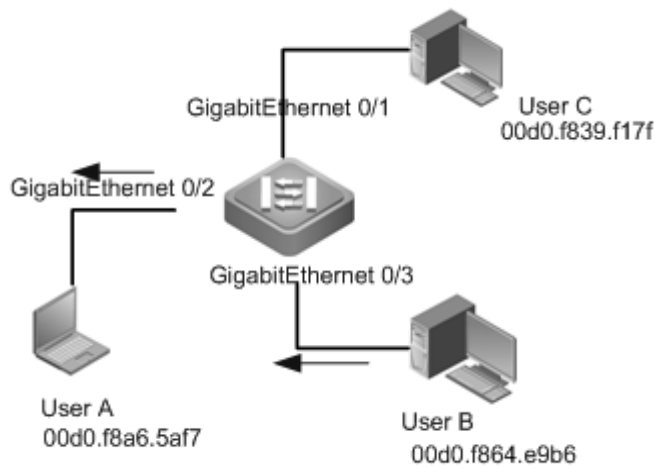
**Figure2 Dynamic Address Learn (Step 1)**

Status	VLAN	MAC address	Interface
Dynamic	1	00d0.f8a6.5af7	GigabitEthernet 0/2

**Figure3 MAC Address Table1**

Upon receiving the packets, UserB will send them to UserA through interface GigabitEthernet 0/3. The MAC address for UserA exists in the MAC address table. Therefore, the packets are forwarded to interface GigabitEthernet 0/2 in the unicast form and the switch learns the MAC address for UserB at the

same time. The difference from the step one is that UserC cannot receive the packets sent from UserB to UserA.



**Figure4 Dynamic Address Learn (Step 2)**

Status	VLAN	MAC address	Interface
Dynamic	1	00d0.f8a6.5af7	GigabitEthernet 0/2
Dynamic	1	00d0.f8a4.e9b6	GigabitEthernet 0/3

**Figure5 MAC Address Table 2**

After the communication between UserA and UserB, the switch learns the source MAC addresses for UserA and UserB. The mutual packets between UserA and UserB are forwarded in the unicast form and UserC cannot receive them again.



**Caution**

In the stack system, the address tables of each member device are asynchronous. For example:

Suppose the device A and device B stack and the device A is the host, send the broadcast packets to the device A, the port receiving the frames on the device A will learn the MAC1 address, which will be recorded in the address table. Since the packets are broadcasted to the device B through the stack port, the stack port on the device B will also learn this MAC1 address but not record it in the address table.

Removing the MAC address learned from the frame-receiving port on the device A, the MAC1 address in the address table will also be removed. However, the stack port of the device B still learn this MAC address, the inconsistency of the hardware address table of the master and slave devices occurs. Send the packets destined to MAC1 address to other ports of the device A, those packets cannot be broadcasted to the device B for the reason that the MAC1 address has already been learned by the stack port of the device B. After this MAC address ages out, the packets are

---

broadcasted to the port of the device B.

The internal mechanism is simply introduced as follows:

To improve the efficiency, the hardware address table runs through the hush bucket mechanism. The address table is divided into several buckets. When learning the MAC addresses, the bucket index value is calculated through the Hash algorithm with the combination of MAC+VID, and is added to this bucket. It will collide if the bucket index values calculated for different combinations of MAC+VID are the same. When all the addresses in the bucket are learned, the bucket overflows and the corresponding MAC address cannot be added to the bucket and will be dropped. To this end, in the actual application environment, the possibility of MAC address learning deny is much greater. While in this circumstance, it does not influence the normal working for the user.

---

## Address Aging

The capacity of MAC address is restricted. The switch updates the MAC address list by learning new addresses and aging out unused addresses.

For an address in the MAC address table, if the switch has not received any packet from the MAC address for a long time (depending on the aging time), the address will be aged out and removed from the MAC address table.

## Static Address

A static address is a manually configured MAC address. A static address is the same as a dynamic address in terms of function. However, you can only manually add and delete a static address rather than learn and age out a static address. A static address is stored in the configuration file and will not be lost even if the device restarts.

By configuring the static address manually, you can bind the MAC address for the network device with the interface in the MAC address table.

## Filtering Address

A filtering address is a manually configured MAC address. When the device receives the packets from a filtering address, it will directly discard them. You can only manually add and delete a filtering address rather than age it out. A filtering address is stored in the configuration file and will not be lost even if the device restarts.

If you want the device to filter some invalid users, you can specify their source MAC addresses as filtering addresses. Consequently, these invalid users cannot communicate with outside through the device.



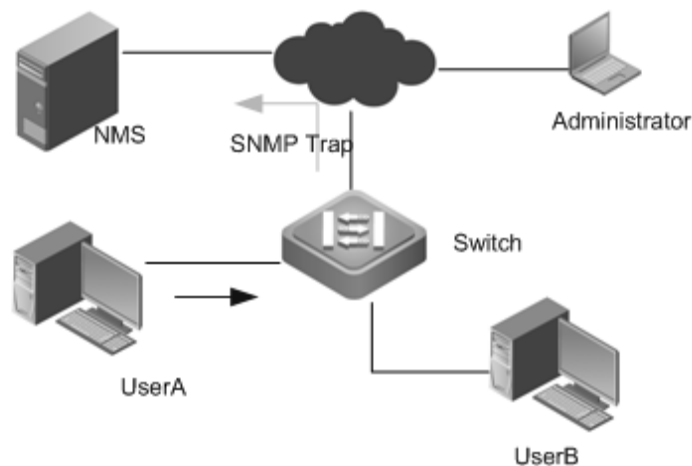
**Caution**

A filtering address is invalid for the packets sent to the CPU. For example, the L2 source MAC address for an ARP packet is a filtering address, this ARP packet can still be sent to the CPU, but cannot be forwarded.

---

## MAC Address Change Notification

The MAC address notification function is an effective way to let you know user changes for the devices in a network.



**Figure-13 MAC address Change Notification**

After the MAC address change notification is enabled, the MAC address change notification information is generated and sent in the SNMP Trap message form to the specified NMS when the switch learns a new MAC address or ages out a learned MAC address.

The notification about adding a MAC address lets you know a newcomer (identified by the MAC address) is using the device. The notification about deleting a MAC address (in the case of that the user did not communicate with the device within the aging time) lets you know that a user does not use the device any more.

When many users use the device, lots of MAC address changes may occur in a short period of time (for example, when the device is powered on), incurring additional network traffic. In order to release network burden, you can set the time interval of sending MAC address notifications. All the notification messages within the interval time will be bundled in one SNMP Trap message. So one notification message includes multiple MAC address changes, reducing network traffic significantly.

When a MAC address change notification is generated, it will be recorded in the MAC address notification history list. Then even though the NMS has not been specified to receive the SNMP Trap message, the administrator can view the information about address change by checking the MAC address notification history list.



**Caution**

MAC address change notification is effective only for dynamic addresses, not for static addresses and filtering addresses.

## IP address and MAC address Binding

### Overview

IP address and MAC address binding lets you filter packets. After you bind an IP address and a MAC address, the switch will only receive the IP packets whose source IP address and MAC address match the binding address ;or it will be discarded.

Taking advantages of IP address and MAC address binding, you can check the legality of the input sources. Note that this function takes precedence over 802.1X, port-based security and ACL effectiveness.

### Address Binding Mode

The address binding mode divides into 3 modes: compatible, loose and strict. By default, the address binding mode is strict. The following table lists the corresponding forwarding rules:

Mode	IPv4 packet forward rule	IPv6 packet forward rule
Strict	Packets with IPV4+MAC are forwarded.	No IPV6 packet is forwarded.
Loose	Packets with IPV4+MAC are forwarded.	All IPV6 packets are forwarded.
Compatible	Packets with IPV4+MAC are forwarded.	The IPV6 packets bound with the source MAC addresses are forwarded.

## Exceptional Ports for the Address Binding

By default, the IP address and MAC address binding function is effective on all ports. You can configure the exceptional ports to make this address binding function ineffective on some ports.



### Note

Because the binding relationship on the uplink port is uncertain, generally the uplink port is configured as the exceptional port. It is not necessary to check the IP address and MAC address binding on the uplink port.

## Related Protocols

*IEEE Std 802.3<sup>TM</sup> Carrier sense multiple access with collision detection (CSMA/CD) access method and physical layer specifications*

*IEEE Std 802.1Q<sup>TM</sup> Virtual Bridged Local Area Networks*

## Default MAC Address Table Configuration

Function	Default
Dynamic address aging time	300s
Dynamic address learning mode	dispersive
Dynamic address synchronization	disabled
Limit of VLAN dynamic address	disabled
MAC address change notification	disabled
Address-bind mode	compatible
Bridge Protocol Frame Forwarding Action	BPDU: not forward 802.1x: forward GVRP: not forward

## Setting Dynamic Addresses

### Clearing Dynamic Addresses

Command	Function
Ruijie# <b>clear mac-address-table dynamic</b>	Clear all dynamic addresses.
Ruijie# <b>clear mac-address-table dynamic address</b> <i>mac-address</i> <b>vlan</b> <i>vlan-id</i>	Clear the specified MAC address. <i>mac-address</i> : the specified MAC address to be cleared. <i>vlan-id</i> :the specified VLAN to which the MAC address to be cleared belongs.
Ruijie# <b>clear mac-address-table dynamic interface</b> <i>interface-id</i> <b>[vlan</b> <i>vlan-id</i> ]	Clear all dynamic addresses on the specified port or Aggregate Port, or clear all dynamic addresses on all interfaces. <i>Interface-id</i> : the specified port or Aggregate Port; <i>vlan-id</i> :the specified VLAN to which the dynamic address to be cleared belongs.
Ruijie# <b>clear mac-address-table dynamic vlan</b> <i>vlan-id</i>	Clear all dynamic addresses in the specified VLAN. <i>vlan-id</i> :the specified VLAN to which the dynamic address to be cleared belongs.

The following example shows how to clear all dynamic addresses in VLAN 1 on interface GigabitEthernet 0/1:

```
Ruijie#clear mac-address-table dynamic interface GigabitEthernet 0/1 vlan 1
```

### Viewing Configurations

Command	Function
Ruijie# <b>show mac-address-table dynamic</b>	Show all dynamic addresses.
Ruijie# <b>show mac-address-table dynamic address</b> <i>mac-address</i> <b>[vlan</b> <i>vlan-id</i> ]	Show the specified dynamic MAC address. <i>mac-address</i> : the specified MAC address. <i>vlan-id</i> :the specified VLAN to which the MAC address belongs.
Ruijie# <b>show mac-address-table dynamic interface</b> <i>interface-id</i> <b>[vlan</b> <i>vlan-id</i> ]	Show all dynamic addresses on the specified port or Aggregate Port. <i>Interface-id</i> : the specified port or Aggregate Port; <i>vlan-id</i> :the specified VLAN to which the dynamic address belongs.



Ruijie# <b>show mac-address-table dynamic vlan <i>vlan-id</i></b>	Show all dynamic addresses in the specified VLAN.  <i>vlan-id</i> :the specified VLAN to which the dynamic address belongs.
Ruijie# <b>show mac-address-table count</b>	Show the statistics in the mac address table.

The following example shows all dynamic MAC addresses in VLAN 1 on interface GigabitEthernet 0/1:

```
Ruijie#show mac-address-table dynamic interface gigabitEthernet 0/1 vlan 1
Vlan          MAC Address          Type      Interface
-----
1             0000.5e00.010c        DYNAMIC   GigabitEthernet 0/1
1             00d0.f822.33aa        DYNAMIC   GigabitEthernet 0/1
1             00d0.f822.a219        DYNAMIC   GigabitEthernet 0/1
1             00d0.f8a6.5af7        DYNAMIC   GigabitEthernet 0/1
```

The following example shows the statistics in the MAC address table:

```
Ruijie# show mac-address-table count
Dynamic Address Count : 30
Static Address Count : 0
Filtering Address Count: 0
Total Mac Addresses : 30
Total Mac Address Space Available: 8159
```

## Setting the Address Aging Time

### Setting the Aging Time

The following table shows how to set the aging time of address:

Command	Function
Ruijie(config)# <b>mac-address-table aging-time [0   10-1000000]</b>	Set the time for an address to be stored in the dynamic MAC address table after it has been learned. It is in the range of 10 to 1000000 seconds, 300 seconds by default. When you set the aging time as 0, the address aging function is disabled and the learned addresses will not be aged.
Ruijie(config)# <b>no mac-address-table aging-time</b>	Restore the aging time to the default value.

The following example shows how to set the address aging time to 180s:

```
Ruijie#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Ruijie(config)#mac-address-table aging-time 180
```

## Viewing Configurations

Command	Function
Ruijie)# <b>show mac-address-table aging-time</b>	Show the aging time of all addresses.

The following example shows how to view the address aging time configurations:

```
Ruijie)#show mac-address-table aging-time
Aging time      : 180 seconds
```



### Caution

The actual aging time may be different from the setting value for the MAC address table. However, it will not be 2 times than the setting value.

## Setting the Management Learning Mode of Dynamic Addresses

### Setting the Dynamic Address Learning Mode

Command	Function
Ruijie(config)# <b>mac-manage-learning dispersive</b>	Set the management learning mode of the dynamic address as the dispersive mode.
Ruijie(config)# <b>mac-manage-learning uniform</b>	Set the management learning mode of the dynamic address as the uniform mode.

The following example shows how to set the dispersive address learning mode:

```
Ruijie)#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Ruijie(config)#mac-manage-learning dispersive
```

### Setting the Uniform Address Learning-Sync

Command	Function
Ruijie(config)# <b>mac-manage-learning uniform learning-synchronization</b>	In the uniform address learning mode, enable dynamic address synchronization.
Ruijie(config)# <b>no mac-manage-learning uniform learning-synchronization</b>	In the uniform address learning mode, disable dynamic address synchronization.
Ruijie(config)# <b>mac-manage-learning uniform</b>	Set the management learning mode of the dynamic address as the uniform mode.

The following example shows how to enable dynamic address synchronization:

```
Ruijie#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Ruijie(config)#mac-manage-learning uniform learning-synchronization
```

## Viewing Configurations

```
Ruijie #show mac-address-table mac-manage-learning
MAC manage-learning
running mode: dispersive.
configuration mode: dispersive.
dynamic address learning-synchronization: off.
```

## Setting the Limit of Dynamic Addresses for a VLAN

### Setting the Limit of Dynamic Addresses for a VLAN

You can set the limit of dynamic MAC addresses that a VLAN can learn.

The table below sets the limit of the dynamic addresses for a VLAN.

Command	Function
Ruijie# <b>configure terminal</b>	Enter the global configuration mode.
Ruijie(config)# <b>vlan [1-4094]</b>	Enter the VLAN configuration mode.
Ruijie(config-vlan)# <b>max-dynamic-mac-count [1-32768]</b>	Set the maximum number of dynamic MAC addresses that the VLAN can learn.

To disable the limit of the dynamic addresses for a VLAN, use the **no max-dynamic-mac-count** command.

The following example shows how to set the maximum dynamic address number to 160:

```
Ruijie#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Ruijie(config)#vlan 1
Ruijie(config-vlan)#max-dynamic-mac-count 160
```



This function will take no effect if non-aforementioned line cards are installed in the switch.

## Viewing Configurations

Show the maximum number of dynamic addresses for a specified VLAN:

```
Ruijie#show mac-address-table max-dynamic-mac-count vlan 1
vlan limit  mac count learning
-----
1    160      6      YES
```

Show the maximum number of dynamic addresses for all VLANs:

```
Ruijie#show mac-address-table max-dynamic-mac-count
vlan limit  mac count learning
-----
1    160      6          YES
3    500     124        YES
```

## Setting the Static MAC Addresses

### Adding and Removing the Static MAC Addresses

You can add a static address to the MAC address table by specifying the destination MAC address, the VLAN (the static address will be added to the address table of this VLAN), and the interface (the packets to the destination MAC address are forwarded to this interface).

To add a static address, execute the following commands:

Command	Function
Ruijie(config)# <b>mac-address-table static</b> <i>mac-address</i> <b>vlan</b> <i>vlan-id</i> <b>interface</b> <i>interface-id</i>	<p><i>mac-addr</i>: Specify the destination MAC address to which the entry corresponds.</p> <p><i>vlan-id</i>: Specify the VLAN to which this address belongs.</p> <p><i>interface-id</i>: specify the interface (physical port or aggregate port) to which the packet is forwarded.</p> <p>Upon receiving the packets to the destination MAC address in the VLAN, the switch will forward them to the interface.</p>
Ruijie(config)# <b>no mac-address-table static</b> <i>mac-address</i> <b>vlan</b> <i>vlan-id</i> <b>interface</b> <i>interface-id</i>	Remove the static MAC address entries.

The following example shows how to configure the static address 00d0.f800.073c. When a packet to this address is received in VLAN 4, it is forwarded to GigabitEthernet 0/3.

```
Ruijie#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Ruijie(config)# mac-address-table static 00d0.f800.073c vlan 4 interface gigabitethernet
0/3
```

The following example shows how to remove the static address 00d0.f800.073c.

```
Ruijie#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Ruijie(config)#no mac-address-table static 00d0.f800.073c vlan 4 interface gigabitethernet
0/3
```

### Viewing Configurations

Command	Function
---------	----------

Command	Function
Ruijie# <b>show mac-address-table static</b>	Show the information of all the static MAC addresses.

The following example shows how to view the information of all the static MAC addresses:

Vlan	MAC Address	Type	Interface
-----	-----	-----	-----
4	00d0.f800.073c	STATIC	GigabitEthernet 0/3

## Setting the Filtering MAC Addresses

### Adding and Removing the Filtering Addresses

To add a filtering address, specify the MAC address to be filtered and the VLAN that the MAC address belongs to. The device will directly discard the packets from the MAC address in the VLAN.

To add a filtering address, execute the following command:

Command	Function
Ruijie(config)# <b>mac-address-table filtering</b> <i>mac-addr vlan vlan-id</i>	mac-addr: Specify the MAC address to be filtered by the device. vlan-id: Specify the VLAN to which this address belongs.
Ruijie(config)# <b>no mac-address-table filtering</b> <i>mac-addr vlan vlan-id</i>	Remove the filtering MAC address entries.

The following example shows how to configure the filtering address 00d0.f800.073c. When a packet to or from this address is received in VLAN 4, it will be discarded.

```
Ruijie#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Ruijie(config)# mac-address-table filtering 00d0.f800.073c vlan 4
```

The following example shows how to remove the filtering address 00d0.f800.073c.

```
Ruijie#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Ruijie(config)#no mac-address-table filtering 00d0.f800.073c vlan 4
```

### Viewing Configurations

Command	Function
Ruijie# <b>show mac-address-table filtering</b>	Show the information of all the filtering MAC addresses.

The following example shows how to view the information of all the filtering MAC addresses:

Vlan	MAC Address	Type	Interface
-----	-----	-----	-----
4	00d0.f800.073c	FILTER	GigabitEthernet 0/3

## Setting MAC Address Change Notification

### Setting MAC Address Change Notification

By default, the global switch of MAC addresses is turned off, so the MAC address change notification function is disabled on all interfaces.

To configure the MAC address change notification function, execute the following command:

Command	Function
Ruijie(config)# <b>snmp-server host</b> <i>host-addr</i> <b>traps</b> [ <b>version</b> {1   2c   3} [ <b>auth</b>   <b>noauth</b>   <b>priv</b> ]] <i>community-string</i>	Configure the NMS to receive the MAC address change notification. <i>host-addr</i> : IP address of the receiver. <i>version</i> : Specify the version of the SNMP Trap message to be sent. <i>community-string</i> : Specify the authentication name carried with the SNMP Trap message.
Ruijie (config)# <b>snmp-server enable traps</b>	Allow the switch to send the SNMP Trap message.
Ruijie(config)# <b>mac-address-table notification</b>	Turn on the global switch of the MAC address change notification function.
Ruijie(config)# <b>mac-address-table notification</b> { <b>interval</b> <i>value</i>   <b>history-size</b> <i>value</i> }	<i>interval value</i> :Interval of generating the MAC address change notification (optional), in the range of 1 to 3600 seconds, 1 second by default. <i>history-size value</i> : Maximum number of the records in the MAC notification history list, in the range of 1 to 200, 50 by default.
Ruijie(config-if)# <b>snmp trap mac-notification</b> { <b>added</b>   <b>removed</b> }	Enable the MAC address change notification on the interface. <b>added</b> : Send a MAC address change notification when a MAC address is <b>added</b> on this interface. <b>Removed</b> : Send a MAC address change notification when an address is deleted.

To disable the MAC address change notification function, use the **no snmp-server enable traps** command in the global configuration mode. To turn off the global switch of the MAC address change notification function, use the **no mac-address-table notification** command. To disable the MAC address change notification function on a specified interface, use the **no snmp trap mac-notification {added | removed}** command in the interface configuration mode.

This example shows how to enable the MAC address change notification function, use public as the authentication

name to send a MAC address change notification to the NMS whose IP address is 192.168.12.54 at the interval of 40 seconds, set the size of the MAC address change history list to 100, and enable the MAC address change notification function on gigabitethernet 0/1 when a MAC address is added or removed.

```
Ruijie(config)# snmp-server host 192.168.12.54 traps public
Ruijie(config)# snmp-server enable traps
Ruijie(config)# mac-address-table notification
Ruijie(config)# mac-address-table notification interval 40
Ruijie(config)# mac-address-table notification history-size 100
Ruijie(config)# interface gigabitethernet 0/1
Ruijie(config-if)# snmp trap mac-notification added
Ruijie(config-if)# snmp trap mac-notification removed
```

## Viewing the MAC Address change Notification Information

In the privileged EXEC mode, you can view the information on the MAC address table of the device by using the commands listed in the following table:

Command	Function
<b>Ruijie# show mac-address-table notification</b>	Show the global configuration of the MAC address change notification function.
<b>Ruijie# show mac-address-table notification interface</b>	Show the configuration of the MAC address change notification on the interface.
<b>Ruijie# show mac-address-table notification history</b>	Show the history list of the MAC address change notification.

The following examples show how to view the MAC address change notification.

View the global configuration of the MAC address change notification:

```
Ruijie# show mac-address-table notification
MAC Notification Feature : Enabled
Interval(Sec): 2
Maximum History Size : 154
Current History Size : 2
Ruijie# show mac-address-table notification interface
Interface          MAC Added Trap MAC Removed Trap
-----
Gi0/1              Disabled      Enabled
Gi0/2              Disabled      Disabled
Gi0/3              Enabled       Enabled
Gi0/4              Disabled      Disabled
Gi0/5              Disabled      Disabled
Gi0/6              Disabled      Disabled
Ruijie# show mac-address-table notification history
History Index:1
Entry Timestamp: 15091
MAC Changed Message :
Operation  VLAN MAC Address  Interface
-----
Added      1    00d0.f808.3cc9  Gi0/1
Removed    1    00d0.f808.0c0c  Gi0/1
History Index:2
```

```
Entry Timestamp: 21891
MAC Changed Message :
Operation   VLAN   MAC Address   Interface
-----
Added      1      00d0.f80d.1083 Gi0/1
```

## Setting IP Address and MAC Address Binding

### Setting IP Address and MAC address Binding

In the global mode, to configure IP address and MAC address binding, execute the following commands.

Command	Function
Ruijie(config)# <b>address-bind</b> <i>ip-address mac-address</i>	Configure IP address and MAC address binding.
Ruijie(config)# <b>address-bind install</b>	Enable the address binding function.

To cancel the IP address and MAC address binding, use the **no address-bind** *ip-address mac-address* command in the global configuration mode.

To disable the address binding function, execute the **no address-bind install** command.

The following example shows how to bind the IP address and MAC address:

```
Ruijie#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Ruijie(config)#address-bind 192.168.5.1 00d0.f800.0001
Ruijie(config)#address-bind install
```



#### Caution

**Problem:** In the stack environment, if one switch learns the MAC address when receiving the IP packets not correspond to the address binding, this MAC address can only be learned by the chip of that switch and cannot be learned by the chips of other switches in the stack environment.

**Phenomenon:** In the stack environment, if one switch learns the MAC address when receiving the IP packets not correspond to the address binding, this address entry is displayed using the **show mac** command and the IP packets can still be broadcasted to other stack switches. The MAC address learning is normal when receiving the non-IP packets or the IP packets correspond to the address binding.

**Workaround:** N/A.

After executing the **address-bind install** command but the IP+MAC binding is not configured, then allow all packets to be transmitted on the interface.

### Setting the Address Binding Mode

In the global mode, to configure the address binding mode, execute the following commands.



Command	Function
Ruijie(config)# <b>address-bind ipv6-mode { compatible  loose   strict }</b>	Configure the address binding mode.
Ruijie(config)# <b>no address-bind ipv6-mode</b>	Restore to the default address binding mode.

The following example shows how to set the address binding mode to strict:

```
Ruijie#configure terminal
```

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

```
Ruijie(config)#address-bind ipv6-mode strict
```

In the IPV6 mode, DHCP Snooping address binding, port security MAC+IP address binding functions are enabled at the same time.



**Caution**

Mode	IPv4 packet forward rule	IPv6 packet forward rule
Strict	Only packets with IPV4+MAC are forwarded.	Only IPV6 packets with IPv6 security address configured are allowed to be forwarded.
Loose	Only packets with IPV4+MAC are forwarded.	All IPV6 packets are allowed to be forwarded.
Compatible	Only packets with IPV4+MAC are forwarded.	Only IPV6 packets bound with the source MAC address or the security address configured are allowed to be forwarded.  security and DOT1X authentication are co-used, all IPV6 packets bound with the MAC address can be transmitted on the interface.

## Setting the Exceptional Ports for the IP Address and MAC Address Binding

To make the IP address and MAC address binding not to take effect on some ports, you can set these ports as exceptional ports. To configure an exceptional port, execute the following command in the global configuration mode.

Command	Function
<b>Ruijie(config)#address-bind uplink interface-id</b>	Configure the exceptional port for the IP address and MAC address binding. <i>Interface-id</i> : port or Aggregate port

Use the **no address-bind uplink interface-id** command to cancel the configuration of the specified exceptional port.

The following example shows how to set the interface GigabitEthernet 0/1 to the exceptional port:

```
Ruijie#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Ruijie(config)# address-bind uplink GigabitEthernet 0/1
```

## Viewing the IP Address and MAC Address Binding Table

To show the IP address and MAC address binding table, use the **show address-bind** command in the privileged EXEC mode:

Command	Function
<b>Ruijie(config)#show address-bind</b>	View the IP address and MAC address binding table.

The following example shows how to view the IP address and MAC address binding table :

```
Ruijie#show address-bind
Total Bind Addresses in System : 1

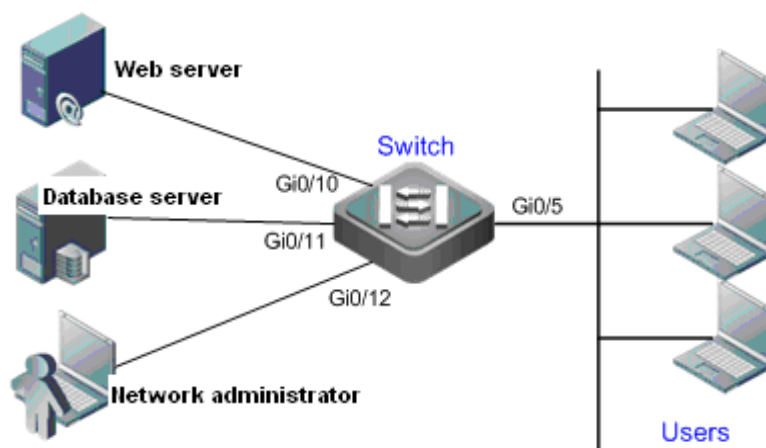
IP Address          Binding MAC Addr
-----
192.168.5.1        00d0.f800.0001
```

## Typical Configuration Examples of MAC Address Table Management

### Configuring Static MAC Addresses

#### Topological Diagram

As Figure-14 shows, the database server connects to the Ethernet switch through the interface GigabitEthernet 0/11, the web server connects to the Ethernet switch through the interface GigabitEthernet 0/10, and the server administrator connects to the switch through the interface GigabitEthernet 0/12. Other users access the web server through the interface GigabitEthernet 0/5. All data are forwarded in VLAN 10.



**Figure 14 Typical Configuration Topology**

## Application Requirements

The static MAC address configuration enables the data exchanged between the web server and the database server, the administrator and the server to be forwarded in the unicast form, preventing these data from being forwarded in the broadcast form in the user network and ensuring the security of the information exchanged between the web server and the database server, the administrator and the server .

## Configuration Tips

The following three keypoints shall be ensured when configuring the static MAC address entries:

1. Specify the destination MAC address in the entry.
2. Specify the Vlan to which this address belongs.
3. Interface ID.

Upon receiving the packets to the destination MAC address in the VLAN, the switch will forward them to the specified interface.

The following table shows the corresponding relationship among the MAC address, VLAN ID and interface ID in this configuration example.

Role	MAC Address	VLAN ID	Interface ID
Web server	00d0.3232.0001	VLAN2	Gi 0/10
Database server	00d0.3232.0002	VLAN2	Gi 0/11
Network administrator	00d0.3232.1000	VLAN2	Gi 0/12

## Configuration Steps

! Enter global configuration mode.

```
Ruijie>en
```

```
Ruijie#configure terminal
```

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

! Add the static MAC addresses (Specify the VLAN and interface to which this address belongs).

```
Ruijie(config)#mac-address-table static 00d0.f8003232.0001 vlan 110 interface
GigabitEthernetGigabitEthernet 0/10
```

```
Ruijie(config)#mac-address-table static 00d0.f8003232.0002 vlan 110 interface
GigabitEthernet0/211
Ruijie(config)#mac-address-table static 00d0.f800.00033232.1000 vlan 110 interface
GigabitEthernet0/312
```

! Display the device configurations.

## Verifications

Display the configured static MAC addresses.

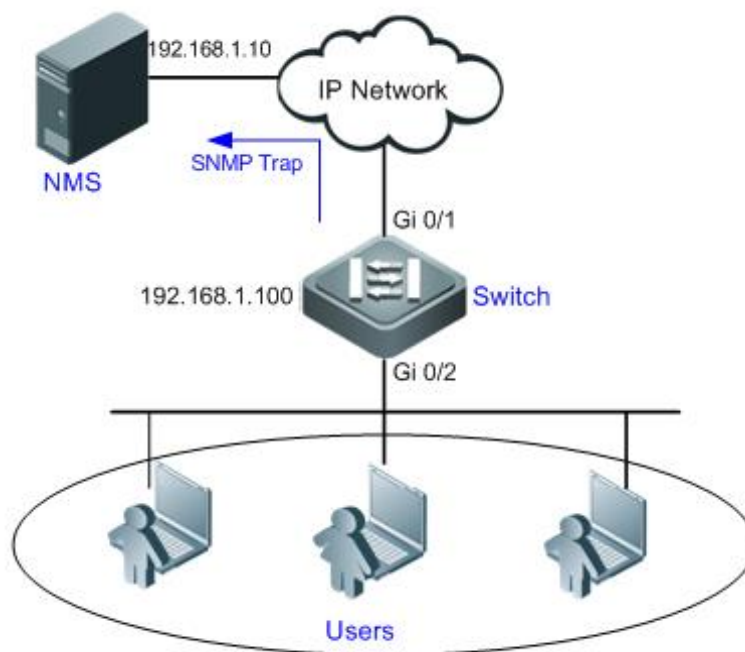
```
Ruijie#show mac-address-table static
```

Vlan	MAC Address	Type	Interface
110	00d0.f8003232.0001	STATIC	GigabitEthernet 0/10
110	00d0.f8003232.0002	STATIC	GigabitEthernet 0/211
110	00d0.f800.00033232.1000	STATIC	GigabitEthernet 0/312

## Configuring Dynamic MAC Addresses Change Notification

### Topological Diagram

As Figure-15 shows, the users connect to the switch through the interface GigabitEthernet 0/2.



**Figure 15 Typical Configuration Topology**

### Application Requirements

In order to facilitate network access management for an administrator, the following requirements are expected through the configuration:

1. Upon receiving a new MAC address or aging a learnt MAC address on the interface connected to the user, the switch will record the address change information in the MAC address notification history list, so that the

administrator could view the information about address change by checking the MAC address notification history list.

2. Meanwhile, the MAC address change notification will be sent in SNMP Trap message form to the specified NMS.

3. When many users use the device, avoid generating lots of MAC address changes in a short period of time to reduce network burden.

## Configuration Tips

1. Enable the MAC address change notification function globally, and configure the MAC address change notification on the interface Gi 0/2.

2. Configure the NMS host address, and enable the switch to actively send the SNMP Trap notification. The route from the switch to the NMS (Network Management Station) should be reachable.

3. Set the interval of sending the MAC address change notification to 300 seconds (the default interval is 1 second). All the notification messages within the interval time will be bundled in one SNMP Trap message. So one notification message includes multiple MAC address changes, reducing network traffic significantly.

## Configuration Steps

The IP address of the device is shown in above figure.

Step1: Enable the global MAC address change notification function on the switch.

```
Ruijie>enable
Ruijie#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Ruijie(config)#mac-address-table notification
```

Step2: Set the interval of sending MAC address change notification to 30 seconds.

```
Ruijie(config)#mac-address-table notification! Display the device configurations.
```

Step3: Enable the MAC address change notification function on the interface Gi 0/2.

```
Ruijie(config)#mac-address-table notification interval 30
```

! Enter Gi 0/2 interface configuration mode.

```
Ruijie(config)#interface gigabitEthernet 0/2
```

! Enable the device to send notification when an address is added on this interface.

```
Ruijie(config-if-GigabitEthernet 0/2)# snmp trap mac-notification added
```

! Enable the device to send notification when an address is deleted on this interface.

```
Ruijie(config-if-GigabitEthernet 0/2)# snmp trap mac-notification removed
Ruijie(config-if-GigabitEthernet 0/2)#exit
```

Step4: Configure the NMS which receives the MAC address change notification, with IP address being 192.168.1.10, message format being Version 2c and authentication name being comefrom2.

```
Ruijie(config)#snmp-server host 192.168.1.10 traps version 2c comefrom2
```

Step5: Enable the device to actively send the Trap message.

```
Ruijie(config)# snmp-server enable traps
```

## Verifications

Step1: Display the global configuration of MAC address change notification.

```
Ruijie#show mac-address-table notification
```

```

MAC Notification Feature : Enabled
Interval (Sec): 300
Maximum History Size : 50
Current History Size : 0

```

Step2: Display the status of MAC address change notification function on the interface.

```

Ruijie#show mac-address-table notification interface gigabitEthernet 0/2

```

Interface	MAC Added Trap	MAC Removed Trap
GigabitEthernet 0/2	Enabled	Enabled

Step3: Display the MAC address table of the interface.

```

Ruijie#show mac-address-table interface gigabitEthernet 0/2

```

Vlan	MAC Address	Type	Interface
1	00d0.3232.0001	DYNAMIC	GigabitEthernet 0/2
1	00d0.3232.0002	DYNAMIC	GigabitEthernet 0/2
1	00d0.3232.0003	DYNAMIC	GigabitEthernet 0/2

Step4: Verify the configuration.

Use the **clear mac-address-table dynamic address 00d0.3232.0003** command to simulate the address aging.

! Display the global configuration of MAC address change notification function.

```

Ruijie#show mac-address-table notification
MAC Notification Feature : Enabled
Interval (Sec): 30
Maximum History Size: 50
Current History Size: 1

```

! Display the MAC address change notification history list.

```

Ruijie#show mac-address-table notification history
History Index : 0
Entry Timestamp: 221683
MAC Changed Message :
Operation:DEL Vlan:1 MAC Addr: 00d0.3232.0003 GigabitEthernet 0/2

```

## Configuring Global IP Address and MAC Binding

### Topological Diagram

As Figure-16 shows, in order to facilitate management, each host is assigned a fixed IP address

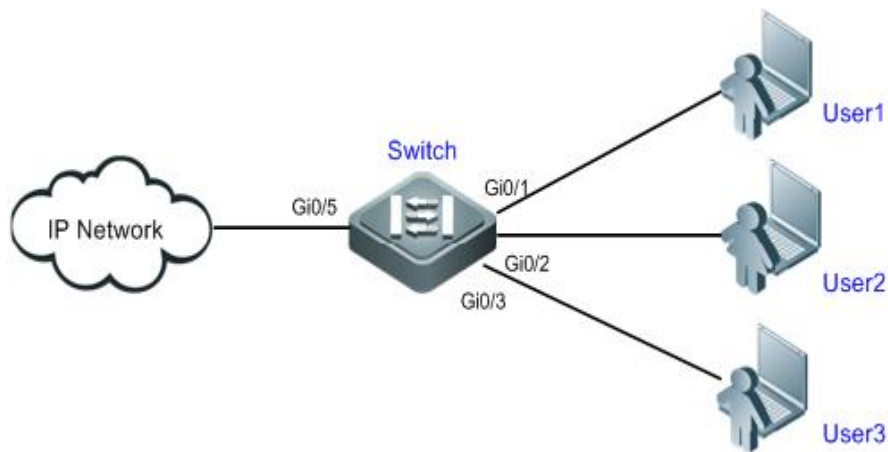


Figure 16 Typical Configuration Topology

Application Requirements

- 1. Prevent the employee from embezzling IP addresses. For example, some employ may embezzle the IP address of higher perssion to obtain the additional information over his permission.
- 2. Mobile officing can be achieved in the department.

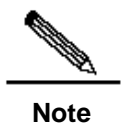
Configuration Tips

Manually configuring the global IP address and MAC address binding can meet the aforementioned requirements. The configuration keypoints are shown below:

- 1. Manually configure the global IP address and MAC address binding. (This example lists 3 users.)

User	MAC Address	IP Address
User1	00d0.3232.0001	192.168.1.10
User2	00d0.3232.0002	192.168.1.20
User3	00d0.3232.1000	192.168.1.30

- 2. Enable the IP address and MAC address binding function globally.
- 3. Configure the uplink port of the switch (Gi 0/5) as an exceptional port.



Note

Because the binding relationship of the IP packets on the uplink port is uncertain, the uplink port is generally configured as the exceptional port. It is not necessary to check the IP address and MAC address binding on the uplink port.

Configuration Steps

Step1: Configure the global IP address and MAC address binding.

Ruijie#configure terminal

! Configure the IP address and MAC address binding for the User1.

Ruijie(config)#address-bind 192.168.1.10 00d0.3232.0001

! Configure the IP address and MAC address binding for the User2.

Ruijie(config)#address-bind 192.168.1.20 00d0.3232.0002

! Configure the IP address and MAC address binding for the User3.

```
Ruijie(config)#address-bind 192.168.1.30 00d0.3232.0003
```

**Step2:** Enable the global IP address and MAC address binding.

```
Ruijie(config)#address-bind install
```

**Step3:** Configure the uplink port Gi 0/5 as an exceptional port.

```
Ruijie(config)#address-bind uplink gigabitEthernet 0/5
```

## Verifications

**Step1:** Display the configuration of IP address and MAC address binding on the switch. Keypoint: whether the binding relationship is correct.

```
Ruijie#show address-bind
```

IP Address	Binding MAC Addr
192.168.1.10	00d0.3232.0001
192.168.1.20	00d0.3232.0002
192.168.1.30	00d0.3232.0003

**Step2:** Display the configuration of the exceptional port.

```
Ruijie#show address-bind uplink
```

Ports	State
Gi0/5	Enabled

**Step3:** Verify the configuration.

The switch (except for the interface Gi 0/5) will only receive the IP packets whose source IP address and MAC address match the binding address; or the packets will be discarded.



# Aggregate Port Configuration

This chapter explains how to configure an aggregate port on Ruijie devices.

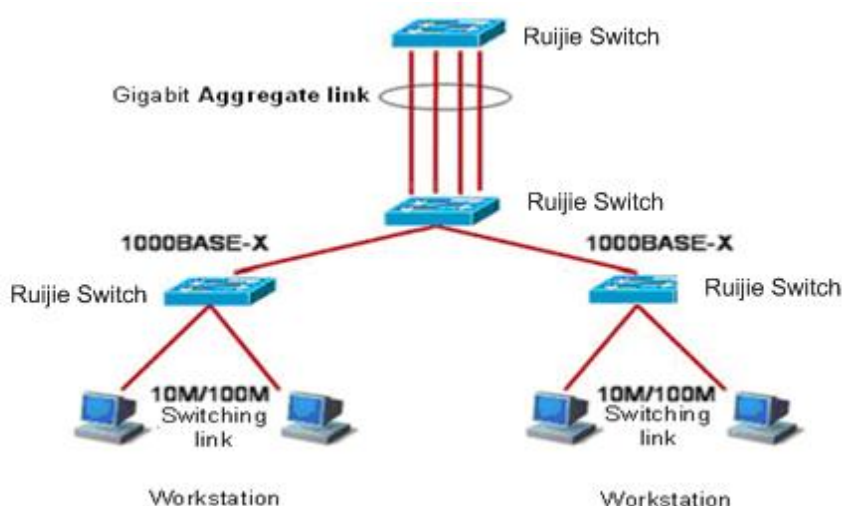
## Overview

### Understanding Aggregate Port

Multiple physical links can be bound into a logical link, called an aggregate port (hereinafter referred to as AP). Ruijie devices provide the AP function that complies with the IEEE802.3ad standard. This function can be used to expand link bandwidth and improve reliability.

AP function supports traffic balancing that evenly allocating the traffic to every member link. AP function also supports link backup. When a link member in an AP is disconnected, the system will automatically allocate the traffic of the member link to other active member links in the AP, except for the broadcast or multicast packets it received.

Typical AP configurations



Each AP includes up to 8 member ports, and the maximum AP numbers supported is 120.

### Understanding Traffic Balancing

Traffic can be evenly distributed on the member links of an AP according to the features such as source MAC address, destination MAC address, combination of source MAC address and destination MAC address, source IP address, destination IP address, and combination of source IP address and destination IP address. The **aggregateport load-balance** command can be used to set the method to distribute traffic.

Source MAC address-based traffic balancing refers to distribute the traffic on the member links of an AP according to the source MAC addresses of packets. Those packets with different source MAC addresses are evenly distributed on the member links of an AP according to different source MAC addresses. Those packets with the same source MAC address are forwarded through the same member

link.

Destination MAC address-based traffic balancing refers to distribute the traffic on the member links of an AP according to the destination MAC addresses of packets. Those packets with different destination MAC addresses are evenly distributed on the member links of an AP according to different destination MAC addresses. Those packets with the same destination MAC address are forwarded through the same member link.

The traffic balancing based on the combination of source MAC address and destination MAC address refers to distribute the traffic on the member links of an AP according to the combination of source MAC address and destination MAC address of packets. Those packets with different source and destination MAC addresses are evenly distributed on the member links of an AP according to different source and destination MAC addresses. Those packets with the same source and destination MAC address are distributed on the same member link.

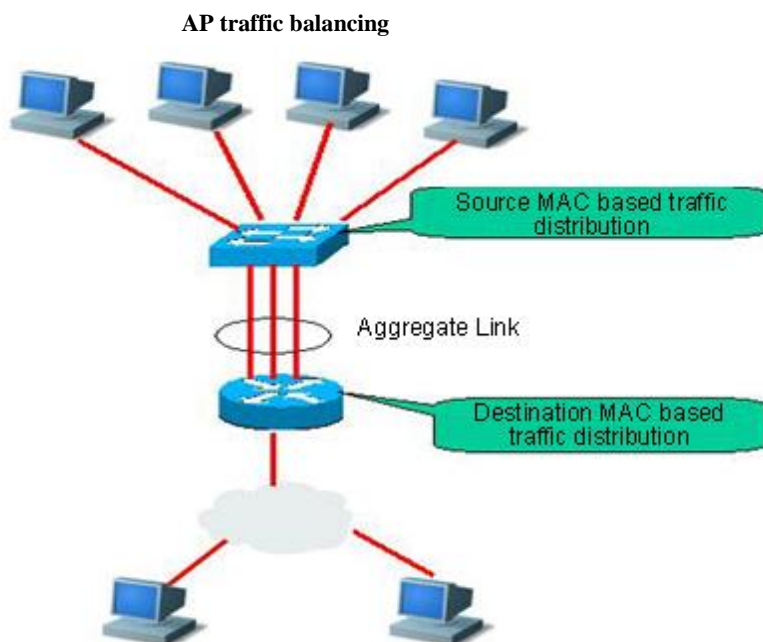
Source IP address- or destination IP address-based traffic balancing refers to distribute the traffic on the member links of an AP according to the source IP addresses or destination IP addresses of packets. Those packets with different source IP addresses or destination IP addresses are evenly distributed on the member links of an AP according to different source or destination IP addresses. Those packets with the same source IP address or destination IP address are forwarded through the same member link. This mode is specific for Layer 3 packets. If layer2 packets are received under this mode, traffic balancing is performed automatically according to the default device setting.

The traffic balancing based on the combination of source IP address and destination IP address refers to distribute the traffic on the member links of an AP according to the combination of source IP address and destination IP address of packets. Those packets with different source and destination IP addresses are evenly distributed on the member links of an AP according to different source and destination IP addresses. Those packets with the same source IP address and destination IP address are forwarded through the same member link. This mode is specific for Layer 3 packets. If layer2 packets are received under this mode, traffic balancing is performed automatically according to the default device setting.

All the above mentioned balancing modes are applicable to AP on Layer 2 and Layer 3.

An appropriate traffic distribution method should be set according to the actual network environments, so that the traffic can be evenly distributed on the links for the maximum utilization of network bandwidth.

In the following diagram, a switch communicates with a router through an AP, and the router serves as the gateway for all the devices inside the network (such as 4 PCs on the top of the diagram). The source MAC addresses of all the packets that the devices outside the network (such as 2 PCs at the bottom of the diagram) send through the router are the MAC address of the gateway. In order to distribute traffic between the router and other hosts on other links, traffic balancing should be performed based on the destination MAC address. However, traffic balancing should be performed based on the source MAC address on the switch.



## Configuring Aggregate Port

### Default Aggregate Port Configuration

The default AP configuration is shown in the table below.

Attribute	Default value
Layer-2 AP interface	None
Layer-2 AP interface	None
Traffic balancing	Traffic is distributed according to the combination of source IP address and destination IP address of the incoming packets.

### Aggregate Port Configuration Guide

- The rates of the member ports of an AP must be the same.
- L2 ports can only be join a L2 AP. L2 attributes of AP including member ports must not be modified.
- An AP does not support port security.
- Once a port is added to an AP, its attributes will be replaced by those of the AP.
- Once a port is removed from an AP, its attributes will be restored to original attributes.



#### Caution

When a port is added to an AP, you cannot perform any configuration on the port before removing the port from the AP.

### Configuring a Layer2 Aggregate Port

In the interface configuration mode, add the interface to an AP by performing the following steps.

Command	Function
Ruijie(config-if-range)# <b>port-group</b> <i>port-group-number</i>	Add the interface to an AP (the system will create the AP if it does not exist).

In the interface configuration mode, use the **no port-group** command to remove a physical port from the AP. The example below shows how to configure the layer2 Ethernet interface 1/0 to a member of layer2 AP 5.

```
Ruijie# configure terminal
Ruijie(config)# interface range gigabitEthernet 0/1
Ruijie(config-if-range)# port-group 5
Ruijie(config-if-range)# end
```

The command **interface aggregateport n** (n is the AP number) in the global configuration mode can be used to directly create an AP (if AP n does not exist).



#### Caution

After adding an ordinary port to an AP, when the port exits from the AP again, the previous configuration of the port will be restored to the default one. Different functions deal with the previous configuration of the AP member port differently. Therefore, it is recommended to view and confirm the port configuration after exiting from the AP.

## Configuring Traffic Balancing on an Aggregate Port

In the configuration mode, configure traffic balancing on the AP by performing the following steps:

Command	Function
Ruijie(config)# <b>aggregateport</b> <b>load-balance { dst-mac   src-mac  </b> <b>src-dst-mac   dst-ip   src-ip  </b> <b>src-dst-ip   src-port  </b> <b>src-dst-ip-l4port   mpls-label }</b>	<p>Set the AP traffic balancing and select the algorithm:</p> <p><b>dst-mac:</b> Distribute traffic according to the destination MAC addresses of the incoming packets.</p> <p><b>src-mac:</b> Distribute traffic according to the source MAC addresses of the incoming packets.</p> <p><b>src-dst-mac:</b> Distribute traffic according to the combination of the source MAC addresses and destination MAC addresses of the incoming packets.</p> <p><b>src-ip:</b> Distribute traffic according to the source IP addresses of the incoming packets.</p> <p><b>dst-ip:</b> Distribute traffic according to the destination IP addresses of the incoming packets.</p> <p><b>src-dst-ip:</b> Distribute traffic according to the combination of the source IP addresses and destination IP addresses of the incoming packets.</p> <p><b>src-port:</b> Distribute traffic according to the source port number of the incoming packets.</p> <p><b>src-dst-ip-l4port:</b> Distribute traffic according to the combination of the source IP addresses, destination IP addresses, L4 source port number, and L4 destination port number.</p>

Command	Function
	<b>mpls-label:</b> Distribute traffic according to the label of each level of MPLS packets.

To restore the traffic balancing configuration of an AP to the default value, execute the **no aggregateport loag-balance** command in the global configuration mode:

## Showing an Aggregate Port

In privileged EXEC mode, show the AP configuration by performing the following steps.

Command	Function
Ruijie# <b>show aggregateport</b> [ <i>port-number</i> ] { <b>load-balance</b>   <b>summary</b> }	Show the AP settings.

Ruijie# **show aggregateport load-balance**

Load-balance : Source MAC address

Ruijie# **show aggregateport 1 summary**

AggregatePort MaxPorts SwitchPort Mode Ports

-----  
Ag1 8 Enabled ACCESS

# LACP Configuration

## Overview

LACP(Link Aggregation Control Protocol) is a protocol based on IEEE802.3ad and aims to implement the dynamic link aggregation and disaggregation. This protocol interacts with its peer by using the LACPDU(Link Aggregation Control Protocol Data Unit).

With LACP enabled on the port, LACP notifies the following information of the port by sending LACPDUs: priority and MAC address of the system, port priority, number and operation key. Upon receiving the information, the peer determines the port that can be aggregated by comparing the received information with the information of other ports on the peer device. In this way, the two parties can reach an agreement in adding/removing the port to/from a dynamic aggregation group.

## Dynamic Link Aggregation Mode

A LACP port can be in one of the three aggregation modes: Active, Passive and Static.

The port in the active state will transceive the LACP packets and negotiate with the peer end, the port in the passive state will only respond to the received LACP packets, and the port in the static mode will not transceive the LACP packets or negotiate with the peer end, see the static AP configuration guide *AP-SCG doc* for detailed configuration.

Port mode	Neighbor port mode
Active mode	Active or passive mode.
Passive mode	Active mode
Static mode	Static mode.

## LACP Port State

The port member in the aggregation group can be in the following 3 states:

When the link state of the port is Down, no packet is forwarded on the port. The port state is **down**.

When the link state of the port is Up, after the LACP negotiation, the port joins in the packet forwarding as a port member in the aggregation group. The port state is **bn dl**.

When the link state of the port is Up, the port fails to join in the packet forwarding because the LACP is not enabled on the port, or the attribute of the port and the master port is inconsistent. The port state is **susp**.

**Note**

- Only the port with full-duplex attribute can be aggregated.
- The port rate, flow-control, media-type and Layer2&3 port attribute must be consistent.
- After the port aggregation, changing the above port attributes will lead to the aggregation failure of other ports in the same aggregation group.

**Caution**

- The LACP cannot be enabled on the ports with the function of forbidding the member ports to add to or leave the AP enabled; and the function of forbidding the member ports to add to or leave the AP cannot be enabled on the LACP member ports. The AP with the function of forbidding the member ports to add to or leave cannot be configured as the LACP AP, and function of forbidding the member ports to add to or leave the AP cannot be enabled on the LACP AP.
- The SYSLOG will be displayed when the LACP fails to leave the AP due to external function limitations, such as: %LACP-5-UNBUNDLE\_FAIL: Interface FastEthernet 0/1 failed to leave the AggregatePort 1. In this case, please modify the configuration to cancel the related configuration of forbidding the member ports to leave the AP, otherwise the normal packets transmission on the AP will be influenced.

## Dynamic Link Aggregation Priority Relations

### LACP System ID

Only one LACP aggregation system can be configured on each device. Each LACP aggregation system has sole system priority. The system ID consists of LACP system priority and the device MAC address. First compare the two system priorities: the lower the system priority is, the higher the system ID will be. Then compare the two device MAC addresses if the system priorities are equal: the smaller the MAC address is, the higher the system ID will be. The system with the higher system ID determines the port state.

### LACP Port ID

Each port owns an independent LACP port priority, which is configurable. The port ID consists of LACP port priority and port number. First compare the two port priorities: the lower the port priority value is, the higher the port ID is. Then compare the two port numbers if the two port priorities are equal: the smaller the port number is, the higher the port ID is.

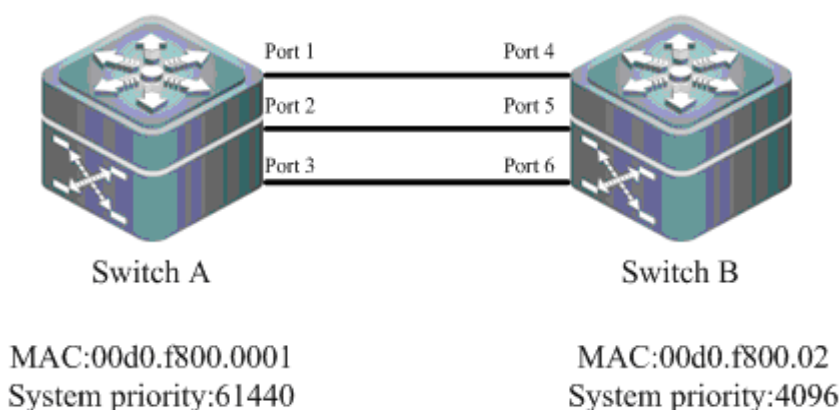
### LACP Master Port

When the dynamic member port is up, LACP selects a port with the highest priority in the aggregation

group based on the port rate, and duplex rate. Only can the ports with the same attributes with the master port be aggregated and join in the packet forwarding in the aggregation group. When the port attributes change, LACP re-selects the master port without disaggregation. But when the new master port is not aggregated, LACP disaggregates the member ports in the aggregation group and re-aggregates.

## LACP Negotiation Procedure

Upon receiving the LACP packets from the peer port, the system ID with higher priority is selected. On the end of higher system ID, set the ports in the aggregation group are to be aggregated in the descending order of port priority (when the number of ports in the aggregation group exceeds the maximum port number, the state of the ports exceeding the aggregation capacity is **superseded**.) Upon receiving the updated LACP packets on the peer port, the corresponding port is to be aggregated.



**Figure-1 LACP Negotiation**

As shown in Figure-1, switch A and switch B are interconnected through the 6 ports. Set the system priority for the switchA and the switchB to be 61440 and 4096 respectively. Enable the LACP function on the 6 ports directly-connected between the switches. Set the aggregation mode for the 3 ports is active, and set the default port priority for the other 3 ports as 32768.

Upon receiving the LACP packets from the switchA, switchB finds its system priority is higher than the switchA, the port4-6 on the switchB are to be aggregated according to the sequence of the port priority. After receiving the updated LACP packets from the switchB, the switchA finds its system priority is lower than the switchB and the port1-3 on the switchA are also aggregated.

## LACP Requirements

LACP is a protocol that automatically add/remove the port to/from the aggregation group. The requirements of the auto-aggregation of those two ports are:

Only can the ports with the same operation key be aggregated;

Only can the ports that are with the same attributes such as port rate and duplex as the master port be dynamically aggregated.

The port link state is UP, the peer port running LACP and the port or the peer port must be in the Active mode.



## LACP Configuration

### Configuring LACP

You can configure the LACP system priority, port priority and administrative key in the aggregation group. All dynamic link groups on one switch share one LACP system priority. Changing the system priority will affect all aggregation groups.

Run the following commands to configure the LACP:

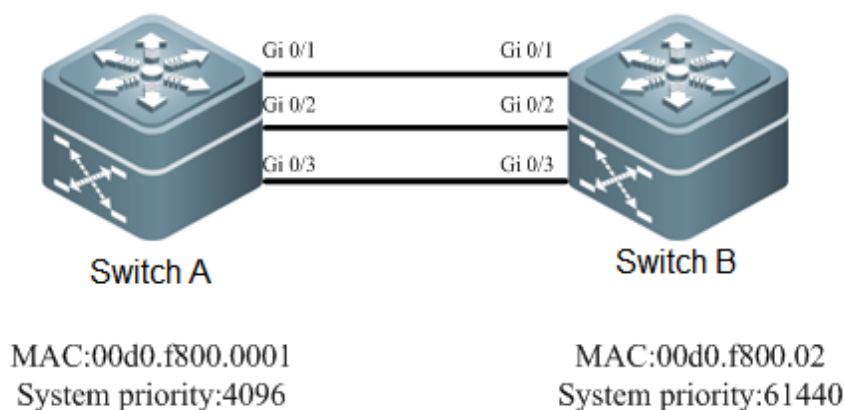
Command	Function
Ruijie# <b>configure</b>	Enter the global configuration mode.
Ruijie(config)# <b>lacp system-priority</b> <i>system-priority</i>	(Optional) Set the LACP system priority, in the range of 0-65535. The default system priority is 32768.
Ruijie(config)# <b>interface</b> <i>interface-id</i>	Enter the interface configuration mode.
Ruijie(config-if)# <b>lacp port-priority</b> <i>port-priority</i>	(Optional) Set the LACP port priority, in the range of 0-65535. The default system priority is 32768.
Ruijie(config-if)# <b>port-group</b> <i>key</i> <b>mode</b> <b>active</b>   <b>passive</b>	Add the port to the aggregation group and specify the LACP port mode. If the aggregation group does not exist, an aggregation group will be created.  <i>key</i> : the administrative key of the aggregation group.  <b>active</b> : the port is added to the dynamic aggregation group in the active mode.  <b>passive</b> : the port is added to the aggregation group in the passive mode.
Ruijie(config-if)# <b>end</b>	Return to the privileged EXEC mode.

### Viewing the LACP Configuration

To view the LACP state, run the following command in the privileged EXEC mode:

Command	Function
Ruijie# <b>show lacp summary</b>	Show the LACP state information.

## LACP Configuration Example



**Figure-2 LACP Link Aggregation**

As shown in the figure-2, on the SwitchA, set the LACP system priority as 4096, enable the LACP on the interface Gi 0/1, Gi 0/2, Gi 0/3, and set the LACP port priority as 4096:

```
SwitchA#configure terminal
SwitchA(config)# lacp system-priority 4096
SwitchA(config)# interface range GigabitEthernet 0/1-3
SwitchA(config-if-range)# lacp port-priority 4096
SwitchA(config-if-range)# port-group 3 mode active
SwitchA(config-if-range)# end
```

On the SwitchB, set the LACP system priority as 61440, enable the LACP on the interface Gi 0/1, Gi 0/2, Gi 0/3, and set the LACP port priority as 61440:

```
SwitchB# configure terminal
SwitchB(config)# lacp system-priority 61440
SwitchB(config)# interface range GigabitEthernet 0/1-3
SwitchB(config-if-range)# lacp port-priority 61440
SwitchB(config-if-range)# port-group 3 mode active
SwitchB(config-if-range)# end
```

After the configuration, if the LACP negotiation succeeds, it prompts the following log:

```
*Feb 25 17:11:31: %LACP-5-BUNDLE: Interface Gi0/1 joined AggregatePort 3.
*Feb 25 17:11:32: %LACP-5-BUNDLE: Interface Gi0/2 joined AggregatePort 3.
*Feb 25 17:11:32: %LACP-5-BUNDLE: Interface Gi0/3 joined AggregatePort 3.
*Feb 25 17:11:32: %LINEPROTO-5-UPDOWN: Line protocol on Interface AggregatePort 3, changed state to up
```

Then show the member port state in the aggregation group on the SwitchA:

```
Ruijie(config)#show LACP summary
Flags: S - Device is requesting Slow LACPDUs
       F - Device is requesting Fast LACPDUs.
       A - Device is in active mode.          P - Device is in passive mode.

Aggregate port 3:
```

Local information:

Port	Flags	State	LACP port	Oper	Port	Port
			Priority	Key	Number	State
Gi0/1	SA	bndl	4096	0x3	0x1	0x3d
Gi0/2	SA	bndl	4096	0x3	0x2	0x3d
Gi0/3	SA	bndl	4096	0x3	0x3	0x3d

Partner information:

Port	Flags	LACP port Priority	Dev ID	Oper	Port	Port
				Key	Number	State
Gi0/1	SA	61440	00d0.f800.0002	0x3	0x1	0x3d
Gi0/2	SA	61440	00d0.f800.0002	0x3	0x2	0x3d
Gi0/3	SA	61440	00d0.f800.0002	0x3	0x3	0x3d

The following table describes the fields:

Field	Description
Local information	Show the local LACP information.
Port	Show the system port ID.
Flags	Show the port state flag: "S" indicates that the LACP is stable and in the state of periodically sending the LACPPDU; "A" indicates that the port is in the active mode.
S	Show the device is requesting slow LACPDUs, that is sending a packet per 30 seconds.
F	Show the device is requesting fast LACPDUs, that is sending a packet every second.
A	Show the port is in the active mode.
P	Show the port is in the passive mode.
State	Show the port aggregation information: "bndl" indicates that the port is aggregated; "Down" represents the disconnection port state; "susp" indicates that the port is not aggregated.
LACP Port Priority	Show the LACP port priority.
Oper Key	Show the port operation key.
Port Number	Show the port number.
Port State	Show the flag bit for the LACP port state.
Partner information	Partly show the LACP information of the peer port.

Dev ID	Partly show the system MAC information of the peer device.
--------	--

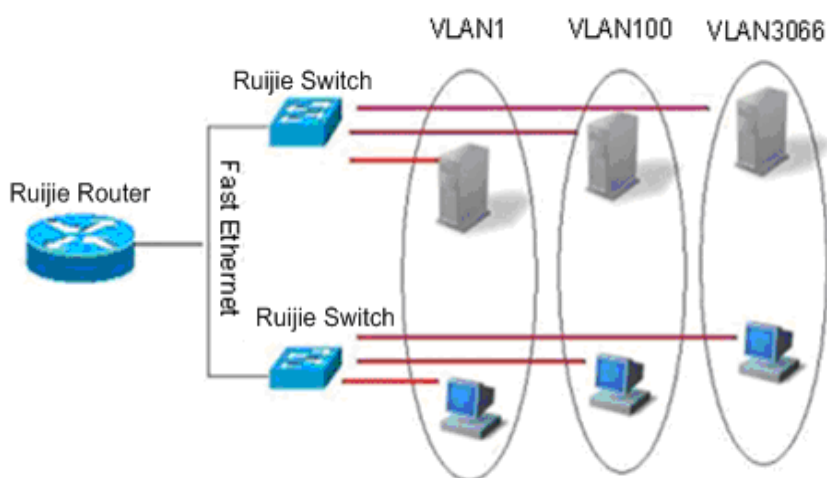
# VLAN Configuration

This chapter describes how to configure IEEE802.1q VLAN.

## Overview

Virtual Local Area Network (VLAN) is a logical network divided on a physical network. VLAN corresponds to the L2 network in the ISO model. The division of VLAN is not restricted by the physical locations of network ports. A VLAN has the same attributes as a common physical network. Except for no restriction on physical location, unicast, broadcast and multicast frames on layer 2 are forwarded and distributed within a VLAN, not being allowed to directly go to other VLANs. Therefore, when a host in a VLAN wants to communicate with another host in another VLAN, a layer 3 device must be used, as shown in the following diagram.

You can define a port as the member of a VLAN. All the terminals connected to the specified port are part of the VLAN. A network can support multiple VLANs. In this case, when you add, delete, and modify users in the VLANs, you do not need to modify the network configuration physically.



Like a physical network, a VLAN is usually connected to an IP subnet. A typical example is that all the hosts in the same IP subnet belong to the same VLAN. A layer 3 device must be used for communication between VLANs. Ruijie L3 devices can perform IP routing between VLANs through SVI (Switch Virtual Interfaces). For the configuration about SVI, refer to *Interface Management Configuration* and *IP Unicast Routing Configuration*.

## Supported VLAN

Complying with IEEE802.1Q Standard, our products support up to 4094 VLANs(VLAN ID 1-4094 ), in which VLAN 1 is the default VLAN that cannot be deleted.

## VLAN Member Type

You can determine the frames that can pass a port and the number of VLANs that the port can belong to by

configuring the VLAN member type of the port. For the detailed description about VLAN member type, see the following table:

Member Type	Port Feature
Access	One access port can belong to only one VLAN, which must be specified manually.
Trunk (802.1Q)	By default, one Trunk port belongs to all the VLANs of the device itself, and it can forward the frames of all the VLANs. However, you can impose restriction by setting a list of allowed VLANs.

## Configuring a VLAN

A VLAN is identified by its VLAN ID. You can add, remove, and modify the VLANs in the range of 2 to 4094 on a device. VLAN 1 is created by a device automatically and cannot be removed.

You can configure the member type of a port in a VLAN, add a port to a VLAN, and remove a port from a VLAN in the interface configuration mode.

## Saving the VLAN Configuration

To save the VLAN configuration in the configuration file, execute the **copy running-config startup-config** command in the privileged EXEC mode. To view VLAN configuration, execute the **show vlan** command.

## Default VLAN Configuration

The following table shows the default configuration of a VLAN.

Parameter	Default Value	Range
VLAN ID	1	1 to 4094
VLAN Name	VLAN xxxx, where xxxx is the VLAN ID	None
VLAN State	Active	Two status: active or inactive

## Creating/Modifying a VLAN

In the privileged EXEC mode, you can create or modify a VLAN by executing the following commands.

Command	Function
Ruijie(config)# <b>vlan</b> <i>vlan-id</i>	Enter a VLAN ID. If you enter a new VLAN ID, the device will create it. If you enter an existing VLAN ID, the device modifies the corresponding VLAN.

Command	Function
Ruijie(config)# <b>name</b> <i>vlan-name</i>	(Optional) Name the VLAN. If you skip this step, the device automatically assigns the VLAN a name of VLAN xxxx, where xxxx is a 4-digit VLAN ID starting with 0. For example, VLAN 0004 is the default name of VLAN 4.

To restore the name of a VLAN to its default, simply enter the **no name** command.

The following example creates VLAN 888, names it test888, and saves its configuration into the configuration file:

```
Ruijie# configure terminal
Ruijie(config)# vlan 888
Ruijie(config-vlan)# name test888
Ruijie(config-vlan)# end
```

## Deleting a VLAN

You cannot delete the default VLAN (VLAN 1).

In the privileged EXEC mode, you can delete a VLAN by executing the following command.

Command	Function
Ruijie(config)# <b>no vlan</b> <i>vlan-id</i>	Enter the VLAN ID that you want to delete.

## Adding Existing Access Ports to Specified VLAN

If you assign a port to an inexistent VLAN, the switch will automatically create that VLAN.

In the privileged EXEC mode, you can assign a port to a VLAN by executing the following command.

Command	Function
Ruijie(config-if)# <b>switchport mode access</b>	Define the member type of the port in a VLAN (L2 ACCESS port).
Ruijie(config-if)# <b>switchport access vlan</b> <i>vlan-id</i>	Assign the port to the VLAN.

The following example adds Ethernet 1/10 to VLAN20 as an access port:

```
Ruijie# configure terminal
Ruijie(config)# interface fastethernet 1/10
Ruijie(config-if)# switchport mode access
Ruijie(config-if)# switchport access vlan 20
Ruijie(config-if)# end
```

The following example shows how to verify the configuration:

```
Ruijie(config)# show interfaces gigabitEthernet 3/1
switchport
Switchport is enabled
Mode is access port
Access vlan is 1, Native vlan is 1
Protected is disabled
Vlan lists is ALL
```

**Caution**

In the R2700 switching card, although the access vlan can also be configured on the trunk port, the access port configuration does not take effect and the port remains in the trunk port. Only the configuration of native vlan and allowed vlan list takes effect.

## Adding Access Ports to the Existing VLAN

In VLAN configuration mode, add the specified Access port to this VLAN. The effect of this command is the same as the command to specify the VLAN to which the interface belongs in interface configuration mode (namely **switchport access vlan *vlan-id***).

Command	Function
Ruijie(config)# <b>vlan <i>vlan-id</i></b>	Type in a VLAN ID. If a new VLAN ID is typed in, the device will create a VLAN. If an existing VLAN ID is typed in, the corresponding VLAN will be modified.
Ruijie(config-vlan)# <b>add interface { <i>interface-id</i>   range <i>interface-range</i> }</b>	Add one or a group of Access ports to the existing VLAN. By default, all layer-2 Ethernet ports belong to VLAN1.
Ruijie(config-vlan)# <b>[no]add interface { <i>interface-id</i>   range <i>interface-range</i> }</b>	Delete one or a group of Access ports from the existing VLAN.
Ruijie(config-vlan)# <b>show interface <i>interface-id</i> switchport</b>	Display the information about layer-2 interface.

**Caution**

This command only applies to Access port.

In terms of these two commands to add interface to the VLAN, the later configured command will override the previously configured command.

The following example adds Access port (GigabitEthernet 0/10) to VLAN20:

```
Ruijie# configure terminal
SwitchA(config)#vlan 20
SwitchA(config-vlan)#add interface GigabitEthernet 0/10
```

The following example shows how to verify the configurations:

```
Ruijie# show interface GigabitEthernet 0/10 switchport

Interface          Switchport  Mode  Access Native Protected  VLAN lists
-----
GigabitEthernet 0/10 enabled ACCESS 20      1      Disabled  ALL
```

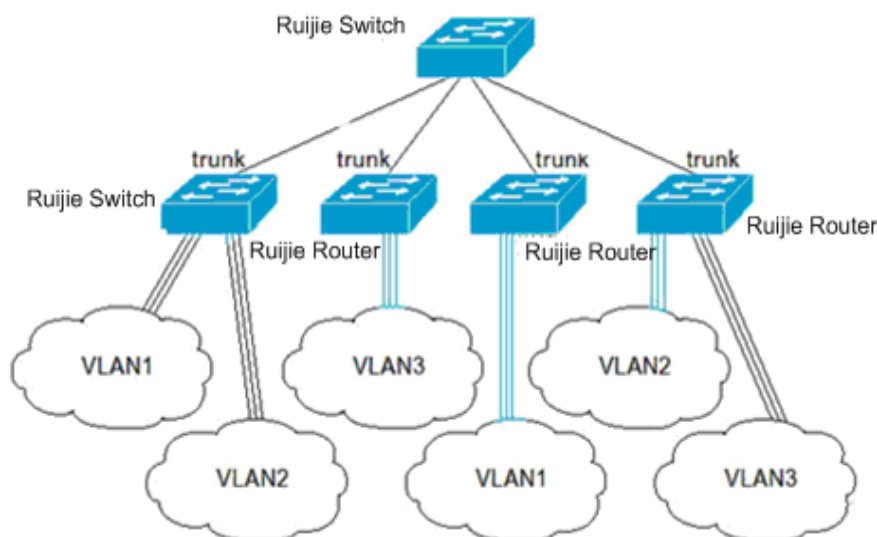


## Configuring VLAN Trunks

### Overview

A trunk is a point-to-point link that connects one or multiple Ethernet switching interfaces to other network devices (for instance, router or switch). A trunk can transmit the traffics of multiple VLANs.

The Trunk encapsulation of Ruijie device is 802.1Q-complied. The following diagram shows a network connected with trunks.



You can set a common Ethernet port or aggregate port to be a trunk port. For the details of aggregate port, refer to *Configuring Aggregate Port*.

In order to switch an interface between the access mode and the trunk mode, use the **switchport mode** command:

Command	Function
Ruijie(config-if)# <b>switchport mode access</b>	Set an interface to the access mode
Ruijie(config-if)# <b>switchport mode trunk</b>	Set an interface to the Trunk mode

A native VLAN must be defined for a trunk port. The untagged packets received and sent through the port are deemed as the packets of the native VLAN. Obviously, the default VLAN ID of the port (that is, the PVID in the IEEE 802.1Q) is the VLAN ID of the native VLAN. Moreover, you must untag them before sending the packets of the native VLAN through the trunk port. The default native VLAN of a trunk port is VLAN 1.

When you configure a trunk link, be sure that the ports on both ends of the trunk belong to the same native VLAN.

### Configuring a Trunk Port

#### Basic Trunk Port Configuration

In the privileged EXEC mode, you can configure a trunk port by executing the following command.

Command	Function
Ruijie(config-if)# <b>switchport mode trunk</b>	Configure the port as a L2 trunk port.
Ruijie(config-if)# <b>switchport trunk native vlan</b> <i>vlan-id</i>	Specify a native VLAN for the port.

To restore all the trunk-related settings of a trunk port to their defaults, use the **no switchport mode** command in the interface configuration mode.

## Defining the Allowed VLAN List of a Trunk Port

By default, the traffic of all VLANs in the range of 1 to 4094 can be transmitted over a trunk port. However, you can restrict the traffic of some VLANs from passing the trunk port by setting its allowed VLAN list.

In the privileged mode, you can modify the allowed VLAN list of a trunk port by executing the following command.

Command	Function
Ruijie(config-if)# <b>switchport trunk allowed vlan</b> {all   [add   remove   except] } <i>vlan-list</i>	<p>(Optional) Configure the allowed VLAN list of the trunk port. The <i>vlan-list</i> parameter may be a VLAN or a series of VLANs. It starts with a small VLAN ID and ends with a large VLAN ID. Both IDs are connected with "-", such as 10–20.</p> <p>All: Add all the allowed VLANs to the allowed VLAN list;</p> <p>add: Add the specified VLAN list to the allowed VLAN list;</p> <p>remove: Remove the specified VLAN list from the allowed VLAN list;</p> <p>except: Add all the VLANs other than the specified VLAN list to the allowed VLAN list.</p>

To restore the allowed VLAN list of the trunk port to its default, execute the **no switchport trunk allowed vlan** command in the interface configuration mode.

The following example removes VLAN 2 from the allowed VLAN list of port 1/15:

```
Ruijie(config)# interface fastethernet 1/15
Ruijie(config-if)# switchport trunk allowed vlan remove 2
Ruijie(config-if)# end
Ruijie# show interfaces fastethernet 1/15 switchport
Interface Switchport Mode Access Native Protected VLAN lists
-----
Gi0/15      enabled    TRUNK 1      1      Disabled  1,3–4094
```

## Configuring a Native VLAN.

Tagged or untagged 802.1Q frames can be received or sent on a trunk port. Untagged frames are used to transmit the traffic of the native VLAN. By default, the native VLAN is VLAN 1.

In the privileged EXEC mode, you can configure a native VLAN for a trunk port by executing the following

command.

Command	Function
Ruijie(config-if)# <b>switchport trunk native vlan</b> <i>vlan-id</i>	Configure a native VLAN.

To restore the native VLAN of a trunk port to its default, execute the **no switchport trunk native vlan** command in the interface configuration command.

If a frame carries the VLAN ID of the native VLAN, it will be automatically untagged when being forwarded through the trunk port.

When you set the native VLAN of a trunk port to an inexistent VLAN, the switch will not automatically create the VLAN. In addition, the native VLAN of a trunk port may be out the allowed VLAN list. In this case, the traffic of the native VLAN cannot pass the trunk port.

## Showing VLAN Information

Only in the privileged EXEC mode can you view the VLAN information, including VLAN VID, VLAN status, member ports of the VLAN, and VLAN configuration. The related commands are listed as below:

Command	Function
<b>show vlan</b> [ <i>id vlan-id</i> ]	Show the information about all or the specified VLAN.

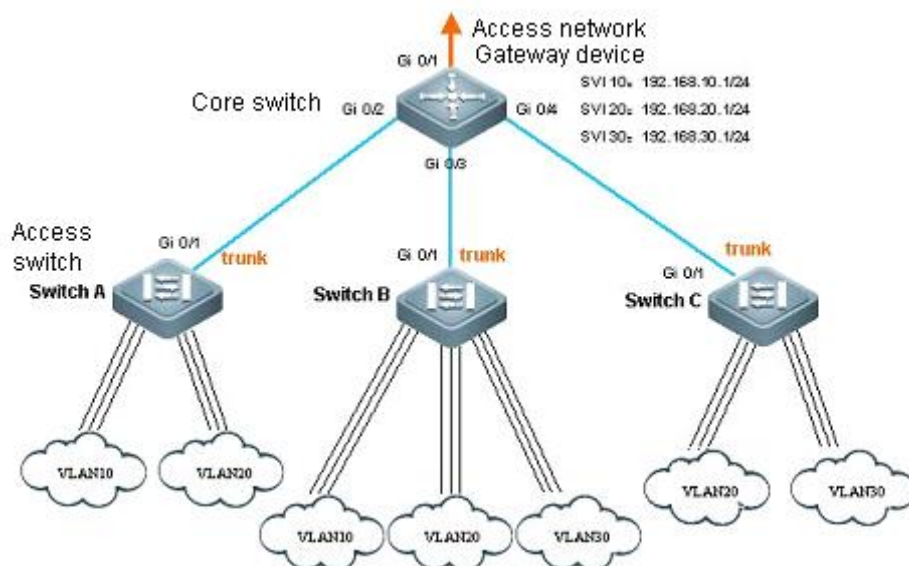
The following example shows the information about a VLAN:

```
Ruijie# show vlan
VLAN  Name          Status          Ports
----  -
1  VLAN0001  STATIC          Gi0/1, Gi0/5, Gi0/6, Gi0/7
                               Gi0/8, Gi0/9, Gi0/10, Gi0/11
                               Gi0/12, Gi0/13, Gi0/14, Gi0/15
                               Gi0/16, Gi0/17, Gi0/18, Gi0/19
                               Gi0/20, Gi0/21, Gi0/22, Gi0/23
                               Gi0/24
10  VLAN0010  STATIC          Gi0/2, Gi0/3
20  VLAN0020  STATIC          Gi0/2, Gi0/3, Gi0/4
30  VLAN0030  STATIC          Gi0/3, Gi0/4
```

```
Ruijie# show vlan id 20
VLAN  Name          Status          Ports
----  -
20  VLAN0020  STATIC          Gi0/2, Gi0/3, Gi0/4
```

## Configuration Examples

### Network Topology



### Networking Requirements

As shown above, an Intranet is divided into VLAN 10, VLAN 20 and VLAN 30 in order to realize layer-2 isolation. The IP subnets corresponding to three VLANs are 192.168.10.0/24, 192.168.20.0/24 and 192.168.30.0/24. The three VLANs are interconnected through the IP forwarding capacity of layer-3 core switch.

### Configuration Tips

This example shows to how to configure the core switch and one of the access switches:

- Configure three VLANs on the core switch; configure the port connecting access switch to trunk port and specify the allowed vlan list to realize layer-2 isolation;
- Configure three SVI interfaces on the core switch to serve as the gateway interfaces for IP subnets corresponding to the three VLANs; configure the corresponding IP addresses;
- Create VLANs on three access switches and assign Access port for each VLAN; specify the trunk port for connecting core switch. This example shows the configuration steps on the access switch of Switch A.

### Configuration Steps

#### Configurations on Core Switch

##### ■ Create VLAN

# Enter the global configuration mode

```
Ruijie#configure terminal
```

# Create VLAN 10

```
Ruijie(config)#vlan 10
```

## # Create VLAN 20

```
Ruijie(config-vlan)#vlan 20
```

## # Create VLAN 30

```
Ruijie(config-vlan)#vlan 30
```

## # Return to the global configuration mode

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

### ■ Configure respective trunk ports and specify the allowed vlan list

## # Enter the interface range of Gi 0/2-4

```
Ruijie(config)#interface range GigabitEthernet 0/2-4
```

## # Configure Gi 0/2-4 as trunk ports

```
Ruijie(config-if-range)#switchport mode trunk
```

## # Return to the global configuration mode

```
Ruijie(config-if-range)#exit
```

## # Enter port Gi 0/2

```
Ruijie(config)#interface GigabitEthernet 0/2
```

## # Delete all vlans from the allowed vlan list of this port

```
Ruijie(config-if)#switchport trunk allowed vlan remove 1-4094
```

## # Add vlan 10 and vlan 20 into the allowed vlan list of this port

```
Ruijie(config-if)#switchport trunk allowed vlan add 10,20
```

## # Enter port Gi 0/3

```
Ruijie(config-if)#interface GigabitEthernet 0/3
```

## # Delete all vlans from the allowed vlan list of this port

```
Ruijie(config-if)#switchport trunk allowed vlan remove 1-4094
```

## # Add vlan 10, vlan 20 and vlan 30 into the allowed vlan list of this port

```
Ruijie(config-if)#switchport trunk allowed vlan add 10,20,30
```

## # Enter port Gi 0/4

```
Ruijie(config-if)#interface GigabitEthernet 0/4
```

## # Delete all vlans from the allowed vlan list of this port

```
Ruijie(config-if)#switchport trunk allowed vlan remove 1-4094
```

## # Add vlan 20 and vlan 30 into the allowed vlan list of this port

```
Ruijie(config-if)#switchport trunk allowed vlan add 20,30
```

## # Return to the global configuration mode

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

### ■ Display vlan configurations on core switch

## # Display vlan information, including vlan id, name, state and member ports

```
Ruijie#show vlan
```

VLAN	Name	Status	Ports
1	VLAN0001	STATIC	Gi0/1, Gi0/5, Gi0/6, Gi0/7 Gi0/8, Gi0/9, Gi0/10, Gi0/11 Gi0/12, Gi0/13, Gi0/14, Gi0/15 Gi0/16, Gi0/17, Gi0/18, Gi0/19 Gi0/20, Gi0/21, Gi0/22, Gi0/23 Gi0/24

```

10 VLAN0010  STATIC      Gi0/2, Gi0/3
20 VLAN0020  STATIC      Gi0/2, Gi0/3, Gi0/4
30 VLAN0030  STATIC      Gi0/3, Gi0/4

```

# Display the vlan state of port Gi 0/2

```

Ruijie#show interface GigabitEthernet 0/2 switchport
Interface Switchport Mode Access Native Protected VLAN lists
-----
Gi0/2      enabled  TRUNK   1      1      Disabled  10,20

```

# Display the vlan state of port Gi 0/3

```

Ruijie#show interface GigabitEthernet 0/3 switchport
Interface Switchport Mode Access Native Protected VLAN lists
-----
Gi0/3      enabled  TRUNK   1      1      Disabled  10,20,30

```

# Display the vlan state of port Gi 0/4

```

Ruijie#show interface GigabitEthernet 0/4 switchport
Interface Switchport Mode Access Native Protected VLAN lists
-----
Gi0/4      enabled  TRUNK   1      1      Disabled  20,30

```

## ■ Create SVI port and specify the IP address

# Enter the global configuration mode

```
Ruijie#configure terminal
```

# Create SVI 10

```
Ruijie(config)#interface vlan 10
```

# Configure the IP address of SVI 10

```
Ruijie(config-if)#ip address 192.168.10.1 255.255.255.0
```

# Create SVI 20

```
Ruijie(config-if)#interface vlan 20
```

# Configure the IP address of SVI 20

```
Ruijie(config-if)#ip address 192.168.20.1 255.255.255.0
```

# Create SVI 30

```
Ruijie(config-if)#interface vlan 30
```

# Configure the IP address of SVI 30

```
Ruijie(config-if)#ip address 192.168.30.1 255.255.255.0
```

# Return to the global configuration mode

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

## Configurations on the Access Switch of Switch A

### ■ Create VLAN

# Enter the global configuration mode

```
Ruijie#configure terminal
```

# Create VLAN 10

```
Ruijie(config)#vlan 10
```

# Create VLAN 20

```
Ruijie(config-vlan)#vlan 20
```

# Return to the global configuration mode

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

### ■ Assign Access port for each VLAN

# Enter the interface range of Gi 0/2-12

```
Ruijie(config) #interface range GigabitEthernet 0/2-12
```

# Configure Gi 0/2-12 as Access ports

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

# Add Gi 0/2-12 to VLAN 10

```
Ruijie(config-if) #switchport access vlan 10
```

# Enter the interface range of Gi 0/13-24

```
Ruijie(config-if) #interface range GigabitEthernet 0/13-24
```

# Configure Gi 0/13-24 as Access ports

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

# Add Gi 0/13-24 to VLAN 20

```
Ruijie(config-if) #switchport access vlan 20
```

# Return to the global configuration mode

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

### ■ Specify the trunk port for connecting core switch

# Enter port Gi 0/1

```
Ruijie(config) #interface GigabitEthernet 0/1
```

# Configure Gi 0/1 as trunk port

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

# Return to global configuration mode

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

# Protocol VLAN Configuration

## Protocol VLAN Technology

Every packet received on a port of the device should be classified and added to a unique VLAN. There are three possibilities:

1. If the packet has no VLAN ID (for instance, UNTAG or Priority packet), and the device only supports port-based VLAN classification, the VLAN ID in the tag added to the packet is the PVID of the inbound port.
2. If the packet has no VLAN ID (for instance, UNTAG or Priority packet), and the device supports protocol type-based VLAN classification, one of the VLAN IDs corresponding to the protocol suite configured on the inbound port will be selected as the VLAN ID in the tag added to the packet. However, if the protocol type of the packet matches none of the protocol suite configured on the inbound port, the VLAN ID will be assigned by port-based VLAN classification.
3. If the packet is tagged, its VLAN is determined by the VLAN ID in the tag.

As a protocol type-based VLAN classification technology, the protocol VLAN classifies the packets that have no VLAN ID and be of the same protocol type to the same VLAN.

The protocol VLAN configuration takes effect for Trunk port and Hybrid port, not for the Access port.

Ruijie products support both global IP address-based VLAN classification, and packet type and Ethernet type-based VLAN classification on a port.

Because IP address-based VLAN classification is a global configuration, once configured, it will apply to all trunk ports and Hybrid ports.

1. If the incoming packet has no VLAN ID, and its IP address matches the configured IP address, this packet will be classified into the configured VLAN.
2. If the incoming packet has no VLAN ID, and its packet type and Ethernet type match those you configured on the inbound port respectively, this packet will be classified into the configured VLAN.

IP address-based VLAN classification takes precedence over packet type and Ethernet type-based VLAN classification. Hence, if you have configured both IP address-based VLAN classification and packet type and Ethernet type-based VLAN classification, and the incoming packet matches them both, IP address-based VLAN classification takes effect.

You should configure a VLAN, trunk port, hybrid port, access port and AP attributes before configuring the protocol VLAN. If you have configured protocol VLAN on a trunk port or a hybrid port, the allowed VLAN list for the trunk port and hybrid port must include all the VLANs related to the protocol VLAN.

## Configuring a Protocol VLAN

### Default Protocol VLAN

No Protocol VLAN is configured by default.

### Configuring IP Address-based VLAN Classification

To configure IP address-based VLAN classification, execute the following commands:



Command	Description
Ruijie# <b>configure terminal</b>	Enter the global configuration mode.
Ruijie(config)# <b>protocol-vlan ipv4</b> <i>address mask address vlan vid</i>	Configure IP address, subnet mask and VLAN classification.
Ruijie(config)# <b>no protocol-vlan ipv4</b> <i>address mask address</i>	Remove the IP address configuration.
Ruijie(config)# <b>no protocol-vlan ipv4</b>	Remove all IP address configuration.
Ruijie(config)# <b>interface</b> <i>interface-id</i>	Enter the interface configuration mode.
Ruijie(config-if)# <b>protocol vlan ipv4</b>	Enable the IP address-based VLAN classification on the interface.
Ruijie(config-if)# <b>no protocol vlan ipv4</b>	Disable the IP address-based VLAN classification on the interface.
Ruijie(config-vlan)# <b>show</b> <b>protocol-vlan ipv4</b>	Show the configured IP address

**Note**

Specify the IP address and subnet mask in the x.x.x.x format.

Available VLAN IDs may vary with different product.

The following command configures the IP address of 192.168.100.3, and the mask of 255.255.255.0 VLAN 100.

```
Ruijie# configure terminal
Ruijie(config)# protocol-vlan ipv4 192.168.100.3 mask 255.255.255.0 vlan 100
Ruijie(config-vlan)# end
Ruijie# show protocol-vlan ipv4
ip          mask          vlan
-----
192.168.100.3  255.255.255.0  100
```

## Configuring Packet Type and Ethernet Type Profile

To configure the packet type and Ethernet type profile, execute the following commands:

Command	Description
Ruijie# <b>configure terminal</b>	Enter the global configuration mode.
Ruijie(config)# <b>protocol-vlan profile</b> <i>id</i> <b>frame-type</b> [ <i>type</i> ] <b>ether-type</b> [ <i>type</i> ]	Configure packet type and Ethernet type profile.
Ruijie(config)# <b>no protocol-vlan profile</b> <i>id</i>	Delete an profile.
Ruijie(config)# <b>no protocol-vlan profile</b>	Clear all profiles.
Ruijie(config-vlan)# <b>show</b> <b>protocol-vlan profile</b> [ <i>id</i> ]	Exit the VLAN mode

Command	Description
Ruijie# <b>configure terminal</b>	Show all profiles.
Ruijie(config)# <b>protocol-vlan profile</b> <i>id</i> <b>frame-type</b> [ <i>type</i> ] <b>ether-type</b> [ <i>type</i> ]	Show a profile.

For example:

```
Ruijie# configure terminal
Ruijie(config)# protocol-vlan profile 1 frame-type ETHERII ether-type EHTER_AARP
Ruijie(config)# protocol-vlan profile 2 frame-type SNAP ether-type 0x809b
Ruijie(config-vlan)# end
Ruijie# show protocol-vlan profile
profile      frame-type  ether-type  Interfaces|vid
-----
1            ETHERII    EHTER_AARP  NULL|NULL
2            SNAP      ETHER_APPLETALK  NULL|NULL
```



#### Note

- 1) The configuration will not become effective until the profile is applied to a port.
- 2) Before updating a profile, you must delete the profile and then reconfigure it.

## Applying a Profile

To apply a profile, execute the following commands:

Command	Description
Ruijie# <b>configure terminal</b>	Enter the global configuration mode.
Ruijie(config)# <b>interface</b> <i>interface-id</i>	Enter the interface configuration mode.
Ruijie(config-if)# <b>protocol-vlan profile</b> <i>id</i> <b>vlan</b> <i>vid</i>	Apply a profile to this port.
Ruijie(config-if)# <b>no protocol-vlan profile</b> <i>id</i>	Clear all profiles on this port .
Ruijie(config-if)# <b>no protocol-vlan profile</b>	Clear a profile on this port
Ruijie(config-if)# <b>show protocol-vlan profile</b>	Show the profile configuration.

The following example applies profile 1 and profile 2 to the GE interface 1 of Slot 3. The VLAN categories are VLAN 101 and 102:

```
Ruijie# configure terminal
Ruijie(config)# interface gi 3/1
Ruijie(config-if)# protocol-vlan profile 1 vlan 101
Ruijie(config-if)# protocol-vlan profile 2 vlan 102
Ruijie(config-if)# end
```

```
Ruijie# show protocol-vlan profile
profile      frame-type  ether-type  Interfaces|vid
-----
1            ETHERII   EHTER_AARP  gi3/1|101
2            SNAP     ETHER_APPLETALK gi3/1|102
```

**Note**

1. All profiles can be applied to each interface.
2. Different VLANs can be specified for the same profile on different interfaces.

## Showing a Protocol VLAN

To show a protocol VLAN, execute the following command:

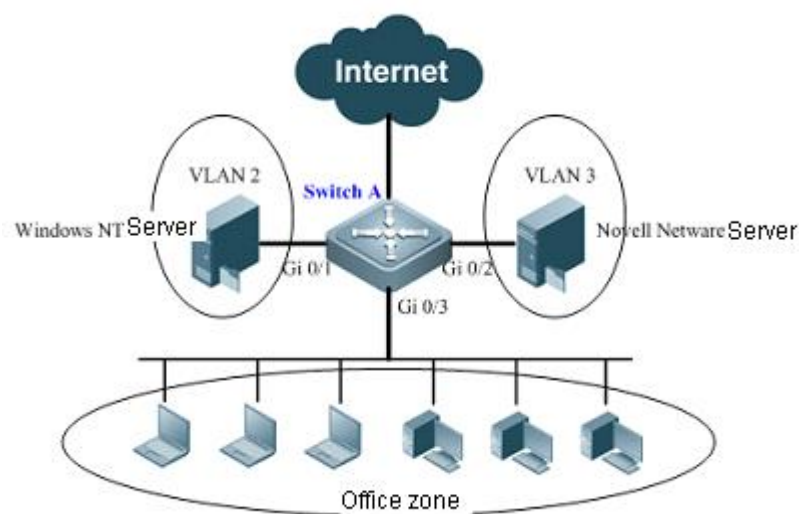
Command	Description
Ruijie# <b>show protocol-vlan</b>	Show a protocol VLAN.

```
Ruijie# show protocol-vlan
ip          mask          vlan
-----
192.168.100.3 255.255.255.0 100
profile      frame-type  ether-type  Interfaces|vid
-----
1            ETHERII   EHTER_AARP  gi3/1|101
2            SNAP     ETHER_APPLETALK gi3/1|1
```

## Typical Protocol VLAN Configuration Examples

### Example of protocol-based VLAN configuration

#### Network Topology



### Diagram for protocol-based VLAN configuration

## Application Requirements

The above figure shows the structure of a Windows NT and Novell Netware interconnected network. The office zone is connected to the layer-3 device of Switch A through Hub. There are different PC users distributed in the office zone, with certain users using Windows NT operating system and supporting IP protocol and other users using Novell Netware operating system and supporting IPX protocol. The entire office zone is connected to Internet and server via the uplink port of Gi 0/3.

Networking requirement:

- Implement layer-2 isolation between Windows NT users and Novell Netware users in order to lessen network traffic.

## Configuration Tips

### Configuration tips:

1. Configure packet type and Ethernet type profiles (in this example, IP packets correspond to Profile 1, and IPX packets correspond to Profile 2).
2. Apply the profile to the uplink port (Gi 0/3) and associate with the VLAN (in this example, associate Profile 1 with VLAN 2 and Profile 2 with VLAN 3).

### Notes:

1. Protocol-based VLAN can only apply to Trunk port and Hybrid port, which can directly connect with Hub or user PCs.
2. PC user can determine its IP network segment according to the protocol-based VLAN (network segment configuration for each VLAN won't be described herein).

## Configuration Steps

### Configure Switch A

Step 1: Enter global configuration mode and create VLAN 2 and VLAN 3.

```
Ruijie#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Ruijie(config)#vlan range 2,3
Ruijie(config-vlan-range)#exit
```

Step 2: Since Windows NT server and Novell Netware server are directly connected with Gi 0/1 and Gi 0/2, we can configure port-based VLANs.

```
Ruijie(config)#interface gigabitEthernet 0/1
Ruijie(config-GigabitEthernet 0/1)#switchport access vlan 2
Ruijie(config-GigabitEthernet 0/1)#exit
Ruijie(config)#interface gigabitEthernet 0/2
Ruijie(config-GigabitEthernet 0/2)#switchport access vlan 3
Ruijie(config-GigabitEthernet 0/2)#exit
```

**Step 3: Configure uplink port Gi 0/3 as a Trunk port.**

```
Ruijie(config)#interface gigabitEthernet 0/3
Ruijie(config-GigabitEthernet 0/3)#switchport mode trunk
```

**Step 4: Configure the corresponding Profile 1 and Profile 2 for IP protocol and IPX protocol respectively (assuming that Ethernet II encapsulation is used, the Ethernet types of IP and IPX are 0X0800 and 0X8137 respectively)**

```
Ruijie(config)#protocol-vlan profile 1 frame-type eTHERII ether-type 0x0800
Ruijie(config)#protocol-vlan profile 2 frame-type eTHERII ether-type 0x8137
```

**Step 5: Apply Profile 1 and Profile 2 to Gi 0/3 in order to classify VLAN 2 and VLAN 3. IP packets received on the port will belong to VLAN 2, and IPX packets received on the port will belong to VLAN 3.**

```
Ruijie(config-GigabitEthernet 0/3)#protocol-vlan profile 1 vlan 2
Ruijie(config-GigabitEthernet 0/3)#protocol-vlan profile 2 vlan 3
Ruijie(config-GigabitEthernet 0/3)#exit
```

**Verification****Step 1: Display configurations of Switch A. Key points: whether profiles have been properly configured for the Protocol VLAN, and whether the port applied with profiles has been properly configured.**

```
Ruijie#show running-config
!
vlan 2
!
vlan 3
!
protocol-vlan profile 1 frame-type ETHERII ether-type 0x800
protocol-vlan profile 2 frame-type ETHERII ether-type 0x8137
!
interface GigabitEthernet 0/1
  switchport access vlan 2
!
interface GigabitEthernet 0/2
  switchport access vlan 3
!
interface GigabitEthernet 0/3
  switchport mode trunk
  protocol-vlan profile 1 vlan 2
  protocol-vlan profile 2 vlan 3
!
```

**Step 2: Display the type of protocol packets matched by profile and the corresponding port number and VLAN ID.**

```
Ruijie#show protocol-vlan profile
```

```
profile frame-type ether-type/DSAP+SSAP interface vlan
```

```
-----
1      ETHERII    0x800                      Gi0/3      2
2      ETHERII    0x8137                     Gi0/3      3
```

## Example of IP address based VLAN configuration

### Network Topology

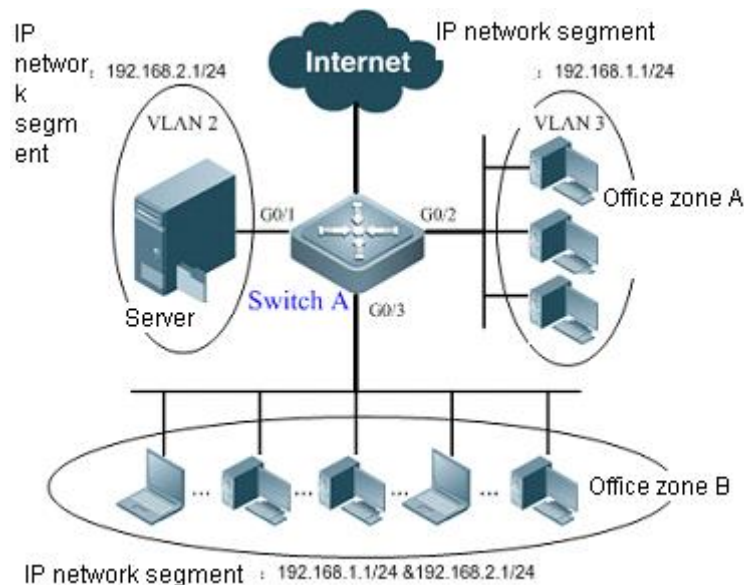


Diagram for IP address based VLAN configuration

### Application Requirements

Office zone A and office zone B are connected to the elayer-3 device of Switch A through hubs. Office users falling within the fixed network segment are distributed in office zone A and belong to a port-based VLAN. Office zone B is distributed by office users falling within two different network segments, and port-based VLAN cannot be realized in this zone.

Networking requirements

- For PC users from office zone B, Switch A shall be able to determine their VLAN according to the IP network segment of packets.

### Configuration Tips

#### Configuration tips:

Globally configure IP address based VLANs (in this example, IP network segment of 192.168.1.1/24 belongs to VLAN 3, and IP network segment of 192.168.2.1/24 belongs to VLAN 2), and enable IP address based VLAN on the uplink port (Gi 0/3).

#### Notes:

IP address based VLAN can only apply to Trunk port and Hybrid port, which can directly connect with Hub or

user PCs.

## Configuration Steps

### Configure Switch A

**Step 1: Enter global configuration mode and create VLAN 2 and VLAN 3.**

```
Ruijie#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Ruijie(config)#vlan range 2-3
Ruijie(config-vlan-range)#exit
```

**Step 2: Configure G0/3 as a Trunk port.**

```
Ruijie(config)#interface gigabitEthernet 0/3
Ruijie(config-GigabitEthernet 0/3)#switchport mode trunk
Ruijie(config-GigabitEthernet 0/3)#exit
```

**Step 3: Since the server is directly connected with port Gi 0/1, this port can be configured to belong to VLAN 2.**

```
Ruijie(config)#interface gigabitEthernet 0/1
Ruijie(config-GigabitEthernet 0/1)#switchport access vlan 2
Ruijie(config-GigabitEthernet 0/1)#exit
```

**Step 4: Configure port Gi 0/2 to belong to VLAN 3.**

```
Ruijie(config)#interface gigabitEthernet 0/2
Ruijie(config-GigabitEthernet 0/2)#switchport access vlan 3
Ruijie(config-GigabitEthernet 0/2)#exit
```

**Step 5: Associate IP network segment of 192.168.1.1/24 with VLAN 3 and IP network segment of 192.168.2.1/24 with VLAN 2.**

```
Ruijie(config)#protocol-vlan ipv4 192.168.1.1 mask 255.255.255.0 vlan 3
Ruijie(config)#protocol-vlan ipv4 192.168.2.1 mask 255.255.255.0 vlan 2
```

**Step 6: On port Gi 0/3, enable IP address based VLAN classification.**

```
Ruijie(config)#interface gigabitEthernet 0/3
Ruijie(config-GigabitEthernet 0/3)# protocol-vlan ipv4
```

## Verification

**Step 1: Display configurations of Switch A. Key points: whether IP address based VLAN classification has been properly configured, and whether the uplink port has been configured as a Trunk port.**

```
Ruijie#show running-config
!
vlan 1
!
vlan 2
!
```

```
vlan 3
!
protocol-vlan ipv4 192.168.1.1 mask 255.255.255.0 vlan 3
protocol-vlan ipv4 192.168.2.1 mask 255.255.255.0 vlan 2
!
interface GigabitEthernet 0/1
    switchport access vlan 2
!
interface GigabitEthernet 0/2
    switchport access vlan 3
!
interface GigabitEthernet 0/3
    switchport mode trunk
!
```

**Step 2: Display the policy configured for matching IP network segment and VLAN ID.**

```
Ruijie#show protocol-vlan ipv4
```

ip	mask	vlan
192.168.1.1	255.255.255.0	3
192.168.2.1	255.255.255.0	2



# Private VLAN Configuration

## Private VLAN Technology

If the service provider offers a VLAN to each subscriber, the service provider supports a limited number of subscribers because one device supports 4096 VLANs at most. On the layer 3 device, each VLAN is assigned with a subnet address or a series of addresses, which results in a waste of IP addresses. In this case, private VLAN comes into being.

A private VLAN divides the layer 2 broadcast domain of a VLAN into several sub domains. Each sub domain consists of a private VLAN pair: primary VLAN and secondary VLAN.

A private VLAN domain can have multiple private VLAN pairs, and each VLAN pair represents a sub domain. All the private VLAN pairs in one private VLAN domain share a primary VLAN. Each sub domain has a different secondary VLAN IDs.

There is only one primary VLAN in each private VLAN domain. The secondary VLAN is used for layer 2 separation in the same private VLAN domain. There are two types of secondary VLANs:

- Isolated VLAN: Layer 2 communication is not possible for the ports in the same isolated VLAN. There is only one isolated VLAN in a private VLAN domain.
- Community VLAN: The ports in the same community VLAN can perform layer 2 communication, but not with the ports in other community VLANs. There can be multiple community VLANs in a private VLAN domain.

Promiscuous port, a port in the primary VLAN, can communicate with any port, including the isolated port and community port of the secondary VLAN in the same private VLAN.

Promiscuous Trunk Port, can be the member port of multiple ordinary VLANs and private VLANs, and can communicate with any port in the same VLAN. In the ordinary VLAN, packet forwarding follows the 802.1Q rule. In the private VLAN, the VID for the tagged packet forwarded from the promiscuous Trunk port, is the VID for the primary VLAN.

Isolated port, a port in the isolated VLAN, can only communicate with the promiscuous port. The packets received on the isolated port are allowed to be forwarded to the Trunk Port, but the packets in the isolated VLAN received on the Trunk Port cannot be forwarded to the isolated port.

Isolated Trunk Port, can be the member port of multiple ordinary VLANs and PVLANS. In the isolated VLAN, the isolated trunk port can only communicate with the promiscuous port; in the community VLAN, it can communicate with the community ports in the same community VLAN and the promiscuous port; in the ordinary VLAN, it follows the 802.1Q rule. The packets in the isolated VLAN received on the isolated trunk port are allowed to be forwarded to the Trunk Port, but the packets in the isolated VLAN received on the Trunk Port cannot be forwarded to the isolated port.

The VID for the tagged packet forwarded from the promiscuous Trunk port, is the VID for the secondary VLAN.

Community port, a port in the community VLAN, can communicate with other community ports in the same community VLAN as well as the promiscuous port in the primary VLAN. However, they cannot communicate with the community ports in other community VLANs and isolated ports in the isolated VLANs.

The following list shows the packet forwarding relationship between various port types:

Output Port Input Port	Promiscuous Port	Isolated Port	Community Port	Isolated Trunk Port (In the same VLAN)	Promiscuous Trunk Port (In the same VLAN)	Trunk Port (In the same VLAN)
Promiscuous port	√	√	√	√	√	√
Isolated Port	√	X	X	X	√	√
Community Port	√	X	√	√	√	√
Isolated Trunk Port (In the same VLAN)	√	X	√	X	√	√
Promiscuous Trunk Port (In the same VLAN)	√	√	√	√	√	√
Trunk Port (In the same VLAN)	√	X	√	X	√	√

The following list shows the whether the VLAN TAG changes or not after the packet forwarding between various port types:

Output Port Input Port	Promiscuous Port	Isolated Port	Community Port	Isolated Trunk Port (In the same VLAN)	Promiscuous Trunk Port (In the same VLAN)	Trunk Port (In the same VLAN)
Promiscuous port	Unchanged	Unchanged	Unchanged	Add the secondary VLAN ID	Add the primary VLAN ID TAG, and unchanged in the other non-private VLAN.	Add the primary VLAN ID TAG
Isolated Port	Unchanged	N/A	N/A	N/A	Add the primary VLAN ID TAG, and unchanged in	Add the isolated VLAN ID TAG

					the other non-private VLAN.	
Community Port	Unchanged	N/A	Unchanged	Add the community VLAN ID TAG	Add the primary VLAN ID TAG, and unchanged in the other non-private VLAN.	Add the community VLAN ID TAG
Isolated Trunk Port (In the same VLAN)	Remove the VLAN TAG	N/A	Remove the VLAN TAG	Unchanged in the non-isolated VLAN.	Add the primary VLAN ID TAG, and unchanged in the other non-private VLAN.	Unchanged
Promiscuous Trunk Port (In the same VLAN)	Remove the VLAN TAG	Unchanged	Unchanged	Add the secondary VLAN ID	Add the primary VLAN ID TAG, and unchanged in the other non-private VLAN.	Unchanged
Trunk Port (In the same VLAN)	Remove the VLAN TAG	N/A	Remove the VLAN TAG	Change to the secondary VLAN ID in the primary VLAN; Unchanged in other non-isolated VLAN.	Add the primary VLAN ID TAG, and unchanged in the other non-private VLAN.	Unchanged
Switch CPU	Untag	Untag	Untag	Add the secondary VLAN ID TAG	Add the primary VLAN ID TAG, and unchanged in the other non-private VLAN.	Add the primary VLAN ID TAG

In a private VLAN, an SVI interface can be created for the primary VLAN rather than the secondary VLANs. A port in the private VLAN can be a SPAN source port instead of a mirrored destination port.

## Configuring a Private VLAN

### Default Private VLAN Configuration

No Private VLAN is configured by default.

### Configuring a VLAN as a Private VLAN

To configure a VLAN as a private VLAN, execute the following commands:

Command	Description
<b>configure terminal</b>	Enter the global configuration mode.
<b>vlan <i>vid</i></b>	Enter the VLAN configuration mode.
<b>private-vlan{community   isolated  primary}</b>	Configure a private VLAN.
<b>no private-vlan{community   isolated   primary}</b>	Remove the configured private VLAN.
<b>end</b>	Exit the VLAN configuration mode.
<b>show vlan private-vlan [<i>type</i>]</b>	Show a private VLAN



#### Note

The member port in the 802.1Q VLAN cannot be declared as a private VLAN. VLAN 1 cannot be declared as a private VLAN as well. If there is a trunk or uplink port in the 802.1Q VLAN, first delete this VLAN from the allowed VLAN list. The following conditions must be met in order to make a private VLAN become active:

1. The primary VLAN is available.
2. The secondary VLANs are available.
3. The secondary VLANs are associated with the primary VLAN.

The following example configures 802.1Q VLAN as a private VLAN:

```
Ruijie# configure terminal
Ruijie(config)# vlan 303
Ruijie(config-vlan)# private-vlan community
Ruijie(config-vlan)# end
Ruijie# show vlan private-vlan community
VLAN Type Status Routed Interface Associated VLANs
---
303 comm inactive Disabled no association
Ruijie#configure terminal
Ruijie(config)#vlan 404
Ruijie(config-vlan)# private-vlan isolated
Ruijie(config-vlan)# end
```

```
Ruijie# show vlan private-vlan
VLAN Type Status Routed Interface Associated VLANs
---
303 comm inactive Disabled no association
404 isol inactive Disabled no association
```

## Associating the Secondary VLANs with the Primary VLAN

To associate the secondary VLANs with the primary VLAN, execute the following commands:

Command	Description
<b>configure terminal</b>	Enter the global configuration mode.
<b>vlan <i>p_vid</i></b>	Enter the primary VLAN configuration mode.
<b>private-vlan association</b> <b>{svlist   add svlist   remove svlist}</b>	Associate with the secondary VLANs.
<b>no private-vlan association</b>	Remove the association with all the secondary VLANs.
<b>end</b>	Exit the VLAN mode.
<b>show vlan private-vlan [<i>type</i>]</b>	Show the private VLAN

For example:

```
Ruijie# configure terminal
Ruijie(config)# vlan 202
Ruijie(config-vlan)# private-vlan association 303-307,309,440
Ruijie(config-vlan)# end
Ruijie# show vlan private-vlan
VLAN Type Status Routed Interface Associated VLANs
---
202 prim inactive Disabled 303-307,309,440
303 comm inactive Disabled 202
304 comm inactive Disabled 202
305 comm inactive Disabled 202
306 comm inactive Disabled 202
307 comm inactive Disabled 202
309 comm inactive Disabled 202
440 comm inactive Disabled 202
```



### Note

This operation is performed in the configuration mode of the VLAN declared as the primary VLAN.

## Mapping Secondary VLANs to the Layer 3 Interface of the Primary VLAN

To map the secondary VLANs to the layer 3 interface of the primary VLAN, execute the following commands:

Command	Description
<b>configure terminal</b>	Enter the global configuration mode.

Command	Description
<b>interface vlan</b> <i>p_vid</i>	Enter the interface configuration mode of the primary VLAN.
<b>private-vlan mapping</b> <b>{svlist   add svlist   remove svlist}</b>	Map the secondary VLANs to the layer 3 SVI of the primary VLAN.
<b>end</b>	Exit the interface configuration mode.

The following example configures Secondary VLAN routing:

```
Ruijie# configure terminal
Ruijie(config)# interface vlan 202
Ruijie(config-if)# private-vlan mapping add 303-307,309,440
Ruijie(config-if)# end
Ruijie#
```



#### Note

The primary VLAN and the secondary VLANs in this process are associated.

## Configuring a Layer 2 Interface as the Host Port of a Private VLAN

To configure a layer 2 interface as the Host Port of a private VLAN, execute the following commands:

Command	Description
<b>configure terminal</b>	Enter the global configuration mode.
<b>interface</b> <interface>	Enter the interface configuration mode. Three kinds of interfaces are available: fastethernet, GE and 10GE.
<b>switchport mode private-vlan host</b>	Configure the interface as the host interface of the private VLAN.
<b>no switchport mode</b>	Remove the configuration.
<b>End</b>	Exit the interface mode.
<b>switchport private-vlan host-association</b> <i>p_vid s_vid</i>	Associate the layer 2 interface with the private VLAN.
<b>no switchport private-vlan host-association</b>	Remove the association.

For example:

```
Ruijie# configure terminal
Ruijie(config)# interface gigabitEthernet 0/2
Ruijie(config-if)# switchport mode private-vlan host
Ruijie(config-if)# switchport private-vlan host-association
202 203
Ruijie(config-if)# end
```

**Note**

The primary VLAN and the secondary VLANs in this process are associated.

## Configuring a Layer 2 Interface as the Isolated PVLAN Trunk Port

To configure a layer 2 interface as the isolated trunk port in the PVLAN, execute the following commands:

Command	Description
Ruijie# <b>configure terminal</b>	Enter the global configuration mode.
Ruijie(config-if)# <b>interface</b> <interface>	Enter the interface configuration mode. Three kinds of interfaces are available: Megabit, Gigabit, 10 Gigabit.
Ruijie(config-if)# <b>switchport mode trunk</b>	Configure the trunk mode.
Ruijie(config-if)# <b>switchport private-vlan association trunk</b> <i>p_vid s_vid</i> OR: Ruijie(config-if)# <b>no switchport private-vlan association trunk</b> <i>p_vid s_vid</i>	Associate the Layer2 port and the private VLAN. <i>p_vid</i> : primary vlan id; <i>s_vid</i> : secondary vlan id.  Remove the configuration.
Ruijie(config-if)# <b>switchport trunk allowed vlan {all   [add   remove   except] } vlan-list</b>	(Optional) Configure the allowed VLAN list on the Trunk port.  <b>all</b> : all supported VLANs in the allowed VLAN list; <b>add</b> : add the specified VLAN list to the allowed VLAN list; <b>remove</b> : remove the specified VLAN from the allowed VLAN list; <b>except</b> : add all VLANs beyond the VLAN list to the allowed VLAN list.  <i>vlan-list</i> : can be a VLAN, or a series of VLAN, for example, 10-20.
Ruijie(config-if)# <b>switchport trunk native vlan</b> <i>vlan-id</i>	Configure the Native VLAN Use the <b>no switchport trunk native</b> command in the interface configuration mode to restore the Trunk Native VLAN list to the default VLAN1.

For example:

```
Ruijie# configure terminal
Ruijie(config)# interface gigabitEthernet 0/2
```

```

Ruijie(config-if)# switchport mode trunk
Ruijie(config-if)# switchport private-vlan association trunk 202 203
Ruijie(config-if)# switchport trunk allowed vlan 100
Ruijie(config-if)# switchport trunk native vlan 100
Ruijie(config-if)# end
Ruijie#

```

## Configuring a Layer 2 Interface as the Promiscuous Trunk Port

To configure a layer 2 interface as the promiscuous trunk port in the PVLAN, execute the following commands:

Command	Description
Ruijie# <b>configure terminal</b>	Enter the global configuration mode.
Ruijie(config-if)# <b>interface</b> <i>&lt;interface&gt;</i>	Enter the interface configuration mode. Three kinds of interfaces are available: Megabit, Gigabit, 10 Gigabit.
Ruijie(config-if)# <b>switchport mode trunk</b>	Configure the trunk mode.
Ruijie(config-if)# <b>switchport private-vlan promiscuous trunk</b> <i>p_vid s_vid</i>	Associate the Layer2 port with the private VLAN. Multiple pairs can be configured. <i>p_vid</i> : primary vlan id; <i>s_vid</i> : secondary vlan id.
Ruijie(config-if)# <b>no switchport private-vlan promiscuous trunk</b> <i>p_vid s_vid</i>	Remove the configuration.
Ruijie(config-if)# <b>switchport trunk allowed vlan {all   [add   remove   except] } vlan-list</b>	(Optional) Configure the allowed VLAN list on the Trunk port. <b>all</b> : all supported VLANs in the allowed VLAN list; <b>add</b> : add the specified VLAN list to the allowed VLAN list; <b>remove</b> : remove the specified VLAN from the allowed VLAN list; <b>except</b> : add all VLANs beyond the VLAN list to the allowed VLAN list. <i>vlan-list</i> : can be a VLAN, or a series of VLAN, for example, 10-20.



Command	Description
<b>Ruijie(config-if)# switchport trunk native vlan <i>vlan-id</i></b>	Configure the Native VLAN Use the <b>no switchport trunk native vlan</b> command in the interface configuration mode to restore the Trunk Native VLAN list to the default VLAN1.

For example:

```
Ruijie# configure terminal
Ruijie(config)# interface gigabitEthernet 0/2
Ruijie(config-if)# switchport mode trunk
Ruijie(config-if)# switchport private-vlan promiscuous trunk 202 203
Ruijie(config-if)# switchport trunk allowed vlan 100
Ruijie(config-if)# switchport trunk native vlan 100
Ruijie(config-if)# end
Ruijie#
```



#### Note

The primary VLAN and the secondary VLANs in this process are associated.

## Configuring a Layer 2 Interface as the Promiscuous Port of a Private VLAN

To configure a layer 2 interface as the promiscuous port of a private VLAN, execute the following commands:

Command	Description
<b>configure terminal</b>	Enter the global configuration mode.
<b>interface &lt;interface&gt;</b>	Enter the interface configuration mode. Three kinds of interfaces are available: Megabit, Gigabit, 10 Gigabit.
<b>switchport mode private-vlan promiscuous</b>	Configure the interface as the promiscuous port of the private VLAN.
<b>no switchport mode</b>	Remove the configuration.
<b>switchport private-vlan mapping p_vid{svlist   add svlist   remove svlist}</b>	Map the secondary VLANs to the promiscuous port.
<b>no switchport private-vlan mapping</b>	Remove the mapping.

For example:

```
Ruijie# configure terminal
Ruijie(config)# interface gigabitEthernet 0/2
Ruijie(config-if)# switchport mode private-vlan promiscuous
Ruijie(config-if)# switchport private-vlan mapping 202 add 203
Ruijie(config-if)# end
```

**Note**

The primary VLAN and the secondary VLANs in this process are associated.

## Showing a Private VLAN

### Showing a Private VLAN

To show a private VLAN, execute the following command:

Command	Description
<b>show vlan private-vlan</b> [ <i>type</i> ]	Show the private VLAN.

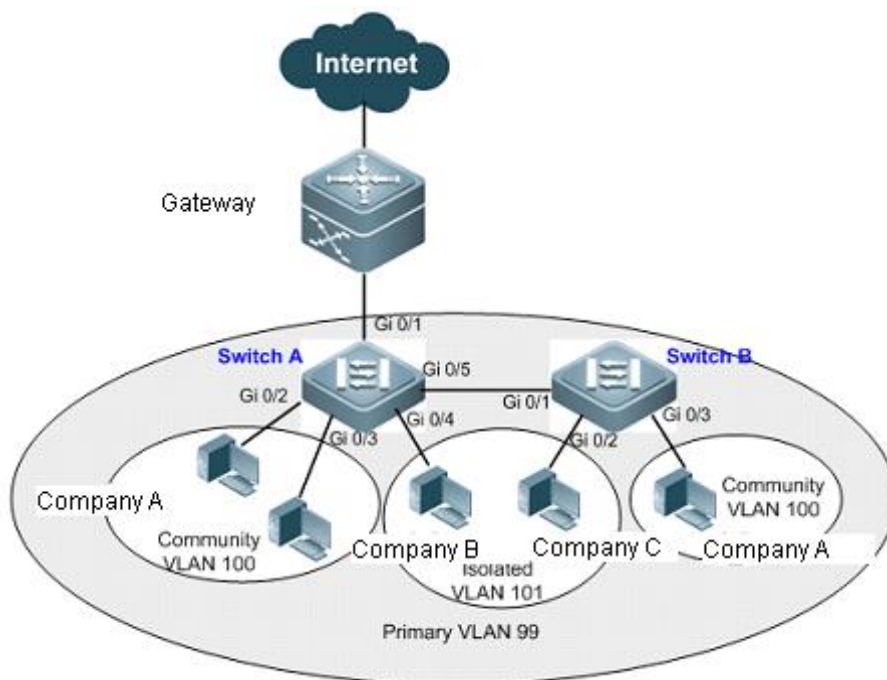
```
Ruijie# show vlan private-vlan
```

VLAN	Type	Status	Routed	Interface	Associated VLANs
202	prim	active	Enabled	Gi0/1	303-307, 309, 440
303	comm	active	Disabled	Gi0/2	202
304	comm	active	Disabled	Gi0/3	202
305	comm	active	Disabled	Gi0/4	202
306	comm	active	Disabled		202
307	comm	active	Disabled		202
309	comm	active	Disabled		202
440	comm	active	Enabled	Gi0/5	202

## Typical PVLAN Configuration Examples

### PVLAN Cross-device Layer-2 Application

#### Topological Diagram



**Topology for PVLAN cross-device layer-2 application**

#### Application Requirements

As shown above, in a hosting service network, company users access the network via Switch A and Switch B. The following requirements must be met:

- Intra-company users shall be able to communicate with each other, while inter-company users shall be isolated from each other.
- All company users share a same gateway address and are able to access Internet.

#### Configuration Tips

- Configuration tips are shown below:

1. All companies shall belong to the same PVLAN (Primary VLAN 99), and users from all companies share a layer-3 interface through this VLAN to communicate with Internet.
2. If there are multiple users in a company, respective companies shall belong to different Community VLANs (company A belonging to Community VLAN 100), so that intra-company users can communicate with each other and inter-company users are isolated from each other.
3. If there is only one user in a company, such companies shall belong to the same Isolated VLAN (company B and company C belonging to Isolated VLAN 101), so that inter-company users are isolated from each other.

- Configuration tips are shown below:

1. To run PVLAN across device, you need to configure the interconnected ports to Trunk Ports.
2. The gateway-connecting port shall be configured as Promiscuous Port; the peer port (interface of gateway device) can be configured as Trunk Port or Hybrid Port, and the Native VLAN shall be the Primary VLAN of PVLAN.

## Configuration Steps

Step 1: Create Primary VLAN and Secondary VLAN on the device.

! Configure Primary VLAN 99, Community VLAN 100 and Isolated VLAN 101 on Switch A.

```
SwitchA#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
SwitchA(config)#vlan 99
SwitchA(config-vlan)#private-vlan primary
SwitchA(config-vlan)#exit
SwitchA(config)#vlan 100
SwitchA(config-vlan)#private-vlan community
SwitchA(config-vlan)#exit
SwitchA(config)#vlan 101
SwitchA(config-vlan)#private-vlan isolated
SwitchA(config-vlan)#exit
```

! Configurations of Switch B are the same as above.

Step 2: Associate Secondary VLAN and Primary VLAN on the device.

! Associate Community VLAN 100, Isolated VLAN 101 and Primary VLAN 99 on Switch A.

```
SwitchA(config)#vlan 99
SwitchA(config-vlan)#private-vlan association 100-101
SwitchA(config-vlan)#exit
```

! Configurations of Switch B are the same as above.

Step 3: Configure the uplink port for connecting gateway device.

! Configure port Gi 0/1 of Switch A as Promiscuous Port

```
SwitchA(config)#interface gigabitEthernet 0/1
SwitchA(config-if-GigabitEthernet 0/1)#switchport mode private-vlan promiscuous
SwitchA(config-if-GigabitEthernet 0/1)#switchport private-vlan mapping 99 100-101
SwitchA(config-if-GigabitEthernet 0/1)#exit
```

Step 4: Associate the user access ports of respective companies to the corresponding Secondary VLANs (as shown in the above figure).

! On Switch A, associate port Gi 0/2 and Gi 0/3 to Community VLAN 100 and associate port Gi 0/4 to Isolated VLAN 101.

```
SwitchA(config)#interface range gigabitEthernet 0/2-3
SwitchA(config-if-range)#switchport mode private-vlan host
SwitchA(config-if-range)#switchport private-vlan host-association 99 100
SwitchA(config-if-range)#exit
SwitchA(config)#interface gigabitEthernet 0/4
SwitchA(config-if-GigabitEthernet 0/4)#switchport mode private-vlan host
SwitchA(config-if-GigabitEthernet 0/4)#switchport private-vlan host-association 99 101
```

! On Switch B, associate port Gi 0/2 to Isolated VLAN 101 and associate port Gi 0/3 to Community VLAN 100.

```
SwitchB(config)#interface gigabitEthernet 0/2
SwitchB(config-if-GigabitEthernet 0/2)#switchport mode private-vlan host
SwitchB(config-if-GigabitEthernet 0/2)# switchport private-vlan host-association 99 101
SwitchB(config-if-GigabitEthernet 0/2)#exit
SwitchB(config)#interface gigabitEthernet 0/3
SwitchB(config-if-GigabitEthernet 0/3)#switchport mode private-vlan host
SwitchB(config-if-GigabitEthernet 0/3)# switchport private-vlan host-association 99 100
SwitchB(config-if-GigabitEthernet 0/3)#exit
```

**Step 5: Configure the connection ports for running PVLAN across device.**

**! Configure port Gi 0/5 of Switch A as Trunk Port**

```
SwitchA(config)#interface gigabitEthernet 0/5
SwitchA(config-if-GigabitEthernet 0/5)#switchport mode trunk
SwitchA(config-if-GigabitEthernet 0/5)#exit
```

**! Configure port Gi 0/1 of Switch B as Trunk Port.**

```
SwitchB(config)#interface gigabitEthernet 0/1
SwitchB(config-if-GigabitEthernet 0/1)#switchport mode trunk
SwitchB(config-if-GigabitEthernet 0/1)#exit
```

## Verify Configurations

**Step 1: Display configurations of respective devices.**

**! Configurations of Switch A**

```
SwitchA#show running-config
!
vlan 99
  private-vlan primary
  private-vlan association add 100-101
!
vlan 100
  private-vlan community
!
vlan 101
  private-vlan isolated
!
interface GigabitEthernet 0/1
  switchport mode private-vlan promiscuous
  switchport private-vlan mapping 99 add 100-101
!
interface GigabitEthernet 0/2
  switchport mode private-vlan host
  switchport private-vlan host-association 99 100
!
interface GigabitEthernet 0/3
  switchport mode private-vlan host
  switchport private-vlan host-association 99 100
```

```

!
interface GigabitEthernet 0/4
    switchport mode private-vlan host
    switchport private-vlan host-association 99 101
!
interface GigabitEthernet 0/5
    switchport mode trunk
!

```

### ! Configurations of Switch B

```

SwitchB#show running-config
!
vlan 99
    private-vlan primary
    private-vlan association add 100-101
!
vlan 100
    private-vlan community
!
vlan 101
    private-vlan isolated
!
interface GigabitEthernet 0/1
    switchport mode trunk
!
interface GigabitEthernet 0/2
    switchport mode private-vlan host
    switchport private-vlan host-association 99 101
!
interface GigabitEthernet 0/3
    switchport mode private-vlan host
    switchport private-vlan host-association 99 100
!

```

**Step 2: Display PVLAN-related configurations on respective devices.**

```

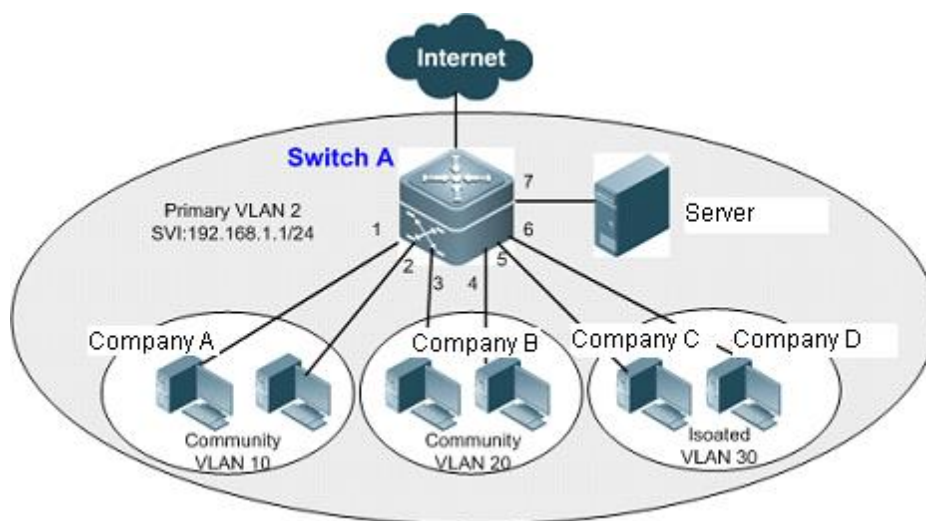
SwitchA#show vlan private-vlan

```

VLAN	Type	Status	Routed	Ports	Associated VLANs
99	primary	active	Disabled	Gi0/1, Gi0/5	100-101
100	community	active	Disabled	Gi0/2, Gi0/3, Gi0/5	99
101	isolated	active	Disabled	Gi0/4, Gi0/5	99

## Layer-3 Application of PVLAN on a Single Device

### Topological Diagram



Topology for layer-3 application of PVLAN on a single device

### Application Requirements

As shown above, in a hosting service network, company users access the network via the layer-3 device of Switch A. The following requirements must be met:

- Intra-company users shall be able to communicate with each other, while inter-company users shall be isolated from each other.
- All company users can access the server.
- All company users share a same gateway address and are able to access Internet.

### Configuration Tips

- 1) Configure PVLAN on the device (Switch A). For detailed configurations, please refer to the configurations described in the section of "PVLAN Cross-device Layer-2 Application".
- 2) Configure the server-connecting port (Gi 0/7) as the Promiscuous Port. All company users can communicate with the server via Promiscuous Port.
- 3) On the layer-3 device (Switch A), configure the gateway address of PVLAN (configure SVI of VLAN2 as 192.168.1.1/24) and configure the layer-3 port mapping of Primary VLAN (VLAN 2) and Secondary VLAN (VLAN 10, 20 and 30). All company users can access Internet via this gateway address.

### Configuration Steps

Step 1: Create Primary VLAN and Secondary VLAN on the device.

! Configure Primary VLAN 2, Community VLAN 10, Community VLAN 20 and Isolated VLAN 30 on Switch A.

```
SwitchA#configure terminal
```

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

```
SwitchA(config)#vlan 2
SwitchA(config-vlan)#private-vlan primary
SwitchA(config-vlan)#exit
SwitchA(config)#vlan 10
SwitchA(config-vlan)#private-vlan community
SwitchA(config-vlan)#exit
SwitchA(config)#vlan 20
SwitchA(config-vlan)#private-vlan community
SwitchA(config-vlan)#exit
SwitchA(config)#vlan 30
SwitchA(config-vlan)#private-vlan isolated
SwitchA(config-vlan)#exit
```

**Step 2: Associate Secondary VLAN and Primary VLAN on the device.**

**! Associate Community VLAN 10, Community VLAN 20, Isolated VLAN 30 and Primary VLAN 2 on Switch A.**

```
SwitchA(config)#vlan 2
SwitchA(config-vlan)#private-vlan association 10,20,30
SwitchA(config-vlan)#exit
```

**Step 3: Associate the user access ports of respective companies to the corresponding Secondary VLANs (as shown in the above figure).**

**! On Switch A, associate ports Gi 0/1 and Gi 0/2 to Community VLAN 10, associate ports Gi 0/3 and Gi 0/4 to community VLAN 20, and associate ports Gi 0/5 and Gi 0/6 to Isolated VLAN 30.**

```
SwitchA(config)#interface range gigabitEthernet 0/1-2
SwitchA(config-if-range)#switchport mode private-vlan host
SwitchA(config-if-range)#switchport private-vlan host-association 2 10
SwitchA(config-if-range)#exit
SwitchA(config)#interface range gigabitEthernet 0/3-4
SwitchA(config-if-range)#switchport mode private-vlan host
SwitchA(config-if-range)#switchport private-vlan host-association 2 20
SwitchA(config-if-range)#exit
SwitchA(config)#interface range gigabitEthernet 0/5-6
SwitchA(config-if-range)#switchport mode private-vlan host
SwitchA(config-if-range)#switchport private-vlan host-association 2 30
SwitchA(config-if-range)#exit
```

**Step 4: Configure the server-connecting port.**

**! Configure port Gi 0/7 of Switch A as Promiscuous Port**

```
SwitchA(config)#interface gigabitEthernet 0/7
SwitchA(config-if-GigabitEthernet 0/7)#switchport mode private-vlan promiscuous
SwitchA(config-if-GigabitEthernet 0/7)#switchport private-vlan mapping 2 10,20,30
SwitchA(config-if-GigabitEthernet 0/7)#exit
```

**Step 5: Configure the gateway address of PVLAN on layer-3 device.**

**! On Switch A, configure the SVI of Primary VLAN 2 as 192.168.1.1/24, and configure Community VLAN 10, Community VLAN 20 and Isolated VLAN 30 mapping.**

```
SwitchA(config)#interface vlan 2
SwitchA(config-if-VLAN 2)#ip address 192.168.1.1 255.255.255.0
SwitchA(config-if-VLAN 2)#private-vlan mapping 10,20,30
```



```
SwitchA(config-if-VLAN 2)#exit
```

## Verify Configurations

### Step 1: Display the configurations of Switch A.

```
SwitchA#show running-config
!
vlan 2
    private-vlan primary
    private-vlan association add 10,20,30
!
vlan 10
    private-vlan community
!
vlan 20
    private-vlan community
!
vlan 30
    private-vlan isolated
!
interface GigabitEthernet 0/1
    switchport mode private-vlan host
    switchport private-vlan host-association 2 10
!
interface GigabitEthernet 0/2
    switchport mode private-vlan host
    switchport private-vlan host-association 2 10
!
interface GigabitEthernet 0/3
    switchport mode private-vlan host
    switchport private-vlan host-association 2 20
!
interface GigabitEthernet 0/4
    switchport mode private-vlan host
    switchport private-vlan host-association 2 20
!
interface GigabitEthernet 0/5
    switchport mode private-vlan host
    switchport private-vlan host-association 2 30
!
interface GigabitEthernet 0/6
    switchport mode private-vlan host
    switchport private-vlan host-association 2 30
!
interface GigabitEthernet 0/7
```

```
switchport mode private-vlan promiscuous
switchport private-vlan mapping 2 add 10,20,30
!
interface VLAN 2
no ip proxy-arp
ip address 192.168.1.1 255.255.255.0
private-vlan mapping add 10,20,30
!
```

**Step 2: Display PVLAN-related configurations.**

```
SwitchA#show vlan private-vlan
```

VLAN	Type	Status	Routed	Ports	Associated VLANs
2	primary	active	Enabled	Gi0/7	10,20,30
10	community	active	Enabled	Gi0/1, Gi0/2	2
20	community	active	Enabled	Gi0/3, Gi0/4	2
30	isolated	active	Enabled	Gi0/5, Gi0/6	2

# Share VLAN Configuration

## Overview

As a VLAN sharing addresses, the Share VLAN can solve the problem that the packets to this MAC address will be broadcast in another VLAN while the switch learns a MAC address in a VLAN. When a VLAN is set to be the Share VLAN, however, it will replicate its learned dynamic and static MAC addresses to other VLANs, and other VLANs also replicate their learned dynamic and static MAC addresses to the Share VLAN. The address triggering this address application procedure is called home address and the replicated addresses are called sub addresses. The sub addresses will not trigger replication anymore. When the home address is deleted or aged out, the sub addresses are deleted or aged out at the same time. However, deleting sub addresses will not bring any influence on the home address.

## Application Model

Packets are forwarded by searching the address table. If the address table has not the destination address, the packets will be broadcasted in a VLAN, as shown in Figure 1.

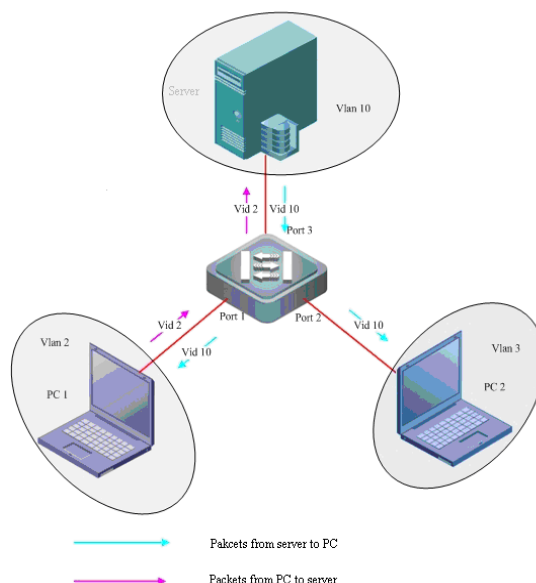


Figure 1 The VID of the packets from PC1 to the server is 2. The switch will learn PC1's address, as shown in Table 1.

Table 1

VLAN	MAC	Address Type	Interface
2	PC1-MAC	DYNAMIC	Port 1

Assume that all the response packets of the server belong to VLAN 10. Since the switch learns PC1's MAC address with VID 2, it will broadcast the response packets whose VID is 10 upon their arrival. Consequently, PC2 will receive the packets that the server sends to PC1, which

are not useful. This wastes bandwidth and PC2's resource. How to avoid this problem? Administrator can set VLAN 10 to be a Share VLAN, so that the switch will replicate the MAC address to VLAN 10 when it learns the MAC address with VID 2.

Table 2

VLAN	MAC	Address Type	Interface
2	PC1-MAC	DYNAMIC	Port 1
10	PC1-MAC	DYNAMIC	Port 1

In this way, when the response packets from the server arrive the switch, the switch can find the address with VID 10 and send them out only through port 1.



#### Note

- A switch supports only one Share VLAN.
- Only replicating dynamic MAC address and static MAC address is allowed.
- The protocol VLAN, private VLAN, remote VLAN or interface address table replication function is mutually exclusive with the Share VLAN, and vice versa.
- The super VLAN cannot be set to be the Share VLAN, and vice versa.
- The sub VLAN cannot be set to be the Share VLAN, and vice versa.
- The MAC addresses in the Share VLAN will not be replicated to the super VLAN, and vice versa.
- Once a sub-address is deleted, it will be replicated only after its home address is aged out or deleted and the sub address is learned again.
- The MAC address replication will fail in case of shortage of the MAC address table. Once replication failed, the home address and replicated sub-address will be deleted if the home address is a dynamic address or the replicated sub-address will be deleted if the home address is a static address.

## Configure Share VLAN

Do the following steps to configure the Share VLAN:

Command	Function
Ruijie(config-vlan)# <b>Share</b>	Enable the Share VLAN.
Ruijie(config-vlan)# <b>no Share</b>	Disable the Share VLAN.

For instance:

```
Ruijie# configure
```

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

```
Ruijie(config)# vlan 10
```

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

```
Ruijie(config)# end
```

## Showing the Share VLAN

Do the following steps to show the Share VLAN:

Command	Function
Ruijie(config-vlan)# <b>show mac-address-table Share</b>	Show the status of MAC address.
Ruijie# <b>show vlan</b>	Show the Share VLAN.

For example:

Show the Share VLAN:

```
Ruijie#show vlan
```

```

VLAN  Name      Status   Ports
----  -
1   VLAN0001  STATIC  Gi0/1, Gi0/2, Gi0/3, Gi0/4
                        Gi0/5, Gi0/6, Gi0/7, Gi0/8
                        Gi0/9, Gi0/10, Gi0/11, Gi0/12
                        Gi0/13, Gi0/14, Gi0/15, Gi0/16
                        Gi0/17, Gi0/18, Gi0/19, Gi0/20
                        Gi0/21, Gi0/22, Gi0/23, Gi0/24
2   VLAN0002  STATIC  Gi0/1
4   VLAN0004  STATIC  Gi0/2
10  VLAN0010  Share   Gi0/1

```

Show the status of the MAC address:

```
Ruijie# show mac-address-table Share
```

```

Vlan  MAC Address      Type      Interface      Status
----  -
2     0040.4650.1e1e  DYNAMIC  GigabitEthernet 0/1 original
10    0040.4650.1e1e  DYNAMIC  GigabitEthernet 0/1 duplicated

```

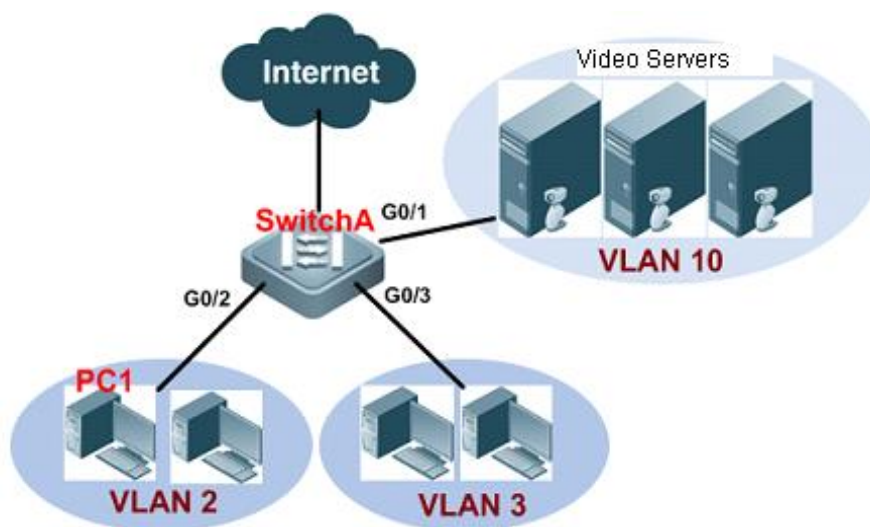
## Typical SHARE VLAN Configuration Example

### SHARE VLAN video-on-demand application

#### Networking Requirements

On an office network, SwitchA is connected with a video-on-demand PC user (PC1) belonging to VLAN 2. It is requested that the access users in VLAN 3 won't be affected while the users in VLAN 2 is access the video server (belonging to VLAN 10), making sure the network resources won't be wasted (namely users in VLAN 3 cannot receive the reply packets sent by video server).

## Network Topology



**SHARE VLAN video-on-demand application**

## Configuration Tips

To meet the needs, we must configure VLAN 10 as a SHARE VLAN on SwitchA.

After PC1 has requested the video program, the video server will reply to the request. When packets reach SwitchA, the switch will insert VLAN 10 Tag according to the PVID value.

On SwitchA, configure VLAN10 as the SHARE VLAN; the addresses learned by the switch will be:

Vlan	MAC	Address Type	Interface
2	PC1-MAC	DYNAMIC	G0/2
10	PC1-MAC	DYNAMIC	G0/2

Packets will be directly sent to PC1 through G0/2, and other users won't be able to receive these reply packets.

## Configuration Steps

1. On SwitchA, configure G0/2 as a hybrid port (default VLAN is 2, and the allowed UNTAG VLANs include VLAN 2 and VLAN 10); configure G0/3 as a hybrid port (default VLAN is 3, and the allowed UNTAG VLANs include VLAN 3 and VLAN 10); configure G0/1 as a hybrid port (default VLAN is 2, and the allowed UNTAG VLANs include all vlans).

```
Ruijie(config)#interface gigabitEthernet 0/2
Ruijie(config-GigabitEthernet 0/2)#switchport mode hybrid
Ruijie(config-GigabitEthernet 0/2)#switchport hybrid native vlan 2
Ruijie(config-GigabitEthernet 0/2)#switchport hybrid allowed vlan untagged 2,10
Ruijie(config)#interface gigabitEthernet 0/3
```

```
Ruijie(config-GigabitEthernet 0/3)#switchport mode hybrid
Ruijie(config-GigabitEthernet 0/3)#switchport hybrid native vlan 3
Ruijie(config-GigabitEthernet 0/2)#switchport hybrid allowed vlan untagged 3,10
Ruijie(config-GigabitEthernet 0/1)#switchport mode hybrid
Ruijie(config-GigabitEthernet 0/1)#switchport hybrid native vlan 10
Ruijie(config-GigabitEthernet 0/1)#switchport hybrid allowed vlan untagged 1-4094
```

## 2. On SwitchA, configure VLAN 10 as the SHARE VLAN;

```
Ruijie(config)#vlan 10
Ruijie(config-vlan)#share
```

## Verification

Step 1: PC1 (assuming that its IP address is 192.168.12.4) shall be able to ping the server (assuming that its IP address is 192.168.12.6);

Step 2: View the information about SHARE VLAN on SwitchA;

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

VLAN	Name	Status	Ports
1	VLAN0001	STATIC	Gi0/1, Gi0/2, Gi0/3, Gi0/4 Gi0/5, Gi0/6, Gi0/7, Gi0/8 Gi0/9, Gi0/10, Gi0/11, Gi0/12 Gi0/13, Gi0/14, Gi0/15, Gi0/16 Gi0/17, Gi0/18, Gi0/19, Gi0/20 Gi0/21, Gi0/22, Gi0/23, Gi0/24
2	VLAN0002	STATIC	Gi0/1, Gi0/2, Gi0/3
3	VLAN0003	STATIC	Gi0/1, Gi0/2, Gi0/3
10	VLAN0010	SHARE	Gi0/1, Gi0/2, Gi0/3

Step 3: View MAC address status on SwitchA (only display the information of port 2; other ports are omitted):

```
Ruijie(config)#show mac-address-table share
```

Vlan	MAC Address	Type	Interface	Status
2	00d0.f864.6909	DYNAMIC	GigabitEthernet 0/2	original
10	00d0.f864.6909	DYNAMIC	GigabitEthernet 0/2	duplicated

# Voice VLAN Configuration

## Introduction to Voice VLAN

### Overview

With the continual development of technology, IP phone is being used more and more widely. It converts analog signals into digital signals which are transmitted over the IP network to the receiver. Then, upon the receipt of data packets, the receiver converts digital signals back to the analog signals. Combined other voice devices, IP phone offers high capacity and low cost voice communications solution for users.

Voice VLAN is specially designed for voice streams. By creating a voice VLAN and adding the ports connecting voice devices to the voice VLAN, users can centrally transmit voice streams in the voice VLAN, and configure QoS specific for voice streams to improve the priority of voice stream transmission and ensure voice quality.

Following figure illustrates the basic networking of Voice VLAN:

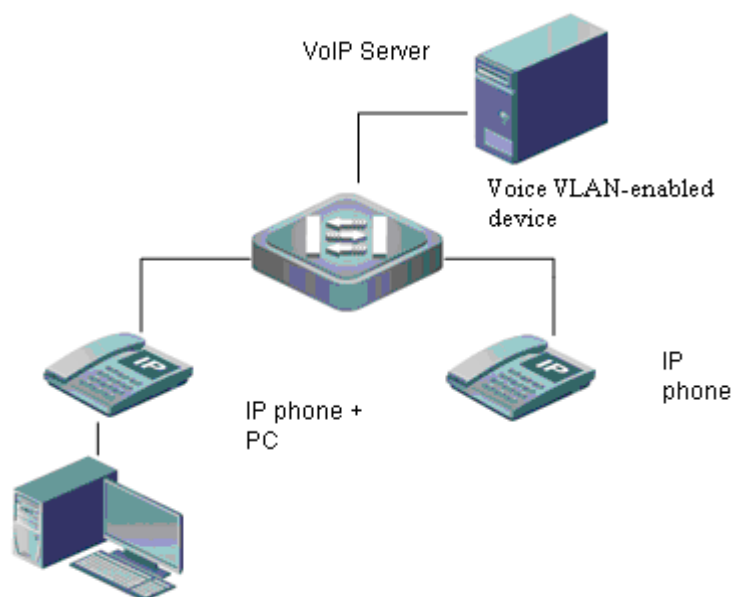


Figure 1 Basic Voice VLAN network topology

There are usually two types of connection (see Fig.1 above) between IP phones and Voice VLAN:

1. IP phones separately access to Voice VLAN with only voice streams transmitted. This type of connection is usually applied to IP phones arrangement in meeting rooms or occasions where PC is not necessary for data processing.
2. PC and IP phones form a daisy chain to access the network with voice and data streams transmitted. In this case, voice streams and data streams are transmitted in voice VLAN and data



VLAN respectively. Generally, this type of connection is applied when office clerks need to conduct both data communication with PC and voice communication with IP phones.

Definition of each role in the basic network topology:

Table 1 Definition of roles in Voice VLAN network

Role	Definition
VoIP Server	The server group (which may be a server undertaking a number of application services or a group of servers that provide different services) may be Call Agent, DHCP server (which assigns automatically IP addresses, Voice VLAN ID, etc. to IP phones) , etc.
Interconnected equipments	The equipments that offer Voice VLAN function
User terminal equipment	IP phones and users' PCs

Voice VLAN-enabled device determines whether the packet is the voice stream to the specific voice device by matching the source MAC address of incoming packet with the OUI (Organizationally Unique Identifier) of the voice device. If so, the packet is partitioned into the voice VLAN for transmission.



#### Note

QUI is the first 24 bits of the MAC address that the IEEE assigns for a vendor. OUI is so unique that users can determine the manufacturer of an equipment.

## Basic Concepts

### Auto mode and manual mode of Voice VLAN

A port can work in the auto mode or manual mode of voice VLAN with different join methods.

#### ■ Auto mode

When a subscriber runs an IP phone and sends protocol packet through a voice VLAN-enabled equipment, the equipment identifies the source MAC address of protocol packet and matches the MAC address with the OUI address set on the switch. If succeed, the equipment will automatically add the input port of the voice message to Voice VLAN and issue the policy to modify the priority of voice message as the one of voice stream of voice VLAN configured on the equipment.

Meanwhile, the subscriber may set Voice VLAN aging time on the equipment. When no voice message is received from the input port within the aging time, the system will delete the port from Voice VLAN. Adding or deleting a port to or from voice VLAN is automatically executed by the system. Port aging mechanism may prevent the speech equipment port out of use for a long time from remaining in Voice VLAN.

#### ■ Manual mode

Users manually add the IP phone connected port to the voice VLAN on voice VLAN supported equipment. In the course IP phone communication, the equipment identifies the source MAC

address of data packet and matches the MAC address with the OUI address of the configured voice VLAN. If succeed, the equipment will automatically add the input port of the voice message to Voice VLAN and issue the policy to modify the priority of voice message as the one of voice stream of voice VLAN configured on the equipment.

In manual mode, adding or deleting a port to or from voice VLAN is done by administrators manually.

No matter which mode is adopted, the tagged packets from IP phone are forwarding by label in the same way as forwarding rule of VLAN.

Generally speaking, there are two kinds of IP phones by the way to obtain IP address and voice VLAN message.

- Automatically acquire IP address and Voice VLAN numbers. This kind of IP phones sends tagged or untagged voice streams.
- Manually configure IP addresses and Voice VLAN numbers. This kind of IP phones can only send tagged voice streams.

Voice VLAN supports transmitting voice streams on Access Port, Trunk Port and Hybrid Port. It is necessary to match port type, working mode of voice VLAN with IP phone type, as shown in the following table:

**Table 2 Matching relationship between port mode and voice stream type**

Voice VLAN working mode	Voice stream type	Port type	Support
Auto mode	Tagged voice stream	Access Port	No
		Private VLAN host-port interface	No
		Private VLAN hybrid-port interface	No
		Trunk Port	Yes; native VLAN of the access port must exist and must not be Voice VLAN. Meanwhile, the port allows native VLAN passing.
		Hybrid Port	Yes; native VLAN of the access port must exist and must not be Voice VLAN. Meanwhile, the port allows native VLAN passing.

	Untagged voice stream	Uplink interface	Yes; native VLAN of the access port must exist and must not be Voice VLAN. Meanwhile, the port allows native VLAN message passing.
		Access Port	No
		Private VLAN host-port interface	No
		Private VLAN hybrid-port interface	No
		Trunk Port	No
		Hybrid Port	No
		Uplink interface	No
	Tagged voice stream	Access Port	No
		Private VLAN host-port interface	No
		Private VLAN hybrid-port interface	No
		Trunk Port	Yes, Native VLAN of the access port must exist and must not be Voice VLAN. Meanwhile, the access port allows native VLAN and Voice VLAN messages passing.
Manual mode			

	Hybrid Port	Yes; Native VLAN of the access port must exist and must not be Voice VLAN. Meanwhile, the port allows native VLAN passing, and the Voice VLAN should be in the list of tagged VLANs whose passing is allowed by the port.
	Uplink interface	Yes; Native VLAN of the access port must exist and must not be Voice VLAN. Meanwhile, the access port allows native VLAN and Voice VLAN messages passing.
Untagged voice stream	Access Port	Yes; Voice VLAN must be consistent with the VLAN which the access port belongs to.
	Private VLAN host-port interface	Yes; Voice VLAN must be configured to be Isolated VLAN or Community VLAN corresponding to the port.
	Private VLAN hybrid-port interface	Yes; Voice VLAN must be configured to be Primary VLAN.
	Trunk Port	Yes; Native VLAN of the access port must be Voice VLAN and the access port allows the VLAN passing.

		Hybrid Port	Yes; Native VLAN of the access port must be Voice VLAN and be in the list of untagged VLANs whose passing is allowed by the access port.
		Uplink interface	No



- 1) When cooperating with 802.1x and Web Authentication for access control, Voice VLAN needs to be configured with security channel and permits OUI address of Voice VLAN for authentication-free VoIP communication.
- 2) If subscribers' IP phones send tagged voice stream and 802.1x authentication and Guest VLAN are enabled on the input port, you need to allocate different VLAN IDs for the voice VLAN, the default VLAN of the input port and the Guest VLAN of 802.1x in order to ensure the normal use of various functions.
- 3) Since Protocol VLAN takes effect only for untagged packets from Trunk Port /Hybrid Port and only tagged voice streams are processed on the Trunk / Hybrid Port under Voice VLAN auto mode, do not set a VLAN as Protocol VLAN and voice VLAN simultaneity.
- 4) Under auto mode, do not configure OUI address as static one; otherwise, auto mode will be affected.

## Voice VLAN safe mode

Safe mode is available for separate transmission of voice streams and data streams. When safe mode is enabled, Voice VLAN only permits voice stream transmission. Only the streams whose source MAC address matches the OUI address of voice VLAN are allowed to transmit in voice VLAN, others are dropped. When safe mode is disabled, the source MAC address of streams will not be checked, and all streams will be permitted to transmit within Voice VLAN.



Under safe mode, only the source MAC address of untagged packets and the packets of voice VLAN tag is checked. Packets are forwarded or dropped by VLAN rules without any influence from Voice VLAN safe/general mode.



It is not recommended to simultaneously transmit voice and data services. If necessary, make sure that safe mode is disabled.

## Working Principles

By transmitting data streams and voice streams in the data VLAN and the voice VLAN respectively, the voice VLAN-supported equipment avoids mutual influence between them. Meanwhile, the equipment issues priority policy to improve the priority of voice streams and guarantee session quality. The basic working principle is described as below:

Step 1: The user creates on the equipment one VLAN dedicated to transmitting voice packets, i.e., Voice VLAN, and enables Voice VLAN function on the port that connects with IP phone.

Step 2: As a key step, the port that connects with IP phone joins Voice VLAN in different ways by the working mode of Voice VLAN:

- Under auto mode, after receiving untagged message from the port, the equipment will match its source MAC address with legal OUI address. If the source MAC is OUI address, the message will be considered to be voice message. And the equipment will automatically join the port in Voice VLAN, and learn this MAC address on the port at the same time.
- Under manual mode, subscribers should manually configure the port which connects with IP phones to join Voice VLAN.

Step 3: Whether under auto mode or manual mode, the equipment will issue a policy and improve the priority of packets whose source MAC address matching the OUI address of voice VLAN. The CoS is set to 6 and DSCP is set to 46 for matched voice packets.

Following these steps, the port that connects with IP phone joins Voice VLAN, and voice packets will be centrally transmitted in Voice VLAN and forwarded out with high priority.

## Protocol Specification

N/A

## Default Configuration

The following table is used to describe the default configuration of Voice VLAN.

Function	Default value
Voice VLAN enablement	Disabled
Voice VLAN safe mode	Enabled
Voice VLAN aging time	One day (1440 minute), only valid under auto mode.
Voice VLAN CoS	6
Voice VLAN DSCP	46
Voice VLAN enablement on port	Disabled
Voice VLAN working mode on port	Auto mode

## Configuring Basic Voice VLAN Features

### Enabling Voice VLAN

Voice VLAN is disabled by default. To enable voice VLAN, run the following commands.

Command	Function
Ruijie# <b>configure terminal</b>	Enter the global configuration mode.
Ruijie(config)# <b>vlan</b> <i>vlan-id</i>	Create a Voice VLAN.
Ruijie(config-vlan)# <b>exit</b>	Exit VLAN configuration mode.
Ruijie(config)# <b>voice vlan</b> <i>vlan-id</i>	Enable Voice VLAN and set one VLAN as Voice VLAN.

To disable voice VLAN, run the no form of this command.

For example:

# Enable Voice VLAN globally and set VLAN 2 as Voice VLAN.

```
Ruijie# configure terminal
```

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

```
Ruijie(config)# vlan 2
```

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

```
Ruijie(config)# voice vlan 2
```



#### Note

When 802.1x and Voice VLAN are enabled simultaneously on a port, IP phones matching the OUI setting of voice VLAN can enable authentication-free voice VLAN communication. For example, PCs and IP phones access to the same port. When 802.1x authentication is enabled on the port, 802.1x authentication is necessary for PCs, not IP phones.



#### Caution

- 1) It is necessary to create corresponding VLAN before configuring Voice VLAN.
- 2) VLAN 1 is default VLAN and does not need creating. However, VLAN 1 must not be set as Voice VLAN.
- 3) A VLAN is not allowed to set as both Voice VLAN and Super VLAN.
- 4) If 802.1x VLAN automatic skip function is enabled on the access port, please do not set the issued VID as Voice VLAN ID in order to ensure normal use of functions.
- 5) Do not configure a VLAN as the Remote VLAN of RSPAN and Voice VLAN simultaneously or otherwise remote port mirroring and voice VLAN may be affected.

## Enabling Voice VLAN on a Port

By default, voice VLAN is disabled on a port. To enable voice VLAN on a port, run the following commands in privileged EXEC mode.

Command	Function
Ruijie# <b>configure terminal</b>	Enter global configuration mode.
Ruijie(config)# <b>interface</b> <i>interface-name</i>	Enter the interface configuration mode, which must be physical interface.
Ruijie(config-if)# <b>voice vlan enable</b>	Enable voice VLAN on the interface.

To disable voice VLAN on the port, run the no form of this command.

For example:

# Enable Voice VLAN on FastEthernet 0/1.

```
Ruijie# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Ruijie(config)# interface fastEthernet 0/1
Ruijie(config-if)# voice vlan enable
```



### Note

You can enable voice VLAN on a port when voice VLAN is disabled globally, but the configuration does not take effect.



### Caution

1) Voice VLAN only supports layer 2 physical ports (Access Port / Trunk Port / Hybrid Port / Uplink Port / Private VLAN port), not AP port or Routed Port.

2) After voice VLAN is enabled on a port, do not switch over the Layer2 mode of the port (Access Port / Trunk Port / Hybrid Port) for normal operation. To switch over Layer 2 mode, disable voice VLAN on the port in advance..

## Configuring Voice VLAN Working Mode on a Port

There are two kinds of Voice VLAN working modes-auto mode and manual mode on the basis of port configuration. For details, refer to Section *Auto mode and manual mode of Voice VLAN*.

By default, voice VLAN works in auto mode on a port. To set working mode, run the following commands.

Command	Function
Ruijie# <b>configure terminal</b>	Enter global configuration mode.
Ruijie(config)# <b>interface</b> <i>interface-name</i>	Enter the interface configuration mode.



```
Ruijie(config-if)# voice vlan mode auto
```

Enable auto mode.  
The working mode of voice VLAN is independent on each interface.

To set the working mode as manual mode, run the no form of this command.

For example:

# Enable auto mode on FastEthernet 0 / 1.

```
Ruijie# configure terminal
```

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

```
Ruijie(config)# interface fastEthernet 0/1
```

```
Ruijie(config-vlan)# voice vlan mode auto
```



#### Note

Once voice VLAN is enabled, do not switch over auto mode and manual mode on the port. If necessary, disable voice VLAN on the port first.

Under auto mode, adding or deleting a port to or from voice VLAN with manual configuration mode is prohibited.

In auto mode, when the default VLAN on the port is different from the Voice VLAN, set the port as a hybrid port and add it to the Voice VLAN in untag mode. And enable the MAC VLAN to add the untag voice flow into the Voice VLAN.



#### Caution

1) When voice VLAN is enabled and works in manual mode on a port, it is necessary to manually add the port to voice VLAN to ensure the effectiveness of voice VLAN.

2) In auto mode, do not set the native VLAN of a port as Voice VLAN for normal operation.

3) For Ruijie products, all VLAN packets can be transmitted on Trunk Port / Hybrid Port by default. Remove voice VLAN from the allowable VLAN list of the port and then enable voice VLAN, ensuring that the port not connecting voice device will not join Voice VLAN or the port unused for a long time always locates in Voice VLAN.

## Configuring Voice VLAN Aging Time

Subscribers may set Voice VLAN aging time on the equipment. When no voice message is received from the input port within the aging time, the equipment will delete the port from Voice VLAN. Only under auto mode does aging time take effect.

To configure the aging time, run the following commands:

Command	Function
Ruijie# configure terminal	Enter global configuration mode.

Ruijie(config)# <b>voice vlan aging</b> <i>minutes</i>	Configure the aging time in the range 5-10000 minutes, 1440 minutes by default.
--	---

To restore the setting to the default value, run the **no** form of this command.

For example:

# Set Voice VLAN Aging time to 10 minutes

```
Ruijie# configure terminal
```

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

```
Ruijie(config)# voice vlan aging 10
```

## Configuring the OUI Address of Voice VLAN

The voice VLAN-supported equipment determines whether the data stream is the voice data stream specific for voice equipment by matching the source MAC address of the data stream with the OUI of voice VLAN. For details on the OUI of voice VLAN, refer to Section *Voice VLAN Overview*.

To configure the OUI address of voice VLAN, run the following commands.

Command	Function
Ruijie# <b>configure terminal</b>	Enter global configuration mode.
Ruijie(config)# <b>voice vlan mac-address</b> <i>mac-addr mask oui-mask [description text]</i>	Configure the OUI address of voice VLAN.
Ruijie(config)# <b>show voice vlan oui</b>	Show the OUI address of voice VLAN.

To delete the OUI address, run the **no** form of this command.

For example:

# Set 0012.3400.0000 as the legal OUI address of voice VLAN.

```
Ruijie# configure terminal
```

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

```
Ruijie(config)# voice vlan mac-address 0012.3400.0000 mask ffff.ff00.0000 description Company A
```

```
Ruijie(config)# show voice vlan oui
```

```
Oui Address      Mask              Description
```

```
0012.3400.0000  ffff.ff00.0000  Company A
```

If the LLDP protocol is supported by both the switch and the voice device, the MAC address of the voice device is identified automatically by the LLDP instead of configuring the Voice VLAN OUI address. Use the **show voice vlan mac-address** command to display the MAC address of voice device which is automatically identified.

For example:

# Suppose that the device has identified one IP phone on the port FastEthernet 0/1 through the LLDP protocol, with the MAC address being 0011.2233.4455

```
Ruijie(config)# show voice vlan mac-address
```

```
MAC Address      Interface          Descriptoin
```

0011.2233.4455 fastEthernet 0/1

**Note**

Voice VLAN's OUI address must not be a multicast address and the configured mask code must be in a continuous form.

## Configuring Voice VLAN Safe Mode

Safe mode is available for separately transmitting voice streams and data streams. When safe mode is enabled, only voice stream is allowed in Voice VLAN to better ensure the quality of voice stream transmission.

To configure safe mode, run the following commands:

Command	Function
Ruijie# <b>configure terminal</b>	Enter global configuration mode.
Ruijie(config)# <b>voice vlan security enable</b>	Enable safe mode. By default, Voice VLAN safe mode is enabled.

To disable safe mode, run the no form of this command.

For example:

# Enable safe mode.

```
Ruijie# configure terminal
```

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

```
Ruijie(config)# voice vlan security enable
```

## Configuring Voice Stream Priority of Voice VLAN

The priority of voice stream in voice VLAN can be improved by modifying CoS and DSCP values. For details on CoS and DSCP, refer to Section *QoS Configuration*.

To configure the priority of voice stream, run the following commands:

Command	Function
Ruijie# <b>configure terminal</b>	Enter global configuration mode.
Ruijie(config)# <b>voice vlan cos</b> <i>cos-value</i>	Set CoS value for voice stream, 6 by default.
Ruijie(config)# <b>voice vlan dscp</b> <i>dscp-value</i>	Set DSCP value for voice stream, 46 by default.

To restore the setting to the default value, run the no form of this command.

For example:

# Configure voice stream priority with CoS of 5 and DSCP of 40.

```
Ruijie# configure terminal
```

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

```
Ruijie(config)# voice vlan cos 5
```

```
Ruijie(config)# voice vlan dscp 40
```

## Showing Voice VLAN Configuration and Status

Voice VLAN provides the following display command for showing various configuration and operation information. Functions of each command is explained as follows:

Command	Function
<b>show voice vlan</b>	Display Voice VLAN configuration information and current status, including working modes of ports enabling Voice VLAN function.
<b>show voice vlan oui</b>	Display OUI address, OUI address mask and descriptive information which current equipment supports.
<b>show voice vlan mac-address</b>	Display the MAC address of the voice device learnt by current device. The MAC address is in the range of the voice device's source address learnt by LLDP or the source address of the voice flow to be jumped to the Voice VLAN.
<b>show vlan</b>	Display the working port of current Voice VLAN with the same display command of general VLAN.

## Voice VLAN Configuration Example

### Voice VLAN Auto Mode

#### Networking requirements

Suppose the configuration under Voice VLAN auto mode has following requirements:

1. Create VLAN 2 as Voice VLAN.
2. Voice VLAN aging time is 1,000 minutes.
3. IP phones with MAC address 0012.3456.7890 send tagged voice stream, and the input port is Trunk-type port Fa0/1 (It is an example here, and when using Voice VLAN function, please refer to Table 2 Matching relationship between port mode and voice stream type of IP phones" of *Section Auto mode and manual mode of Voice VLAN*. Native VLAN of the port is VLAN 5.
4. The equipment allows voice messages with OUI address of "0012.3400.0000" and mask code of "ffff.ff00.0000" being transmitted through Voice VLAN.
5. PC connected underneath with input port Fa 0/ 1 needs 802.1x authentication.

## Networking topology

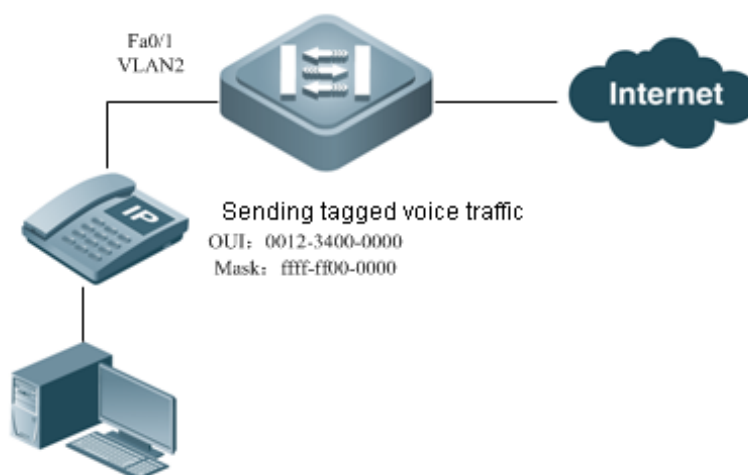


Figure 2 Networking topology for configuring Voice VLAN auto mode

## Configuration precaution

Since the downstream device connecting is the one sending tagged voice streams through trunk port and voice VLAN works in auto mode, the native VLAN of Fa0/1 must exist and must not be voice VLAN and native VLAN is permitted.

VLAN 5 is the native VLAN and VLAN 2 is non voice VLAN. By default, trunk port permits all VLANs. To use auto mode properly and prevent the port not connecting voice device from joining voice VLAN, remove VLAN 5 from the VLAN allowable list of Fa0/1.

Since 802.1x authentication should be enabled on Fa0/1, you need to set security tunnel and permit voice streams with OUI address of "0012.3400.0000" and mask code of "ffff.ff00.0000".

## Configuring procedure

1) Create VLAN 2 as Voice VLAN.

# create VLAN 2 and enable Voice VLAN of VLAN 2.

```
Ruijie# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Ruijie(config)# vlan 2
Ruijie(config-vlan)# exit
Ruijie(config)# voice vlan 2
```

2) Voice VLAN Aging time is 1,000 minutes.

# Set Voice VLAN aging time.

```
Ruijie(config)# voice vlan aging 1000
```

3) Permit voice streams with OUI address of "0012.3400.0000" and mask code of "ffff.ff00.0000" being transmitted through Voice VLAN.

# Configure Voice VLAN OUI address.

```
Ruijie(config)# voice vlan mac-address 0012.3400.0000 mask ffff.ff00.0000
```

4) The access port is Trunk-type port Fa 0 / 1, and native VLAN of the port is VLAN 5.

# set Fa0/1 as Trunk Port.

```
Ruijie(config)# interface fastEthernet 0/1
```

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

# set VLAN 5 of Fa0/1 as native VLAN.

```
Ruijie(config-if)# switchport hybrid native vlan 5
```

# Remove Voice VLAN from the allowable VLAN list of Fa0/1

```
Ruijie(config-if)# switchport trunk allowed vlan remove 2
```

# Enable Voice VLAN on Fa0/1

```
Ruijie(config)# interface fastEthernet 0/1
```

```
Ruijie(config-if)# voice vlan enable
```

5) Enable 802.1x function on the port simultaneously.

# Configure expert ACL and permit the streams matching OUI address.

```
Ruijie(config)# expert access-list extended safe_channel
```

```
Ruijie(config-exp-nacl)# permit ip any 0012.3400.0000 ffff.ff00.0000 any any
```

# configure security tunnel.

```
Ruijie(config)# security global access-group safe_channel
```

# Set Fa0/1 with 802.1 x enabled as controlled port.

```
Ruijie(config)# interface fastEthernet 0/1
```

```
Ruijie(config-if)# dot1x port-control auto
```

# For methods of configuring other 802.1x functions, refer to Section *802.1x Configuration*

## Showing configuration

# Show current Voice VLAN status.

```
Ruijie(config)# show voice vlan
```

```
Voice Vlan status: ENABLE // Enabling global Voice VLAN
```

```
Voice Vlan ID : 2 // Voice VLAN ID is 2
```

```
Voice Vlan security mode: Security // Enable global safe mode
```

```
Voice Vlan aging time: 1440minutes
```

```
Voice Vlan cos : 6
```

```
Voice Vlan dscp : 46
```

```
Current voice vlan enabled port mode:
```

```
PORT MODE
```

```
-----
```

```
Fa0/1 AUTO // Fa 0/1 enables Voice VLAN as auto mode
```

# Viewing Voice VLAN OUI address of the equipment

```
Ruijie(config)# show voice vlan oui
```

```
Oui Address Mask Description
```

```
0012.3400.0000 ffff.ff00.0000
```

## Voice VLAN Manual Mode

### Networking requirements

- 1) Create VLAN 2 as Voice VLAN.
- 2) IP phones with MAC address 0012.3456.7890 send untagged voice stream; and the access port is Hybrid-type port Fa0/1.
- 3) Fa0/1 works in manual mode.

The equipment allows voice messages with OUI address of "0012.3400.0000" and mask code of "ffff.ff00.0000" being transmitted through Voice VLAN. And the descriptor is "Company A".

### Networking topology

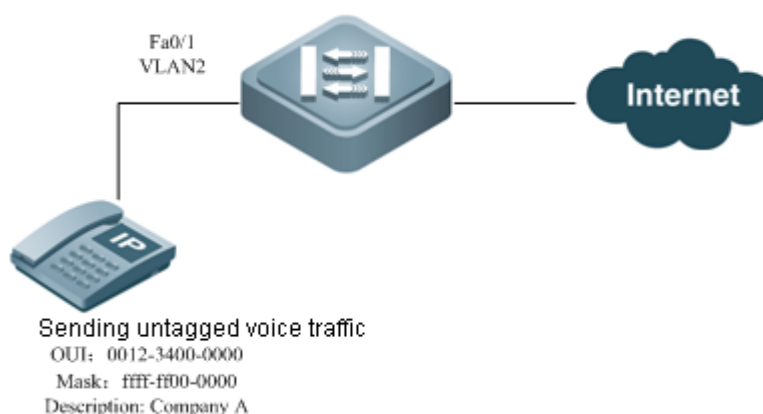


Figure 3 Networking topology for configuring Voice VLAN manual mode

### Points for configuration

According to networking requirements, followings should be paid attention to during Voice VLAN configuration of the equipment: Since Fa 0 / 1 connects beneath with Hybrid Port sending untagged voice stream, and Voice VLAN mode is manual mode, according to the matching relationship, native VLAN of Fa 0 / 1 must be Voice VLAN and Voice VLAN must be in the list of untagged VLANs allowed to pass the port. Among networking requirements, therefore, native VLAN of Fa0/1 should be set as 2 (Voice VLAN ID), meanwhile it is necessary to join VLAN 2 in the list of untagged VLANs allowed to pass Fa 0 / 1 during configuration.

### Configuring procedure

- 1) Create VLAN 2 as Voice VLAN.

# create VLAN 2 and enable Voice VLAN function of VLAN 2.

```
Ruijie# configure terminal
```

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

```
Ruijie(config)# vlan 2
```

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

```
Ruijie(config)# voice vlan 2
```

The equipment allows voice messages with OUI address of "0012.3400.0000" and mask code of "ffff.ff00.0000" being transmitted through Voice VLAN. And the descriptor is "Ruijie".

#### # Configure Voice VLAN OUI address

```
Ruijie(config)# voice vlan mac-address 0012.3400.0000 mask ffff.ff00.0000 description Company A
```

4) The access port is Hybrid-type port Fa 0/1, and native VLAN of the port is VLAN 2.

#### # set Fa 0/1 as Hybrid Port

```
Ruijie(config)# interface fastEthernet 0/1
Ruijie(config-if)# switchport mode hybrid
```

#### # set Voice VLAN as native VLAN of Fa 0/1

```
Ruijie(config-if)# switchport hybrid native vlan 2
```

#### # Join Voice VLAN (i.e., VLAN 2) in the list of untagged VLANs that join Fa 0/1

```
Ruijie(config-if)# switchport hybrid allowed vlan add untagged 2
```

#### # Enable Voice VLAN function of Fa 0/1

```
Ruijie(config)# interface fastEthernet 0/1
Ruijie(config-if)# voice vlan enable
```

## Display verification

#### # Show current Voice VLAN status.

```
Ruijie(config)# show voice vlan

Voice Vlan status: ENABLE           // Enabling global Voice VLAN
Voice Vlan ID      : 2              // Voice VLAN ID is 2
Voice Vlan security mode: Security  // Enable global safe mode
Voice Vlan aging time: 1440minutes
Voice Vlan cos      : 6
Voice Vlan dscp      : 46
Current voice vlan enabled port mode:
PORT                MODE
-----
Fa0/1                MANUAL          // Fa 0/1 enables Voice VLAN as manual mode

# Viewing Voice VLAN OUI address of the equipment

Ruijie(config)# show voice vlan oui

Oui Address      Mask      Description
0012.3400.0000  ffff.ff00.0000  Company A
```

## Data Stream and Voice Stream Isolation

### Networking requirements

1. Create VLAN 2 as the Voice VLAN and VLAN 3 as the data VLAN.



2. PC is connected to IP phone and sends untagged data streams. IP phone is connected to the switch and sends untagged voice streams, with MAC address being 0012.3456.7890. The access port is the Hybrid port of Fa0/1.
3. Fa0/1 operates in manual mode.
4. The switch will forward voice packets with OUI address being 0012.3400.0000 and mask being ffff.ff00.0000 through Voice VLAN, and will forward packets with other addresses through Data VLAN.

## Networking topology

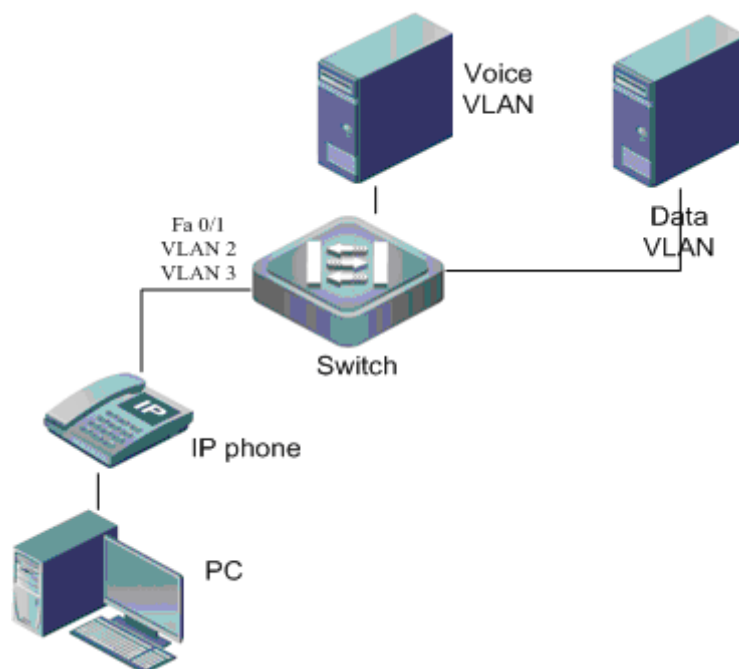


Figure 4 Networking topology of Voice VLAN and data stream isolation

## Configuration tips

According to networking requirements, the configuration of Voice VLAN on the switch shall pay attention to: Since untagged voice streams are sent on Fa0/1, we need to configure the mode of Voice VLAN as manual mode. To realize the isolation of data streams and voice streams, MAC VLAN must be enabled on Fa0/1, so that voice streams can be directed to VLAN 2. The native VLAN of Fa0/1 must be data VLAN, and to ensure that the incoming data streams and voice streams are both untagged. Data VLAN and Voice VLAN must be included in the list of untagged VLANs permitted on the port. Meanwhile, to ensure that data streams can be forwarded, the security mode must be disabled on the interface.

## Configuring procedure

1) Create Voice VLAN and data VLAN

# Create data VLAN

```
Ruijie# configure terminal
```

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

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

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

### # Create VLAN2 and enable Voice VLAN in VLAN 2

```
Ruijie(config)# vlan 2
```

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

```
Ruijie(config)# voice vlan 2
```

2) Configure to forward voice packets with OUI address being 0012.3400.0000 and mask being ffff.ff00.0000 through Voice VLAN.

### # Configure the OUI address of Voice VLAN

```
Ruijie(config)# voice vlan mac-address 0012.3400.0000 mask ffff.ff00.0000 description Company  
A
```

3) The access port should be the hybrid port of Fa0/1, and the native VLAN is VLAN 3.

### # Configure Fa0/1 as a Hybrid Port

```
Ruijie(config)# interface fastEthernet 0/1
```

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

### # Configure Voice VLAN as the native VLAN of Fa0/1

```
Ruijie(config-if)# switchport hybrid native vlan 3
```

### # Include Voice the VLAN (namely VLAN2) into the untagged list of Fa0/1

```
Ruijie(config-if)# switchport hybrid allowed vlan add untagged 2-3
```

### # Enable the Voice VLAN and MAC VLAN on Fa0/1 and disable the security mode

```
Ruijie(config)# interface fastEthernet 0/1
```

```
Ruijie(config-if)# voice vlan enable
```

```
Ruijie(config-if)# no voice vlan security enable
```

```
Ruijie(config-if)# mac-vlan enable
```

## Verification

### # Display the current status of Voice VLAN

```
Ruijie(config)# show voice vlan
```

```
Voice Vlan status: ENABLE // Voice VLAN is enabled globally
```

```
Voice Vlan ID : 2 // Voice VLAN ID is 2
```

```
Voice Vlan security mode: Normal // Disable security mode
```

```
Voice Vlan aging time: 1440minutes
```

```
Voice Vlan cos : 6
```

```
Voice Vlan dscp : 46
```

```
Current voice vlan enabled port mode:
```

```
PORT MODE
```

```
-----
```

```
Fa0/1 MANUAL // Enable Voice VLAN on Fa0/1 (manual mode)
```

# Display the MAC addresses of voice device discovered by the switch

```
Ruijie(config)# show voice vlan mac-address
```

MAC Address	Interface	Description
0012.3456.7890	fastEthernet 0/1	Company A

# View MAC VLAN entries

```
Ruijie# show mac-vlan all
```

The following MAC VLAN address exist:

S: Static D: Dynamic

MAC ADDR	MASK	VLAN ID	PRIO	STATE
0012.3456.7890	ffff.ffff.ffff	2	0	D

## Automatic Voice Device Detection

### Networking requirements

1. Create VLAN 2 as the Voice VLAN and VLAN 3 as the data VLAN.
2. PC is connected to IP phone and sends untagged data streams. IP phone is connected to the switch, supports the LLDP protocol and sends untagged voice streams, with MAC address being 0012.3456.7890. The access port is the Hybrid port of Fa0/1.
3. Fa0/1 operates in manual mode.
4. The user expects the switch to automatically detect voice device and direct voice streams and data streams to Voice VLAN and Data VLAN respectively.

### Networking topology

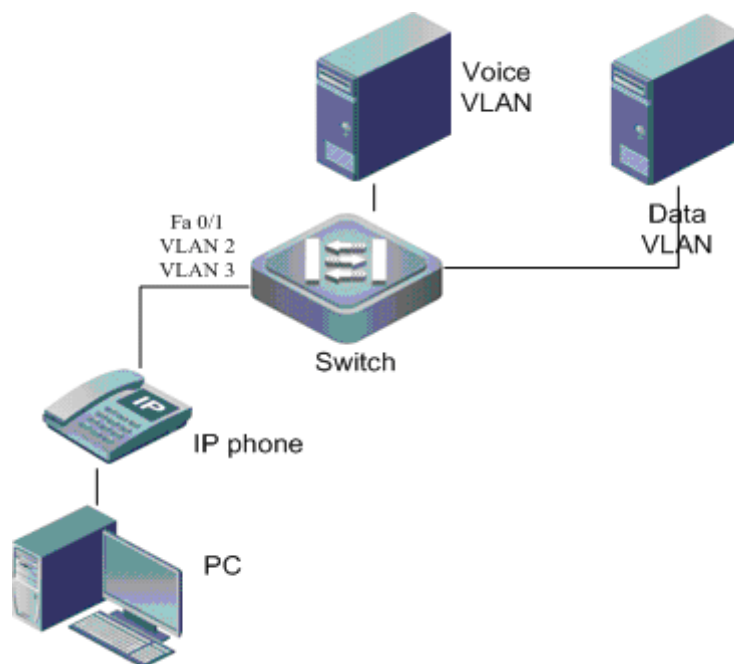


Figure 4 Networking topology of automatic detection of voice device

## Configuration tips

According to networking requirements, it is required to use LLDP to discover voice device, while LLDP is enabled by default. Firstly, we need to confirm that LLDP is not disabled on the switch. The configuration of Voice VLAN on the switch shall pay attention to: Since untagged voice streams are sent on Fa0/1, we need to configure the mode of Voice VLAN as manual mode. To realize the isolation of data streams and voice streams, MAC VLAN must be enabled on Fa0/1, so that voice streams can be directed to VLAN 2. The native VLAN of Fa0/1 must be data VLAN, and to ensure that the incoming data streams and voice streams are both untagged. Data VLAN and Voice VLAN must be included in the list of untagged VLANs permitted on the port. Meanwhile, to ensure that data streams can be forwarded, the security mode must be disabled on the interface.

## Configuring procedure

### 1) Create the Voice VLAN and data VLAN

#### # Create data VLAN

```
Ruijie# configure terminal  
Enter configuration commands, one per line. End with CNTL/Z.  
Ruijie(config)# vlan 3  
  
Ruijie(config-vlan)# exit
```

#### # Create VLAN2 and enable the Voice VLAN in VLAN 2

```
Ruijie(config)# vlan 2  
Ruijie(config-vlan)# exit  
Ruijie(config)# voice vlan 2
```

### 2) The access port should be the hybrid port of Fa0/1, and the native VLAN is VLAN 3.

#### # Configure Fa0/1 as a Hybrid Port

```
Ruijie(config)# interface fastEthernet 0/1  
Ruijie(config-if)# switchport mode hybrid
```

#### # Configure the Voice VLAN as the native VLAN of Fa0/1

```
Ruijie(config-if)# switchport hybrid native vlan 3
```

#### # Include Voice VLAN (namely VLAN2) into the untagged list of Fa0/1

```
Ruijie(config-if)# switchport hybrid allowed vlan add untagged 2-3
```

#### # Enable Voice VLAN and MAC VLAN on Fa0/1 and disable security mode

```
Ruijie(config)# interface fastEthernet 0/1  
Ruijie(config-if)# voice vlan enable  
Ruijie(config-if)# no voice vlan security enable  
Ruijie(config-if)# mac-vlan enable
```

## Verification

#### # Display the current status of Voice VLAN

```
Ruijie(config)# show voice vlan
```

```
Voice Vlan status: ENABLE          // Voice VLAN is enabled globally
Voice Vlan ID      : 2              // Voice VLAN ID is 2
Voice Vlan security mode: Normal    // Disable security mode
Voice Vlan aging time: 1440minutes
Voice Vlan cos      : 6
Voice Vlan dscp      : 46
Current voice vlan enabled port mode:
PORT                MODE
-----
Fa0/1                MANUAL          // Enable Voice VLAN on Fa0/1 (manual mode)
```

# Display the MAC addresses of voice device discovered by the switch

```
Ruijie(config)# show voice vlan mac-address
MAC Address      Interface      Description
0012.3456.7890    fastEthernet 0/1    Company A
```

# MSTP Configuration

## MSTP Overview

### STP and RSTP

#### STP and RSTP Overview

Ruijie series supports both the STP protocol and the RSTP protocol, as well as complying with the IEEE 802.1D and IEEE 802.1w standards.

The STP protocol can prevent broadcast storm caused by link loops and provide link redundancy and backup. For the layer 2 Ethernet, there is only one active channel between two LANs to avoid broadcast storm. However, it is necessary to set up redundant links to improve the reliability of a LAN. Furthermore, some channels should be in the backup status in order to take up its work when a link fails. It is obviously hard to control this process by manual. The STP protocol can complete this work automatically. It enables a device in a LAN to:

- Discover and activate an optimal tree-type topology of the LAN.
- Detect and fix failures and automatically update the network topology to offer the possible optimal tree-type structure at any time.

The LAN topology is automatically calculated by a set of bridge parameters set by the administrator. The proper configuration of these parameters is helpful to offer an optimal solution.

The RSTP protocol is completely compatible with the 802.1D STP protocol downward. As with traditional protocol, the RSTP protocol can prevent loop and offer link redundancy. The most critical feature of the RSTP protocol is quickness. If the bridges in a LAN support the RSTP protocol and are configured appropriately by administrators, it will take no more than 1 second to re-span the topology tree once the network topology changes (it takes about 50 seconds for traditional STP protocol to re-span the topology tree).



#### Caution

For the switch buffer control, see the chapter *Buffer Control* in *Configuring QOS*.

### Bridge Protocol Data Units (BPDU):

A stable tree-type topology depends on the following elements :

- The unique bridge ID of each bridge consists of the bridge priority and the MAC address.
- The root path cost refers to the cost from a bridge to the root bridge.
- Each port ID consists of the port priority and port number.

By exchanging the Bridge Protocol Data Units (BPDU) frame destined to the multicast address 01-80-C2-00-00-00 (in hex), bridges gets the information necessary for building the optimal tree-type topology.

A BPDU is comprised of the following elements:

- Root Bridge ID (root bridge ID that a bridge considers)
- Root Path cost (Root Path cost of a bridge).

- Bridge ID (ID of a bridge).
- Message age (the live time of the message)
- Port ID (port ID sending the message).
- Forward-Delay Time, Hello Time and Max-Age: time parameters.
- Other flag bits, such as network topology change and port status.

Once a port of a bridge receives a BPDU message whose priority is higher than its priority (or smaller bridge ID and smaller root path cost), the bridge will store this message on the port while updating and propagating them to all other ports. If the BPDU with lower priority is received, the bridge will discard this message.

This mechanism propagates a BPDU message of higher priority in the whole network. As a result:

- A bridge is elected to be the root bridge in the network.
- Each bridge other than the root bridge has a root port that offers a shortest path to the root bridge.
- Each bridge will calculate the shortest path to the root bridge.
- Each LAN has a designated bridge that lies in the shortest path between this LAN and the root bridge. The port for connecting the designated bridge and the LAN is referred to as the designated port.
- The root port and the designated port are in the forwarding status.
- Other ports beyond the spanning tree are in the discarding status.

## Bridge ID

As specified in IEEE 802.1W standard, each bridge has a unique bridge ID based on which the root bridge is elected in spanning tree algorithm. The bridge ID consists of eight bytes, in which the last six bytes are the MAC address of the bridge, and the first two bytes are shown in the table below. Of which, the first four bits denote the priority, while the last twelve bits denote the system ID for extending the protocol in the future. This value is 0 in the RSTP, so the priority of the bridge should be configured as the multiple of 4096.

	Priority value				System ID											
Bit	16	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1
Value	32768	16384	8192	4096	2048	1024	512	256	128	64	32	16	8	4	2	1

## Spanning-Tree Timers

The following describes three timers impacting the performance of spanning tree.

- Hello timer: Interval to send the BUDU message.
- Forward-Delay timer: Interval to change the port status, that is, the time interval at which the port switches from the listening status to the learning status and vice versa when the RSTP protocol runs in the compatible STP protocol mode.
- Max-Age timer: The longest time for the BPDU message. The system will discard the message when the timer times out.

## Port Roles and Status

A port plays a role to present its function in the network topology.

- Root port: The port that provides the shortest path to the root bridge.

- Designated port: The port through which each LAN is connected to the root bridge.
- Alternate port: The alternate port of the root port that will take up its work when the root port fails.
- Backup port: The backup port of the designated port. If two ports of a bridge are connected to a LAN, the port with higher priority is the designated port and the other one is the backup port.
- Disable port: The port that is not in the active status, namely, the ports whose operation status is down.

Figure 1, Figure 2 and Figure 3 below show the roles of various ports:

R = Root port    D = Designated port    A = Alternate port    B = Backup port

Unless otherwise stated, the priorities of these ports are in the descending order from left to right.

Figure-1

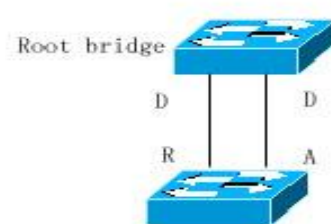


Figure-2

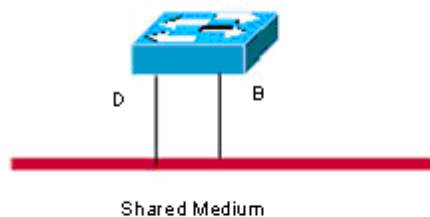
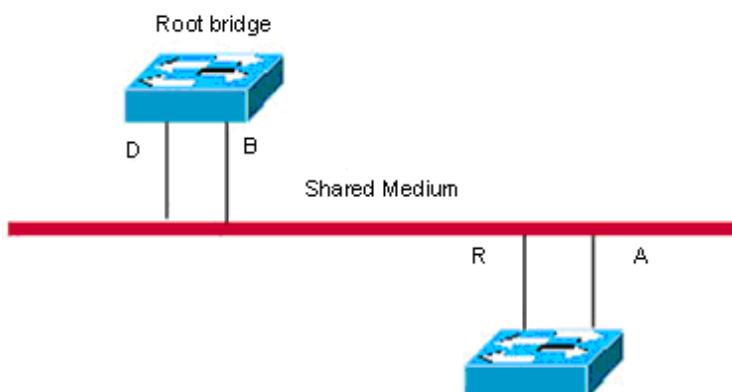


Figure-3



There are three port states for every port to indicate whether the data packet is forwarded and control the topology of the whole spanning tree.

- Discarding: Neither forward the received frame nor learn about the source Mac address.
- Learning: Do not forward the received frame, but learn about the source Mac address, so it is a transitional status.



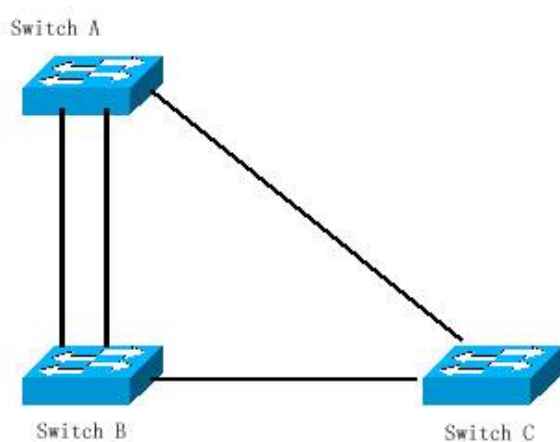
- Forwarding: Both forward the received frame and learn about the source Mac address.

For the stable network topology, only the root port and designated port can be the forwarding status, while other ports are only in the discarding status.

### Generating a Network Topology Tree (Typical Application Solution)

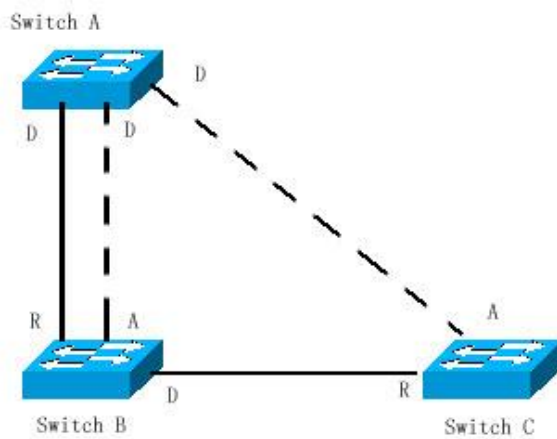
We now describe how the STP and RSTP protocols span a tree-type structure by the mixed network topology. As shown in Figure 4, the bridge IDs of Switches A, B and C are assumed in the ascending order. Namely, Switch A presents the highest priority. There is the 1000M link between switch A and switch B, and the 10M link between switch A and switch C, while it is the 100M link between switch B and switch C. Switch A acts as the backbone switch of this network and implements the link redundancy for both Switch B and Switch C. Obviously, broadcast storm would occur if all these links are active.

Figure-4



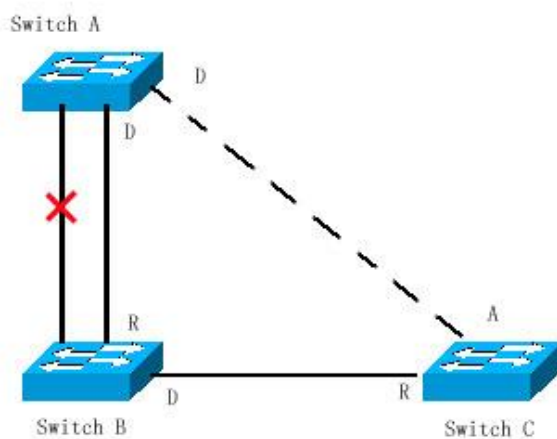
If all of these three switches enable the Spanning Tree protocol, they will select switch A as the root bridge by exchanging BPDU message. Once Switch B detects that two ports are connected to Switch A, it will select the port with the highest priority as the root port, while another one is selected as the alternate port. Meanwhile, Switch C detects that it can reach Switch A through Switch B or directly. However, Switch C discovers that the cost of the path from Switch B to Switch A is lower than that directly (For the costs corresponding to various paths, refer to table \*\*\*), so Switch C selects the port connected with Switch B as the root port, while the one that connected with Switch A as the alternate port. Various ports enter the corresponding status after their roles are determined. As a result, the network topology is generated as shown in Figure 5.

Figure-5



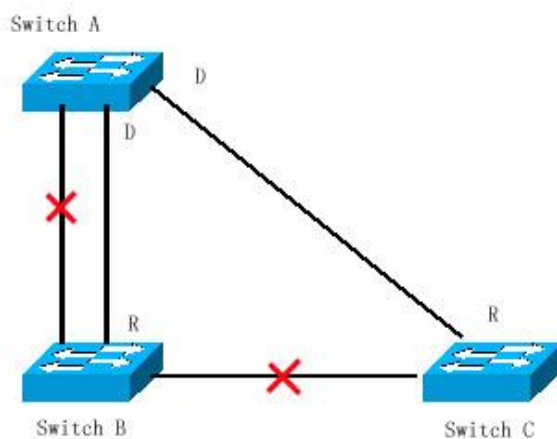
If the active path between Switch A and Switch B fails, the backup path will work. Consequently, the network topology is generated as shown in Figure 6.

Figure-6



If the path between Switch B and Switch C fails, Switch C will automatically switch the alternate port to the root port. Consequently, the network topology is generated as shown in Figure 7.

Figure-7



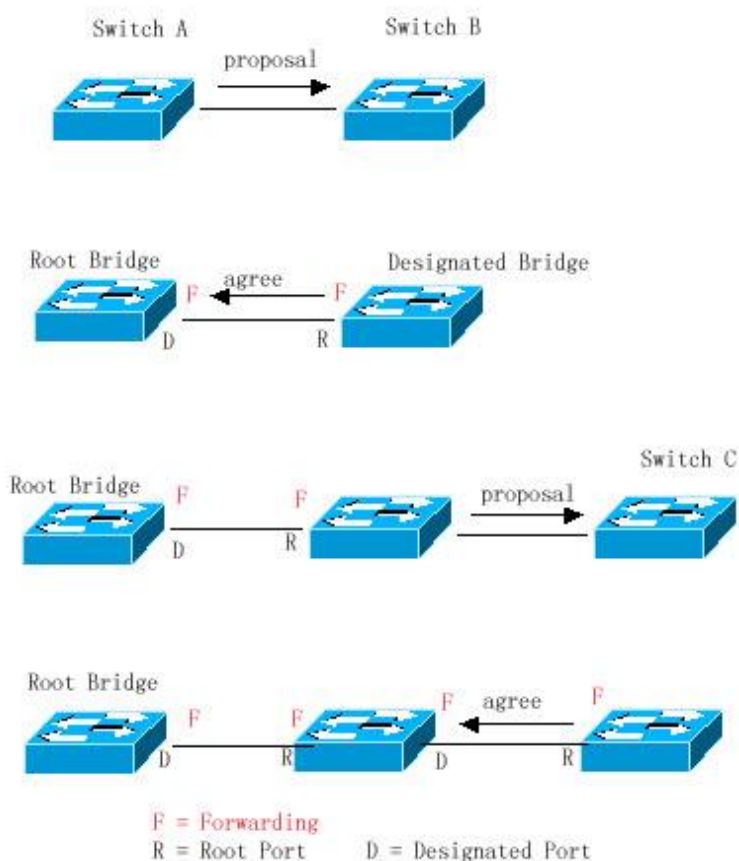
## Rapid Convergence of RSTP

The following introduces the special function of RSTP: enabling rapid forwarding on a port.

The STP protocol will forward packets after 30s since the port roles are selected, which is twice as the Forward-Delay Time (you can set the Forward-Delay Time, which is 15s by default). Furthermore, the root port and designated port of each bridge will carry out the forwarding again after 30s, so it will take about 50s to stabilize the tree-type structure of the whole network topology.

The forwarding procedure of the RSTP protocol is different from that of the STP protocol. As shown in Figure 8, Switch A sends the specific proposal message of the RSTP protocol. Switch B detects that the priority of Switch A is higher than itself, takes the Switch A as the root bridge and the port that receives the message as the root port and forwards the proposal message. Then it sends the Agree message to Switch A through the root port. Upon the receipt of the proposal message, Switch A will forward the message through its designated port. After that, Switch sends the proposal message through the designated port to extend the spanning tree in turn. In theory, the RSTP protocol can immediately restore the tree-type network structure to implement rapid convergence when the network topology changes.

Figure-8



### Caution

“Point-to-point Connection” between ports is required for the above “handshaking” process. In order to make full use of you device, do not use non-point-to-point connection between devices.

Other than Figure 9, other schematics in this chapter are the point-to-point connection. The following lists the example figure of the non point-to-point connection.

Example of Non Point-to-point Connection:

Figure-9

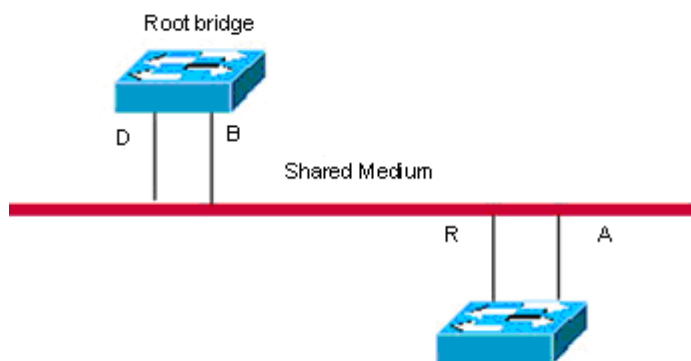
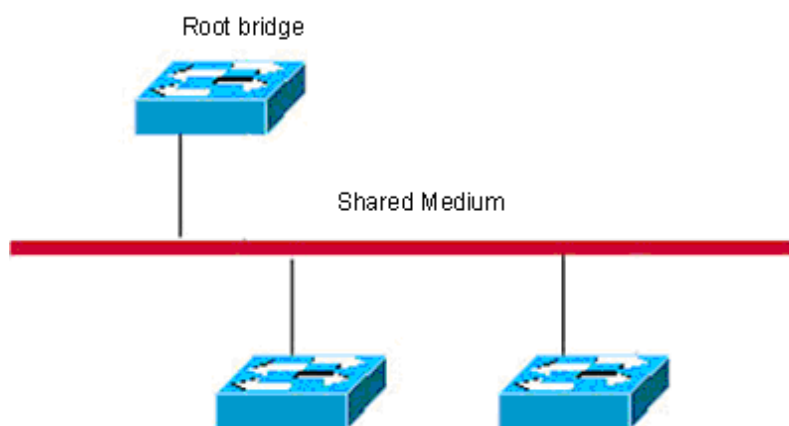
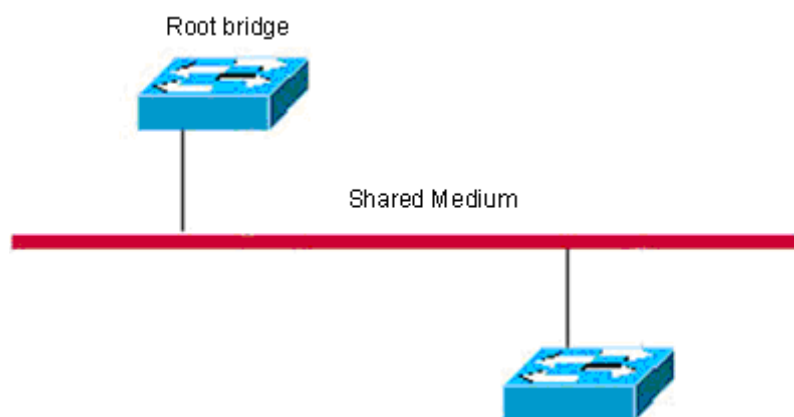


Figure-10



In addition, the following figure is a point-to-point connection and should be differentiated by users carefully.

Figure-11



### Compatibility of RSTP and STP

The RSTP protocol is completely compatible with the STP protocol. It will judge whether the connected bridge supports the STP protocol or the RSTP protocol by the version number of the received BPDU message automatically. Only the forwarding process of the STP protocol is executed in the case of that the bridge supports the STP protocol. This cannot maximize the performance of the RSTP protocol.

Furthermore, using the RSTP protocol and the STP protocol will cause a problem. As shown in Figure 17-12, Switch A supports the RSTP protocol, while Switch B supports the STP protocol. Both switches are connected

with each other. Switch A will send the STP BPDU message to Switch B for compatibility. However, if Switch A is connected with the RSTP-enabled Switch C, Switch A still sends the STP BPDU message, and thus causing that Switch C considers Switch A an STP-enabled bridge. As a result, two RSTP-supported switches run the STP protocol, reducing their efficiency greatly.

For this reason, the RSTP protocol provides the protocol-migration function to send the RSTP BPDU message forcibly in case that the peer bridge must support RSTP. In this way, Switch C will detect the bridge connected with it supports the RSTP protocol, so both two devices can run the RSTP protocol as shown in Figure 13.

Figure-12 Protocol Migration

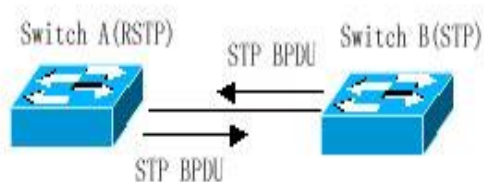
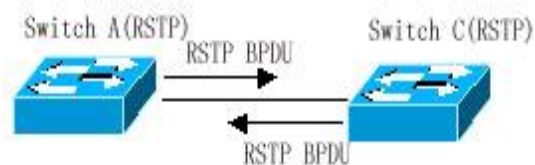


Figure-13



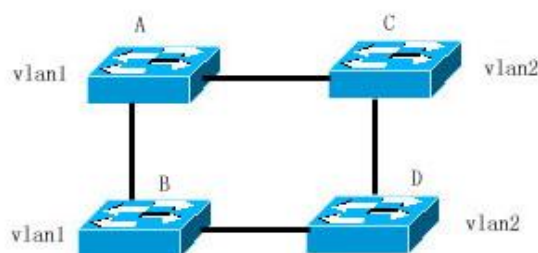
## MSTP Overview

Ruijie series supports the MSTP protocol, a new spanning-tree protocol derived from the traditional STP and RSTP protocols that includes the rapid forwarding mechanism of the RSTP protocol itself.

Since traditional spanning tree protocols are not related to a VLAN, the following problems may occur in a specific network topology.

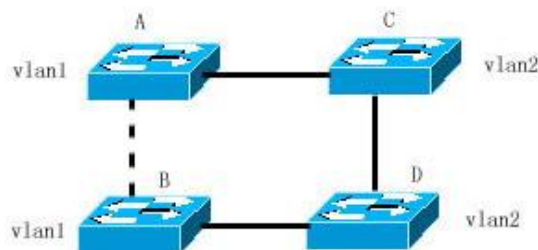
As shown in Figure 14, Switches A and B are located in Vlan1, and switches C and D in Vlan2. They form a loop.

Figure-14



If the cost of the path from Switch A through Switch C, Switch D to Switch B is smaller than that of the direct path from Switch A to Switch B, the latter path will be torn down, as shown in Figure 15. Packets in Vlan1 cannot be forwarded because Switches C and D do not contain Vlan1. In this way, Vlan1 of Switch A cannot communicate with Vlan1 of Switch B.

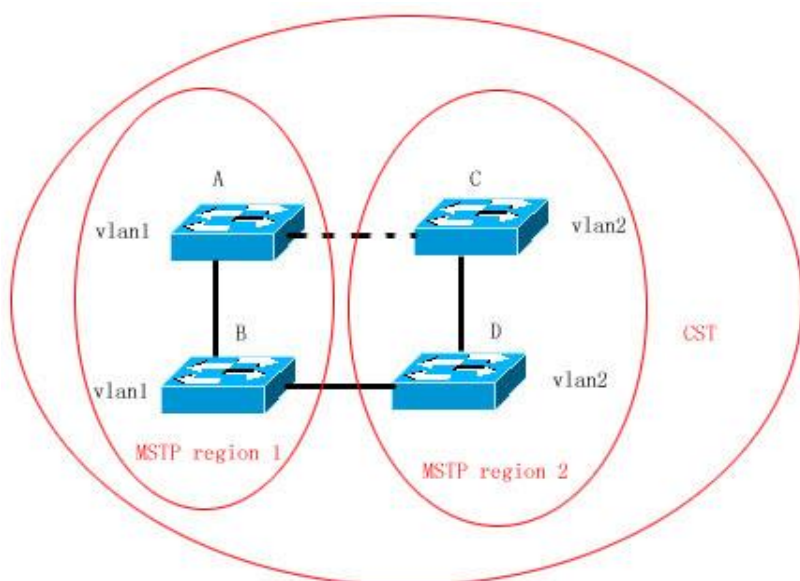
Figure-15



The MSTP protocol is developed to address this problem. It partitions one or more vlans of the switch into an instance, so the switches with the same instance configuration form a region (MST region) to run a separated spanning tree (this internal spanning-tree is referred to as the IST). The MST region is equivalent to a large device, which executes the spanning tree algorithm with other MST regions to obtain a whole spanning tree, referred to as the common spanning tree (CST).

With this algorithm, the above mentioned network can form the topology shown in Figure 16. Switches A and B are within the MSTP region 1 without a loop, so no path is discarded. This is also the case in the MSTP region 2. Region 1 and region 2 serve as two large devices respectively. There is a loop between them, so one path is discarded according to related configuration.

Figure-16



In this way, no loop occurs and the communication between the devices in a VLAN works as well.

### How to Partition MSTP regions

According to above description, MSTP regions should be partitioned rationally and the switches in a MSTP region should be configured similarly for the MSTP protocol to work properly.

The MST configuration information contains:

- MST region name (name): A string of up to 32 bytes identifying the MSTP region.
- MST revision number: A revision number of 16 bits identifying the MSTP region.
- MST instance-vlan table: Each device can create up to 64 instances with IDs ranging from 1 to 64). Instance 0 always exists, so the system totally supports 65 instances. You can

allocate 1 to 4094 VLANs for different instances (0 to 64) as needed, and the unallocated VLANs belong to instance 0 by default. In this way, each MSTI (MST instance) is a VLAN group and executes the spanning tree algorithm within the MSTI according to the MSTI information of the BPDU without the effect of the CIST and other MSTIs.

You can use the **spanning-tree mst configuration** command in the global configuration mode to enter the MST configuration mode and configure above information.

The MSTP BPDU carries above information. If a device has received the same MST configuration information of the BPDU as that of itself, it considers that the device connecting to this port belong to the same MST region as itself.

You are recommended to configure the instance-vlan table while the STP protocol is disable, and then enable the MSTP protocol to ensure the stability and convergence of the network topology.

### Spanning Tree within a MSTP region (IST)

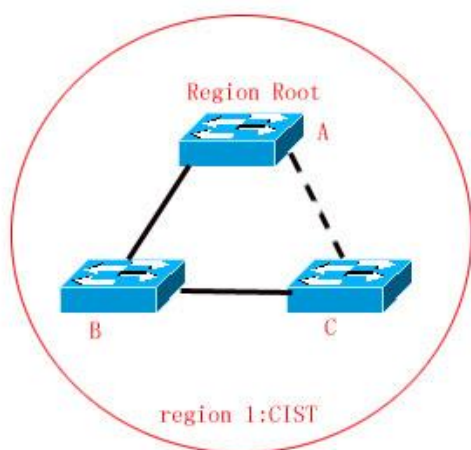
After MSTP regions are partitioned, a root bridge is elected for every instance within a region and the port role is determined for every port on a switch. A port is forwarded or discarded within an instance depends on its role.

In this way, the IST (Internal Spanning Tree) is formed by exchanging the MSTP BPDU message, and various instances have their own spanning trees (MSTI). The spanning tree corresponding to the instance 0 is referred to as the CIST (Common Instance Spanning Tree) in conjunction with CST. That is to say, each instance provides each VLAN group with a single network topology without loop.

As shown in the following figure, Switches A, B and C form a loop within the region 1.

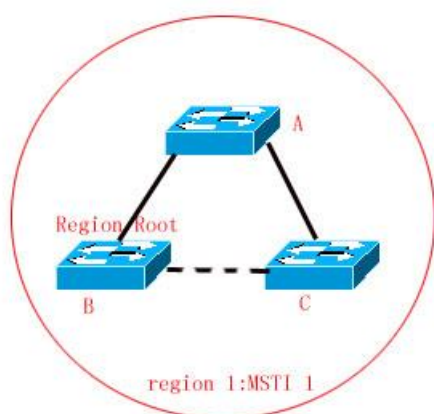
Switch A with the highest priority is selected as the region root in the CIST (instance 0). Then, the path between Switches A and C is discarded according to other parameters. Hence, for the VLAN group of instance 0, only the path from switch A to B and switch B to switch C are available, which break the loop of the VLAN group.

Figure-17



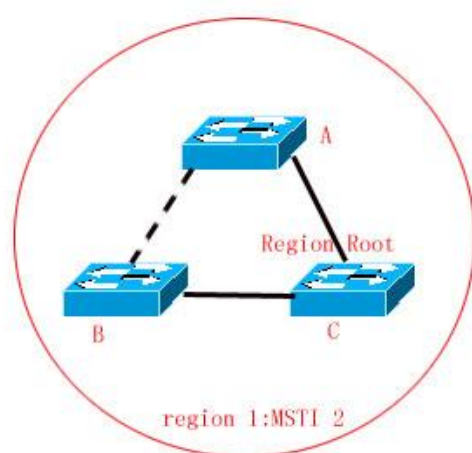
As shown in Figure 18, switch C with the highest priority is selected as the region root in the MSTI 1 (instance 1). Then, the path between switch A and B is discarded according to other parameters. Hence, for the VLAN group of instance 1, only the path from switch A to switch B and switch A to switch C are available, which break the loop of the VLAN group.

Figure-18



As shown in Figure 19, switch B with the highest priority is selected as the region root in the MSTI 2 (instance 2). Then, the path between switch B and switch C is discarded according to other parameters. Hence, for the VLAN group of instance 2, only the path from switch A to switch B and switch B to switch C are available, which break the loop of the VLAN group.

Figure-19



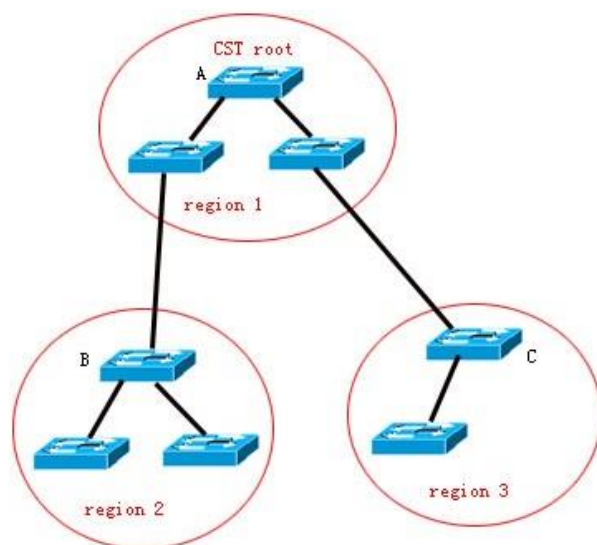
It should note that the MSTP protocol is not concerned on which VLAN a port belongs to, so users should configure corresponding path costs and priorities for ports according to actual VLAN configuration to prevent the MSTP protocol from breaking the loop unnecessarily.

### Spanning Tree between MSTP regions (CST)

For CST, each MSTP region is equivalent to a large-sized device, and different MSTP regions also form a large-sized network topology tree, referred to as CST (common spanning tree). As shown in Figure 20, for CST, switch A with the smallest bridge ID is selected as the root of the entire CST (CST Root) and the CIST Regional Root in this region. In Region 2, since the root path cost from switch B to the CST root is the lowest one, switch B is selected as the CIST Regional Root in this region. Similarly, switch C is selected as the CIST Regional Root in Region 3.



Figure-20



The CIST Regional Root is not necessarily the device with the smallest bridge ID in that region. It is the device in the region that has the lowest root path cost to the CIST root.

At the same time, the root port of the CIST regional root takes a new port role for the MSTI, namely the **Master port**, as the outlet of all instances, which is forwarded to all instances. In order to make the topology more stable, it is recommended to configure the outlet of the regions to the CIST root on one device of this region as much as possible!

## Hop Count

The IST and MSTI will not take the message age and Max age to calculate whether the BPDU message is timeout. Instead, they use the mechanism similar to the TTL of IP packets, namely hop count.

You can set it by using the **spanning-tree max-hops** command in the global configuration mode. The hop count is reduced by 1 when the BPDU message passes through a device in a region starting from the region root bridge until it is 0, which means the BPDU message is timeout. A device will discard the BPDU message whose hop count is 0.

In order to be compatible with the STP protocol and the RSTP protocol out a region, the MSTP protocol still remains the Message age and Max age mechanisms.

## Compatibility of MSTP with RSTP and STP

For the STP protocol, the MSTP protocol will send the STP BPDU to be compatible with it like the RSTP protocol. For detailed information, refer to the Compatibility of RSTP and STP section.

For the RSTP protocol, it will process the CIST part of the MSTP BPDU, so it is not necessary for the MSTP to send the RSTP BPDU to be compatible with it.

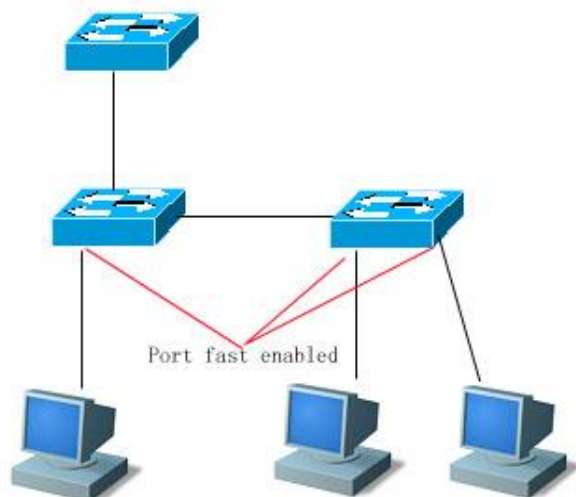
Each device that runs the STP or RSTP protocol is an independent region, and does not form the same region with any other device.

## Overview of Optional Features of MSTP

### Understanding Port Fast

If a port of a device is connected with the network terminal directly, this port can be set as the Port Fast to forward packets directly. The port does not need to wait 30 seconds before forwarding packets, which is the case when the port is not set to Port Fast. The following figure indicates which ports of a device can be set to Port Fast.

Figure-21



If the BPDU message is received from the Port Fast enabled port, its Port Fast operational state is disabled. At this time, this port will execute the forwarding by normal STP algorithm.

### Understanding AutoEdge

If the specified port doesn't receive the BPDU message sent by the downstream port within a certain period of time (3 seconds), the port will be considered that it connects a network device and set as an edge port to enter the Forwarding status directly. An edge port will be automatically identified as a non-edge port after receiving the BPDU message.

You can disable the automatic identification function of the edge port by the **spanning-tree autoedge disabled** command.

This function is enabled by default.

**Caution**

- 1) When the AutoEdge function conflicts with the manually-configured Port Fast function, the latter shall prevail.
- 2) AutoEdge function can be used for rapid negotiation forwarding between the designated port and the downstream port, so the STP protocol doesn't support AutoEdge. If the designated port is in the forwarding status, Autoedge does not take effect on the port. It will take effect during repaid renegotiation such as plugging/unplugging network cables.
- 3) If a port enables the BPUD Filter, it forwards the BPDU message directly, but not be identified as the edge port automatically.
- 4) AutoEdge function is only applicable for the designated port.
- 5) AutoEdge complies with the standard definition of IEEE 802.1D (version 2004), in which the parameter range of Bridge Hello Time has been modified as 1.0-2.0. Therefore, you shall confirm that the Hello Time value is within the range when using AutoEdge function, or the risk of temporary loop will occur. It is recommended to disable AutoEdge function if it is necessary to exceed the range of Hello Time.

## Understanding BPDU Guard

The BPDU guard can be enabled globally or on individual interface. There are some slightly difference between these two ways.

You can use the **spanning-tree portfast bpduguard default** command to open the global BPDU guard enabled status in the global configuration mode. In this status, if the BPDU message is received through a Port Fast-enabled port or a AutoEdge port, this port will enter the error-disabled status, indicating the configuration error. At the same time, the port will be closed to show that some illegal users may add a network device to the network, which change the network topology.

You can also use the **spanning-tree bpduguard enable** command to enable BPDU guard on individual interface in the interface configuration mode (it is not related to whether it is AutoEdge port or not ). Under this situation, it will enter the error-disabled status if this interface receives the BPDU message.

## Understanding BPDU Filter

The BPDU filter can be enabled globally or on individual interface. There are some slightly difference between these two ways.

You can use the **spanning-tree portfast bpdufilter default** command to enable the BPDU filter globally in the global configuration mode. In this status, the BPDU messages cannot be received or sent through a Port Fast-enabled port or a AutoEdge port, leading to no BPDU messages received by the host directly connecting the port. The BPDU filter will be disabled when the Port Fast is disabled for the AutoEdge port receives the BPDU message.

You can also use the **spanning-tree bpdufilter enable** command to enable the BPDU filter on individual interface in the interface configuration mode (it is not related to whether it is AutoEdge port or not). In this situation, this interface will not receive or transmit the BPDU message, but execute the forwarding directly.

## Understanding Tc-protection

TC-BPDU messages are BPDU messages carrying with TC flag. When the L2 switch receives these messages, the network topology will change and the MAC address table will be deleted. And for L3 switch, the route table will be deleted and the port state in the ARP entry will change. To prevent the switch from processing abovementioned operations when pseudo TC-BPDU messages attack maliciously, too-heavy burden and network turbulence, the TC-protection function comes into being.

Tc-protection can only be enabled or disabled globally. It is enabled by default.

Once Tc-protection is enabled, the switch will delete the message within a certain period of time (usually 4 seconds) after receiving the TC-BPDU message while monitoring the TC-BPDU message. If it receives the TC-BPDU message during this period, it will perform the delete operation again after this period expires. This eliminates the need of frequently deleting MAC address entries and ARP entries.

## Understanding TC Guard

The Tc-Protection function can reduce the removal of MAC address entries and ARP entries when a lot number of TC messages are generated in a network. However, you need to do more delete operations in case of TC message attack. Furthermore, the TC message is propagated and will have an effect on the whole network. The TC Guard function allows you to disable the propagation of the TC message globally or on ports. When TC Guard function is configured globally or on a port, the port will shield the TC messages received or produced to prevent from propagating them to other ports. In this way, this function can manage TC message attack in the network and maintain the network stability. Moreover, this function can prevent from interrupting core routes due to the oscillation of the devices on the access layer.



### Caution

Network communication will be broken off if you use tc-guard function incorrectly.

You are recommended to enable this function when you ensure that there is illegal tc message attack in the network.

If you enable global tc-guard, then all the ports will not spread tc message. It is applicable for those devices that are accessed on the desk to enable this function.

If you enable interface tc-guard, then the topology change and tc message received on this port will not be spreaded to other ports. It is applicable for up-link ports especially aggregated ports to enable this function.

## Understanding TC Filtering

With the TC Guard function enabled, the port will not propagate TC message to other ports participating in the spanning tree calculation on the local device. The TC message here includes the TC message received on the port, and the TC message produced by the port itself. The latter one refers to the TC message generated when the forwarding state of the port changes (For example, port state change from block to forwarding), which indicates the topology may be changed.

As TC message propagation is prevented by TC Guard, the device will not clear the MAC addresses of the corresponding ports when the topology changes, resulting in data forwarding failure.

TC filtering is introduced to solve the above problems. TC filtering will process the TC message in the condition of normal topology change instead of the TC message received on the port, so that address clearing and core route

interruption caused by frequent UP/DOWN on the port without Portfast configured can be solved, and the core routing entries can be updated in time when the topology changes.

**Caution**

By default, the TC filtering function is enabled.

## Understanding BPDU Source MAC Check

The global of the BPDU source MAC check function is to prevent malicious attack on the switch by sending the BPDU message manually and thus cause the MSTP protocol work abnormally. When the peer switch connected to a port in the point-to-point mode is determined, enabling the BPDU source MAC check function can receive only the BPDU message from the remote switch and discard all other BPDU messages to protect against malicious attacks. You can configure the corresponding MAC addresses for the BPDU source MAC check function on a specific port in the interface mode. Only one MAC address is configured for one port. BPDU source MAC check can be disabled by using the **no bpdu src-mac-check** command. In this case, any BPDU message is received on the port.

## Understanding Invalid Length Filtering for BPDU

When the Ethernet length field of the BPDU message exceeds 1500 bits, this BPDU message is discarded in order to avoid receiving invalid BPDU messages.

## Understanding ROOT Guard

In network design, root bridge and backup root bridge are always divided in the same region. Due to error configuration of ascendant and malicious attack in the network, it is possible that root bridge receives configuration message of higher priority and loses the current root bridge position, leading to error turbulence of network topology, which Root Guard function can prevent from occurring.

When enabling Root Guard, it enforces the port role of all the instances as specified port. Once the port receives configuration message of higher priority, Root Guard will set the interface as root-inconsistent (blocked). If there is no configuration message of higher priority during the time long enough, the port will be restored to be the original normal status.

You shall disable ROOT Guard function if this function results in the blocked status for interfaces and it needs manual configuration to restore to the normal status. You can use the command **spanning-tree guard none** in the interface configuration mode to disable Root Guard function.

**Caution**

1. Incorrectly using ROOT Guard leads to network link breakdown.
2. If you enable ROOT Guard on non-designated port, the non-designated port will be enforced as designated port and show BKN status(blocking status).
3. If MST0 enters BKN status because it receives configuration message of higher priority on a port, ROOT Guard will enforce the port in all the other instances to enter BKN status.
4. ROOT Guard or LOOP Guard takes effect at the same time. That is , they cannot both take effect at the same time .
5. The AutoEdge function is disabled when enabling the ROOT Guard-enabled port.

## Understanding LOOP Guard

Due to breakdown of one-way link, root port or backup port becomes designated port, being ready to forward because they cannot receive BPDU, causing the loop in the network, which Loop Guard function can prevent.

For the ports configured loop guard, if they cannot receive BPDU, the port roles will be migrated. However, the port state is always set as discarding till the port receive BPDU again and recalculate spanning tree.

**Caution**

You can enable LOOP Guard based on global or interface.

ROOT Guard or LOOP Guard takes effect at the same time. That is , they cannot both take effect at the same time .

The AutoEdge function on all interfaces is ineffective when enabling LOOP Guard function globally.

The AutoEdge function on the interface is ineffective when enabling LOOP Guard function in the interface configuration mode.

## Configuring MSTP

### Default Spanning Tree Configuration

The following table lists the default configuration of the Spanning Tree protocol.

Item	Default value
Enable State	Disable
STP MODE	MSTP
STP Priority	32768
STP port Priority	128
STP port cost	Automatically determine according to port rate.

Item	Default value
Hello Time	2 seconds
Forward-delay Time	15 seconds
Max-age Time	20 seconds
Default calculation method of the Path Cost	Long
Tx-Hold-Count	3
Link-type	Automatically determine by the duplex status of the port.
Maximum hop count	20
Corresponding relationship between vlan and instance	All VLANs belong to instance 0 Only instance 0 exists

You can restore the STP parameters to its default configuration (except for disabling STP) by using the **spanning-tree reset** command.

## Enabling and Disabling the Spanning Tree Protocol

The spanning tree protocol is disabled on the device by default.

To enable the spanning tree protocol, execute the following command in the privileged EXEC mode:

Command	Function
Ruijie# <b>configure terminal</b>	Enter the global configuration mode.
Ruijie(config)# <b>spanning-tree</b>	Enable the spanning tree protocol.
Ruijie(config)# <b>end</b>	Return to the privileged EXEC mode.
Ruijie# <b>show spanning-tree</b>	Verify the configuration.
Ruijie# <b>copy running-config startup-config</b>	Save the configuration.

To disable the spanning tree protocol, use the **no spanning-tree** command in the global configuration mode.

## Configuring the Spanning Tree Mode

According to the 802.1-related protocols, it is not necessary for administrators to set much for three versions of the spanning tree protocols such as the STP, RSTP and MSTP. These versions are compatible with one another naturally. However, given that some manufacturers will not develop the spanning tree protocol by standards, it may cause some compatibility problem. Hence, we provide a command to facilitate administrators to switch to the lower version of the spanning tree protocol for compatibility when they detect that this device is not compatible with that of other manufacturers.

Note: When you switch to the RSTP or STP version from the MSTP version, all information about MSTP Region will be cleared.

The default mode of the device is MSTP.

To enable the spanning tree protocol, execute the following command in the privileged EXEC mode:

Command	Function
Ruijie# <b>configure terminal</b>	Enter the global configuration mode.

Command	Function
Ruijie(config)# <b>spanning-tree mode mstp/rstp/stp</b>	Switch the spanning tree version.
Ruijie(config)# <b>end</b>	Return to the privileged EXEC mode.
Ruijie# <b>show spanning-tree</b>	Verify the configuration.
Ruijie# <b>copy running-config startup-config</b>	Save the configuration.

To restore the spanning tree mode to the default value, use the **no spanning-tree mode** command in the global configuration mode.

## Configuring Switch Priority

Switch priority allows you to select the root and draw the topology of a network. It is recommended that administrators set the core device with higher priority (or smaller value) to facilitate the stabilization of the whole network. You can assign different switch priorities for various instances so that various instances can run separate spanning tree protocol. Only the priority of CIST (Instance 0) is related to the devices between different regions. As mentioned in Bridge ID, there are 16 values for the priority, and all of them are multiples of 4096, which are 0, 4096, 8192, 12288, 16384, 20480, 24576, 28672, 32768, 36864, 40960, 45056, 49152, 53248, 57344, and 61440. The default value is 32768.

To configure switch priority, execute the following command in the global configuration mode:

Command	Function
Ruijie# <b>configure terminal</b>	Enter the global configuration mode.
Ruijie(config)# <b>spanning-tree [mst instance-id] priority priority</b>	Configure different switch priorities for different instances. This command configures the switch priority for instance 0 without the instance-id parameter. <i>instance-id</i> : ID of the instance in the range from 0 to 64. <i>priority</i> : switch priority in the range from 0 to 61440 and is increased by the integral multiple of 4096, 32768 by default.
Ruijie(config)# <b>end</b>	Return to the privileged EXEC mode.
Ruijie# <b>show running-config</b>	Verify the configuration.
Ruijie# <b>copy running-config startup-config</b>	Save the configuration.

To restore the switch priority to the default value, use the **no spanning-tree mst instance-id priority** command in the global configuration mode.

## Configuring Port Priority

When two ports are connected to the shared media, the device will set the one of the higher priority (or smaller value) to be the forwarding status and the one of the lower priority (or larger value) to be the discarding status. If the two ports are of the same priority, the device will set the one with the smaller port number to the forwarding status. You can assign different port priorities to various instances on one port, by which various instances can run



the separated spanning tree protocols.

Same as device priority, it has 16 values, all a multiple of 16. They are 0, 16, 32, 48, 64, 80, 96, 112, 128, 144, 160, 176, 192, 208, 224, and 240 respectively. The default value is 128.

To configure a port priority, execute the following commands in the privileged EXEC mode:

Command	Function
Ruijie# <b>configure terminal</b>	Enter the global configuration mode.
Ruijie(config)# <b>interface</b> <i>interface-id</i>	Enter the interface configuration mode. A legal interface contains a physical port and an aggregate Link.
Ruijie(config-if)# <b>spanning-tree</b> [ <b>mst</b> <i>instance-id</i> ] <b>port-priority</b> <i>priority</i>	Configure different priorities for different instances. The command without the <i>instance-id</i> parameter will configure a port priority for instance 0. <i>instance-id</i> : Interface ID in the range of 0 to 64. <i>priority</i> : Port priority of an instance in the range 0 to 240. Furthermore, it is increased by the integral multiple of 16, 128 by default.
Ruijie(config-if)# <b>end</b>	Return to the privileged EXEC mode.
Ruijie# <b>show spanning-tree</b> [ <b>mst</b> <i>instance-id</i> ] <b>interface</b> <i>interface-id</i>	Verify the configuration.
Ruijie# <b>copy running-config startup-config</b>	Save the configuration.

To restore the port priority to the default value, execute the **no spanning-tree mst *instance-id* port-priority** command in the interface configuration mode.

## Configuring Path Cost of a Port

The switch determines a root port upon the total of the path costs along the path from a port to the root bridge. The port the total of paths costs from the port to the root bridge is the smallest is elected the root port. Its default value is calculated by the media speed of the port automatically. The higher the media speed, the smaller the cost is. It is not necessary for administrators to change it for the path cost calculated in this way is most scientific. You can assign different cost paths for various instances on one port, by which various instances can run the separated spanning tree protocols.

To configure the path cost of a port, execute the following commands in the privileged EXEC mode:

Command	Function
Ruijie# <b>configure terminal</b>	Enter the global configuration mode.
Ruijie(config)# <b>interface</b> <i>interface-id</i>	Enter the interface configuration mode. A legal interface contains a physical port and an aggregate Link.

Command	Function
Ruijie(config-if)# <b>spanning-tree</b> [mst <i>instance-id</i> ] <b>cost</b> <i>cost</i>	Configure different priorities for different instances. The command without the <i>instance-id</i> parameter will configure a port priority for instance 0.  <i>instance-id</i> : Interface ID in the range of 0 to 64.  <i>cost</i> : Path cost of the port in the range of 1 to 200,000,000. The default value is calculated by the media rate of the port automatically.
Ruijie(config-if)# <b>end</b>	Return to the privileged EXEC mode.
Ruijie# <b>show spanning-tree</b> [mst <i>instance-id</i> ] <b>interface</b> <i>interface-id</i>	Verify the configuration.
Ruijie# <b>copy running-config startup-config</b>	Save the configuration.

To restore the path cost of a port to the default value, execute the **no spanning-tree mst *cost*** command in the interface configuration mode.

## Configuring the Default Calculation Method of Path Cost (path cost method)

If the path cost of a port is the default value, the device will calculate the path cost of this port by port rate. However, IEEE 802.1d-1998 and IEEE 802.1t specify different path cost values for a port rate respectively. The value range of the 802.1d-1998 is short (1 to 65535), while the value range of the 802.1t is long (1 to 200,000,000).

There are two modes for the Cost value of AP: 1) our private mode fixes it to: the Cost value of the physical port \* 95%; 2) the standard value is 20,000,000,000/ the actual link bandwidth of AP (The actual link bandwidth is: the bandwidth of member port \* the number of UP member ports). Administrators should unify the path cost standard of the whole network. The default mode is long (IEEE 802.1t Mode).

The following table lists the path costs set for different port rates in two standards.

Port Rate	Interface	IEEE 802.1d (short)	IEEE 802.1t (long)	IEEE 802.1t (long standard)
10M	Common Port	100	2000000	2000000
	Aggregate Link	95	1900000	$2000000 \div \text{linkupcnt}$
100M	Common Port	19	200000	200000
	Aggregate Link	18	190000	$200000 \div \text{linkupcnt}$
1000M	Common Port	4	20000	20000
	Aggregate Link	3	19000	$20000 \div \text{linkupcnt}$
10000M	Common Port	2	2000	2000
	Aggregate Link	1	1900	$2000 \div \text{linkupcnt}$

**Note**

1. The default path cost mode is long. After changing the path cost to the standard mode, the cost of AP will vary with the number of UP member ports. The change of port cost value may result in network topology change.
2. For the static AP, the linkupcnt in the table is the number of UP member ports; for the LACP AP, the linkupcnt refers to the number of member ports participating in AP data forwarding. If there is no linkup on the member port, the linkupcnt is 1. For detailed configurations about AP and LACP, refer to *AP-SCG* and *LACP-SCG*.

To configure the default calculation method of path cost, execute the following commands in the privileged EXEC mode:

Command	Function
Ruijie# <b>configure terminal</b>	Enter the global configuration mode.
Ruijie(config)# <b>spanning-tree pathcost method</b> {{ <b>long</b> [ <b>standard</b> ]}   <b>short</b> }	Configure the default calculation method of the port path cost as long, standard long or short, with long by default.
Ruijie(config)# <b>end</b>	Return to the privileged EXEC mode.
Ruijie# <b>show running-config</b>	Verify the configuration.
Ruijie# <b>copy running-config startup-config</b>	Save the configuration.

To restore the setting to the default value, execute the **no spanning-tree pathcost** method command in the global configuration mode.

## Configuring Hello Time

Configure the interval of sending the BPDU message. The default value is 2s.

To configure the Hello Time, execute the following commands in the privileged EXEC mode:

Command	Function
Ruijie# <b>configure terminal</b>	Enter the global configuration mode.
Ruijie(config)# <b>spanning-tree hello-time</b> <i>seconds</i>	Configure the hello time ranging from 1 to 10s, 2s by default.
Ruijie(config)# <b>end</b>	Return to the privileged EXEC mode.
Ruijie# <b>show running-config</b>	Verify the configuration.
Ruijie# <b>copy running-config startup-config</b>	Save the configuration.

To restore the hello time to the default value, execute the **no spanning-tree hello-time** command in the global configuration mode.

## Configuring Forward-Delay Time

Configure the interval for changing port status. The default value is 15s.

To configure the forward-delay time, execute the following commands in the global configuration mode:

Command	Function
Ruijie# <b>configure terminal</b>	Enter the global configuration mode.
Ruijie(config)# <b>spanning-tree forward-time</b> <i>seconds</i>	Configure the forward delay time ranging from 4 to 30s, 15s by default.
Ruijie(config)# <b>end</b>	Return to the privileged EXEC mode.
Ruijie# <b>show running-config</b>	Verify the configuration.
Ruijie# <b>copy running-config startup-config</b>	Save the configuration.

To restore the forward-delay time to the default value, execute the **no spanning-tree forward-time** command in the global configuration mode.

## Configuring Max-Age Time

Configure the maximum period of time before the BPDU message is aged out. The default value is 20s.

In the privilege mode, perform these steps to configure the Max-Age Time:

Command	Function
Ruijie# <b>configure terminal</b>	Enter the global configuration mode.
Ruijie(config)# <b>spanning-tree max-age</b> <i>seconds</i>	Configure the max age time ranging from 6 to 40s, 20s by default.
Ruijie(config)# <b>end</b>	Return to the privileged EXEC mode.
Ruijie# <b>show running-config</b>	Verify the configuration.
Ruijie# <b>copy running-config startup-config</b>	Save the configuration.

To restore the max age time to the default value, execute the **no spanning-tree max-age** command in the global configuration mode.



### Caution

Hello Time, Forward-Delay Time and Max-Age Time have their own value ranges. Meanwhile, the following condition must be addressed:  $2 * (\text{Hello Time} + 1.0 \text{ seconds}) \leq \text{Max-Age Time} \leq 2 * (\text{Forward-Delay} - 1.0 \text{ second})$ . Otherwise, it may cause the topology instability

## Configuring Tx-Hold-Count

Configure the maximum number of the BPDU message sent per second, 3 by default.

To configure the Tx-Hold-Count, execute the following commands in the global configuration mode:

Command	Function
Ruijie# <b>configure terminal</b>	Enter the global configuration mode.
Ruijie(config)# <b>spanning-tree tx-hold-count</b> <i>numbers</i>	Configure the maximum number of the BPDU message sent per second in the range of 1 to 10, 3 by default.
Ruijie(config)# <b>end</b>	Return to the privileged EXEC mode.

Command	Function
Ruijie# <b>show running-config</b>	Verify the configuration.
Ruijie# <b>copy running-config startup-config</b>	Save the configuration.

To restore the Tx-Hold-Count to the default value, execute the **no spanning-tree tx-hold-count** command in the global configuration mode.

## Configuring Link-type

Configure the link-type of a port. This is crucial for rapid RSTP convergence. For details, refer to Rapid RSTP Convergence. Without configuration, the device will set the link type of a port according to its duplex status automatically, with point-to-point for the full duplex port and shared for the half duplex port.

To configure the link type of a port, execute the following commands in the interface configuration mode:

Command	Function
Ruijie# <b>configure terminal</b>	Enter the global configuration mode.
Ruijie(config)# <b>interface interface-id</b>	Enter the interface configuration mode.
Ruijie(config-if)# <b>spanning-tree link-type point-to-point/shared</b>	Configure the link type of the interface, with point-to-point for the full duplex port and shared for the half duplex port. Point-to-point indicates the rapid forwarding is enabled on the port.
Ruijie(config-if)# <b>end</b>	Return to the privileged EXEC mode.
Ruijie# <b>show running-config</b>	Verify the configuration.
Ruijie# <b>copy running-config startup-config</b>	Save the configuration.

To restore the link type of a port to the default value, execute the **no spanning-tree link-type** command in the interface configuration mode.

## Configuring Protocol Migration Processing

This command is to check the version globally or on individual port. For related information, refer to Compatibility of RSTP and STP.

Command	Function
Ruijie# <b>clear spanning-tree detected-protocols</b>	Forcibly check the version on all ports.
Ruijie# <b>clear spanning-tree detected-protocols interface interface-id</b>	Check the version forcibly on the port.

## Configuring an MSTP Region

To deploy several devices in the same MSTP Region, you have to configure these devices with the same name, the same revision number, and the same Instance-VLAN table.

You can assign a VLAN to instances 0 to 64 respectively as required. The remaining VLANs will be automatically assigned to instance 0. One vlan can only be of an instance.

It is recommended to configure the Instance-VLAN table when the MSTP protocol is disabled. After configuration, you should enable the MSTP protocol again to ensure the stability and convergence of the network topology.

To configure an MSTP region, execute the following commands in the global configuration mode:

Command	Function
Ruijie# <b>configure terminal</b>	Enter the global configuration mode.
Ruijie(config)# <b>spanning-tree mst configuration</b>	Enter the MST configuration mode.
Ruijie(config-mst)# <b>instance</b> <i>instance-id</i> <b>vlan</b> <i>vlan-range</i>	<p>Add a VLAN group to a MST instance.</p> <p><i>instance-id</i>: Instance ID ranging from 0 to 64.</p> <p><i>vlan-range</i>: VLAN range in the range 1 to 4094.</p> <p>For instance:</p> <p>The <b>instance 1 vlan 2-200</b> command is to add VLAN 2-200 to instance 1.</p> <p>The <b>instance 1 vlan 2,20,200</b> command is to add VLAN 2, VLAN 20 and VLAN 200 to instance 1.</p> <p>You can use the <b>no</b> option of this command to delete a VLAN from an instance, and the deleted VLAN will be added to instance 0 automatically.</p>
Ruijie(config-mst)# <b>name</b> <i>name</i>	Specify the MST configuration name, a string of up to 32 bytes.
Ruijie(config-mst)# <b>revision</b> <i>version</i>	Specify the MST revision number in the range 0 to 65535. The default value is 0.
Ruijie(config-mst)# <b>show spanning-tree mst configuration</b>	Verify the configuration.
Ruijie(config-mst)# <b>end</b>	Return to the privileged EXEC mode.
Ruijie# <b>copy running-config startup-config</b>	Save the configuration.

To restore the MST region configuration to the default value, execute the **no spanning-tree mst configuration** command in the global configuration mode. You can use the **no instance** *instance-id* command to delete an instance. Similarly, the **no name** and **no revision** commands can be used to restore the MST name and MST revision number settings to the default value, respectively.

The following is the example of configuration:

```
Ruijie(config)# spanning-tree mst configuration
Ruijie(config-mst)# instance 1 vlan 10-20
Ruijie(config-mst)# name region1
Ruijie(config-mst)# revision 1
Ruijie(config-mst)# show spanning-tree mst configuration
Multi spanning tree protocol : Enable Name [region1]
Revision 1
Instance Vlans Mapped
-----
```

```
0 1-9,21-4094
```

```
1 10-20
```

```
-----
Ruijie(config-mst)# exit
```

```
Ruijie(config)#
```



### Caution

Before configuring vlan and instance mapping relationship, please ensure that all configured VLANs have been created. Otherwise, the association of vlan and instance on part of the products may be failed.

## Configuring Maximum-Hop Count

Maximum-Hop Count means how many devices the BPDU message will pass through in a MSTP region before being discarded. This parameter takes effect for all instances.

To configure the Maximum-Hop Count, execute the following commands in the global configuration mode:

Command	Function
Ruijie# <b>configure terminal</b>	Enter the global configuration mode.
Ruijie(config)# <b>spanning-tree max-hops</b> <i>hop-count</i>	Configure the Maximum-Hop Count ranging from 1 to 40, 20 by default.
Ruijie(config)# <b>end</b>	Return to the privileged EXEC mode.
Ruijie# <b>show running-config</b>	Verify the configuration.
Ruijie# <b>copy running-config startup-config</b>	Save the configuration.

To restore the Maximum-Hop Count to the default value, execute the **no spanning-tree max-hops** command in the global configuration mode.

## Configuring Interface Compatibility Mode

In interface compatibility mode, when a port sends BPDU, it will carry different MSTI information according to the current port attribute to realize interconnection with other vendors.

To configure the interface compatibility mode, execute the following commands in the privileged EXEC mode:

Command	Function
Ruijie# <b>configure terminal</b>	Enter the global configuration mode.
Ruijie(config)# <b>interface</b> <i>interface-id</i>	Enter the Interface configuration mode.
Ruijie(config-if)# <b>spanning-tree compatible enable</b>	Enable interface compatibility mode.
Ruijie(config-if)# <b>end</b>	Return to the privileged EXEC mode.
Ruijie# <b>show running-config</b>	Check configuration items.
Ruijie# <b>copy running-config startup-config</b>	Save the configuration.

To remove the settings, you can execute command **no spanning-tree compatible enable**.

## Configuring Optional MSTP Features

### Default Setting of Optional Spanning Tree Features

All the optional features are disabled by default, except for AutoEdge and TC filtering functions.

### Enabling Port Fast

Enabling Port Fast lets a port directly forward the BPDU message. When Port Fast is disabled due to the receipt of the BPDU message, the port will participate in the STP algorithm and forward the BPDU message normally.

To enable Port Fast, execute the following commands in the global configuration mode:

Command	Function
Ruijie# <b>configure terminal</b>	Enter the global configuration mode.
Ruijie(config)# <b>interface</b> <i>interface-id</i>	Enter the interface configuration mode. A legal interface contains a physical port and an Aggregate Link.
Ruijie(config-if)# <b>spanning-tree Portfast</b>	Enable Port Fast on the interface.
Ruijie(config-if)# <b>end</b>	Return to the privileged EXEC mode.
Ruijie# <b>show spanning-tree interface</b> <i>interface-id</i> <b>portfast</b>	Verify the configuration.
Ruijie# <b>copy running-config startup-config</b>	Save the configuration.

To disable Port Fast, execute the **spanning-tree portfast disable** command in the interface configuration mode.

You can use the **spanning-tree portfast default** command in the global configuration mode to enable Port Fast on all ports.

### Disabling AutoEdge

If the designated port does not receive any BPDU messages within 3 seconds, it is identified as the edge port automatically. However, Port Fast Operational State is disabled if the AutoEdge port receives BPDU messages. AutoEdge is enabled by default.

To disable AutoEdge, execute the following commands in the global configuration mode:

Command	Function
Ruijie# <b>configure terminal</b>	Enter the global configuration mode.
Ruijie(config)# <b>interface</b> <i>interface-id</i>	Enter the interface configuration mode. A legal interface contains a physical port and an Aggregate Link.
Ruijie(config-if)# <b>spanning-tree autoedge</b>	Enable AutoEdge on the interface.
Ruijie(config-if)# <b>end</b>	Return to the privileged EXEC mode.



Command	Function
Ruijie# <b>show spanning-tree interface <i>interface-id</i> portfast</b>	Verify the configuration.
Ruijie# <b>copy running-config startup-config</b>	Save the configuration.

To disable AutoEdge, execute the **spanning-tree autoedge disable** command in the interface configuration mode.

## Enabling BPDU Guard

After BPDU Guard is enabled, a port will in the error-disabled status after receiving the BPDU packet.

To configure the BPDU guard, execute the following commands in the global configuration mode:

Command	Function
Ruijie# <b>configure terminal</b>	Enter the global configuration mode.
Ruijie(config)# <b>spanning-tree portfast Bpduguard default</b>	Enable the BPDU Guard globally.
Ruijie(config)# <b>interface <i>interface-id</i></b>	Enter the interface configuration mode. A legal interface contains a physical port and an aggregate link.
Ruijie(config-if)# <b>spanning-tree portfast</b>	Enable Port Fast on the interface before the bpduguard configuration takes effect globally.
Ruijie(config-if)# <b>end</b>	Return to the privileged EXEC mode.
Ruijie# <b>show running-config</b>	Verify the configuration.
Ruijie# <b>copy running-config startup-config</b>	Save the configuration.

To disable BPDU Guard, execute the **no spanning-tree portfast bpduguard default** command in the global configuration command.

To enable or disable BPDU Guard on an interface, execute the **spanning-tree bpduguard enable** command or the **spanning-tree bpduguard disable** command on the interface respectively.

## Enabling BPDU Filter

A port neither transmit nor receive the BPDU message after the BPDU filter is enabled.

To configure the BPDU Filter, execute the following commands in the global configuration mode:

Command	Function
Ruijie# <b>configure terminal</b>	Enter the global configuration mode.
Ruijie(config)# <b>spanning-tree portfast bpdupfilter default</b>	Enable BPDU filter globally.
Ruijie(config)# <b>interface <i>Interface-id</i></b>	Enter the interface configuration mode. A legal interface contains a physical port and an aggregate link.
Ruijie(config-if)# <b>spanning-tree Portfast</b>	Enable portfast on this interface before the bpduguard configuration takes effect globally.

Command	Function
Ruijie(config-if)# <b>end</b>	Return to the privileged EXEC mode.
Ruijie# <b>show running-config</b>	Verify the configuration.
Ruijie# <b>copy running-config startup-config</b>	Save the configuration.

To disable BPDU Filter, execute the **no spanning-tree portfast bpdupfilter default** command in the global configuration mode.

To enable or disable BPDU Filter on an interface, execute the **spanning-tree bpdupfilter enable** command or the **spanning-tree bpdupfilter disable** command in the interface configuration mode.

## Enabling Tc\_Protection

To configure Tc\_Protection, execute the following commands in the global configuration mode:

Command	Function
Ruijie# <b>configure terminal</b>	Enter the global configuration mode.
Ruijie(config)# <b>spanning-tree tc-protection</b>	Enable Tc-Protection
Ruijie(config)# <b>end</b>	Return to the privileged EXEC mode.
Ruijie# <b>show running-config</b>	Verify the configuration.
Ruijie# <b>copy running-config startup-config</b>	Save the configuration.

To disable Tc\_Protection, execute the **no spanning-tree tc-protection** command in the global configuration mode.

## Enabling TC Guard

To enable TC Guard globally, execute the following commands in the global configuration mode:

Command	Function
Ruijie# <b>configure terminal</b>	Enter the global configuration mode.
Ruijie(config)# <b>spanning-tree tc-protection tc-guard</b>	Enable TC Guard globally.
Ruijie(config)# <b>end</b>	Return to the privileged EXEC mode.
Ruijie# <b>show running-config</b>	Verify the configuration.
Ruijie# <b>copy running-config startup-config</b>	Save the configuration.

To configure TC Guard on an interface, execute the following commands in the interface configuration mode:

Command	Function
Ruijie# <b>configure terminal</b>	Enter the global configuration mode.

Command	Function
Ruijie(config)# <b>interface</b> <i>Interface-id</i>	Enter the interface configuration mode. A legal interface includes a physical port and an aggregate link.
Ruijie(config-if)# <b>spanning-tree tc-guard</b>	Enable TC Guard on this interface.
Ruijie(config-if)# <b>end</b>	Return to the privileged EXEC mode.
Ruijie# <b>show running-config</b>	Verify the configuration.
Ruijie# <b>copy running-config startup-config</b>	Save the configuration.

## Enabling TC Filtering

To enable TC filtering, execute the following commands:

Command	Function
Ruijie# <b>configure terminal</b>	Enter the global configuration mode.
Ruijie(config)# <b>interface</b> <i>interface-id</i>	Enter interface configuration mode. The valid interface includes physical port and Aggregate Link.
Ruijie(config)# <b>spanning-tree ignore tc</b>	Enable TC filtering for this interface.
Ruijie(config)# <b>end</b>	Return to the privileged EXEC mode.
Ruijie# <b>show running-config</b>	Verify the configuration.
Ruijie# <b>copy running-config startup-config</b>	Save the configuration.

By default, the TC filtering function is enabled. To disable TC filtering, use the **no spanning-tree ignore tc** command in interface configuration mode.

## Enabling BPDU Source MAC check

After the BPDU source MAC check is enabled, the switch accepts only the BPDU message from the specified MAC address.

To configure the BPDU source MAC check, execute the following commands in the interface configuration mode:

Command	Function
Ruijie# <b>configure terminal</b>	Enter the global configuration mode.
Ruijie(config)# <b>interface</b> <i>interface-id</i>	Enter the interface configuration mode. A legal interface includes a physical port and an aggregate link.
Ruijie(config-if)# <b>bpdu src-mac-check</b> H.H.H	Enable BPDU source MAC check.
Ruijie(config-if)# <b>end</b>	Return to the privileged EXEC mode.

Command	Function
Ruijie# <b>show running-config</b>	Verify the configuration.
Ruijie# <b>copy running-config startup-config</b>	Save the configuration.

To disable BPDU source MAC check, execute the **no bpdu src-mac-check** command in the interface mode.

## Enabling Root Guard

To configure interface ROOT Guard, execute the following commands in the privileged mode:

Command	Function
Ruijie# <b>configure terminal</b>	Enter the global configuration mode.
Ruijie(config)# <b>interface</b> <i>interface-id</i>	Enter the interface configuration mode. Valid interface includes physical port and Aggregate Link.
Ruijie(config-if)# <b>spanning-tree guard root</b>	Enable interface ROOT Guard.
Ruijie(config-if)# <b>end</b>	Return to the privileged EXEC mode.
Ruijie# <b>show running-config</b>	Verify the configuration.
Ruijie# <b>copy running-config startup-config</b>	Save the configuration.

## Enabling Loop Guard

To configure global LOOP Guard, execute the following commands in the privileged EXEC mode:

Command	Function
Ruijie# <b>configure terminal</b>	Enter the global configuration mode.
Ruijie(config)# <b>spanning-tree loopguard default</b>	Enable global LOOP Guard.
Ruijie(config)# <b>end</b>	Return to the privileged EXEC mode.
Ruijie# <b>show running-config</b>	Verify the configuration.
Ruijie# <b>copy running-config startup-config</b>	Save the configuration.

To configure interface LOOP Guard, execute the following commands in the privileged EXEC mode:

Command	Function
Ruijie# <b>configure terminal</b>	Enter the global configuration mode.
Ruijie(config)# <b>interface</b> <i>interface-id</i>	Enter the interface configuration mode. Valid interface includes physical port and Aggregate Link.

Command	Function
Ruijie(config-if)# <b>spanning-tree guard loop</b>	Enable interface Loop Guard.
Ruijie(config-if)# <b>end</b>	Return to the privileged EXEC mode.
Ruijie# <b>show running-config</b>	Verify the configuration.
Ruijie# <b>copy running-config startup-config</b>	Save the configuration.

## Disabling Interface Guard

To disable interface ROOT or LOOP Guard, execute the following commands in the privileged EXEC mode:

Command	Function
Ruijie# <b>configure terminal</b>	Enter the global configuration mode.
Ruijie(config)# <b>interface</b> <i>interface-id</i>	Enter the interface configuration mode. Valid interface includes physical port and Aggregate Link.
Ruijie(config-if)# <b>spanning-tree guard none</b>	Disable interface Loop Guard.
Ruijie(config-if)# <b>end</b>	Return to the privileged EXEC mode.
Ruijie# <b>show running-config</b>	Verify the configuration.
Ruijie# <b>copy running-config startup-config</b>	Save the configuration.

## Showing MSTP Configuration and Status

You can use the following show commands to view the configuration of MSTP:

Command	Meaning
Ruijie# <b>show spanning-tree</b>	Show the information on the parameters and topology of MSTP.
Ruijie# <b>show spanning-tree summary</b>	Show the information on various instances and port forwarding status of MSTP.
Ruijie# <b>show spanning-tree inconsistentports</b>	Show the block port due to root guard or loop guard.
Ruijie# <b>show spanning-tree mst Configuration</b>	Show the configuration information of the MST region.
Ruijie# <b>show spanning-tree mst</b> <i>instance-id</i>	Show the MSTP information of an instance.

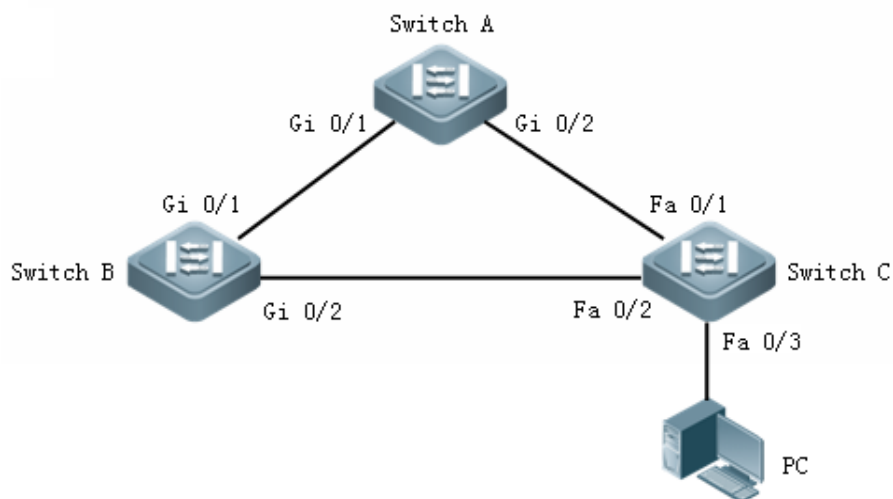
Command	Meaning
Ruijie# <b>show spanning-tree mst</b> <i>instance-id interface interface-id</i>	Show the MSTP information of the specified instance of the interface.
Ruijie# <b>show spanning-tree interface</b> <i>interface-id</i>	Show the MSTP information of all the instances of the interface.
Ruijie# <b>show spanning-tree forward-time</b>	Show forward-time.
Ruijie# <b>show spanning-tree Hello Time</b>	Show Hello time.
Ruijie# <b>show spanning-tree max-hops</b>	Show max-hops.
Ruijie# <b>show spanning-tree tx-hold-count</b>	Show tx-hold-count.
Ruijie# <b>show spanning-tree pathcost Method</b>	Show pathcost method.

## MSTP Configuration Example

### Configuration Purpose

1. Interconnect three switches to construct a triangle ring network and MSTP configuration mode.
2. Set the corresponding VLAN-INSTANCE mapping, MST configuration name, MST Revision Number and the instance priority on the switches.
3. View the MSTP configurations.
4. Enable BPDU Guard function globally and set PortFast function on the port connecting to the PC directly.

### Topology



### Configuration Steps

#### 1) Configuring Switch A

# Set interface Gi0/1 and Gi 0/2 as Trunk port and create VLAN 2 and VLAN 3

```
Ruijie# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Ruijie(config)# interface gigabitEthernet 0/1
Ruijie(config-if)# switchport mode trunk
Ruijie(config-if)# exit
Ruijie(config)# interface gigabitEthernet 0/2
Ruijie(config-if)# switchport mode trunk
Ruijie(config-if)# exit
Ruijie(config)# vlan 2
Ruijie(config-vlan)# exit
Ruijie(config)# vlan 3
Ruijie(config-vlan)# exit
```

# Set the spanning tree to MSTP mode, VLAN 2-Instance 1 and VLAN 3-Instance 2 mapping, and set the MST configuration name to Ruijie, MST Revision Number to 1. View the MST configurations and enable the spanning tree protocol.

```
Ruijie(config)# spanning-tree mode mstp
Ruijie(config)# spanning-tree mst configuration
Ruijie(config-mst)# instance 1 vlan 2
%Warning:you must create vlans before configuring instance-vlan relationship
Ruijie(config-mst)# instance 2 vlan 3
%Warning:you must create vlans before configuring instance-vlan relationship
Ruijie(config-mst)# name Ruijie
Ruijie(config-mst)# revision 1
Ruijie(config-mst)# show
Multi spanning tree protocol : Enable
Name      : Ruijie
Revision  : 1
Instance  Vlans Mapped
-----
0          : 1, 4-4094
1          : 2
2          : 3
-----
Ruijie(config-mst)# exit
Ruijie(config)# spanning-tree
Enable spanning-tree.
```

# Set the priority for Instance 0 to 4096

```
Ruijie(config)# spanning-tree mst 0 priority 4096
```

## 2) Configuring Switch B

# Set interface Gi0/1 and Gi 0/2 as Trunk port and create VLAN 2 and VLAN 3

```
Ruijie(config)# interface gigabitEthernet 0/1
Ruijie(config-if)# switchport mode trunk
Ruijie(config-if)# exit
Ruijie(config)# interface gigabitEthernet 0/2
Ruijie(config-if)# switchport mode trunk
Ruijie(config-if)# exit
Ruijie(config)# vlan 2
Ruijie(config-vlan)# exit
Ruijie(config)# vlan 3
Ruijie(config-vlan)# exit
```

# Set the spanning tree to MSTP mode, VLAN 2-Instance 1 and VLAN 3-Instance 2 mapping, and set the MST configuration name to Ruijie, MST Revision Number to 1. View the MST configurations and enable the spanning tree protocol.



```
Ruijie(config)# spanning-tree mode mstp
Ruijie(config)# spanning-tree mst configuration
Ruijie(config-mst)# instance 1 vlan 2
%Warning:you must create vlans before configuring instance-vlan relationship
Ruijie(config-mst)# instance 2 vlan 3
%Warning:you must create vlans before configuring instance-vlan relationship
Ruijie(config-mst)# name Ruijie
Ruijie(config-mst)# revision 1
Ruijie(config-mst)# exit
Ruijie(config)# spanning-tree
Enable spanning-tree.
```

# Set the priority for Instance 0 to 4096

```
Ruijie(config)# spanning-tree mst 1 priority 4096
```

### 3) Configuring Switch C

# Set interface Gi0/1 and Gi 0/2 as Trunk port and create VLAN 2 and VLAN 3

```
Ruijie(config)# interface fastEthernet 0/1
Ruijie(config-if)# switchport mode trunk
Ruijie(config-if)# exit
Ruijie(config)# interface fastEthernet 0/2
Ruijie(config-if)# switchport mode trunk
Ruijie(config-if)# exit
Ruijie(config)# vlan 2
Ruijie(config-vlan)# exit
Ruijie(config)# vlan 3
Ruijie(config-vlan)# exit
```

# Set the spanning tree to MSTP mode, VLAN 2-Instance 1 and VLAN 3-Instance 2 mapping, and set the MST configuration name to Ruijie, MST Revision Number to 1. View the MST configurations and enable the spanning tree protocol.

```
Ruijie(config)# spanning-tree mode mstp
Ruijie(config)# spanning-tree mst configuration
Ruijie(config-mst)# instance 1 vlan 2
%Warning:you must create vlans before configuring instance-vlan relationship
Ruijie(config-mst)# instance 2 vlan 3
%Warning:you must create vlans before configuring instance-vlan relationship
Ruijie(config-mst)# name Ruijie
Ruijie(config-mst)# revision 1
Ruijie(config-mst)# exit
Ruijie(config)# spanning-tree
Enable spanning-tree.
```

# Set the highest priority for Instance 2

```
Ruijie(config)# spanning-tree mst 2 priority 4096
```

# Enable BPDU Guard function globally and set the interface Fa 0/3 to Port Fast-enabled port.

```
Ruijie(config)# spanning-tree portfast bpduguard default
Ruijie(config)# interface fastEthernet 0/3
Ruijie(config-if)#spanning-tree portfast
%Warning: portfast should only be enabled on ports connected to a single host. Connecting hubs,
Ruijiees, bridges to this interface when portfast is enabled,can cause temporary loops.
Ruijie(config-if)# end
```

# View the spanning tree configurations

```
Ruijie# show spanning-tree
StpVersion : MSTP
SysStpStatus : ENABLED
MaxAge : 20
HelloTime : 2
ForwardDelay : 15
BridgeMaxAge : 20
BridgeHelloTime : 2
BridgeForwardDelay : 15
MaxHops: 20
TxHoldCount : 3
PathCostMethod : Long
BPDUGuard : enabled
BPDUFilter : Disabled
LoopGuardDef : Disabled
##### mst 0 vlans map : 1, 4-4094
BridgeAddr : 00d0.f82a.aa8e
Priority: 32768
TimeSinceTopologyChange : 0d:0h:19m:44s
TopologyChanges : 1
DesignatedRoot : 1000.00d0.f822.33aa
RootCost : 0
RootPort : 1
CistRegionRoot : 1000.00d0.f822.33aa
CistPathCost : 200000
##### mst 1 vlans map : 2
BridgeAddr : 00d0.f82a.aa8e
Priority: 32768
TimeSinceTopologyChange : 0d:0h:1m:46s
TopologyChanges : 7
DesignatedRoot : 1001.00d0.f834.56f0
RootCost : 200000
RootPort : 2
##### mst 2 vlans map : 3
BridgeAddr : 00d0.f82a.aa8e
Priority: 4096
```

```
TimeSinceTopologyChange : 0d:0h:1m:44s
TopologyChanges : 5
DesignatedRoot : 1002.00d0.f82a.aa8e
RootCost : 0
RootPort : 0
```

# View the spanning tree configurations on the interface Fa 0/1

```
Ruijie# show spanning-tree interface fastEthernet 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 :1, 4-4094
PortState : forwarding
PortPriority : 128
PortDesignatedRoot : 1000.00d0.f822.33aa
PortDesignatedCost : 0
PortDesignatedBridge :1000.00d0.f822.33aa
PortDesignatedPort : 8002
PortForwardTransitions : 1
PortAdminPathCost : 200000
PortOperPathCost : 200000
Inconsistent states : normal
PortRole : rootPort
##### MST 1 vlans mapped :2
PortState : discarding
PortPriority : 128
PortDesignatedRoot : 1001.00d0.f834.56f0
PortDesignatedCost : 0
PortDesignatedBridge :8001.00d0.f822.33aa
PortDesignatedPort : 8002
PortForwardTransitions : 5
PortAdminPathCost : 200000
PortOperPathCost : 200000
Inconsistent states : normal
PortRole : alternatePort
##### MST 2 vlans mapped :3
PortState : forwarding
PortPriority : 128
PortDesignatedRoot : 1002.00d0.f82a.aa8e
```

```
PortDesignatedCost : 0
PortDesignatedBridge :1002.00d0.f82a.aa8e
PortDesignatedPort : 8001
PortForwardTransitions : 1
PortAdminPathCost : 200000
PortOperPathCost : 200000
Inconsistent states : normal
PortRole : designatedPort
```

# Transparent Transmission of Protocol Frames Configuration

## Overview

The protocol frame transparent transmission function enables protocol frames to be forwarded to other network devices when a specific protocol is enabled.

The protocols that support transparent transmission include BPDU, GVRP, 802.1X, reserved multicast protocol, and Cisco private STP (PVST) protocol. The protocol frames are described as follows:

**BPDU frames:** Frames used in spanning tree protocols, including frames stipulated by the IEEE standards and Ruijie private protocol frames. This document configures transparent transmission for Ruijie's BPDU frames, which are identified by the Layer 2 destination MAC address 01D0:F800:0000.

**GVRP frames:** Frames used for VLAN registration, including frames stipulated by the IEEE standards and Ruijie private protocol frames. This document configures transparent transmission for Ruijie private GVRP frames, which are identified by the Layer 2 destination MAC address 01D0:F800:0021.

**802.1X frames:** Standard frames developed by the IEEE for authentication of users accessing the network, including frames stipulated by the IEEE standards and private protocol frames of Ruijie. The frames are identified by the Layer 2 destination MAC address, which is 0180:C200:0003 for standard protocol frames and 01D0:F800:0003 for Ruijie 802.1X frames.

**Reserved multicast protocol frames:** Reserved multicast addresses stipulated by the IEEE. These reserved multicast addresses are identified by the Layer 2 destination MAC addresses. The multicast addresses that support transparent transmission range from 0180:C200:0000 to 0180:C200:FFFF in this document. If these addresses conflict with those of the 802.1X frames, the addresses in the 802.1X frames are prior to use.

**PVST frames:** Cisco's spanning tree protocol frames. These frames are identified by the destination MAC address 0100:0CCC:CCCD.

## Configuring Transparent Transmission of Protocol Frames

The default setting of transparent transmission of protocol frames are listed below. When the relevant protocol is disabled, these protocol frames are regarded as Layer 2 multicast addresses.

Feature	Default
Transparent transmission of BPDU frames	Disabled
Transparent transmission of GVRP frames	Disabled
Transparent transmission of 802.1X frames	Enabled
Transparent transmission of reserved multicast frames	Enabled

Transparent transmission of PVST frames	Enabled
---	---------

## Configuring Transparent Transmission of BPDU Frames

Execute the following commands globally to enable transparent transmission of BPDU frames:

Command	Function
Ruijie# <b>configure terminal</b>	Enters the global configuration mode
Ruijie(config)# <b>bridge-frame forwarding protocol bpdu</b>	Enables transparent transmission of BPDU frames
Ruijie(config)# <b>end</b>	Returns to the privileged mode

## Configuring Transparent Transmission of GVRP Frames

Execute the following commands globally to enable transparent transmission of GVRP frames:

Command	Function
Ruijie# <b>configure terminal</b>	Enters the global configuration mode
Ruijie(config)# <b>bridge-frame forwarding protocol gvrp</b>	Enables transparent transmission of GVRP frames
Ruijie(config)# <b>end</b>	Returns to the privileged mode

## Configuring Transparent Transmission of 802.1X Frames

Execute the following commands globally to enable transparent transmission of 802.1X frames:

Command	Function
Ruijie# <b>configure terminal</b>	Enters the global configuration mode
Ruijie(config)# <b>bridge-frame forwarding protocol 802.1x</b>	Enables transparent transmission of 802.1X frames
Ruijie(config)# <b>end</b>	Returns to the privileged mode

## Configuring Transparent Transmission of Reserved Multicast Frames

Execute the following commands globally to enable transparent transmission of reserved multicast frames:

Command	Function
Ruijie# <b>configure terminal</b>	Enters the global configuration mode.
Ruijie(config)# <b>bridge-frame forwarding protocol reserved-multicast</b>	Enables transparent transmission of reserved multicast frames.
Ruijie(config)# <b>end</b>	Returns to the privileged mode.

## Configuring Transparent Transmission of PVST Frames

Execute the following commands globally to enable transparent transmission of Cisco's PVST frames:

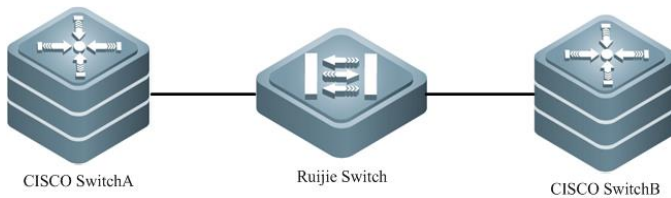
Command	Function
Ruijie# <b>configure terminal</b>	Enters the global configuration mode.
Ruijie(config)# <b>bridge-frame forwarding protocol cisco-pvst</b>	Enables transparent transmission of Cisco's PVST frames.
Ruijie(config)# <b>end</b>	Returns to the privileged mode.

## Configuration Example

### Configuration Example

#### Networking topology

Figure 1-1. Simple configuration of transparent transmission of PVST frames



#### Configuration requirements

In this network topology, Ruijie switch is working with Cisco devices. Enable Cisco PVST on the Cisco switches and the multicast function on the Ruijie switch. Make sure that Cisco PVST works properly.

#### Configuration procedure

- 1) Configure transparent transmission of PVST frames on the Ruijie switch.

```
SwitchA# configure terminal
SwitchA(config)# bridge-frame forwarding protocol cisco-pvst
SwitchA(config)# end
```

# GVRP Configuration

## Overview

GVRP (GARP VLAN Registration Protocol) is a GARP (Generic Attribute Registration Protocol) application that dynamically configures and propagates VLAN membership.

Through GVRP protocol, the device can:

- Listen to GVRP PDUs on each port, learn the VLAN information registered on GVRP-aware devices connected according to such GVRP PDUs, and then configure VLAN members on the port receiving GVRP PDUs.
- Propagate VLAN information on each port by sending GVRP PDUs. The VLAN information propagated includes the statically configured VLANs and those learned from other devices via GVRP.

Through GVRP, devices on the switching network can dynamically create VLAN and maintain the consistency of VLAN configurations in a real-time manner. Through automatic declaration of VLAN ID within the network, GVRP well reduces the possibility of faults caused by inconsistent configurations. In case of any change in the VLAN configurations on a device, GVRP can automatically change the VLAN configurations on the connected devices, thus reducing manual configuration works to be done by the user.

GARP and GVRP are defined in the following standards:

- IEEE standard 802.1D
- IEEE standard 802.1Q

## Configure GVRP

### Default Configurations

The following table shows the default configurations of GVRP:

Function	Default setting
GVRP global enable state	Disabled
GVRP dynamic creation of VLANs	Disabled
GVRP base vlan id	VLAN 1 (only effective under MSTP environment)
GVRP registration mode	Enable
GVRP applicant state	Normal, (Ports do not declare VLANs when in STP blocking state)



<b>GVRP timers</b>	Join Time: 200 ms Leave Time: 600 ms Leaveall Time: 10,000 ms
--------------------	---

## GVRP Configuration Guidelines

- GVRP must be enabled on two interconnected devices. GVRP information will only be propagated on Trunk Links, and the information propagated includes all VLANs on the current device, no matter they are dynamically learned or manually configured.
- When running STP (Spanning-tree Protocol), only ports in "Forwarding" state will be GVRP participants (receiving and sending GVRP PDUs); only ports in "Forwarding" state will have their VLAN information propagated by GVRP.
- All VLAN Ports added by GVRP are Tagged Ports.
- All VLAN information dynamically learned by GVRP will not be saved in the system. It means that such information will be lost after the device resets. The user cannot save such dynamically learned VLAN information.
- The user cannot change the parameters of dynamic VLANs created by GVRP.
- All devices requiring exchanging GVRP information must have consistent GVRP Timers (Join, Leave, Leaveall).

## Enable GVRP

You must enable GVRP globally before running GVRP.

When GVRP is not enabled globally, you can configure other GVRP parameters, but these GVRP configurations will only take effect after running GVRP.

Enable GVRP globally:

Command	Function
Ruijie(config)# <b>[no] gvrp enable</b>	Enable GVRP (if it is disabled)

Configuration example:

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

## Enable Dynamic VLAN Creation

When a port receives messages (limited only to Joinin Joinempty) indicating a VLAN which doesn't exist on the local device, GVRP may create this VLAN. The user can control whether or not to create VLAN dynamically.

Enable dynamic VLAN creation:

Command	Function
Ruijie(config)# <b>[no] gvrp dymanic-vlan-creation enable</b>	Enable GVRP to create VLAN dynamically (if it is disabled)

The user cannot change the parameters of dynamic VLANs created by GVRP.

Configuration example:

```
Ruijie# configure
Enter configuration commands, one per line. End with CNTL/Z.
Ruijie(config)# gvrp dymanic-vlan-creation enable
Ruijie(config)# end
```

## Configure the GVRP VLAN

In the context without STP (Spanning-tree protocol), all available ports can be GVRP participants.

In the context with SST (Single Spanning-tree), only ports showing "Forwarding" state in the current SST Context can be GVRP participants. In the context with MST (Multiple Spanning-tree), GVRP can run in the Spanning-tree Context which VLAN 1 is affiliated with, and the user cannot specify other Spanning-tree Contexts.

## Configure Port Registration Mode

There are two port registration modes:

- GVRP Registration Normal
- GVRP Registration Disabled

Configuring a port in **normal registration** mode allows dynamic creation (if dynamic VLAN creation is enabled), registration, and deregistration of VLANs on the port.

When a port is configured to "disabled registration" mode, no dynamic VLAN registration or deregistration will be allowed.

Configure GVRP Registration Mode of port:

Command	Function
Ruijie(config-if)# <b>[no] gvrp registration mode {normal   disabled}</b>	Configure GVRP registration mode of the port

These two registration modes will not affect static VLANs on the port. The static VLANs created by the user are always "Fixed Registrar".

Example of enabling Registration Mode on port 1:

```
Ruijie# configure
Enter configuration commands, one per line. End with CNTL/Z.
Ruijie(config)# interface gigabitethernet 1/1
Ruijie(config-if)# gvrp registration mode enable normal
Ruijie(config-if)# end
```

## Configure Port Declaration Mode

There are two declaration modes to control whether the port will send GVRP declarations.

### ■ GVRP Normal Applicant

Allowing the declaration of VLANs on the port, including all dynamic and static VLANs.

### ■ GVRP Non-Appllicant

Prohibiting the declaration of VLANs on the port.

Configure declaration mode of the port:

Command	Function
Ruijie(config-if)# <b>[no] gvrp applicant state {normal   non-appllicant}</b>	Configure GVRP declaration mode of the port

Example of configuring Applicant Mode on port 1:

```
Ruijie# configure
Enter configuration commands, one per line. End with CNTL/Z.
Ruijie(config)# interface gigabitethernet 1/1
Ruijie(config-if)# gvrp applicant state normal
Ruijie(config-if)# end
```

## Configure GVRP Timers

GVRP uses three timers:

### 1. Join Timer

Join timer controls the maximum latency before the port sends declaration, and the actual sending interval will range between 0 and this maximum latency. The default value is 200ms.

### 2. Leave Timer

Leave Timer controls the time required to delete port from VLAN after receiving the Leave Message. If the port receives Join Message again during this period, then the port will maintain VLAN membership, and the timer become void. If the port doesn't receive Join Message before the timer runs out, then the port will be deleted from the VLAN membership table. The default value is 600ms.

### 3. LeaveAll Timer

LeaveAll Timer controls the minimum interval to send LeaveAll Message on the port. If the port receives LeaveAll Message before the timer runs out, then the timer will start timing again; if the timer runs out, it will send LeaveAll Message on the port and to the port as well, thus triggering the Leave Timer. The default value is 10,000ms. The actual sending interval ranges between Leaveall and Leaveall+Join.

**Caution**

When configuring the timer, make sure Leave Value is greater than or equal to three times the Join Value (Leave  $\geq$  Join  $\times 3$ ). Meanwhile, Leaveall must be greater than Leave (Leaveall  $>$  Leave). If the aforementioned conditions cannot be met, the timer configuration may fail. For example, after setting Leave Timer to 600ms, the system may prompt an error if you configure Join Timer to 320ms. To achieve successful configuration, when Join Timer is set to 350ms, the Leave Timer must be greater than 1050ms.

The effective size for timer configuration is 10ms.

Make sure all interconnected GVRP devices use the same GVRP Timer configurations, or else the GVRP may not function well.

Adjust the value of GVRP Timer:

Command	Function
Ruijie(config)# [no] <b>gvrp timer</b> {join   leave   leaveall} <i>timer-value</i>	Set the timer value of port

Example of setting GVRP Join Timer:

```
Ruijie# configure
Enter configuration commands, one per line. End with CNTL/Z.
Ruijie(config)# gvrp timer join 1000
Ruijie(config)# end
```

## Display the GVRP Configurations

### Display GVRP Statistics

GVRP statistics are calculated by port. For details about how to use the command to display statistics and the meaning of each statistical value, please refer to the command of "**show gvrp statistics**".

Display the GVRP statistics for the port:

Command	Function
Ruijie# <b>show gvrp statistics</b> { <i>interface-id</i>   all}	Display statistics for the port

Example of displaying GVRP statistics:

```
Ruijie# show gvrp statistics gigabitethernet 1/1
Interface GigabitEthernet 3/1
RecValidGvrpPdu    0
RecInvalidGvrpPdu  0
```

```

RecJoinEmpty    0
RecJoinIn       0
RecEmpty        0
RecLeaveEmpty    0
RecLeaveIn       0
RecLeaveAll      0
SentGvrpPdu     0
SentJoinEmpty   0
SentJoinIn      0
SentEmpty       0
SentLeaveEmpty   0
SentLeaveIn      0
SentLeaveAll     0
JoinIndicated   0
LeaveIndicated   0
JoinPropagated  0
LeavePropagated  0

```

To clear all GVRP statistics so that it will restart calculation:

Command	Function
Ruijie# <b>clear gvrp statistics</b> { <i>interface-id</i>   <b>all</b> }	Clear all statistics for the port

Example of clearing GVRP statistics for port 1:

```
Ruijie# clear gvrp statistics gigabitethernet 1/1
```

## Display GVRP status

Execute "**show gvrp status**" command to display the current GVRP status. This command can be used to display the dynamic ports of dynamically created VLANs and static VLANs.

Command	Function
Ruijie# <b>show gvrp status</b>	Display current GVRP status

Configuration example:

```

Ruijie# show gvrp status
VLAN 1
Dynamic Ports:
DVLAN 5
Dynamic Ports:
Port:GigabitEthernet 3/1

```

## Display Current GVRP Configurations

Execute "**show gvrp configuration**" command to display the current GVRP status. This command can be used to display the dynamic ports of dynamically created VLANs and static VLANs.

Command	Function
Ruijie# <b>show gvrp configuration</b>	Display current GVRP configurations

### Configuration example:

```
Ruijie# show gvrp configuration
Global GVRP Configuration:
GVRP Feature:enabled
GVRP dynamic VLAN creation:enabled
Join Timers(ms):200
Join Timers(ms):600
Join Timers(ms):10000
Port based GVRP Configuration:
Port:GigabitEthernet 3/1 app mode:normal reg mode:normal
Port:GigabitEthernet 3/2 app mode:normal reg mode:normal
Port:GigabitEthernet 3/3 app mode:normal reg mode:normal
Port:GigabitEthernet 3/4 app mode:normal reg mode:normal
Port:GigabitEthernet 3/5 app mode:normal reg mode:normal
Port:GigabitEthernet 3/6 app mode:normal reg mode:normal
Port:GigabitEthernet 3/7 app mode:normal reg mode:normal
Port:GigabitEthernet 3/8 app mode:normal reg mode:normal
Port:GigabitEthernet 3/9 app mode:normal reg mode:normal
Port:GigabitEthernet 3/10 app mode:normal reg mode:normal
Port:GigabitEthernet 3/11 app mode:normal reg mode:normal
Port:GigabitEthernet 3/12 app mode:normal reg mode:normal
```

# LLDP Configuration

## Introduction to LLDP

### LLDP Overview

Drafted by IEEE 802.1AB, LLDP (Link Layer Discovery Protocol) can detect network topology change and identify what the change is. With LLDP, a device sends local device information as TLV (Type, Length and Value) triplets in LLDP Data Units (LLDPDUs) to the neighbor devices, and at the same time, stores the device information received in LLDPDUs sent from the LLDP neighbors in a standard management information base (MIB) to be accessed by the network management system.

Through LLDP, the network management system can learn about the state of topological connections, such as which ports of the device are connected to other devices, the rate of ports on both sides of link, and whether the duplex mode is matched. The network administrator can quickly locate and eliminate faults according to such information.

### Basic Concepts

#### LLDPDU

LLDPDU refers to the data units encapsulated in LLDP packets, and comprises multiple TLV sequences, including three fixed TLVs, a number of optional TLVs and an End of TLV. The detailed format of LLDPDU is shown in Fig 1:

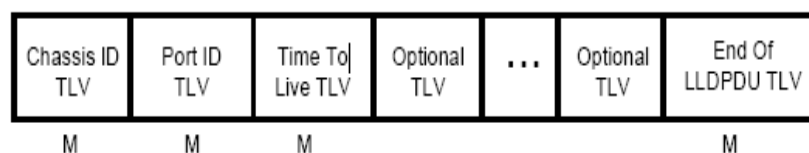


Fig 1 LLDPDU format

\* M refers to fixed TLV.

In LLDPDU, Chassis ID TLV, Port ID TLV, Time To Live TLV and End Of LLDPDU TLV are fixed TLVs, while other TLVs are optional.

#### LLDPDU Encapsulation Format

LLDP packet supports two encapsulation formats: Ethernet II and SNAP (Subnetwork Access Protocols).

Ethernet II encapsulated LLDPDU format is shown in Fig 2:

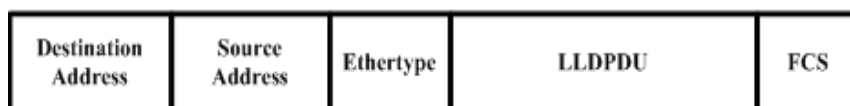


Fig 2 Ethernet II encapsulated LLDPDU format

Specifically:

- Destination Address: destination MAC address. It is fixed to 01-80-C2-00-00-0E, a multicast address.
- Source Address: source MAC address, layer-2 MAC address of device.
- Ethertype: the Ethernet type, 0x88CC.
- LLDPDU: LLDP Data Unit.
- FCS: frame check sequence.

SNAP-encapsulated LLDPDU format is shown in Fig 3:

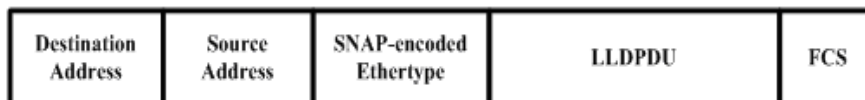


Fig 3 SNAP-encapsulated LLDPDU format

Specifically:

- Destination Address: destination MAC address. It is fixed to 01-80-C2-00-00-0E, a multicast address.
- Source Address: source MAC address, layer-2 MAC address of device.
- SNAP-encoded Ethertype: SNAP-encapsulated Ethernet type, AA-AA-03-00-00-00-88-CC.
- LLDPDU: LLDP Data Unit.
- FCS: frame check sequence.

## TLV

TLVs encapsulated in LLDPDU can fall into two broad categories:

- Basic management TLVs
- Organizationally specific TLVs

Basic management TLVs are a group of basic TLVs for network management. The organizationally specific TLVs are TLVs defined by standards organizations and other organizations, such as IEEE 802.1, IEEE 802.3 and etc.

### 1. Basic management TLVs

Basic management TLVs include two types of TLVs: fixed TLVs and optional TLVs. Fixed TLVs must be included in LLDPDU, while optional TLVs can be included or excluded according to need.

Basic management TLVs are shown in Table 1:

Type	Description	Use in LLDPDU
End Of LLDPDU TLV	End mark of LLDPDU, occupying 2 bytes	Fixed
Chassis ID TLV	Used to identify the device, and is generally represented with MAC address	Fixed
Port ID TLV	ID of the LLDPDU	Fixed



	sending port	
Time To Live TLV	Life of local information on the neighbor device. When TLV with 0 TTL is received, the corresponding neighbor information must be deleted.	Fixed
Port Description TLV	Port description of LLDPDU sending port	Optional
System Name TLV	Name of the sending device	Optional
System Description TLV	Description of the sending device, including hardware/software version, operating system and etc.	Optional
System Capabilities TLV	Identifies the primary functions of the sending device, such as bridging, routing and relaying.	Optional
Management Address TLV	Management address, including interface number and OID (object Identifier).	Optional

Table 3 Basic management TLV

**Note**

Basic management TLVs are supported by the LLDP protocol used by Ruijie switch products.

## 2. Organizationally specific TLVs

Different organizations (such as IEEE 802.1, IEEE 802.3, IETF or device suppliers) may define specific TLVs to advertise specific information about the device, and OUI (Organizationally Unique Identifier) is used to identify different organizations.

Organizationally specific TLVs are optional TLVs advertised in LLDPDU according to user's actual needs. Currently, commonly found organizationally specific TLVs include:

### 1) IEEE 802.1 organizationally specific TLVs

IEEE 802.1 organizationally specific TLVs are shown in Table 2:

Type	Description
Port VLAN ID TLV	VLAN identifier of the sending port
Port And Protocol VLAN ID TLV	Protocol VLAN identifier of the sending port
VLAN Name TLV	Name of VLAN with which the device is configured
Protocol Identity TLV	Protocols supported by the port

Table 4 IEEE 802.1 organizationally specific TLVs

**Note**

LLDP protocol used by Ruijie switch products doesn't support the sending of Protocol Identity TLV, but allows the reception of such TLV.

## 2) IEEE 802.3 organizationally specific TLVs

IEEE 802.3 organizationally specific TLVs are shown in Table 3:

Type	Description
MAC/PHY Configuration/Status TLV	The bit-rate and duplex capabilities of the sending port and support for auto negotiation.
Power Via MDI TLV	Power supply capability of the port
Link Aggregation TLV	Indicate the link aggregation capability of the port and the aggregation status.
Maximum Frame Size TLV	The maximum frame size supported by the port.

Table 5 IEEE 802.3 organizationally specific TLVs

**Note**

IEEE 802.3 organizationally specific TLVs are supported by the LLDP protocol used by Ruijie switch products.

## 3) LLDP-MED TLVs

LLDP-MED is the extension of IEEE 802.1AB LLDP protocol, so that the user can conveniently deploy VoIP (Voice Over IP) network and fault detection. It provides multiple applications such as network policy

configuration, device detection, PoE management and directory management, providing a cost-effective and easy-to-use solution for deploying voice devices in Ethernet.

LLDP-MED TLVs are shown in Table 4:

Type	Description
LLDP-MED Capabilities TLV	Whether the device supports LLDP-MED, the type of LLDP-MED TLV encapsulated in LLDPDU, and the type of current device (network connection device or endpoint)
Network Policy TLV	Advertise VLAN configuration of the specific port, supported applications (voice and video, for example), and the Layer 2 priorities.
Location Identification TLV	Location identifier information for an endpoint, used to accurately locate the endpoint in applications such as network topology collection.
Extended Power-via-MDI TLV	Provide more advanced power supply management.
Inventory – Hardware Revision TLV	Hardware version of MED device
Inventory – Firmware Revision TLV	Firmware version of MED device
Inventory – Software Revision TLV	Software version of MED device
Inventory – Serial Number TLV	Serial number of MED device
Inventory – Manufacturer Name TLV	Vendor name of MED device
Inventory – Model Name TLV	Model name of MED device
Inventory – Asset ID TLV	Asset ID of MED device, used for directory management and asset tracking.

Table 6 LLDP-MED TLVs

**Note**

LLDP-MED TLVs are supported by the LLDP protocol used by Ruijie switch products.

## Working Principles

### Operating Modes of LLDP

LLDP provides three operating modes:

- TxRx: sending and receiving LLDPDUs.
- Rx Only: only sending LLDPDUs.
- Tx Only: only receiving LLDPDUs.

When the LLDP operating mode of a port changes, the port will initialize the protocol state machine. To prevent LLDP from being initialized too frequently during times of frequent operating mode change, you can configure a re-initialization delay.

### Mechanism for Transmitting LLDPDUs

An LLDP-enabled port operating in TxRx mode or Tx Only mode will send LLDPDUs both periodically and when the local device information changes. To avoid frequent LLDPDU sending during times of frequent local device information change, an interval is introduced between two successive LLDPDUs. This interval can be configured manually.

LLDP provides two types of packets:

- Standard LLDPDUs: including the management and configuration information about local device.
- Shutdown LLDPDU: When LLDP sending mode is disabled or when the port is administratively shut down, shutdown LLDPDU will be sent. Shutdown LLDPDU generally comprises Chassis ID TLV, Port ID TLV, Time To Live TLV and End Of LLDP TLV, with the TTL in Time To Live TLV being 0. When the device receives shutdown LLDPDUs, it will consider the neighbor no longer available and delete neighbor information.

When LLDP operating mode changes from shutdown or Rx to TxRx or Tx, or when a new neighbor is detected (namely new LLDPDUs are received and no such neighbor information is stored locally), to allow the neighbor device to quickly study the information about this device, the fast sending mechanism will be initiated. The fast sending mechanism adjusts the LLDPDU sending interval to 1 second and continuously transmits a certain number of LLDPDUs.

### Mechanism for Receiving LLDPDUs

A LLDP-enabled port operating in TxRx mode or Rx Only mode will be able to receive LLDPDUs, and will check the validity of received LLDPDUs to verify they are new neighbor information or updates of existing neighbor information. The neighbor information will be stored on the local device. Meanwhile, an aging timer will be set according to the value in TTL TLV carried in the LLDPDU. If the TTL value is zero, the information is aged out immediately.

## Protocol Specifications

The protocols and standards related to LLDP include:

1. IEEE 802.1AB 2005: Station and Media Access Control Connectivity Discovery
2. ANSI/TIA-1057: Link Layer Discovery Protocol for Media Endpoint Devices

## Default Configurations

The following table describes the default configurations of LLDP.

Function	Default setting
Globally enable LLDP	Enabled
Enable LLDP on the port	Enabled
Operating mode of LLDP	TxRx
Port re-initialization delay	2 seconds
LLDPDU transmit interval	30 seconds
LLDPDU transmit delay	2 seconds
Neighbor information aging timer	120 seconds
LLDPDU encapsulation format	Ethernet II
Enable LLDP Trap	Disabled
LLDP error detection	Enabled

## Configuring LLDP Basic Functions

### Enabling LLDP

By default, LLDP is enabled globally and on each port. To make LLDP take effect on certain ports, you must enable LLDP both globally and on these ports.

Execute the following steps to disable LLDP globally and on each port.

Command	Function
<code>Ruijie(config)#no lldp enable</code>	Disable LLDP globally.
<code>Ruijie(config)# interface interface-name</code>	Enter interface configuration mode. LLDP runs on the actual physical interface (for AP port, it runs on AP's member port). LLDP is not supported on stacking port or VSL port.
<code>Ruijie(config-if)#no lldp enable</code>	Disable LLDP on the interface.
<code>Ruijie(config-if)#show lldp status</code>	Display LLDP state.

To enable LLDP globally or on the port, execute "lldp enable" command.

**Caution**

Disabling the LLDP globally will disable LLDP on the device. Meanwhile, the device will send Shutdown LLDPDUs to neighbor devices in order to delete the corresponding LLDP information.

**Note**

The port can learn up to 5 neighbors.

If a neighbor device does not support the LLDP, but its downlink device does, the information of non-directly connected devices may be learnt on the port as the neighbor device may forward the LLDP packets.

Configuration example:

# Globally disable LLDP and display LLDP state.

```
Ruijie(config)#no lldp enable

Ruijie(config)#show lldp status

Global status of LLDP: Disable
```

## Configuring LLDP Operating Mode

By default, LLDP is enabled on the interface and operates in TxRx mode. The user can change the operating mode to Tx mode or Rx mode as needed. Execute the following steps to configure LLDP operating mode.

Command	Function
Ruijie(config)# <b>interface</b> <i>interface-name</i>	Enter interface configuration mode. LLDP runs on the actual physical interface (for AP port, it runs on AP's member port). LLDP is not supported on stacking port or VSL port.
Ruijie(config-if)# <b>lldp mode { tx   rx   txrx }</b>	Configure LLDP operating mode. The configurable operating modes include Tx, Rx and TxRx.
Ruijie(config-if)# <b>show lldp status interface</b> <i>interface-name</i>	Display LLDP state on the interface.

Configuration example:

# Configure LLDP operating mode as Tx on the interface and display LLDP state on the interface

```
Ruijie(config)#interface gigabitethernet 0/1

Ruijie(config-if-GigabitEthernet 0/1)#lldp mode tx

Ruijie(config-if GigabitEthernet 0/1)#show lldp status interface gigabitethernet 0/1

Port [GigabitEthernet 0/1]

Port status of LLDP           : Enable

Port state                    : UP
```

```

Port encapsulation          : Ethernet II

Operational mode           : TxOnly

Notification enable        : NO

Error detect enable        : YES

Number of neighbors        : 0

Number of MED neighbors    : 0

```

## Configuring the Advertisable TLVs

By default, all TLVs other than Location Identification TLV can be advertised on the interface. Execute the following steps to configure advertisable TLVs on the interface.

Command	Function
Ruijie(config)# <b>interface</b> <i>interface-name</i>	Enter interface configuration mode. LLDP runs on the actual physical interface (for AP port, it runs on AP's member port). LLDP is not supported on stacking port or VSL port.
Ruijie(config-if)# <b>lldp tlv-enable</b> { <b>basic-tlv</b> { <b>all</b>   <b>port-description</b>   <b>system-capability</b>   <b>system-description</b>   <b>system-name</b> }   <b>dot1-tlv</b> { <b>all</b>   <b>port-vlan-id</b>   <b>protocol-vlan-id</b> [ <i>vlan-id</i> ]   <b>vlan-name</b> [ <i>vlan-id</i> ] }   <b>dot3-tlv</b> { <b>all</b>   <b>link-aggregation</b>   <b>mac-physic</b>   <b>max-frame-size</b>   <b>power</b> }   <b>med-tlv</b> { <b>all</b>   <b>capability</b>   <b>inventory</b>   <b>location</b> { <b>civic-location</b>   <b>elin</b> } <b>identifier</b> <i>id</i>   <b>network-policy</b> <b>profile</b> [ <i>profile-num</i> ]   <b>power-over-ethernet</b> } }	By default, all TLVs other than Location Identification TLV can be advertised on the interface.
Ruijie(config-if)# <b>show lldp</b> <b>tlv-config</b> <b>interface</b> <i>interface-name</i>	Display the attributes of advertisable TLVs.

**Note**

- When configuring basic management TLVs, IEEE 802.1 organizationally specific TLVs and IEEE 802.3 organizationally specific TLVs, if "all" parameter is specified, all corresponding optional TLVs will be advertised.
- When configuring LLDP-MED TLVs, if "all" parameter is specified, all LLDP-MED TLVs other than Location Identification TLV will be advertised.
- When configuring LLDP-MED Capability TLV, the LLDP-MED MAC/PHY TLV must be configured as advertisable; When removing the LLDP-MED MAC/PHY TLV, you need to remove LLDP-MED Capability TLVs first.
- When configuring LLDP-MED TLVs, the LLDP-MED Capability TLV must be configured as advertisable in order to further configure other LLDP-MED TLVs as advertisable.
- In order not to advertise LLDP-MED Capability TLV, other LLDP-MED TLVs shall be configured as non-advertisable, so that LLDP-MED TLVs are not advertised.
- For the meaning of respective key words of "lldp tlv-enable", please refer to the descriptions given in "LLDP-CREF".
- When a device downlinks an IP phone, if it supports LLDP-MED, you can deliver policies to the IP phone by configuring network policy TLV. The voice stream tag and QOS are modified by the IP phone and the voice vlan function is not needed, but you need to configure the port connected with the IP phone as a trusted QOS port. If the IP phone does not support LLDP-MED, you must configure the voice vlan function and manually enter the MAC address of the phone into the OUI list of voice vlan.

## Configuration example:

# Configure to disable the advertisement of Port And Protocol VLAN ID TLV specified by IEEE 802.1.

```
Ruijie(config)#interface gigabitethernet 0/1

Ruijie(config-if-GigabitEthernet 0/1)#no lldp tlv-enable dot1-tlv protocol-vlan-id

Ruijie(config-if-GigabitEthernet 0/1)#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	NO	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

## Configuring the Management address Advertised in LLDPDU

The management address of a device is used by the network management system to identify and manage the device. By default, the management address is advertised in LLDPDU, and is the IPv4 address of the lowest-ID VLAN carried on the port.

Execute the following steps to configure the management address to be advertised in LLDPDU:

Command	Function
Ruijie(config)# <b>interface</b> <i>interface-name</i>	Enter interface configuration mode. LLDP runs on the actual physical interface (for AP port, it runs on AP's member port). LLDP is not supported on stacking port or VSL port.
Ruijie(config-if)# <b>lldp</b> <b>management-address-tlv</b> <i>[ip-address]</i>	Configure the management address advertised in LLDPDU

Ruijie(config-if)# <b>show lldp local-information interface interface-name</b>	Display LLDP local information about a specific interface.
--	--

**Note**

- By default, the management address is advertised in LLDPDU, 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 local IP address 127.0.0.1 will be advertised as the management address.

## Configuration example:

# Configure the management address advertised in LLDPDU as 192.168.1.1 and display the corresponding configuration.

```
Ruijie(config)#interface gigabitEthernet 0/1

Ruijie(config-if-GigabitEthernet 0/1)#lldp management-address-tlv 192.168.1.1

Ruijie(config-if-GigabitEthernet 0/1)#show lldp local-information interface GigabitEthernet 0/1

Lldp local-information of port [GigabitEthernet 0/1]

  Port ID type           : Interface name
  Port id                : GigabitEthernet 0/1
  Port description       :

  Management address subtype : ipv4
  Management address       : 192.168.1.1
  Interface numbering subtype : ifIndex
  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 : 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         : dot3MauType100BaseTXFD: 2 pair category 5 UTP, full
duplex mode

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

```

## Configuring the Number of Fast Sent LLDPDUs

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.

Command	Function
<b>Ruijie(config)#lldp fast-count count</b>	Configure the number of fast sent LLDPDUs. Default: 3; configurable range: 1-10.
<b>Ruijie(config-if)#show lldp status</b>	Display LLDP state.

Configuration example:

# Configure the number of fast sent LLDPDUs to 5.

```

Ruijie(config)#lldp fast-count 5

Ruijie(config)#show lldp status

Global status of LLDP                : Enable

Neighbor information last changed time :

Transmit interval                    : 30s

Hold multiplier                      : 4

Reinit delay                        : 2s

Transmit delay                      : 2s

Notification interval               : 5s

Fast start counts                   : 5

```

## Configuring TTL Multiplier and LLDPDU Transmit interval

The value of Time To Live TLV in LLDPDU = TTL multiplier × LLDPDU transmit interval + 1. Therefore, the TTL of local device information on the neighbor device can be controlled by adjusting TTL multiplier.

The LLDPDU transmit interval can be adjusted. Execute the following steps to configure TTL multiplier and LLDPDU transmit interval.

Command	Function
Ruijie(config)#lldp hold-multiplier <i>value</i>	Configure TTL multiplier. Default: 4; configurable range: 2-10.
Ruijie(config)#lldp timer tx-interval <i>seconds</i>	Configure LLDPDU transmit interval. Default: 30 seconds; configurable range: 5-32768 seconds.
Ruijie(config-if)#show lldp status	Display LLDP state.

Configuration example:

# Configure TTL multiplier to 3 and LLDPDU transmit interval to 20 seconds. By this time, the TTL of local device information on the neighbor device is 61 seconds.

```

Ruijie(config)#lldp hold-multiplier 3

Ruijie(config)#lldp timer tx-interval 20

Ruijie(config)#show lldp status

Global status of LLDP                : Enable

Neighbor information last changed time :

Transmit interval                    : 20s

Hold multiplier                      : 3

Reinit delay                        : 2s

Transmit delay                      : 2s

Notification interval               : 5s

```

Fast start counts : 3

## Configuring LLDPDU Transmit Delay

An LLDP-enabled port will send LLDPDUs when the local device information changes. To avoid frequent LLDPDU sending during times of frequent local device information change, we can configure LLDPDU transmit delay to control the frequent transmission of LLDPDUs. The default transmit delay is 2 seconds. Execute the following steps to configure the LLDPDU transmit delay.

Command	Function
Ruijie(config)# <b>lldp timer tx-delay seconds</b>	Configure LLDPDU transmit delay
Ruijie(config)# <b>show lldp status</b>	Display LLDP state.

Configuration example:

# Configure LLDPDU transmit delay to 3 seconds and display LLDP state.

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

Ruijie(config)#show lldp status

Global status of LLDP           : Enable

Neighbor information last changed time :

Transmit interval               : 30s

Hold multiplier                 : 4

Reinit delay                   : 2s

Transmit delay                  : 3s

Notification interval          : 5s

Fast start counts               : 3
```

## Configuring Port Re-initialization Delay

When the LLDP operating mode of a port changes, the port will initialize the protocol state machine. To prevent LLDP from being initialized too frequently during times of frequent operating mode change, you can configure port re-initialization delay. Execute the following steps to configure port re-initialization delay:

Command	Function
Ruijie(config)# <b>lldp timer reinit-delay seconds</b>	Configure port re-initialization delay.
Ruijie(config)# <b>show lldp status</b>	Display LLDP state.

Configuration example:

# Configure the port re-initialization delay to 3 seconds and display LLDP state.

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

Ruijie(config)#show lldp status
```

```

Global status of LLDP                : Enable

Neighbor information last changed time :

Transmit interval                    : 30s

Hold multiplier                      : 4

Reinit delay                        : 3s

Transmit delay                      : 2s

Notification interval                : 5s

Fast start counts                    : 3

```

## Configuring LLDP Trap

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.

To prevent excessive LLDP traps from being sent, you can set an interval for sending LLDP Traps. If LLDP information change is detected during this interval, traps will be sent to the network management server.

By default, LLDP Trap is disabled.

Execute the following steps to configure LLDP Trap:

Command	Function
<b>Ruijie(config)#lldp timer notification-interval seconds</b>	Configure the interval for sending LLDP Traps. Default: 5 seconds; configurable range: 5-3600 seconds.
<b>Ruijie(config)# interface interface-name</b>	Enter interface configuration mode. LLDP runs on the actual physical interface (for AP port, it runs on AP's member port). LLDP is not supported on stacking port or VSL port.
<b>Ruijie(config-if)#lldp notification remote-change enable</b>	Enable LLDP Trap. LLDP Trap is disabled by default.
<b>Ruijie(config-if)#show lldp status</b>	Display LLDP state.

Configuration example:

# Enable LLDP Trap and configure the interval for sending LLDP Traps to 10 seconds.

```

Ruijie(config)#lldp timer notification-interval 10

Ruijie(config)#interface gigabitethernet 0/1

Ruijie(config-if-GigabitEthernet 0/1)#lldp notification remote-change enable

Ruijie(config-if-GigabitEthernet 0/1)#show lldp status

Global status of LLDP                : Enable

```

```

Neighbor information last changed time :

Transmit interval                : 30s

Hold multiplier                  : 4

Reinit delay                     : 2s

Transmit delay                   : 2s

Notification interval            : 10s

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              : YES

Error detect enable              : YES

Number of neighbors              : 0

Number of MED neighbors          : 0

```

## Configuring LLDP Error Detection

Configure 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, LOG information will be printed to notify the administrator.

Execute the following steps to configure LLDP error detection:

Command	Function
Ruijie(config)# <b>interface</b> <i>interface-name</i>	Enter interface configuration mode. LLDP runs on the actual physical interface (for AP port, it runs on AP's member port). LLDP is not supported on stacking port or VSL port.
Ruijie(config-if)# <b>lldp error-detect</b>	Configure LLDP error detection. LLDP error detection is enabled by default.
Ruijie(config-if)# <b>show lldp status interface</b> <i>interface-name</i>	Display LLDP state on the interface.

Configuration example:

## # Configure LLDP error detection.

```

Ruijie(config)#interface gigabitethernet 0/1

Ruijie(config-if-GigabitEthernet 0/1)#lldp error-detect

Ruijie(config-if-GigabitEthernet 0/1)#show lldp status interface gigabitethernet 0/1

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          : 0

Number of MED neighbors      : 0

```

## Configuring LLDPDU Encapsulation Format

By default, LLDPDUs are encapsulated in Ethernet II frames. The configurable encapsulation formats include Ethernet II and SNAP.

When configured to Ethernet II format, the device can only send and receive Ethernet II-encapsulated LLDP packets.

When configured to SNAP format, the device can only send and receive SNAP-encapsulated LLDP packets.

Execute the following steps to configure LLDPDU encapsulation format:

Command	Function
Ruijie(config)# <b>interface</b> <i>interface-name</i>	Enter interface configuration mode. LLDP runs on the actual physical interface (for AP port, it runs on AP's member port). LLDP is not supported on stacking port or VSL port.
Ruijie(config-if)# <b>lldp encapsulation snap</b>	Configure LLDPDU encapsulation format to SNAP.
Ruijie(config-if)# <b>show lldp status interface</b> <i>interface-name</i>	Display LLDP state on the interface.



### Caution

To guarantee normal communication between local device and neighbor device, the same LLDPDU encapsulation format must be used.

Configuration example:

# Configure LLDPDU encapsulation format to SNAP and display the corresponding configuration.



```

Ruijie(config)#interface gigabitethernet 0/1

Ruijie(config-if-GigabitEthernet 0/1)#lldp encapsulation snap

Ruijie(config-if-GigabitEthernet 0/1)#show lldp status interface gigabitethernet 0/1

Port [GigabitEthernet 0/1]

Port status of LLDP          : Enable

Port state                   : UP

Port encapsulation           : Snap

Operational mode             : RxAndTx

Notification enable          : NO

Error detect enable          : YES

Number of neighbors          : 0

Number of MED neighbors      : 0

```

## Configuring LLDP Network Policy

By default, LLDP message adopts the network policy TLV which has no application type.

You can configuring the network policy by performing the following steps:

Command	Function
Ruijie(config)# <b>lldp network-policy profile</b> <i>profile-num</i>	Enter the LLDP network-policy configuration mode.
Ruijie(config-lldp-network-policy)# { <b>voice</b>   <b>voice-signaling</b> } <b>vlan</b> { { <i>vlan-id</i> [ <b>cos</b> <i>cvalue</i>   <b>dscp</b> <i>dvalue</i> ] }   { <b>dot1p</b> [ <b>cos</b> <i>cvalue</i>   <b>dscp</b> <i>dvalue</i> ] }   <b>none</b>   <b>untagged</b> } <b>no</b> { <b>voice</b>   <b>voice-signaling</b> } <b>vlan</b>	Configure LLDP network policy.



In release 10.4 (3b16), this function is supported by all switch products.

Configuration Example:

# Configure the network policy TLV of the LLDP message released by interface 1 to 1: The application type VLAN ID of voice is 3, cos is 4 and DSCP is 6:

```

Ruijie#config
Ruijie(config)#lldp network-policy profile 1
Ruijie(config-lldp-network-policy)# voice vlan 3 cos 4
Ruijie(config-lldp-network-policy)# voice vlan 3 dscp 6
Ruijie(config-lldp-network-policy)#exit
Ruijie(config)# interface gigabitethernet 0/1
Ruijie(config-if-GigabitEthernet 0/1)# lldp tlv-enable med-tlv network-policy profile 1

```

## Configuring Civic Address Information of a Device

You can configure the address information of a device by performing the following steps:

Command	Function
Ruijie(config)# <b>lldp location civic-location identifier</b> <i>id</i>	Enter the LLDP civic address configuration mode.
Ruijie(config-lldp-civic)# <b>device-type</b> <i>device-type</i>	Configure a device type, switch by default.
Ruijie(config-lldp-civic)# { <b>country</b>   <b>state</b>   <b>county</b>   <b>city</b>   <b>division</b>   <b>neighborhood</b>   <b>street-group</b>   <b>leading-street-dir</b>   <b>trailing-street-suffix</b>   <b>street-suffix</b>   <b>number</b>   <b>street-number-suffix</b>   <b>landmark</b>   <b>additional-location-information</b>   <b>name</b>   <b>postal-code</b>   <b>building</b>   <b>unit</b>   <b>floor</b>   <b>room</b>   <b>type-of-place</b>   <b>postal-community-name</b>   <b>post-office-box</b>   <b>additional-code</b> } <i>ca-word</i>	Configure LLDP civic address information.



In release 10.4 (3b16), this function is supported by all switch products.

Configuration Example:

# Configure the address of interface 1 on a device to: Switch, country: CH, city: Fuzhou and postal code: 350000.

```
Ruijie#config
Ruijie(config)#lldp location civic-location identifier 1
Ruijie(config-lldp-civic)# country CH
Ruijie(config-lldp-civic)# city Fuzhou
Ruijie(config-lldp-civic)# postal-code 350000
Ruijie(config-lldp-civic)# exit
Ruijie(config)# interface gigabitethernet 0/1
Ruijie(config-if-GigabitEthernet 0/1)# lldp tlv-enable location civic-location identifier 1
```

## Configuring Information about the Emergency Phone Number of a Device

You can configure information about the emergency phone number of a device by performing the following steps:

Command	Function
Ruijie(config)# <b>lldp location elin identifier</b> <i>id</i> <b>elin-location</b> <i>tel-number</i>	Configure information about the emergency phone number.

Configuration Example:

# Configure the emergency phone number of interface 1 on a device to 085285555556:

```
Ruijie#config
Ruijie(config)#lldp location elin identifier 1 elin-location 085283671111
Ruijie(config)# interface gigabitethernet 0/1
Ruijie(config-if-GigabitEthernet 0/1)# lldp tlv-enable location elin identifier 1
```

## Displaying and Clearing Configurations

Command	Function
---------	----------

<b>show lldp local-information</b> [global   interface interface-name]	Display the device information to be sent to neighbor device.
<b>show lldp location</b> { civic-location   elin } { identifier id   interface interface-name   static }	Display information about the civic address or the emergency phone number of the local device.
<b>show lldp neighbors</b> [interface interface-name] [detail]	Display information about the neighbor connected by this port.
<b>show lldp network-policy profile</b> [profile-num]	Display the configuration of LLDP network policy.
<b>show lldp statistics</b> [global   interface interface-name]	Display LLDP statistics.
<b>show lldp status</b> [interface interface-name]	Display LLDP state.
<b>show lldp tlv-config</b> [interface interface-name]	Display the advertisable optional TLVs.
<b>clear lldp statistics</b> [interface interface-name]	Clear LLDP statistics.
<b>clear lldp table</b> [interface interface-name ]	Clear information about neighbors of LLDP.

Configuration example:

# Display the information about the neighbor device connected to the port:

```
Ruijie# show lldp neighbors detail
```

```
Lldp neighbor-information of port [GigabitEthernet 0/1]
```

```
Neighbor index          : 1
Device type             : LLDP Device
Update time             : 12minute 40seconds
```

```
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 0/2
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(100)/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      :
```

**Note**

For the specific meaning of LLDP information displayed, please refer to the descriptions given in "LLDP Command Reference".

## Typical LLDP Configuration Examples

### Use LLDP to View Topological Connections

#### Networking Requirements

- Devices required

Two Ethernet switches (Switch A and Switch B), one MED device (taking IP Phone as the example) and one NMS (Network management System).

- Configuration required

LLDP is enabled by default. No further configuration is needed.

#### Network Tpology

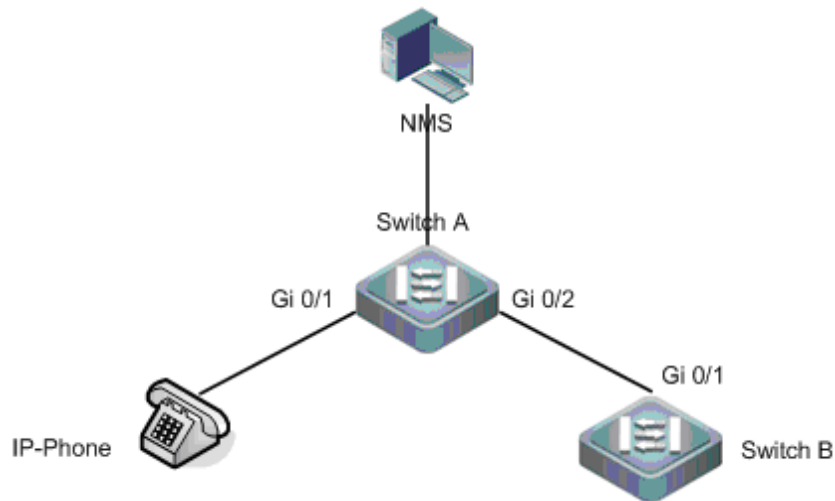


Fig 4 Basic topological diagram of LLDP

### Configuration Tips

1. LLDP operating mode on the port is TxRx.
2. LLDPDU transmit times will use default values, namely LLDPDU transmit interval is 30 seconds and LLDPDU transmit delay is 2 seconds.

### Configuration Steps

By default, LLDP is enabled, and no further configuration is needed.

### Verification

1. Display the information about the neighbor device connecting with Switch A.

# Display the information about the neighbor device on Switch A.

```
Ruijie# show lldp neighbors gigabitethernet 0/2
```

Capability codes:

(R) Router, (B) Bridge, (T) Telephone, (C) DOCSIS Cable Device  
(W) WLAN Access Point, (P) Repeater, (S) Station, (O) Other

Local Intf	Port ID	Capability	Aging-time
Gi 0/2	Gi 0/1	B,R	120

Total entries displayed: 1

The above messages show that the port of neighbor device connected to port 2 of switch A is Gi 0/1. The neighbor device allows bridging and routing.

# Display the detailed information about the neighbor device connected to port Gi 0/2 of Switch A.

```
Ruijie# show lldp neighbors interface gigabitethernet 0/2 detail
```

```
Lldp neighbor-information of port [GigabitEthernet 0/2]
```

Neighbor index : 1

Device type : LLDP Device

Update time : 5minutes 39seconds

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      :

```

## Use LLDP Error Detection Feature to Perform Error Detection

### Networking Requirements

- Devices required  
two Ethernet switches (Switch A and Switch B)
- Configuration required  
LLDP is enabled by default. No further configuration is needed.

### Network Topology

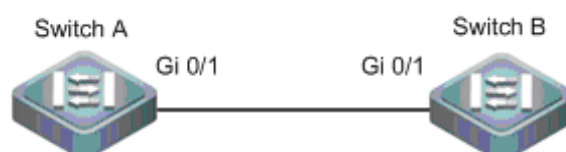




Fig 5 Basic topological diagram of LLDP

### Configuration Tips

1. LLDP operating mode on the port is TxRx.
2. LLDPDU transmit times will use default values, namely LLDPDU transmit interval is 30 seconds and LLDPDU transmit delay is 2 seconds.
3. LLDP error detection is enabled by default. No further configuration is needed.

### Configuration Steps

1. Configure the bit-rate of port Gi 0/1 of Switch A to 100M.

```
Ruijie#config
```

```
Ruijie(config)#interface gigabitethernet 0/1
```

```
Ruijie(config-if-GigabitEthernet 0/1)#speed 100
```

```
%Warning: the speed/duplex of port GigabitEthernet 0/1 may not match with it's neighbor.
```

The above messages show that bit-rate and duplex capabilities of port 1 may not match with that of port on neighbor device.

### Verification

While the administrator is carrying out VLAN configuration, port bit-rate and duplex configuration, aggregation port configuration and port MTU configuration, if the information doesn't match with the configurations of neighbor device the corresponding error messages will be prompted.

# QinQ Configuration

## Introduction to QinQ

For QinQ, as specified in IEEE 802.1ad, there are so many names in the industry, for instance, dot1q-tunneling, Tag in Tag, VLAN VPN and Stack VLAN. Since the VLAN Tag domain defined in IEEE 802.1Q has only 12 bits for VLAN ID, the device supports up to 4094 VLANs. In real application environments, for example, especially in MAN, a lot number of VLANs are necessary for separation of users. 4094 VLANs is not enough to address this requirement. The principle of QinQ is that a packet is encapsulated with the VLAN tag of the network of an ISP before arriving the network and the original VLAN tag on the packet serves as data, so that the packet travels the network with two tags. The packet is propagated in the ISP's network by outer VLAN tag (or the VLAN tag of ISP's network), which is stripped when the packet leaves. Then the packet is propagated in the private network by the VLAN tag of the private network.

As shown in Figure 1, the packets from Network A's VLAN 1001 are added with the outer VLAN tag 1005 before entering the ISP's network. Hence, the packets carry with two tags and be propagated in the ISP's network by the outer VLAN tag 1005. The outer VLAN tag 1005 will be stripped when the packets leave the ISP's network. In Network B, the packets are propagated by VLAN tag 1001.

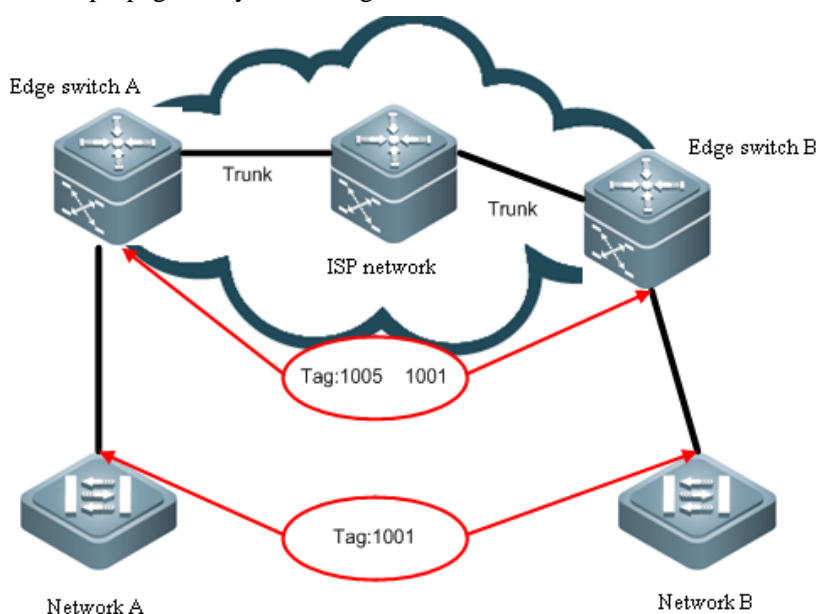


Figure 1 QinQ sketch map

The following figure illustrates the course of adding two tags. The ingress of edge device is dot1q-tunnle port (or abbreviated as tunnel port). All frames entering the edge device are considered to be untagged, no matter whether are really untagged or tagged with 802.1Q tag, and then are encapsulated with the tag of ISP. VLAN ID is the default VLAN of tunnel port.

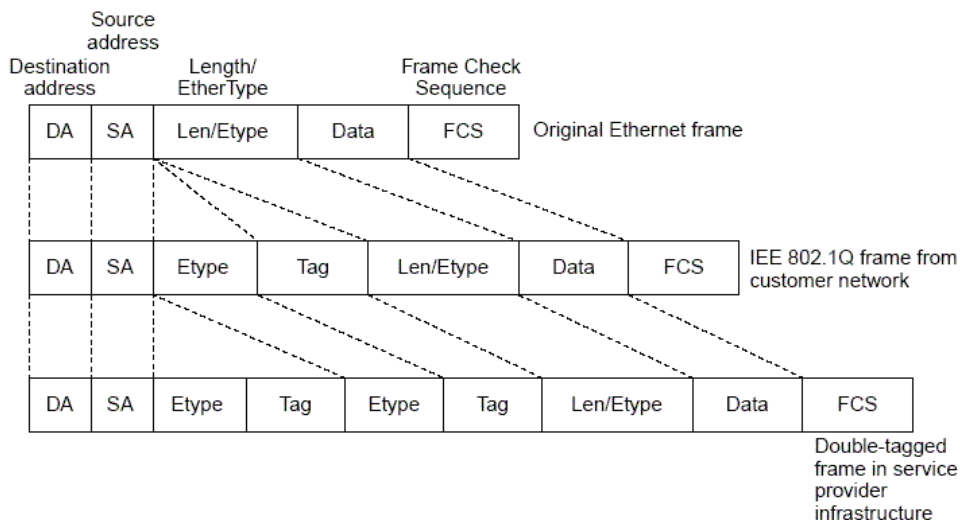


Figure 2 Packet structure with two tags

## Basic QinQ

Basic QinQ is enabled based on port. When tunnel port is configured, the device will add the VLAN tag of the default VLAN of the tunnel port to the packet arriving the tunnel port. If the packet is already of a VLAN tag, this means it has two tags. Basic QinQ is simple, but the encapsulation of outer VLAN tag is not flexible enough.

## Flexible QinQ

Flexible QinQ can flexibly encapsulate different outer VLAN tags for different flows by flow classification method like user VLAN tag, MAC address, IP protocol, source address, destination address, priority or port number of application program.

You can:

- ◆ Add outer VLAN tag by inner VLAN tag
- ◆ Modify inner VLAN tag by outer VLAN tag
- ◆ Modify outer VLAN tag by inner VLAN tag
- ◆ Add outer VLAN tag by ACL
- ◆ Modify outer VLAN tag by ACL
- ◆ Modify inner VLAN tag by ACL

## VLAN mapping

VLAN Mapping is used to replace the private-network VLAN Tag carried in user packets with public-network VLAN Tag, so that the packets will be transmitted according to the network layout of public network. When packets return to user's private network, the VLAN Tag is restored to the original private-network VLAN Tag as per the same rule, so that packets can reach the destination correctly. VLAN Mapping supports the following mapping relations:

- One-to-one VLAN mapping: change Tag VID of packets to another specified Tag VID.
- Many-to-one VLAN mapping: change Tag VIDs of packets from multiple VLANs to the same Tag VID.

As shown below, 1:1 VLAN MAPPING is mainly deployed on the corridor switch to carry the same service of different users on different VLANs, so as to distinguish different users; N:1 VLAN MAPPING is mainly deployed

on the sci-tech park switch to carry the same service of different users on one VLAN, so as to save VLAN resources.

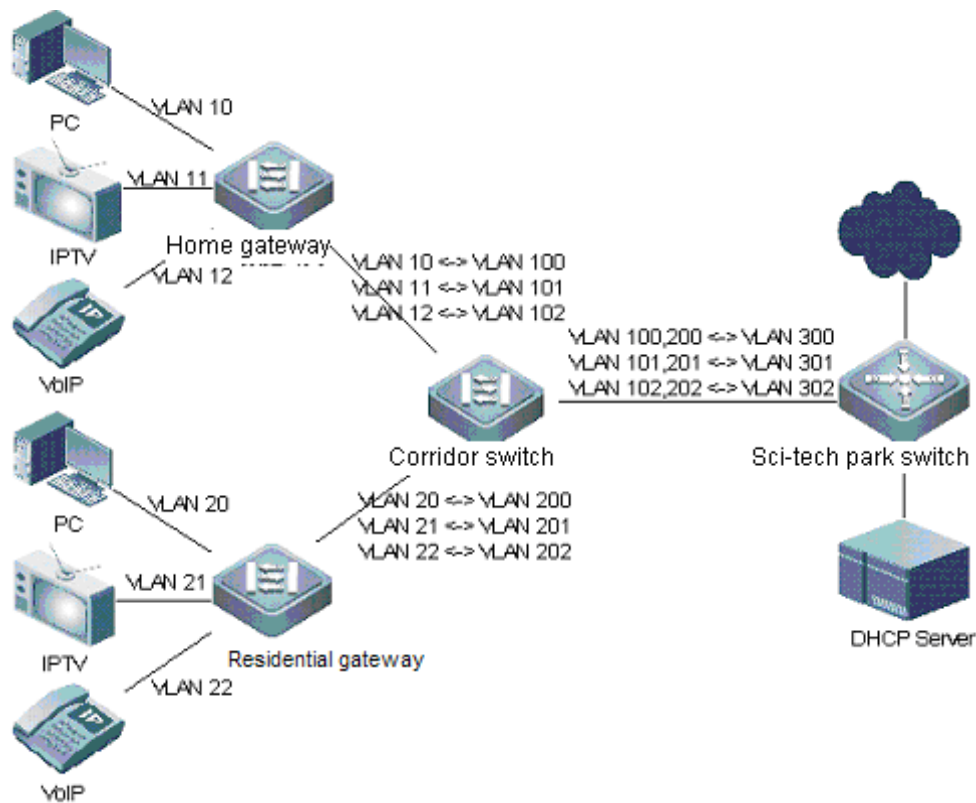


Figure3 Diagram for 1:1 VLAN Mapping and N:1 VLAN mapping

### The 1st approach to realize one-to-one VLAN mapping

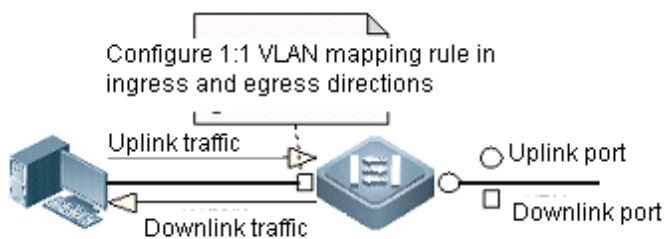
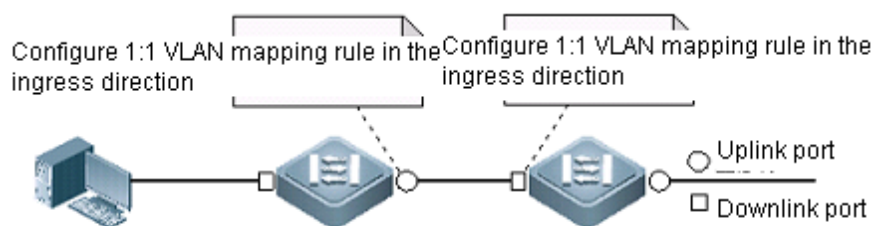


Figure 4 The 1st approach to realize 1:1 VLAN mapping

- ✧ For uplink traffic as shown in Figure 4, by configuring VLAN mapping rule in the ingress direction on the downlink port, the original VLAN Tag is mapped to the new VLAN Tag.
- ✧ For downlink traffic as shown in Figure 4, by configuring VLAN mapping rule in the egress direction on the downlink port, the VLAN Tag of packets is mapped to the original VLAN Tag.

## The 2nd approach to realize one-to-one VLAN mapping



**Figure 5 The 2nd approach to realize 1:1 VLAN mapping**

For uplink traffic as shown in Fig 5, by configuring VLAN mapping rule in the ingress direction on the downlink port, the original VLAN Tag is mapped to the new VLAN Tag.

For downlink traffic as shown in Fig 5, by configuring VLAN mapping rule in the ingress direction on the uplink port, the VLAN Tag of packets is mapped to the original VLAN Tag.

## The approach to realize many-to-one VLAN mapping



**Figure 6 The approach to realize N:1 VLAN mapping**

For uplink traffic as shown in Fig 6, by configuring VLAN mapping rule in the ingress direction on the downlink port, the original VLAN Tag is mapped to the new VLAN Tag.

Mapping of downlink traffic is currently not support.

## Other functions

### TPID setting and priority duplication and mapping

The Ethernet frame tag includes four fields-TPID (Tag Protocol Identifier), User Priority, CFI and VLAN ID. By default, TPID uses 0x8100 specified in IEEE 802.1Q. Some vendors' devices, however, set the TPID of the outer tag of packs to 0x9100 or other values. To compatible with these devices, QinQ offers the function to configure the TPID of packets based on port. In the course of packet transmission, the TPID of the outer VLAN tag of packets are replaced with the set value.

Priority duplication refers to duplicating the priority of inner tag (user tag) to outer tag (ISP tag) when adding outer tag.

Priority mapping refers to setting the priority of outer tag (ISP tag) by inner tag (user tag) when adding outer tag.

### MAC address duplication

For flow-based flexible QinQ, the switch learns VID of native VLAN. Hence, in case of flow-based VLAN translation, when the peer sends back packets, flooding may occur for the MAC address cannot be obtained.

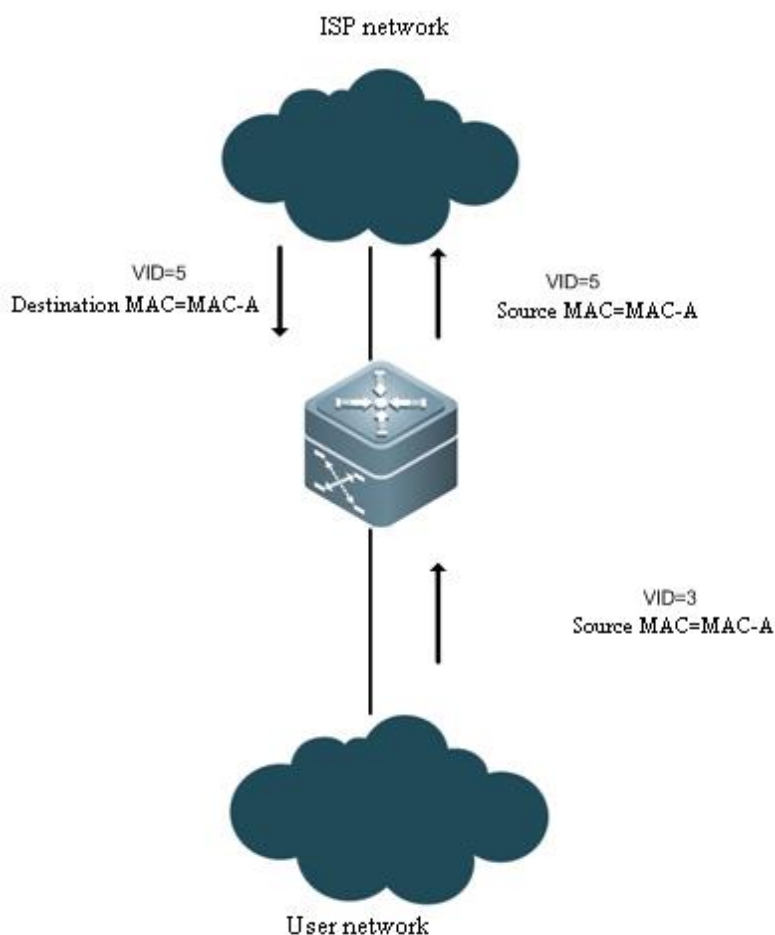


Figure 3 Learn MAC address of flexible QinQ packet

As shown in the above figure, the switch connects to user network through dot1q-tunnel port, on which VLAN 4 is set to be native VLAN. The packets of VLAN 3 are encapsulated with VLAN 5 tag as outer tag. When the switch receives a packet from VLAN 3, it adds VLAN 5 tag as outer tag to the packet. Meanwhile, VLAN 4 learns MAC-A for the native VLAN of the receiving port is VLAN 4. However, VLAN 5 has not learned MAC-A and the packet is flooded.

To solve the problem on flooding the packets back from the public network, duplicate the MAC address of native VLAN to the VLAN whether outer tag locates. Similarly, you can execute reverse MAC address duplication to solve the problem on flooding the packets to the public network.

### Layer 2 protocol transparent transmission

Layer 2 packet transparent transmission enables transmitting Layer 2 packets between networks without influencing ISP networks. When Layer 2 protocol packets arrive at the edge device on one side, the destination MAC address is changed as private address for forwarding in ISP networks. Then when the packets arrive the

edge device on other side, the destination MAC address is changed back to public address. This ensures transparent transmission of Layer 2 protocol packets in ISP networks.

## Uplink port

Uplink port essentially is a special trunk port. The difference is that the packets outputted from the uplink port are tagged, but the packets outputted from the trunk port (when they are forwarded from native VLAN) are untagged. A typical example is the port of a user network connecting to an ISP network.

## Configuring QinQ

This chapter includes:

- Default QinQ Configurations
- Restriction of QinQ Configuration
- Configuring Basic QinQ
- Configuring Flexible QinQ
- Configuring Other QinQ Functions

### Default QinQ Configurations

By default, basic QinQ, flexible QinQ and other QinQ functions are disabled.

### Restriction of QinQ Configuration

The following restrictions apply to QinQ configuration:

- The routed ports cannot be configured as tunnel ports.
- The 802.1x function cannot be enabled on the port configured as a tunnel port.
- Port security cannot be enabled on the port configured as a tunnel port.
- For the ACL applied on the tunnel port, the inner keyword is necessary to match the VID of user tag.
- It is recommended to configure the egress of user network connecting the ISP network as uplink port as well. If the TPID of ISP tag is set on the QinQ-enabled port of the user network, the TPID of ISP tag of uplink port should be set with the same value.
- QinQ does not support hot backup.
- The MTU of a port is 1500 bytes by default. A packet will be increased by 4 bytes when it is added with outer VLAN tag. It is recommended to increase the MTU value of ports in ISP network at an appropriate extent, or at least 1504 bytes.
- Once QinQ is enabled on a port, to enable IGMP Snooping, you need set SVGL sharing mode or otherwise IGMP Snooping does not function on the port with QinQ enabled.

### Configuring Basic QinQ

In the global configuration mode, input the **interface** command to enter the interface configuration mode. Follow these steps to configure a tunnel port:

Command	Function
<b>configure terminal</b>	Enter the global configuration mode.
<b>interface</b> <interface>	Enter the interface configuration mode.
<b>switchport mode dot1q-tunnel</b>	Set the port as a dot1q-tunnel port.
<b>switchport dot1q-tunnel allowed vlan</b> [add] { tagged   untagged } v_list	Add the allowed VLAN for dot1q-tunnel port and specify that whether the VLAN is tagged or not when outputting the packets of allowed VLAN.
<b>switchport dot1q-tunnel allowed vlan</b> <b>remove</b> v_list	Delete the allowed VLAN on the dot1q-tunnel port.
<b>switchport dot1q-tunnel native vlan</b> VID	Set the default VLAN for the dot1q-tunnel port.
<b>End</b>	Exit the interface mode.
<b>show running-config</b>	Show the configuration.

**Note**

It is not recommended to set the native VLAN of trunk port in the ISP network as the default VLAN of tunnel port, because the tag with native VID will be stripped off on trunk port.

The following example demonstrates how to configure a QinQ port:

```
Ruijie(config)# interface fastEthernet 0/1
Ruijie(config-if)# switchport mode dot1q-tunnel
Ruijie(config-if)# switchport dot1q-tunnel nativ vlan 20
Ruijie(config-if)# switchport dot1q-tunnel allowed vlan tagged 100-200
Ruijie(config)# end
```

## Configuring Flexible QinQ

### Configure VID add policy table

For an incoming packet on dot1q-tunnel port, in some case, it is necessary to specify the VID of outer tag for the packet during forwarding according to the VID of the tags of the packet. Run the **dot1q outer-vid** command to specify the outer VID when adding outer tag to inner VID list. With this command, you can specify an internal VLAN and add the same outer VID as the inner VID, and add the egress to the untagged port set of the VLAN. In addition, the packets with original inner tag can be outputted via egress.

Command	Function
<b>configure terminal</b>	Enter the global configuration mode.
<b>interface</b> intf-id	Enter the interface configuration mode.
<b>switchport mode dot1q-tunnel</b>	Set the port as a dot1q-tunnel port.
<b>dot1q outer-vid</b> VID <b>register inner-vid</b> v_list	Configure the protocol-based policy to add the VID of outer tag.



Command	Function
<b>no dot1q outer-vid VID register inner-vid v_list</b>	Remove the configuration
<b>end</b>	Exit the interface mode.
<b>show running-config</b>	Show the configuration.

The following example adds the VID 3 of outer tag when the VID of the tag of incoming packet is 4-22:

```
Ruijie# configure
Ruijie(config)# interface gigabitEthernet 0/1
Ruijie(config-if)# switchport mode dot1q-tunnel
Ruijie(config-if)# switchport dot1q-tunnel allowed vlan add tagged 3
Ruijie(config-if)# dot1q outer-vid 3 register inner-vid 4-22
Ruijie(config-if)# end
```

### Configure outer tag-based VID change policy table

For the packets incoming from Access port, Trunk port, Hybrid port and Uplink port, sometimes you need to change the VIDs of outer tags according to the VIDs of outer tags of incoming packets. Run the **dot1q relay-vid VID translate local-vid v\_list** command to change the local VID (VID of outer tag before change) list.

Command	Function
<b>configure terminal</b>	Enter the global configuration mode.
<b>interface intf-id</b>	Enter the interface configuration mode.
<b>switchport mode port-type</b>	Set the port as Access port, Trunk port, Uplink port or Hybrid port.
<b>dot1q relay-vid VID translate local-vid v_list</b>	Configure the policy to change the VID of outer tag according to original VID of outer tag.
<b>no dot1q relay-vid VID translate local-vid v_list</b>	Remove the configuration
<b>end</b>	Exit the interface mode.
<b>show running-config</b>	Show the configuration.

The following example changes the VID of outer tag as 100 when the VID of outer tag of incoming packets is 10-20.

```
Ruijie(config)# interface gigabitEthernet 0/1
Ruijie(config-if)# switchport mode trunk
Ruijie(config-if)# dot1q relay-vid 100 translate local-vid 10-20
Ruijie(config-if)# end
```

### Configure inner tag-based VID change policy table

For the packets incoming from Access port, Trunk port, Hybrid port and Uplink port, sometimes you need to change the VIDs of outer tags according to the VIDs of inner tags of incoming packets. Run the **dot1q relay-vid VID translate inner-vid v\_list** command to change the local VID (VID of outer tag before change) list.

Command	Function
---------	----------

Command	Function
<b>configure terminal</b>	Enter the global configuration mode.
<b>interface</b> <i>intf-id</i>	Enter the interface configuration mode.
<b>switchport mode</b> <i>port-type</i>	Set the port as Access port, Trunk port, Uplink port or Hybrid port.
<b>dot1q relay-vid</b> <i>VID</i> <b>translate</b> <b>inner-vid</b> <i>v_list</i>	Configure the policy to change the VID of outer tag according to the inner tag.
<b>no dot1q relay-vid</b> <i>VID</i> <b>translate</b> <b>inner-vid</b> <i>v_list</i>	Remove the configuration
<b>end</b>	Exit the interface mode.
<b>show running-config</b>	Show the configuration.

The following example changes the VID of outer tag as 100 when the VID of inner tag of incoming packets is 10-20.

```
Ruijie(config)# interface gigabitEthernet 0/1
Ruijie(config-if)# switchport mode trunk
Ruijie(config-if)# dot1q relay-vid 100 translate inner-vid 10-20
Ruijie(config-if)# end
```

### Configure inner tag+outer tag based VID change policy table

For ingress packets on Access, Trunk, Hybrid and Uplink ports, sometimes we need to change the VID of outer Tag to different values. Use "**dot1q new-outer-vlan** *VID* **translate old-outer-vlan** *vid* **inner-vlan** *v\_list*" command to specify the new outer VID, old outer VID and inner Tag list, and use "**no dot1q new-outer-vlan** *VID* **translate old-outer-vlan** *vid* **inner-vlan** *v\_list*" command to remove the configuration. Please refer to command reference for detailed commands.

The configuration steps are shown below:

Command	Function
<b>configure terminal</b>	Enter the global configuration mode.
<b>interface</b> <i>intf-id</i>	Enter the interface configuration mode.
<b>switchport mode</b> <i>port-type</i>	Configure to Access, Trunk, Uplink or Hybrid port.
<b>dot1q new-outer-vlan</b> <i>VID</i> <b>translate</b> <b>old-outer-vlan</b> <i>vid</i> <b>inner-vlan</b> <i>v_list</i>	Configure outer Tag + inner Tag based outer Tag VID mapping rule.
<b>no dot1q new-outer-vlan</b> <i>VID</i> <b>translate</b> <b>old-outer-vlan</b> <i>vid</i> <b>inner-vlan</b> <i>v_list</i>	Remove the outer Tag + inner Tag based outer Tag VID mapping rule.
<b>end</b>	Exit the interface mode.
<b>show translation-table</b>	Show the configuration.

The following example shows how to map the vid to 3888 when inner Tag VID and outer Tag VID of ingress packets are 2001-3000 and 1888 respectively.

```
Ruijie(config)# vlan 1888, 3888
Ruijie(config)# interface gigabitEthernet 0/1
Ruijie(config-if)# switchport mode trunk
Ruijie(config-if)# dot1q new-outer-vlan 3888 translate old-outer-vlan 1888 inner-vlan 2001-3000
Ruijie(config-if)# end
```

## Configure flow-based VID change policy table

### Configure VID add policy table

For an incoming packet on dot1q-tunnel port, in some case, it is necessary to specify the VID of outer tag for the packet according to its content. Run the **traffic-redirect access-group acl nested-vlan VID in** command to specify the VID of outer tag when the packet incoming from the dot1q-tunnel port matches ACL.

Command	Function
<b>configure terminal</b>	Enter the global configuration mode.
<b>interface intf-id</b>	Enter the interface configuration mode.
<b>switchport mode dot1q-tunnel</b>	Set the port as a dot1q-tunnel port.
<b>traffic-redirect access-group acl nested-vlan VID in</b>	Configure the flow-based policy to add the VID of outer tag.
<b>no traffic-redirect access-group acl nested-vlan VID in</b>	Remove the configuration
<b>end</b>	Exit the interface mode.
<b>show running-config</b>	Show the configuration.

**Note**

- ◆ Flow-based VID change policy table takes precedence over protocol-based VID change policy table.
- ◆ When you configure member port on AP, the configured VID add policy or VID change policy will be deleted. Reconfiguration of VID add policy or VID change policy is necessary. It is recommended to configure VID policy on AP after configuring member port.
- ◆ Once ACL is deleted, the ACL related policies will be deleted as well.
- ◆ When the packets with the tag larger than or equal to Layer 2 are received on the dot1q-tunnel port, you can add tag by flow-based match rule.
- ◆ If a packet matches two or more flow policies without priority specified simultaneously, the early configured policy takes effect.

The following example adds the VID 9 to the packets from 1.1.1.3:

```
Ruijie# configure
Ruijie(config)# ip access-list standard 20
Ruijie(config-acl-std)# permit host 1.1.1.3
Ruijie(config-acl-std)# exit
Ruijie(config)# interface gigabitEthernet 0/1
Ruijie(config-if)# switchport mode dot1q-tunnel
Ruijie(config-if)# traffic-redirect access-group 20 nested-vlan 10 in
Ruijie(config-if)# end
```

### Configure outer VID change policy table

For the packets incoming from Access port, Trunk port, Hybrid port and Uplink port, sometimes you need to change the VIDs of outer tags according to the contents of incoming packets. Run the **traffic-redirect access-group *acl* outer-vlan *VID* in** command to change the VID of outer tag of the packets matching ACL.

Command	Function
<b>configure terminal</b>	Enter the global configuration mode.
<b>interface <i>intf-id</i></b>	Enter the interface configuration mode.
<b>switchport mode <i>port-type</i></b>	Set the port as Access port, Trunk port, Uplink port or Hybrid port.
<b>traffic-redirect access-group <i>acl</i> outer-vlan <i>VID</i> in</b>	Change the VID of outer tag according to the flow.
<b>no traffic-redirect access-group <i>acl</i> outer-vlan</b>	Remove the configuration
<b>end</b>	Exit the interface mode.
<b>show running-config</b>	Show the configuration.

**Note**

- ◆ Flow-based outer VID change policy table takes precedence over protocol-based outer VID change policy table.
- ◆ When you configure member port on AP, the configured VID add policy or VID change policy will be deleted. Reconfiguration of VID add policy or VID change policy is necessary. It is recommended to configure VID policy on AP after configuring member port.
- ◆ Once ACL is deleted, the ACL related policies will be deleted as well.
- ◆ If a packet matches two or more flow policies without priority specified simultaneously, the early configured policy takes effect.

The following example changes the VID of outer tag as 3 for the packets from 1.1.1.1:

```
Ruijie# configure
Ruijie(config)# ip access-list standard 2
Ruijie(config-acl-std)# permit host 1.1.1.1
Ruijie(config-acl-std)# exit
Ruijie(config)# interface gigabitEthernet 0/1
Ruijie(config-if)# switchport mode trunk
Ruijie(config-if)# traffic-redirect access-group 2 outer-vlan 3 in
Ruijie(config-if)# end
```

### Configure inner VID change policy table

For the packets outgoing from Access port, Trunk port, Hybrid port and Uplink port, sometimes you need to change the VIDs of inner tags according to the contents of outgoing packets. Run the **traffic-redirect access-group acl inner-vlan VID out** command to change the VID of inner tag of the packets matching ACL.

Command	Function
<b>configure terminal</b>	Enter the global configuration mode.
<b>interface <i>intf-id</i></b>	Enter the interface configuration mode.
<b>switchport mode <i>port-type</i></b>	Set the port as Access port, Trunk port, Uplink port or Hybrid port.
<b>traffic-redirect access-group <i>acl</i> inner-vlan <i>VID</i> out</b>	Change the VID of inner tag according to the flow.
<b>no traffic-redirect access-group <i>acl</i> inner-vlan</b>	Remove the configuration
<b>end</b>	Exit the interface mode.
<b>show running-config</b>	Show the configuration.

**Note**

- ◆ Flow-based outer VID change policy table takes precedence over protocol-based outer VID change policy table.
- ◆ When you configure member port on AP, the configured VID add policy or VID change policy will be deleted. Reconfiguration of VID add policy or VID change policy is necessary. It is recommended to configure VID policy on AP after configuring member port.
- ◆ Once ACL is deleted, the ACL related policies will be deleted as well.
- ◆ If a packet matches two or more flow policies without priority specified simultaneously, the early configured policy takes effect.

The following example changes the VID of inner tag as 6 for the packets to 1.1.1.2:

```
Ruijie# configure
Ruijie(config)# ip access-list standard to_6
Ruijie(config-acl-std)# permit host 1.1.1.2
Ruijie(config-acl-std)# exit
Ruijie(config)# interface gigabitEthernet 0/1
Ruijie(config-if)# switchport mode trunk
Ruijie(config-if)# traffic-redirect access-group to_6 inner-vlan 6 out
Ruijie(config-if)# end
```

**Caution**

When you configure flow-based policy table, inner VID is necessary to match user VID, or otherwise outer VID is matched.

## Configuring VLAN mapping

- Configure one-to-one VLAN mapping
- Configure many-to-one VLAN mapping

### Configuring one-to-one VLAN mapping

On the access, trunk, hybrid or uplink port, execute the following steps to configure one-to-one VLAN mapping. Please refer to command reference for details about relevant commands.

The configuration steps are shown below:

Command	Function
<b>configure terminal</b>	Enter the global configuration mode.
<b>interface</b> <i>intf-id</i>	Enter the interface configuration mode.
<b>switchport mode</b> <i>port-type</i>	Set the port as Access port, Trunk port, Uplink port or Hybrid port.

Command	Function
<b>vlan-mapping-in</b> <i>vlan cvlan remark svlan</i>	Configure one-to-one VLAN mapping in ingress direction. It will map Customer VLAN ID of ingress packets to the specified Server VLAN ID.
<b>no</b> <b>vlan-mapping-in</b> <i>vlan cvlan remark svlan</i>	Disable one-to-one VLAN mapping in the ingress direction.
<b>vlan-mapping-out</b> <i>vlan svlan remark cvlan</i>	Configure one-to-one VLAN mapping in egress direction. It will restore the Server VLAN ID of egress packets to the original Customer VLAN ID.
<b>no</b> <b>vlan-mapping-out</b> <i>vlan svlan remark cvlan</i>	Disable one-to-one VLAN mapping in the egress direction.
<b>end</b>	Exit the interface configuration mode.
<b>show</b> <b>interface</b> <i>[ intf-id ]</i> <b>vlan-mapping</b>	Show the configuration.

The following example changes the VID in the Tag of ingress packets from 3 to 4 before forwarding

```
Ruijie# configure
Ruijie# vlan range 3-4
Ruijie(config)# interface gigabitEthernet 0/1
Ruijie(config-if)# switchport mode trunk
Ruijie(config-if)# vlan-mapping-in vlan 3 remark 4
Ruijie(config-if)# vlan-mapping-out vlan 4 remark 3
Ruijie(config-if)# end
```

## Configuring many-to-one VLAN mapping

On the access, trunk, hybrid or uplink port, execute the following steps to configure many-to-one VLAN mapping. Please refer to command reference for details about relevant commands.

The configuration steps are shown below:

Command	Function
<b>configure terminal</b>	Enter the global configuration mode.
<b>interface</b> <i>intf-id</i>	Enter the interface configuration mode.
<b>switchport mode</b> <i>port-type</i>	Set the port as Access port, Trunk port, Uplink port or Hybrid port.
<b>vlan-mapping-in</b> <i>vlan cvlan-list remark svlan</i>	Configure many-to-one VLAN mapping in ingress direction. It will map multiple Customer VLAN ID of ingress packets to the same Server VLAN ID specified.

Command	Function
<b>no vlan-mapping-in vlan <i>cvlan-list</i></b> <b>remark <i>svlan</i></b>	Disable many-to-one VLAN mapping.
<b>end</b>	Exit the interface configuration mode.
<b>show interface[ <i>intf-id</i> ]</b> <b>vlan-mapping</b>	Show the configuration.

The following example changes the VIDs in the Tag of ingress packets from 3-7 to 8 before forwarding.

```
Ruijie# configure
Ruijie# vlan range 3-8
Ruijie(config)# interface gigabitEthernet 0/1
Ruijie(config-if)# switchport mode trunk
Ruijie(config-if)# vlan-mapping-in vlan 3-7 remark 8
Ruijie(config-if)# end
```



#### Note

- When VLAN mapping is configured, the VLAN ID of packets sent to CPU will become the new VLAN ID.
- The user is not suggested to configure VLAN mapping and flexible QinQ on the same port at the same time.

## Configuring Other QinQ Functions

### Configuring an Uplink Port

In the global configuration mode, input the **interface** command to enter the interface configuration mode. Follow these steps to configure an uplink port:

Command	Description
<b>configure terminal</b>	Enter the global configuration mode.
<b>interface &lt;interface&gt;</b>	Enter the interface configuration mode.
<b>switchport mode uplink</b>	Configure the port as an uplink port.
<b>end</b>	Exit the interface mode.
<b>show running-config</b>	Show the configuration.

The following example demonstrates how to configure an uplink port:

```
Ruijie(config)# interface gigabitEthernet 0/1
Ruijie(config-if)# switchport mode up-link
Ruijie(config)# end
```

### Configuring the TPID Value of ISP Tag

In the global configuration mode, input the **interface** command to enter the interface configuration mode. Follow



these steps to configure the TPID value of ISP tag:

Command	Description
<b>configure terminal</b>	Enter the global configuration mode.
<b>interface</b> <interface>	Enter the interface configuration mode.
<b>frame-tag tpid</b> <tpid>	Set the TPID value of ISP tag. If you want to set it as 0x9100, directly enter frame-tag tpid 9100. Note that the hexadecimal system is used by default. This function takes effect on egress.
<b>end</b>	Exit the interface mode.
<b>show frame-tag tpid</b>	View the TPID value list on the port.

The following example demonstrates how to configure TPID:

```
Ruijie(config)# interface gigabitethernet 0/1
Ruijie(config-if)# frame-tag tpid 9100
Ruijie(config)# end
Ruijie# show frame-tag tpid interface gigabitethernet 0/1
Port      tpid
-----
Gi0/1     0x9100
```

<b>Product support</b>	<p>◆ Do not set TPID to be 0x0806(ARP), 0x0200(PUP), 0x8035(RARP), 0x0800(IP), 0x86DD(IPv6), 0x8863/0x8864(PPPoE), 0x8847/0x8848(MPLS), 0x8137(IPX/SPX), 0x8000(IS-IS), 0x8809(LACP), 0x888E(802.1x), 0x88A7(cluster), and 0x0789(reserved).</p>
------------------------	--

## Configuring Priority Duplication

Follow these steps to duplicate the priority of inner tag to outer tag:

Command	Description
<b>configure terminal</b>	Enter the global configuration mode.
<b>interface</b> <interface>	Enter the interface configuration mode.
<b>mls qos trust cos</b>	Configure the interface to be trust CoS mode.
<b>inner-priority-trust enable</b>	Copy the priority value of the inner tag (user tag) to the priority value of the outer tag (ISP tag).
<b>End</b>	Exit the interface mode.
<b>show inner-priority-trust</b>	View the priority duplication configuration of the user tag.

**Note**

- ◆ You can configure priority duplication of the user tag only on the dot1q-tunnel port, whose priority is higher than QoS in the trusted mode but lower than flow-based QoS.
- ◆ Priority duplication and priority mapping cannot be enabled on one interface at the same time.

The following example shows how to configure the priority duplication of the user tag:

```
Ruijie(config)# interface gigabitethernet 0/1
Ruijie(config-if)# mls qos trust cos
Ruijie(config-if)# inner-priority-trust enable
Ruijie(config)# end
Ruijie# show inner-priority-trust interface gigabitethernet 0/1
Port      inner-priority-trust
-----  -
```

Gi0/1 enable

## Configuring Priority Mapping

Follow these steps to set the priority of outer tag by the priority of inner tag:

Command	Description
<b>configure terminal</b>	Enter the global configuration mode.
<b>interface &lt;interface&gt;</b>	Enter the interface configuration mode.
<b>dot1q-Tunnel cos inner-cos-value remark-cos outer-cos-value</b>	Set the priority of outer tag (ISP tag) by the priority value of the inner tag (user tag).
<b>end</b>	Exit the interface mode.
<b>show interface intf-name remark</b>	View the priority mapping configuration of the user tag.

**Note**

- You can configure priority duplication of the user tag only on the dot1q-tunnel port, whose priority is higher than QoS.
- Priority duplication and priority mapping cannot be enabled on one interface at the same time.
- Priority mapping takes effect only when trust none is configured.

```
inner pri   0   1   2   3   4   5   6   7
-----
outer pri   0   1   2   3   4   5   6   7
```

The following example shows how to configure the priority mapping of the user tag:

```
Ruijie(config)# interface gigabitethernet 0/1
Ruijie(config-if)# dot1q-Tunnel cos 3 remark-cos 5
Ruijie(config)# end
Ruijie# show interface gigabitethernet 0/1 remark
Ports      Type      From value  To value
-----  -
Gi0/1      Cos-To-Cos  3           5
```

## Configuring Address Duplication

Follow these steps to duplicate the learned dynamic address from one VLAN to another VLAN:

Command	Description
<b>configure terminal</b>	Enter the global configuration mode.
<b>interface</b> <interface>	Enter the interface configuration mode.
<b>mac-address-mapping</b> <i>x</i> <b>source-vlan</b> <i>src-vlan-list</i> <b>destination-vlan</b> <i>dst-vlan-id</i>	Configure the learned dynamic address from the source VLAN to the destination VLAN.
<b>end</b>	Exit the interface mode.
<b>show interface</b> <i>intf-name</i> <b>mac-address-mapping</b> <i>x</i>	View the address duplication configuration.



### Note

- ◆ Disabling inter-VLAN MAC address duplication will remove all learned MAC address entries of other VLANs from the destination VLAN.
- ◆ Inter-VLAN MAC address duplication can be set only once for a VLAN on a port. To modify the configuration, delete it first.
- ◆ This function cannot be used in conjunction with share VLAN. MAC address cannot be duplicated into dynamic VLAN.
- ◆ Up to 8 destination VLANs can be configured on a port. Address duplication takes effect even though the port is not in the specific destination VLAN.
- ◆ Address duplication cannot be enabled on host/promiscuous port, mirroring destination port or the port with port security and 802.1x enabled.
- ◆ The priority of duplicated address is higher than dynamic address but lower than other types of address.
- ◆ When the source MAC address is aging, the duplicated address is aging as well. This also applies to deleting MAC address.
- ◆ Hot backup is not supported. When master-slave handover occurs, it is recommended users to disable and then enable address duplication.
- ◆ The MAC address entries obtained by inter-VLAN MAC address duplication cannot be deleted by hand. To delete these entries, disable inter-VLAN MAC address duplication.

The following example shows how to configure address duplication of the user tag:

```
Ruijie(config)# interface gigabitethernet 0/1
Ruijie(config)# switchport mode trunk
```

```

Ruijie(config-if) #mac-address-mapping destination-vlan5 source-vlan
1-3
Ruijie(config) # end
Ruijie# show interface mac-address-mapping
Ports      destination-VID      Source-VID-list
-----
Gi0/1      5                          1-3

```

## Configuring Transparent Transmission of L2 Protocol Packets

### Configuring Transparent Transmission of STP Protocol Packets

In the privileged EXEC mode, you can configure transparent transmission of STP protocol packets by the following steps:

Command	Description
<b>configure terminal</b>	Enter the global configuration mode.
<b>l2protocol-tunnel stp</b>	Configure to enable transparent transmission of STP protocol packets globally.
<b>interface</b> <i>interface-id</i>	Enter the interface configuration mode.
<b>l2protocol-tunnel stp enable</b>	Enable transparent transmission of STP protocol packets on the interface.
<b>show l2protocol-tunnel stp</b>	View the configuration.

An example below shows how to enable transparent transmission of STP protocol packets:

```

Ruijie# configure
Ruijie(config) # l2protocol-tunnel stp
Ruijie(config) # interface fa 0/1
Ruijie(config-if) # l2protocol-tunnel stp enable

```


### Configuring Transparent Transmission of GVRP Protocol Packets

In the privileged EXEC mode, you can configure transparent transmission of GRVP protocol packets by the following steps:

Command	Description
<b>configure terminal</b>	Enter the global configuration mode.
<b>l2protocol-tunnel gvrp</b>	Configure to enable transparent transmission of GRVP protocol packets globally.
<b>interface</b> <i>interface-id</i>	Enter the interface configuration mode.
<b>l2protocol-tunnel gvrp enable</b>	Enable transparent transmission of GRVP protocol packets on the interface.
<b>show l2protocol-tunnel gvrp</b>	View the configuration.

An example below shows how to enable transparent transmission of GVRP protocol packets:

```
Ruijie# configure
Ruijie(config)# l2protocol-tunnel gvrp
Ruijie(config)# interface fa 0/1
Ruijie(config-if)# l2protocol-tunnel gvrp enable
```

 <p><b>Note</b></p>	<p>Enabling transparent transmission on the interface takes effect only after this function is enabled globally. Once enabled, the interface does not join the protocol computation. If the packets received are destined to special multicast address, this implies that there is something wrong in the network and thus the packets are directly dropped.</p>
--	--


## Configuring Transparent Transmission Address

In the privileged EXEC mode, you can configure transparent transmission address by the following steps:

Command	Description
<b>configure terminal</b>	Enter the global configuration mode.
<b>l2protocol-tunnel {stp   GVRP} tunnel-dmac mac-address</b>	Configure the transparent transmission address of corresponding protocol.
<b>show l2protocol-tunnel stp</b>	View the configuration.

An example below shows how to configure the transparent transmission address of STP protocol:

```
Ruijie# configure
Ruijie(config)# l2protocol-tunnel stp tunnel-dmac 011AA9 000005
```

 <p><b>Note</b></p>	<p>The addresses available for STP protocol are 01d0f8 000005, 011AA9 000005, 010FE2 000003, 01000C CDCDD0, 01000C CDCDD1, 01000C CDCDD2, and the addresses available for GVRP protocol are 01d0f8 000006 and 011AA9 000006.</p> <p>Without transparent transmission address configured, by default, the last bit of the first byte of the OUI of the local device is set to 1 plus the next three bytes (stp:000005; gvrp:000006) as multicast address. For instance, the local device's MAC address is 00d0f8000001, then the transparent transmission address for STP protocol is 01d0f8000005.</p>
--	--

## Show QinQ Informaiton

In the privileged EXEC mode, use the following command to show QinQ configuration.

Command	Description
---------	-------------

Ruijie# <b>show dot1q-tunnel</b>	Show the enablement state of dot1q-tunnel port.
Ruijie# <b>show interface</b> [ <i>intf-id</i> ] <b>dot1q-tunnel</b>	Show the configuration of dot1q-tunnel port.
Ruijie# <b>show registration-table</b> [ <b>interface</b> <i>intf-id</i> ]	Show the protocol-based VID change policy table on the dot1q-tunnle port.
Ruijie# <b>show translation-table</b> [ <b>interface</b> <i>intf-id</i> ]	Show the protocol-based VID change policy table on the Access, Trunk and Hybird ports.
Ruijie# <b>show traffic-redirect</b> [ <b>interface</b> <i>intf-id</i> ]	Show the flow-based VID change policy table.
Ruijie# <b>show frame-tag tpid interface</b> [ <i>intf-id</i> ]	Show the TPID value on the interface.
Ruijie# <b>show inner-priority-trust</b>	Show the priority duplication configuration.
Ruijie# <b>show interface intf-name remark</b>	Show the priority mapping configuration.
Ruijie# <b>show mac-address-mapping</b>	Show the address duplication configuration.
Ruijie# <b>show l2protocol-tunnel</b> { <b>gvrp</b>   <b>stp</b> }	Show the transparent transmission configuration of Layer 2 protocols.

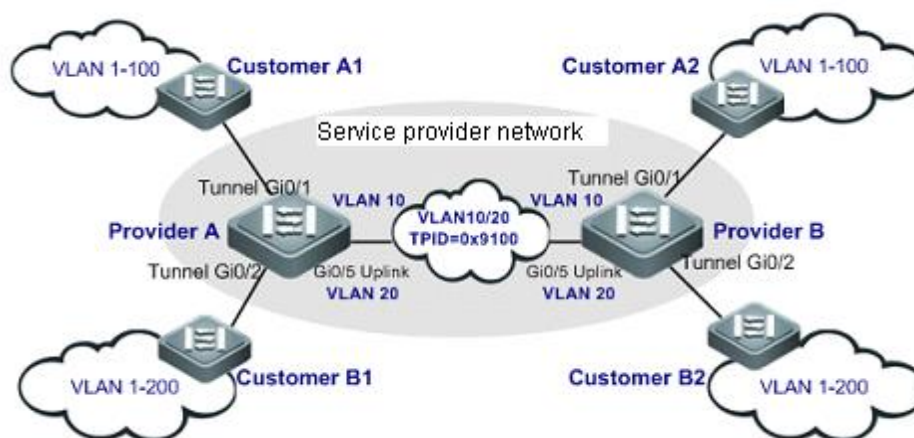
## Typical QinQ configuration example

### Using basic QinQ to realize layer-2 VPN service

#### Topological diagram

Company A and B have their respective offices, and each office has its respective network. As shown below, Customer A1, Customer A2, Customer B1 and Customer B2 are all edge devices of Company A and Company B. Customer A1 and Customer B1 access the public network through the provider edge device of Provider A, while Customer A2 and Customer B2 access the public network through the provider edge device of Provider B. The VLAN range of the office network used by Customer A1-A2 is VLAN1-100, and that used by Customer B1-B2 is VLAN1-200.

Provider A and Provider B are devices of another manufacturer, with TPID being 0x9100.



**Figure 8 Topology for using basic QinQ to realize layer-2 VPN service**

## Application requirements

The service provider provides VPN service for Company A and Company B, and the specific requirements are shown below:

1. The data of both companies can preserve the original VLAN information when being sent to the peer side.
2. Data with same VLAN ID won't cause conflict during transmission over ISP network.

## Configuration tips

1. You don't need to distinguish the traffic of downlink users. Enabling basic QinQ on the provider edge devices (Provider A and Provider B) will meet the needs.
2. The TPID of Ruijie switches is different from the TPID used by other manufacturers. You need to configure on the Uplink interface of provider edge devices (Provider A and Provider B) and set TPID to the same value with third-party devices.



### Note

1. In QinQ configuration model, when the service-network-connecting uplink port of edge device or the interconnecting ports of service provider devices are Trunk ports or Hybrid ports, please don't set the native vlan of trunk ports or hybrid ports to the default vlan of tunnel port, because packets leaving the trunk port or hybrid port will be stripped off the Tag with VID being its native vlan.
2. QinQ-enabled device will encapsulate the outer Tag of other VLAN for user packets and won't forward packets as per the original VLAN in the packets. Therefore, there is no need to create user's VLAN on the device.

## Configuration Steps

### 1) Configure Provider A

Step 1: Create provider VLAN 10 and VLAN 20 to distinguish the traffic of two users

```
Ruijie#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Ruijie(config)#vlan 10
Ruijie(config-vlan)#exit
Ruijie(config)#vlan 20
Ruijie(config-vlan)#exit
```

Step 2: Enable basic QinQ on the interface connecting to the network of Company A, and use VLAN 10 to transmit the traffic of Company A through tunnel.

```
Ruijie(config)#interface gigabitEthernet 0/1
```

```
Ruijie(config-if-GigabitEthernet 0/1)#switchport mode dot1q-tunnel
Ruijie(config-if-GigabitEthernet 0/1)#switchport dot1q-tunnel native vlan 10
Ruijie(config-if-GigabitEthernet 0/1)#switchport dot1q-tunnel allowed vlan add untagged
10
```

Step 3: Enable basic QinQ on the interface connecting to the network of Company B, and use VLAN 20 to transmit the traffic of Company B through tunnel.

```
Ruijie(config)#interface gigabitEthernet 0/2
Ruijie(config-if-GigabitEthernet 0/2)#switchport mode dot1q-tunnel
Ruijie(config-if-GigabitEthernet 0/2)#switchport dot1q-tunnel native vlan 20
Ruijie(config-if-GigabitEthernet 0/2)#switchport dot1q-tunnel allowed vlan add untagged
20
```

#### Step 4: Configure Uplink port

```
Ruijie(config)# interface gigabitEthernet 0/5
Ruijie(config-if-GigabitEthernet 0/5)#switchport mode uplink
```

Step 5: On the Uplink port, set the TPID value of egress packets to 0x9100, which can be recognized by third-party devices.

```
Ruijie(config-if-GigabitEthernet 0/5)#frame-tag tpid 9100
```

### 2) Configure Provider B

Configurations on Provider B are the same as those on Provider A. Please refer to the configurations on Provider A given above.

### Verification

Step 1: Verify whether the tunnel ports have been properly configured. Key points: whether port type is dot1q-tunnel, whether the outer Tag VLAN is Native VLAN and is included in the allowed VLAN list of the port, and whether the uplink port on provider edge device is Uplink, Trunk or Hybrid port.

Ruijie#show running-config

```
interface GigabitEthernet 0/1
  switchport mode dot1q-tunnel
  switchport dot1q-tunnel allowed vlan add untagged 10
  switchport dot1q-tunnel native vlan 10
  spanning-tree bpdufilter enable
!
interface GigabitEthernet 0/2
  switchport mode dot1q-tunnel
  switchport dot1q-tunnel allowed vlan add untagged 20
  switchport dot1q-tunnel native vlan 20
  spanning-tree bpdufilter enable
```



```

!
interface GigabitEthernet 0/5
    switchport mode uplink
    frame-tag tpid 0x9100

```

Step 2: Verify the QinQ configuration of respective ports again. Key points are the same as Step 1.

```

Ruijie#show interfaces dot1q-tunnel

=====Interface Gi0/1=====
Native vlan: 10
Allowed vlan list:1,10,
Tagged vlan list:

=====Interface Gi0/2=====
Native vlan: 20
Allowed vlan list:1,20,
Tagged vlan list:

```

Step 3: Verify the TPID configuration. Key point: whether the interface is Uplink port, TPID value.

```

Ruijie#show frame-tag tpid

Ports      Tpid
-----
Gi0/5      0x9100

```

Steps to verify configurations on Provider B are the same as those on Provider A. Please refer to the verification steps on Provider A given above.

## C-Tag based flexible QinQ to distinguish traffic

### Topological diagram

The following figure shows the networking diagram of metropolitan area network for C-Tag based flexible QinQ to classify the traffic. Broadband Internet and IPTV are all important services carried on the metropolitan area network. As shown below, client devices converge at the corridor switch, and broadband Internet and IPTV traffic will be classified by assigning different VLANs. Broadband Internet users fall within VLAN 101-200, while IPTV users fall within VLAN 201-300.

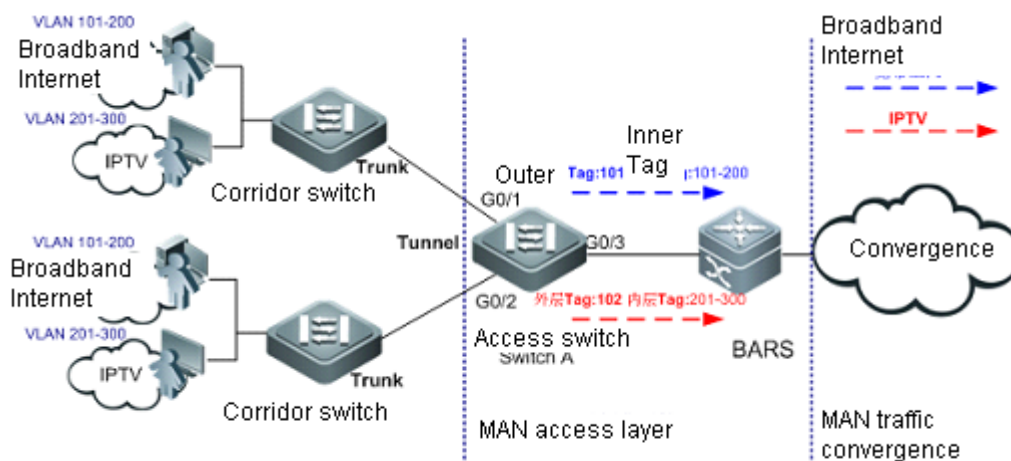


Figure 9 C-Tag based flexible QinQ to realize Internet access service

## Application requirements

Broadband Internet and IPTV traffic shall be identified by VLAN ID, so as to apply different QoS service policies to different traffic.

## Configuration tips

Configure C-Tag based flexible QinQ on MAN access layer switch's two interfaces (G0/1 and G0/2 of Switch A) connecting with the corridor convergence switches. The application requirements can be met by classifying service traffic as per inner VLAN Tag.

Flexible QinQ VLAN label planning for adding S-Tag on the basis of C-Tag traffic classification

Device	Service	Inner VLAN Tag	Outer VLAN Tag	Traffic classification rule
Switch A	Broadband Internet	101-200	101	C-Tag VLAN range
Switch A	IPTV	201-300	201	C-Tag VLAN range



### Note

QinQ-enabled device will encapsulate the outer Tag of other VLAN for user packets and won't forward packets as per the original VLAN in the packets. Therefore, there is no need to create user's VLAN on the device.

## Configuration Steps

### • Configure Switch A

Step 1: Create provider VLAN 101 and VLAN 201 to distinguish the traffic of different services

```
Ruijie#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Ruijie(config)#vlan 101
Ruijie(config-vlan)#exit
Ruijie(config)#vlan 201
Ruijie(config-vlan)#exit
```

**Step 2: On the downlink port of access switch, configure flexible QinQ for adding outer VLAN Tag on the basis of C-Tag**

```
Ruijie(config)#interface range gigabitEthernet 0/1-2
Ruijie(config-if-range)# switchport mode dot1q-tunnel
```

**! Configure Gi 0/1 and Gi 0/2 as Tunnel ports**

```
Ruijie(config-if-range)# switchport dot1q-tunnel allowed vlan add untagged 101,201
```

**! Add provider VLAN 101 and VLAN 201 into the allowed VLAN list of Tunnel port, and configure to strip the provider Tag when the peer packets return to the Tunnel port.**

```
Ruijie(config-if-range)# dot1q outer-vid 101 register inner-vid 101-200
```

**! Configure to add the tag of vlan 101 (S-tag) to vlan 101-200 (C-tag) data frames entering Tunnel port for transmission over the provider network**

```
Ruijie(config-if-range)# dot1q outer-vid 201 register inner-vid 201-300
```

**! Configure to add the tag of vlan 201 (S-tag) to vlan 201-300 (C-tag) data frames entering Tunnel port for transmission over the provider network.**

**Step 3: Configure Uplink port**

```
Ruijie(config)# interface gigabitEthernet 0/3
Ruijie(config-if-GigabitEthernet 0/3)#switchport mode uplink
```



**Note**

Outer Tag VLAN (including Native VLAN) shall be allowed on Tunnel port, and packets of such VLAN shall be allowed to pass the Internet-accessing interface. In this example, the Native VLAN of Tunnel port is the default VLAN1, which is allowed by default.

## Verification

**Step 1: Verify whether the configurations are correct. Key points: whether the type of downlink interface is dot1q-tunnel, whether the outer Tag VLAN is included in the allowed VLAN list of the interface, whether the mapping policy on the interface is correct, and whether the uplink port has been properly configured.**

```
Ruijie#show running-config interface gigabitEthernet 0/1

interface GigabitEthernet 0/1
    switchport mode dot1q-tunnel
```

```

switchport dot1q-tunnel allowed vlan add untagged 101,201
dot1q outer-vid 101 register inner-vid 101-200
dot1q outer-vid 201 register inner-vid 201-300
spanning-tree bpdufilter enable
!
interface GigabitEthernet 0/2
switchport mode dot1q-tunnel
switchport dot1q-tunnel allowed vlan add untagged 101,201
dot1q outer-vid 101 register inner-vid 101-200
dot1q outer-vid 201 register inner-vid 201-300
spanning-tree bpdufilter enable
!
interface GigabitEthernet 0/3
switchport mode uplink

```

Step 2: Verify the QinQ configuration of respective ports again. Key points are the same as Step 1.

```

Ruijie#show interfaces dot1q-tunnel

=====Interface Gi0/1=====
Native vlan: 1
Allowed vlan list:1,101,201
Tagged vlan list:

=====Interface Gi0/2=====
Native vlan: 1
Allowed vlan list:1, 101,201
Tagged vlan list:

```

Step 3: Verify the mapping rule for adding Tag on the basis of C-Tag. Key points: whether the mapping between inner VLAN tag and outer VLAN tag is correct.

```

Ruijie#show registration-table

Ports          Outer-VID  Inner-VID-list
-----
Gi0/1          101       101-200
Gi0/1          201       201-300
Gi0/2          101       101-200
Gi0/2          201       201-300

```

## ACL-based flexible QinQ to distinguish traffic

### Topological diagram

The following figure shows the networking diagram for ACL-based flexible QinQ deployed on the metropolitan area network. The service provider provides broadband access and IPTV services to users. There are many out-of-date and low-end network access devices on user's network, making it impossible to effectively distinguish traffic according to VLAN ID. All types of services are carried in the same VLAN.

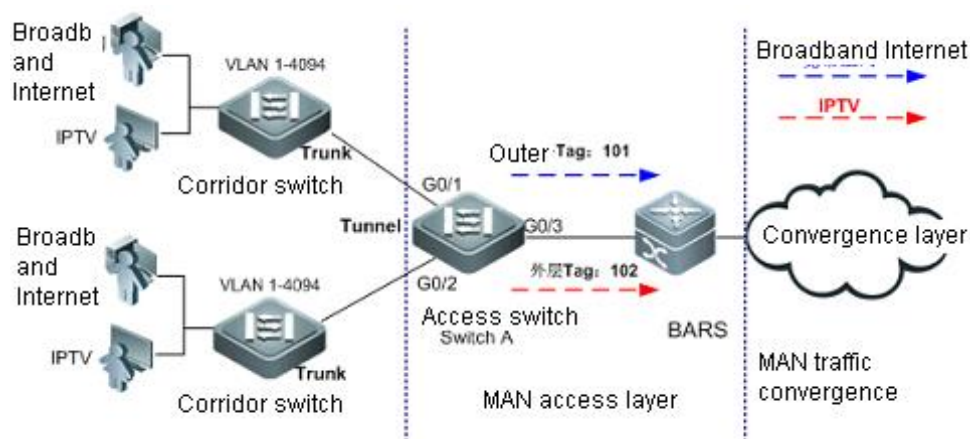


Figure 10 ACL-based flexible QinQ to realize Internet access service

### Application requirements

Broadband Internet and IPTV traffic of downstream users shall be identified by protocol, so as to apply different QoS service policies to different traffic.

### Configuration tips

Configure the ACL based flexible QinQ on MAN access layer switch's two interfaces (G0/1 and G0/2 of Switch A) connecting with the corridor convergence switches, so as to distinguish user traffic and meet the application requirements.

Generally, PPPOE dialing is used in broadband Internet service, with protocol number being 0x8863/0x8864 typically; IPoE is used in IPTV service, with protocol number being 0x0800 typically.

#### Flexible QinQ VLAN label planning for adding S-Tag on the basis of ACL traffic classification

Device	Service	Inner VLAN Tag	Outer VLAN Tag	Traffic classification rule
Switch A	Broadband (PPPoE)	1-4094	101	Protocol number: 0x8863/0x8864

Switch A	IPTV (IPoE)	1-4094	201	Protocol number: 0x0800
----------	----------------	--------	-----	-------------------------------

## Configuration Steps

### ● Configure Switch A

#### Step 1: Create ACL for distinguishing traffic

```
Ruijie#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Ruijie(config)# expert access-list extended acl1
! Matching protocol type 0x8863/0x8864 of PPPOE
Ruijie(config-exp-nacl)# permit 0x8863 any any
Ruijie(config-exp-nacl)# permit 0x8864 any any
Ruijie(config-exp-nacl)#exit
Ruijie(config)# expert access-list extended acl2
! Matching protocol type 0x0800 of IPOE
Ruijie(config-exp-nacl)#permit 0x0800 any any
```

#### Step 2: Create provider VLAN 101 and VLAN 201 to distinguish the traffic of different users.

```
Ruijie#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Ruijie(config)#vlan 101
Ruijie(config-vlan)#exit
Ruijie(config)#vlan 201
Ruijie(config-vlan)#exit
```



#### Note

QinQ-enabled device will encapsulate the outer Tag of other VLAN for user packets and won't forward packets as per the original VLAN in the packets. Therefore, there is no need to create user's VLAN on the device.

#### Step 3: On the downlink port of access switch, configure flexible QinQ for adding outer VLAN Tag on the basis of ACL

```
Ruijie(config)#interface range gigabitEthernet 0/1-2
Ruijie(config-if-range)# switchport mode dot1q-tunnel
```

! Configure Gi 0/1 and Gi 0/2 as Tunnel ports

```
Ruijie(config-if-range)#switchport dot1q-tunnel allowed vlan add untagged 101,201
```

! Add provider VLAN 101 and VLAN 201 into the allowed VLAN list of Tunnel port, and configure to strip the provider Tag when the peer packets return to the Tunnel port.

```
Ruijie(config-if-range)#traffic-redirect access-group acl1 nested-vlan 101 in
```

! Configure to add the tag of vlan 101 (S-tag) to data frames matching ACL1 and entering Tunnel port for transmission over the provider network

```
Ruijie(config-if-range)#traffic-redirect access-group acl2 nested-vlan 201 in
```

! Configure to add the tag of vlan 201 (S-tag) to data frames matching ACL2 and entering Tunnel port for transmission over the provider network

#### Step 4: Configure GigabitEthernet 0/3 as an Uplink port

```
Ruijie(config)# interface gigabitEthernet 0/3
Ruijie(config-if-GigabitEthernet 0/3)#switchport mode uplink
```



#### Note

Outer Tag VLAN (including Native VLAN) shall be allowed on Tunnel port, and packets of such VLAN shall be allowed to pass the Internet-accessing interface. In this example, the Native VLAN of Tunnel port is the default VLAN1, which is allowed by default.

## Verification

Step 1: Verify whether the configurations of Tunnel port are correct. Key points: whether the interface type is dot1q-tunnel, whether the outer Tag VLAN is included in the allowed VLAN list of the interface, and whether the policy on the interface has been properly configured.

# View the configurations on GigabitEthernet 0/1

```
Ruijie#show running-config interface gigabitEthernet 0/1

interface GigabitEthernet 0/1
  switchport mode dot1q-tunnel
  switchport dot1q-tunnel allowed vlan add untagged 101,201
  traffic-redirect access-group acl1 nested-vlan 101 in
  traffic-redirect access-group acl2 nested-vlan 201 in
  spanning-tree bpdufilter enable
!
interface GigabitEthernet 0/2
  switchport mode dot1q-tunnel
  switchport dot1q-tunnel allowed vlan add untagged 101,201
  traffic-redirect access-group acl1 nested-vlan 101 in
  traffic-redirect access-group acl2 nested-vlan 201 in
  spanning-tree bpdufilter enable
!
interface GigabitEthernet 0/3
  switchport mode uplink
```

Step 2: Verify the QinQ configuration of respective ports again. Key points are the same as Step 1.

```
Ruijie#show interfaces dot1q-tunnel
```

```

=====Interface Gi0/1=====
Native vlan: 1
Allowed vlan list:1,101,201
Tagged vlan list:

=====Interface Gi0/2=====
Native vlan: 1
Allowed vlan list:1,101,201
Tagged vlan list:

```

**Step 3: Verify whether ACL configurations are correct. Key point: whether ACL entries are correct.**

```

Ruijie#show access-lists

expert access-list extended acl1
 10 permit 0x8863 any any
 20 permit 0x8864 any any

```

**! Match broadband service traffic**

```

expert access-list extended acl2
 10 permit 0x800 any any

```

**! Match IPTV service traffic**

**Step 4: Verify the mapping rule for adding Tag based on traffic. Key point: whether the mapping between inner VLAN tag and outer VLAN tag is correct.**

```

Ruijie#show traffic-redirect

Ports      Type      VID      Match-filter
-----
Gi0/1      Nested-vid 101      acl1
Gi0/1      Nested-vid 201      acl2
Gi0/2      Nested-vid 101      acl1
Gi0/2      Nested-vid 201      acl2

```



## Typical BPDU Tunnel configuration example

### Topological diagram

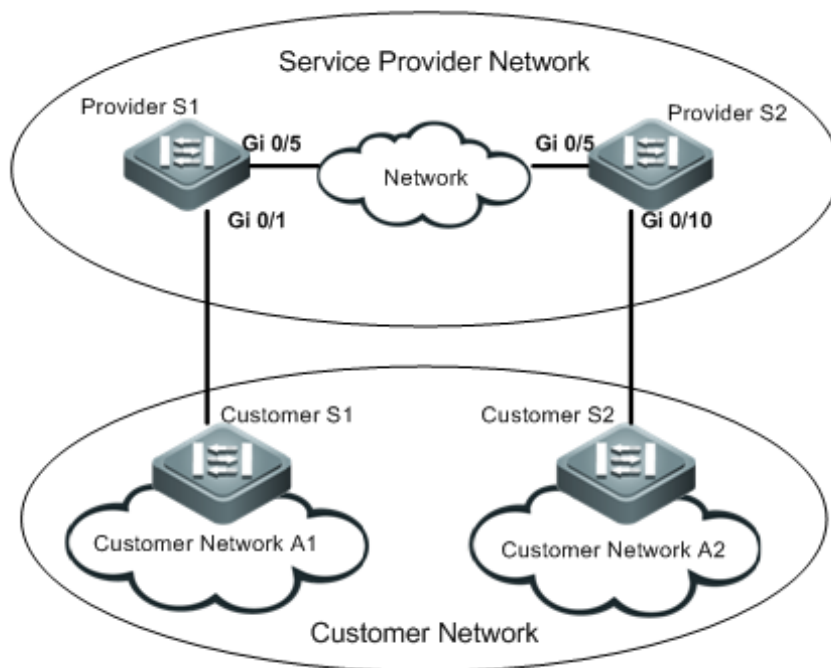


Figure 11 Topological diagram for BPDU Tunnel application

As shown above, the upper part is the provider network, and the lower part is the user network. The provider network includes edge devices of Provider S1 and Provider S2. Customer Network A1 and Customer Network A2 are two sites of the same user at different geographical locations. Customer S1 and Customer S2 are the access devices connecting user network with provider network, and access the provider network through Provider S1 and Provider S2 respectively.

### Application requirements

1. Packets from user network are transmitted over provider network in VLAN200.
2. Customer Network A1 and Customer Network A2 at different geographical locations can participate in unified spanning tree calculation across the provider network without affecting the provider network.

### Configuration tips

1. Enabling basic QinQ on the provider edge devices (Provider S1 and Provider S2) will meet the first need.
2. Enabling STP transparent transmission on provider edge devices (Provider S1 and Provider S2) will allow the provider network to transmit STP packets from user network through BPDU tunnel.

**Note**

In QinQ configuration model, when the service-network-connecting uplink port of edge device or the interconnecting ports of service provider devices are Trunk ports or Hybrid ports, please don't set the native vlan of trunk ports or hybrid ports to the default vlan of tunnel port, because packets leaving the trunk port or hybrid port will be stripped off the Tag with VID being its native vlan.

## Configuration Steps

### ● Configure Provider S1

#### Step 1: Create provider VLAN 200

```
Ruijie#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Ruijie(config)#vlan 200
Ruijie(config-vlan)#exit
```

Step 2: Enable basic QinQ on the interface connecting to the user network, and use VLAN 200 to transmit the traffic of user network through tunnel.

```
Ruijie(config)#interface gigabitEthernet 0/1
Ruijie(config-if-GigabitEthernet 0/1)#switchport mode dot1q-tunnel
Ruijie(config-if-GigabitEthernet 0/1)#switchport dot1q-tunnel native vlan 200
Ruijie(config-if-GigabitEthernet 0/1)#switchport dot1q-tunnel allowed vlan add untagged 200
```

Step 3: Enable STP transparent transmission on the interface connecting to the user network.

```
Ruijie(config-if-GigabitEthernet 0/1)#l2protocol-tunnel stp enable
Ruijie(config-if-GigabitEthernet 0/1)#exit
```

Step 4: Enable global STP protocol transparent transmission.

```
Ruijie(config)#l2protocol-tunnel stp
```

#### Step 5: Configure Uplink port

```
Ruijie(config)# interface gigabitEthernet 0/5
Ruijie(config-if-GigabitEthernet 0/5)#switchport mode uplink
```

### ● Configure Provider S2

Configurations on Provider S2 are the same as those on Provider S1. Please refer to the configurations on Provider S1 given above.

## Verification

Step 1: Verify the configurations of STP protocol transparent transmission. Key point: whether STP protocol transparent transmission has been enabled.

```
Ruijie#show l2protocol-tunnel stp

L2protocol-tunnel: Stp Enable
GigabitEthernet 0/1 l2protocol-tunnel stp enable
```

Step 2: Verify whether the tunnel ports have been properly configured. Key points: whether port type is dot1q-tunnel, whether the outer Tag VLAN is Native VLAN and is included in the allowed VLAN list of the port, and whether the uplink port on provider edge device is Uplink port.

```
Ruijie#show running-config
interface GigabitEthernet 0/1
  switchport mode dot1q-tunnel
  switchport dot1q-tunnel allowed vlan add untagged 200
  switchport dot1q-tunnel native vlan 200
  l2protocol-tunnel stp enable
  spanning-tree bpdufilter enable
!
interface GigabitEthernet 0/5
  switchport mode uplink
```

Steps to verify configurations on Provider S2 are the same as those on Provider S1. Please refer to the verification steps on Provider S1 given above.

# MAC VLAN Configuration

## Introduction to MAC VLAN

### Overview

With the popularization of mobile officing, the terminal device will no longer use a fixed port to access network. This time it may use port A to access network, and next time it may use port B to access network. If port A and port B have different VLAN configurations, then the terminal device will be assigned to a different VLAN when it accesses network for the second time, and will be unable to use resources of the former VLAN. If port A and port B share the same VLAN configurations, then the security problem will arise when port B is allocated to other terminal devices. How to allow different terminals to access respective VLANs freely on the same port? The feature of MAC VLAN is thereby introduced.

MAC address based VLAN (MAC VLAN) is a brand-new VLAN configuration approach. It is generally used in conjunction with 802.1X VLAN assignment function to allow secure and flexible access of 802.1X terminals. When a 802.1x user passes the authentication, the switch will automatically generate MAC VLAN entry according to the VLAN assigned by the authentication server and the MAC address of the user. The network administrator can also pre-configure the MAC-to-VLAN mapping on the switch.

The greatest advantage of MAC VLAN is that: when user changes its physical location (from one switch to another switch), there is no need to reconfigure the VLAN on the port used by the user. Therefore, such MAC address based VLAN can be considered a user-based VLAN.

### Basic concepts

NA

### Working principle

When switch receives the packet, it will compare the source MAC of data traffic with the MAC address specified in the MAC VLAN entry. If matched, the packets will be forwarded to the VLAN specified by the MAC VLAN entry; otherwise, the packets will be forwarded to the VLAN as per the rule configured on the port.

In order to assign PC to the specified VLAN when it accesses from any switch, we can configure through the following two schemes:

- Static configuration through CLI. The user can manually configure MAC-to-VLAN mapping on the local switch.
- Automatic configuration through the authentication server (802.1X VLAN assignment). When the user passes authentication, the switch will dynamically create the MAC-to-VLAN mapping according to information provided by the authentication server. When user terminates the session, the switch will automatically delete such mapping. This scheme will require you to configure MAC-to-VLAN mapping on the authentication server. Please refer to "802.1X Configuration" for details about "802.1X VLAN Assignment".

MAC VLAN entry can support both configuration schemes (configure on the local device and the authentication server), but the configurations in both schemes must be identical in order to take effect. Otherwise, the

first-executed configuration will prevail.



#### Note

1. MAC VLAN can only be configured on HYBRID port.
2. During static configuration or dynamic generation of MAC VLAN entry, the specified VLAN must exist already.
3. Super VLAN (including Sub VLAN), Remote VLAN and Private VLAN cannot use the same VLAN as MAC VLAN.
4. If the VLAN specified already exists in MAC VLAN entry, this VLAN cannot be deleted. Before deleting this VLAN, you must first delete all statically configured MAC VLAN entries associated with this VLAN. Meanwhile, the sessions of all 802.1x users associated with VLAN must be terminated (delete all dynamic MAC VLAN entries).
5. The MAC address must be a unicast address.
6. MAC VLAN entry applies to all HYBRID ports on which MAC VLAN function is enabled.

## Protocol specification

NA

## Configure MAC VLAN

The following section describes how to configure the basic characteristics of MAC VLAN:

### Default configurations of MAC VLAN

The following table describes the default configurations of MAC VLAN.

Function	Default Setting
Port-based MAC VLAN	Disabled
Globally add/delete static MAC VLAN entry	None

### Enable/disable port-based MAC VLAN

By default, the port-based MAC VLAN function is disabled. All MAC VLAN entries won't take effect on the port. Enter port configuration mode and execute the following steps to enable MAC VLAN on the port.

Command	Function
Ruijie# <b>configure terminal</b>	Enter global configuration mode.
Ruijie(config)# <b>interface</b> <i>interface-name</i>	Enter port configuration mode; first configure the port to hybrid port.
Ruijie(config-if)# <b>mac-vlan enable</b>	Enable MAC VLAN on the port.
Ruijie(config-if)# <b>end</b>	Return to privilege mode.

Command	Function
Ruijie# <b>show mac-vlan interface</b>	Display the list of ports on which MAC VLAN is enabled.

Configuration example:

```
Ruijie# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Ruijie(config)# interface fastethernet 0/10
Ruijie(config-if)# mac-vlan enable
Ruijie(config-if)# end
Ruijie# show mac-vlan interface

MAC VLAN is enabled on following interface:
-----
fastethernet 0/10
```

## Globally add/Delete static MAC VLAN Entry

The user needs to configure MAC-to-VLAN mapping in the global configuration mode. Optional configuration includes 802.1p priority, with default value being 0.

Configure MAC VLAN in the global configuration mode as per the following steps:

Command	Function
Ruijie(config)# <b>mac-vlan mac-address</b> <i>mac-address</i> [ <b>mask</b> <i>mac-mask</i> ] <b>vlan</b> <i>vlan-id</i> [ <b>priority</b> <i>pri_val</i> ]	Configure MAC-to-VLAN mapping. You can also specify the MAC address mask and priority.
Ruijie(config)# <b>no mac-vlan all</b>	Delete all static MAC VLAN entries.
Ruijie(config)# <b>no mac-vlan mac-address</b> <i>mac-address</i> [ <b>mask</b> <i>mac-mask</i> ]	Delete static MAC VLAN entry with the specified MAC.
Ruijie(config)# <b>no mac-vlan vlan</b> <i>vlan-id</i>	Delete static MAC VLAN entry with the specified VLAN.

Configuration example:

```
Ruijie# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Ruijie(config)# mac-vlan mac-address 0000.0000.0001 vlan 2 priority 3
Ruijie(config)# no mac-vlan mac-address 0000.0000.0001
Ruijie(config)# no mac-vlan vlan 2
Ruijie(config)# no mac-vlan all
Ruijie(config)# end
```



### Caution

For the port on which MAC VLAN is enabled, if the packets received can simultaneously match MAC VLAN entries with mask being all-Fs and mask being not all-Fs, the MAC VLAN entry with mask being not all-Fs will prevail.

## View MAC VLAN configurations

The following section describes how to configure the basic configurations of MAC VLAN:

### View MAC VLAN entries

To view statically configured and dynamically generated MAC VLAN entries, execute the following steps in the privilege mode:

Command	Function
Ruijie# <b>show mac-vlan all</b>	Display all MAC VLAN entries, including static and dynamic entries.
Ruijie# <b>show mac-vlan dynamic</b>	Display dynamically generated MAC VLAN entries
Ruijie# <b>show mac-vlan static</b>	Display statically configured MAC VLAN entries
Ruijie# <b>show mac-vlan vlan</b> <i>vlan-id</i>	Display MAC VLAN entry with the specified VLAN.
Ruijie# <b>show mac-vlan mac-address</b> <i>mac-address</i> [ <i>mask mac-mask</i> ]	Display MAC VLAN entry with the specified MAC address.

Configuration example: View all MAC VLAN entries

```
Ruijie# show mac-vlan all
```

The following MAC VLAN address exist:

S: Static D: Dynamic

MAC ADDR	MASK	VLAN ID	PRIO	STATE
0000.0000.0001	ffff.ffff.ffff	2	0	D
0000.0000.0002	ffff.ffff.ffff	3	3	S
0000.0000.0003	ffff.ffff.ffff	3	3	S&D

Total MAC VLAN address count: 3

### View MAC VLAN enable/disable status on all ports

To view ports on which MAC VLAN is enabled, execute the following steps in the privilege mode:

Command	Function
Ruijie# <b>show mac-vlan interface</b>	Display MAC VLAN enable/disable status on all ports.

Configuration example: Display MAC VLAN enable/disable status on all ports.

```
Ruijie# show mac-vlan interface
```

MAC VLAN is enabled on following interface:

-----

fastethernet 0/3

fastethernet 0/10

## Typical MAC VLAN configurations

As shown in Fig 1: PC-A1 and PC-A2 belong to Department A and are assigned to VLAN 100; PC-B1 and PC-B2 belong to Department B and are assigned to VLAN 200. Due to personnel flow, the company has provided a interim officing space in the meeting room, but the accessing PC must be assigned to the VLAN of the its own department. For example, PC-A1 can only be assigned to VLAN 100 after accessing, and PC-B1 can only be assigned to VLAN 200 after accessing.

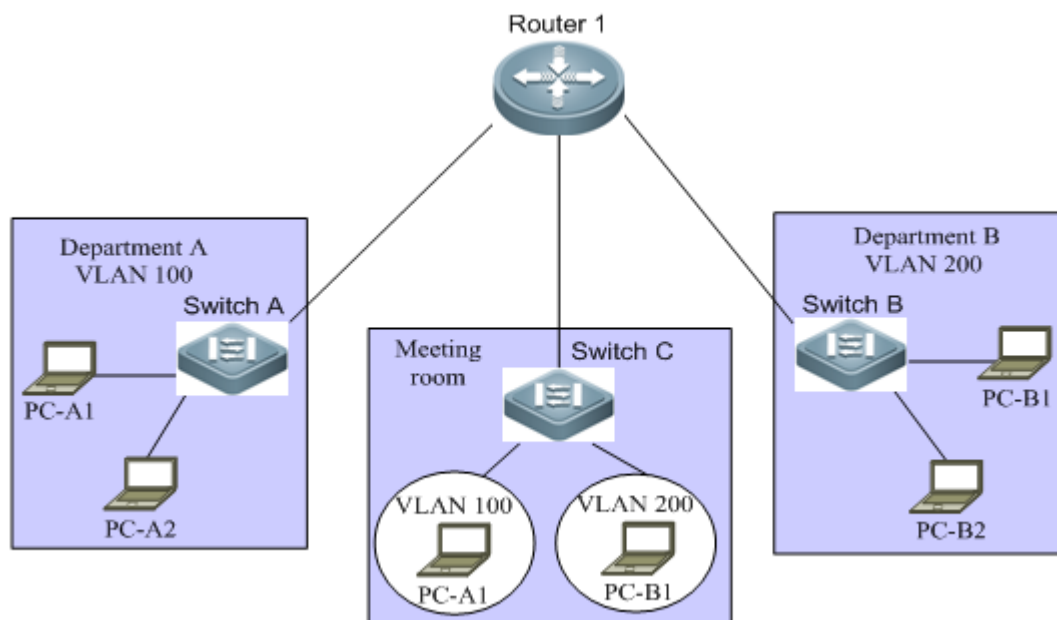


Fig 1 Typical application diagram of MAC VLAN

Since the port in the meeting room for PC to access network may change from time to time, we can use the function of MAC VLAN to map the MAC address of employee's PC to the VLAN of his/her department. No matter which port is used to access network, the employee's PC can always be assigned to the VLAN of his/her department.

### Static MAC VLAN configuration

If authentication of PC is not required, we can statically configure MAC VLAN entry to meet the aforementioned needs.

Configurations on Switch C:

Step 1: Configure the port connected with Router 1 to TRUNK port:

```
Ruijie(config) # interface interface_name
Ruijie(config-if) # switchport mode trunk
```

Step 2: Configure all PC-connecting ports to HYBRID ports, enable MAC VLAN and change the default UNTAG VLAN list.

```
Ruijie(config) # interface interface_name
Ruijie(config-if) # switchport mode hybrid
Ruijie(config-if) # switchport hybrid allowed vlan add untagged 100,200
Ruijie(config-if) # mac-vlan enable
```

Step 3: Configure MAC VLAN entry.



```
Ruijie(config)# mac-vlan mac-address PC-A1-mac vlan 100  
Ruijie(config)# mac-vlan mac-address PC-B1-mac vlan 200
```

Configure the corresponding MAC VLAN entries as per step 3 for all PCs accessing network via Switch C.

## MAC VLAN + 802.1x VLAN assignment configuration

If PCs are subject to 802.1x authentication, together with the function of 802.1x VLAN assignment, the MAC VLAN entries can be generated dynamically and the aforementioned access requirements can be met then.

Configurations on Switch C:

Step 1 and 2 are the same as those described in static MAC VLAN configuration.

Step 3: Enable 802.1x on the port and allow VLAN assignment.

```
Ruijie(config-if)# dot1x port-control auto  
Ruijie(config-if)# dot1x dynamic-vlan enable
```

The aforementioned needs can be met through the above configurations.

# ERPS Configuration

## Introduction to ERPS

### Overview

ERPS (Ethernet Ring Protection Switching) is a ring net protection protocol developed by ITU (also called G.8032). It is a link layer protocol applied on Ethernet ring network. When the Ethernet ring network is intact, ERPS can avoid the broadcast storm caused by the data ring; when one node on the ring is disconnected, it can promptly recover the communication between respective nodes on the ring network.

Metropolitan area network and enterprise network are mostly constructed into ring network to provide high reliability. Any node failure on the ring will compromise network service. RPR and Ethernet ring are the common technologies applied in ring network. RPR needs special hardware and high costs, while Ethernet ring network is increasingly developed with lower costs. Therefore, Ethernet ring is widely applied in the metropolitan area network and enterprise network.

Currently, STP is also an alternative technology to address the problems of layer-2 ring network. STP is a proven technology with longer convergence time (second level). ERPS is a link layer protocol specially applied on Ethernet ring network featuring faster convergence rate than STP.

### Basic Concepts

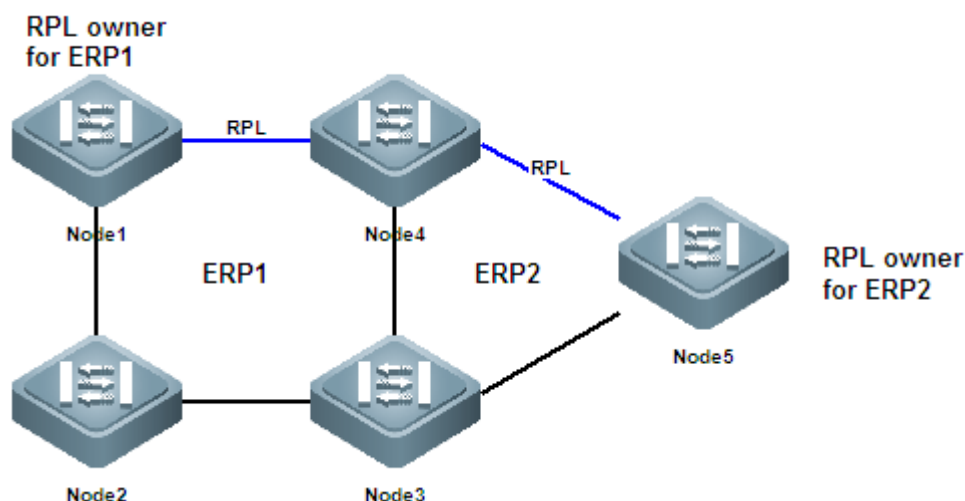


Fig 2 ERPS networking diagram

### Ethernet ring

Ethernet ring can be divided into Ethernet major-ring and Ethernet sub-ring:

Ethernet major-ring: Ring-connected Ethernet network topology.

Ethernet sub-ring: The Ethernet sub-ring doesn't constitute a closed ring. It is connected to other rings or network at interconnection nodes, and belongs to other rings together with the interconnection node or forms a closed-ring topology together with the network channel.

Each Ethernet ring (no matter the major-ring or the sub-ring) is featured by the following two states:

Idle state: When the physical links of ring network are connected;

Protection state: When a certain physical link on the ring network is disconnected.

**Caution**

According to the descriptions in G.8032 (ITU-T G.8032/Y.1344 Amendment 1), for intersecting rings, two interconnection nodes must be linked directly without any other device.

## Node

Every device on the Ethernet ring is called a node.

For a certain Ethernet ring, the nodes can be divided into the following roles:

RPL owner node: This node is adjacent to the RPL link and is responsible for blocking RPL link to avoid the formation of loop on the network. Each Ethernet ring (no matter the major-ring or the sub-ring) only has one RPL owner node. As shown in Figure 1, Node1 is the RPL owner node of Ethernet ring ERP1, while Node5 is the RPL owner node of Ethernet sub-ring ERP2.

Non-RPL owner node: Nodes other than the RPL owner node. As shown in Figure 1, nodes other than Node1 and Node5 are all called the non-RPL owner nodes of respective rings.

Globally speaking (not against a specific Ethernet ring), the nodes can be divided into the following roles:

Interconnection nodes: The ring nodes which are common to both intersecting rings. As shown in Figure 1, Node3 and Node4 are called interconnection nodes.

Non-interconnection nodes: The ring nodes that only belong to a specific Ethernet ring. As shown in Figure 1, nodes other than Node3 and Node4 are called non-interconnection nodes.

## Link and channel

RPL (Ring Protection Link): Each Ethernet ring (no matter the major-ring or the sub-ring) only has one RPL. When the Ethernet ring is in idle state, RPL link will be in blocking state and will not forward data packets in order to avoid the formation of loop. As shown in Figure 1, the link between Node1 and Node4 is the RPL link of Ethernet ring ERP1; Node1 blocks RPL port (the port that the RPL link is on). The link between Node4 and Node5 is the RPL link of Ethernet ring ERP2; Node5 blocks RPL port.

Sub-ring link: The link that belongs to and controlled by the sub-ring. As shown in Figure 1, assuming that ERP1 is the major-ring and ERP2 is the sub-ring, then the link between Node4 and Node5 and the link between Node3 and Node5 shall be the link of sub-ring ERP2, while other links shall belong to major-ring ERP1. (Please note: The link between Node3 and Node4 belongs to major-ring ERP1 instead of sub-ring ERP2. It is not controlled by ERP2.)

R-APS (Ring Auto Protection Switch) virtual channel: The channel used to transmitted sub-ring protocol packets between interconnection nodes but doesn't belong to the sub-ring. As shown in Figure 1, since Node1 blocks the RPL link and the protocol packets of sub-ring ERP2 are transmitted on Ethernet ring

ERP1 via the link between Node3 and Node4, the direct link between Node3 and Node4 is therefore called the R-APS virtual channel of sub-ring ERP2.

## VLAN

ERPS has two types of VLANs: R-APS VLAN and data VLAN.

**R-APS VLAN:** R-APS VLAN is used to transmit ERPS protocol packets. All ERP ring ports belong to R-APS VLAN, and only those ports can join this VLAN. R-APS VLAN differs from ring to ring, and the interface of R-APS VLAN must not be configured with any IP address.

**Data VLAN:** Different from R-APS VLAN, the data VLAN is used to transmit data packets. The data VLAN main can contain either ERP ring ports or non-ERP ring ports.



### Caution

Different ERP rings must be configured with different R-APS VLANs, or else the protocol may become abnormal. Packets of different ERP rings are distinguished via R-APS VLAN.

## ERPS Protocol Packets

The types and roles of ERPS protocol packets (also called R-APS packets) are shown below:

Packet type	Description
SF (Signal Fail) packets	When the local link of a node is down, SF packets will be sent to inform other nodes.
NR (No Request) packets	When the local link of a node recovers from failure, NR packets will be sent to inform the RPL owner node.
NR NB (No Request, RPL Blocked) packets	Sent by RPL owner node. When all devices on the ERP ring are fault-free, the RPL owner will periodically send these packets.
Flush packets	Sent by the interconnection node on the intersecting ring; used to inform other devices on the major-ring of the topological changes to the sub-ring.

## ERPS Timers

ERPS timers and their roles are shown below:

Packet type	Description
Holdoff timer	This timer is used to filter out intermittent link faults which may ERPS to switch topology continuously. After configuring this timer, when link fault is detected, ERPS will not switch topology immediately. Instead, it will wait until the timer runs out and then implement topology switching after verifying that the link fault remains.

Guard timer	This timer is used to prevent the device from receiving outdated R-APS messages. When the device detects that a link has recovered from fault, it will send out link recovery messages and start the guard timer. Before the guard timer runs out, except for the flush packets indicating the changes in sub-ring topology, all other packets will be discarded directly without processing.
WTR (Wait-to-restore) timer	This timer is only effective for RPL owner device. It is mainly used to avoid the misjudgment of ring status by RPL owner. When RPL owner detects a fault recovery, it will not implement topology switching immediately. Instead, it will wait until the WTR timer runs out and then implement topology switching after verifying that the Ethernet ring has recovered from the fault. If ring fault is detected again before the WTR timer runs out, the WTR timer will be canceled and no topology switching will be implemented.

## Working Principle

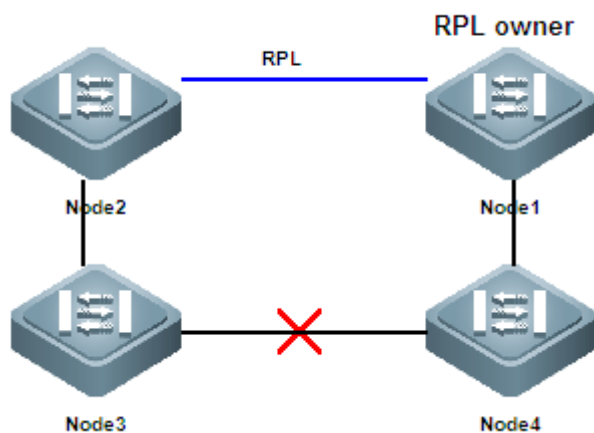


Fig 3 ERPS single ring

### Normal status

All nodes are connected in ring structure in the physical topology.

Link protection protocol prevents the formation of loop by blocking the RPL link. As shown in Figure 2, the link between Node1 and Node2 is the RPL link.

Fault detection of each link between adjacent nodes.

### Link failure

Fault detected by the node which is adjacent to the fault.

The adjacent nodes will block the failed link and send out R-APS (SF) messages to inform other nodes on the ring about such fault. As shown in Figure 2, assuming that the link between Node3 and Node4 fails, then Node3 and Node4 will send R-APS (SF) messages to each node on the ring after having blocked the failed link.

R-APS (SF) messages trigger RPL owner node and unblock the RPL port. R-APS (SF) messages will also trigger all nodes to upgrade their MAC entries and ARP/ND entries, and the nodes will go into protection state.

### Link recovery

When the fault recovers, the adjacent nodes will maintain the blocking state and send out R-APS (NR) messages indicating that there is no local fault.

When RPL owner node has received the first R-APS (NR) message, it will start the WTR timer.

When WTR timer runs out, RPL owner node will block RPL and send out R-APS (NR, RB) messages.

When other nodes receive such messages, they will upgrade their MAC entries and ARP/ND entries. The node sending R-APS (NR) messages will stop sending messages periodically and unblock the blocked port.

The link node returns to idle state.

### Load balancing

On the same ring network, there may be data traffic of multiple VLANs. ERPS can realize the load sharing of traffic, namely the traffic of different VLANs will be forwarded along different paths.

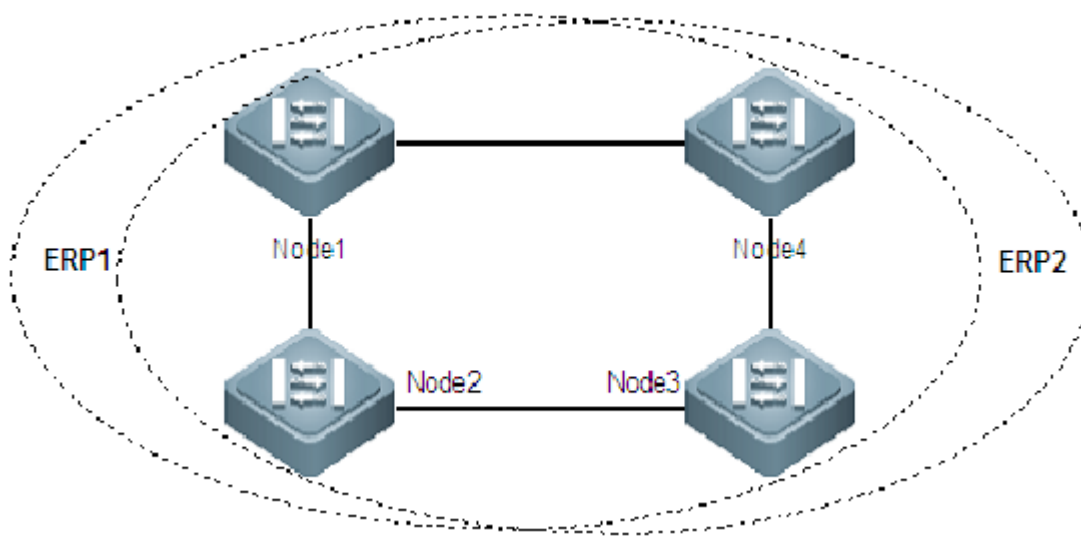


Fig 4 Single ring load sharing

By configuring multiple Ethernet rings on the same physical ring, different Ethernet rings will forward the traffic of different VLANs (VLAN protection), allowing load sharing.

As shown in Figure 3, a physical link carries two Ethernet rings, which protect different VLANs. Node1 is the RPL owner of ERP1, and Node3 is the RPL owner of ERP2. Through configuration, different VLANs can block different links, allowing load sharing on the single ring.

**Note**

Given the concepts of major-ring and sub-ring, the aforementioned working principle of single ring can directly apply to the intersecting rings. The intersecting rings operate independently as the single ring.

## Typical Network topologies

The normal operation of ERPS relies on the correct configurations by the user. Typical network topologies are introduced below:

### Single ring

As shown in Figure 2, there is only one ring in the network topology. There are only one RPL owner node and one RPL link, and all nodes have the same R-APS VLAN.

### Tangent rings

As shown in Figure 4, two rings in the network topology shares the same device; each ring has only one RPL owner node and only one RPL link. Different rings shall have different R-APS VLANs.

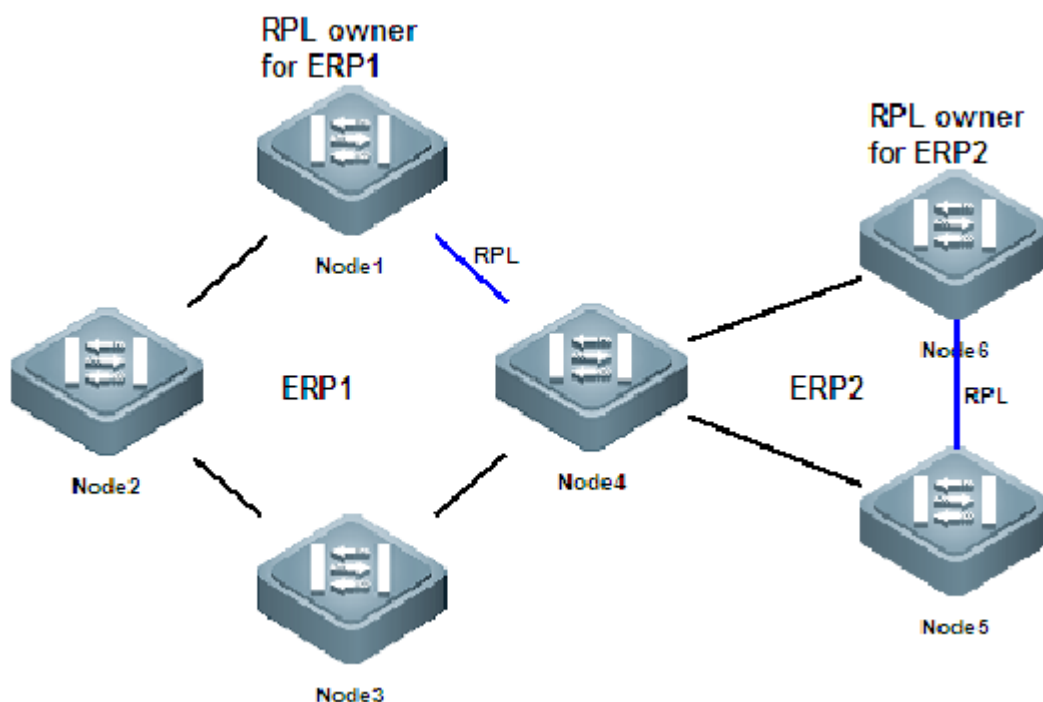


Fig 5 Topology diagram of tangent rings

### Intersecting rings

Apart from the tangent rings topology as shown in Figure 1, the topology structure of intersecting rings as shown in Figure 5 is also supported. Two or more rings share the same link (intersecting nodes must be connected directly with any other node); each ring has only one RPL owner node and only one RPL link. Different rings shall have different R-APS VLANs.

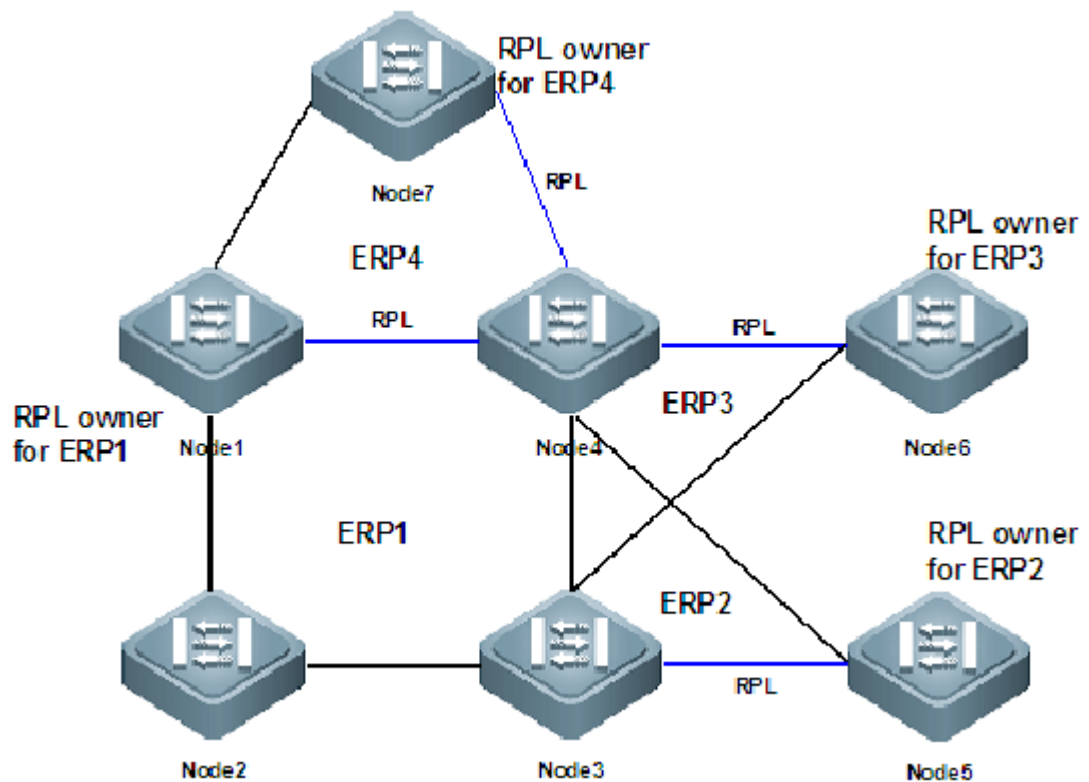


Fig 6 Topology diagram of multiple intersecting rings

**Note**

This protocol also supports more flexible topology. For example: one ring being tangent to multiple rings; each link on one ring carrying multiple sub-rings; one ring being tangent to multiple rings while also intersecting with multiple rings. These instances will not be shown one by one here.

## Protocol Apecification

Protocol specifications related to ERPS include:

ITU-T G.8032/Y.1344

ITU-T G.8032/Y.1344 Amendment 1

## Default Configurations

The following table describes the default configurations of ERPS.

Function	Default setting
R-APS VLAN	No R-APS VLAN is configured
ERP ring	No ERP ring is configured
RPL	No RPL is configured



Enable ERPS globally and on the specific ring	ERPS is not enabled globally or on the specific ring
Associate sub-ring with other Ethernet rings	Sub-ring is not associated with other Ethernet rings
Sub-ring topology change propagation	Sub-ring topology change propagation is not enabled
Timers	Holdoff time: 0 Guard time: 500 milliseconds WTR time: 2 minutes
Load balancing	Load balancing is not configured
Link state monitoring method	Monitor physical link state (up or down), not by OAM

## Configure the Basic Characteristics of ERPS

The following section describes how to configure the basic characteristics of ERPS:

As shown below:

(Required) Configure R-APS VLAN

(Required) Configure ERP ring

(Required) Configure RPL

(Optional) Enable ERPS

(Optional) Associate sub-ring with other Ethernet rings

(Optional) Enable sub-ring topology change propagation

(Optional) Configure timers

(Optional) Configure load balancing

(Optional) Configure link state monitoring method

Display ERPS configurations

### Configure R-APS VLAN

R-APS VLAN is used to transmit ERPS protocol packets. By default, no R-APS VLAN is configured. Enter privilege mode and execute the following steps to configure R-APS VLAN.

Command	Function
Ruijie# <b>configure terminal</b>	Enter global configuration mode
Ruijie(config)# <b>erps raps-vlan</b> <i>vlan-id</i>	Create R-APS VLAN and enter ERPS configuration mode. The vlan-id must be the used VLAN on the device.

To delete R-APS VLAN, execute "no erps raps-vlan vlan-id" command in the global configuration mode.

Configuration example:

# Enter privilege mode.

```
Ruijie# configure terminal
```

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

# Configure global R-APS VLAN.

```
Ruijie(config)# erps raps-vlan 4093
```



#### Note

- 1) R-APS VLAN must be the unused VLAN on the device. VLAN 1 cannot be configured as R-APS VLAN.
- 2) Different devices on the same Ethernet ring must be configured with the same R-APS VLAN.

## Configure ERP Ring

ERP ring configuration involves the configurations of Ethernet major-ring and Ethernet sub-ring, which will be detailed below:

By default, no Ethernet major-ring is configured. Enter privilege mode and execute the following steps to configure Ethernet major-ring.

Command	Function
Ruijie# <b>configure terminal</b>	Enter global configuration mode
Ruijie(config)# <b>interface</b> <i>interface-name1</i> Ruijie(config-if)# <b>switchport mode trunk</b> Ruijie(config-if)# <b>exit</b> Ruijie(config)# <b>interface</b> <i>interface-name2</i> Ruijie(config-if)# <b>switchport mode trunk</b> Ruijie(config-if)# <b>exit</b> Ruijie(config)# <b>erps raps-vlan</b> <i>vlan-id</i> Ruijie(config-erps)# <b>ring-port</b> <b>west</b> <i>interface-name1</i> <b>east</b> <i>interface-name2</i>	Configure Ethernet major-ring: 1) Configure the link mode and default VLAN of the port 2) Enter ERPS configuration mode 3) Specify the port of ERP ring in ERPS mode

To delete Ethernet major-ring, execute "no ring-port" command in the erps mode.

Configuration example:

# Enter privilege mode.

```
Ruijie# configure terminal
```

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

# Configure the link mode and default VLAN of the Ethernet ring port.

```
Ruijie(config)# interface fastEthernet 0/1
```

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

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

```
Ruijie(config)# interface fastEthernet 0/2
Ruijie(config-if)# switchport mode trunk
Ruijie(config-if)# exit
```

# Enter erps configuration mode.

```
Ruijie(config)# erps raps-vlan 4093
```

# Configure the port to join Ethernet ring and participate in ERPS protocol computation.

```
Ruijie(config-erps4093)# ring-port west fastEthernet 0/1 east fastEthernet 0/2
```

Ethernet sub-ring is generally configured only at the interconnection node of the intersecting rings. By default, no sub-ring is configured. Enter privilege mode and execute the following steps to configure Ethernet sub-ring.

Command	Function
Ruijie# <b>configure terminal</b>	Enter global configuration mode
Ruijie(config)# <b>interface</b> interface-name Ruijie(config-if)# <b>switchport mode trunk</b> Ruijie(config-if)# <b>exit</b> Ruijie(config)# <b>erps raps-vlan</b> vlan-id Ruijie(config-erps)# <b>ring-port west virtual-channel east</b> interface-name	At the interconnection node of the intersecting rings, the first option to configure sub-ring: 1) Configure the link mode and default VLAN of the port 2) Enter ERPS configuration mode 3) Specify the port of ERP ring in ERPS mode (west port is virtual-channel)
<b>Or:</b>	
Ruijie(config)# <b>interface</b> interface-name Ruijie(config-if)# <b>switchport mode trunk</b> Ruijie(config-if)# <b>exit</b> Ruijie(config)# <b>erps raps-vlan</b> vlan-id Ruijie(config-erps)# <b>ring-port west interface-name east virtual-channel</b>	At the interconnection node of the intersecting rings, the second option to configure sub-ring: 1) Configure the link mode and default VLAN of the port 2) Enter ERPS configuration mode 3) Specify the port of ERP ring in ERPS mode (east port is virtual-channel)

To delete Ethernet sub-ring, execute "no ring-port" command in the erps mode.

Configuration example:

# Enter privilege mode.

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

# Configure the link mode and default VLAN of the Ethernet ring port.

```
Ruijie(config)# interface fastEthernet 0/3
Ruijie(config-if)# switchport mode trunk
Ruijie(config-if)# exit
```

# Enter erps configuration mode.

```
Ruijie(config)# erps raps-vlan 100
```

# Configure the port to join Ethernet ring and participate in ERPS protocol computation.

```
Ruijie(config-erps100)# ring-port west fastEthernet 0/3 east virtual-channel
```



#### Caution

- 1) When the port joins the ERP ring, the trunk attribute of the port can no longer be changed.
- 2) After enabling the ERPS protocol of a particular ring, the ERP ring-port can no longer be changed.
- 3) If the ring-port is configured to virtual-channel, then this ring is considered as a sub-ring.
- 4) The port running ERPS won't participate in STP computation; ERPS will not share the same port with RERP and REUP.

## Configure RPL

By default, no RPL is configured. Enter privilege mode and execute the following steps to configure RPL.

Command	Function
Ruijie# <b>configure terminal</b>	Enter global configuration mode
Ruijie(config)# <b>erps raps-vlan</b> <i>vlan-id</i>	Enter ERPS configuration mode
Ruijie(config-erps)# <b>rpl-port</b> {west   east} [ <b>rpl-owner</b> ]	Configure RPL

To delete RPL, execute "no rpl-port" global configuration command in the erps mode.

Configuration example:

# Enter privilege mode.

```
Ruijie# configure terminal
```

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

# Configure the link mode and default VLAN of the Ethernet ring port.

```
Ruijie(config)# interface fastEthernet 0/1
```

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

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

```
Ruijie(config)# interface fastEthernet 0/2
```

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

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

# Enter erps configuration mode.

```
Ruijie(config)# erps raps-vlan 4093
```

# Configure the port to join Ethernet ring and participate in ERPS protocol computation.

```
Ruijie(config-erps4093)# ring-port west fastEthernet 0/1 east fastEthernet 0/2
```

# Specify the connected port and the RPL owner of RPL link

```
Ruijie(config-erps4093)# rpl-port west rpl-owner
```



#### Caution

- 1) Each ring needs and can only have one RPL link and one RPL owner node.
- 2) Before specifying RPL, the ERP ring must have been configured; after deleting ERP ring, RPL configurations will be deleted automatically.
- 3) After enabling ERPS protocol on the specific ring, the RPL configurations can no longer be changed.

## Enable ERPS

By default, ERPS is disabled globally and on the specific ring. Enter privilege mode and execute the following steps to enable ERPS globally and on the specific ring.

Command	Function
Ruijie# <b>configure terminal</b>	Enter global configuration mode
Ruijie(config)# <b>erps enable</b>	Enable ERPS globally
Ruijie(config)# <b>erps raps-vlan</b> <i>vlan-id</i>	Enter ERPS configuration mode
Ruijie(config-erps)# <b>state enable</b>	Enable ERPS on the specific ring

To disable ERPS, execute "no erps enable" command in the global configuration mode or execute "no state enable" command in the erps configuration mode.

Configuration example:

# Enter privilege mode.

```
Ruijie# configure terminal
```

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

# Configure the link mode and default VLAN of the Ethernet ring port.

```
Ruijie(config)# interface fastEthernet 0/1
```

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

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

```
Ruijie(config)# interface fastEthernet 0/2
```

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

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

# Enter erps configuration mode.

```
Ruijie(config)# erps raps-vlan 4093
```

# Configure the port to join Ethernet ring and participate in ERPS protocol computation.

```
Ruijie(config-erps4093)# ring-port west fastEthernet 0/1 east fastEthernet 0/2
```

# Enable ERPS on the specific ring

```
Ruijie(config-erps4093)# state enable
```

# Enable ERPS globally.

```
Ruijie(config-erps4093)# exit
```

```
Ruijie(config)# erps enable
```



#### Caution

- 1) Only after enabling ERPS protocol globally and on the specific ring, the ERPS protocol can then truly run on the specific ring.
- 2) A non-RPL owner node does not need to be configured with a RPL port. Please perform the configuration on the port connected with the RPL link if you want to configure a RPL port.

## Associate Ethernet Ring with its Sub-rings

By default, the Ethernet ring is not associated with its sub-rings. Enter privilege mode and execute the following steps to associate Ethernet ring with its sub-rings.

Command	Function
Ruijie# <b>configure terminal</b>	Enter global configuration mode
Ruijie(config)# <b>erps raps-vlan</b> <i>vlan-id</i>	Enter ERPS configuration mode of the Ethernet ring
Ruijie(config-erps)# <b>associate sub-ring raps-vlan</b> <i>vlan-list</i>	Configure to associate Ethernet ring with its sub-rings

To delete the association between sub-ring and other Ethernet rings, execute "**no associate sub-ring raps-vlan** *vlan-list*" command in erps configuration mode.

Configuration example:

# Enter privilege mode.

```
Ruijie# configure terminal
```

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

# Configure Ethernet major-ring.

```
Ruijie(config)# interface fastEthernet 0/1
```

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

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

```
Ruijie(config)# interface fastEthernet 0/2
```

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

```
Ruijie(config-if)# exit

Ruijie(config)# erps raps-vlan 4093

Ruijie(config-erps4093)# ring-port west fastEthernet 0/1 east fastEthernet 0/2
```

#### # Configure Ethernet sub-ring.

```
Ruijie(config)# erps raps-vlan 100

Ruijie(config)# interface fastEthernet 0/3

Ruijie(config-if)# switchport mode trunk

Ruijie(config-if)# exit

Ruijie(config)# erps raps-vlan 100

Ruijie(config-erps100)# ring-port west fastEthernet 0/3 east virtual-channel
```

#### # Associate sub-ring with other Ethernet rings.

```
Ruijie(config)# erps raps-vlan 4093

Ruijie(config-erps4093)# associate sub_ring raps-vlan 100
```



- 1) This command shall be configured at all nodes on the Ethernet ring, so that the ERPS protocol packets of the sub-ring can be transmitted on the Ethernet ring.
- 2) Association is aimed to transmit sub-ring protocol packets in other Ethernet rings; the user can accomplish this goal via other means (such as configuring the permit VLAN of the port). However, the user must guarantee that only the two ERPS ring ports can pass sub-ring protocol packets, which are discarded on other ports, or else packets of other VLANs may penetrate the R-APS VLAN of sub-ring and cause impacts to the ERPS ring.

## Enable Sub-ring Topology Change Propagation

After sub-ring topology change propagation is enabled at the interconnection node of intersecting rings, if sub-ring topology is changed and the link between interconnection nodes is failed or blocked, the interconnection nodes will send packets to node on other associated Ethernet rings to renew the topology.

By default, the sub-ring topology change propagation is not enabled. Enter privilege mode and execute the following steps to configure sub-ring topology change propagation.

Command	Function
Ruijie# <b>configure terminal</b>	Enter global configuration mode
Ruijie(config)# <b>erps raps-vlan vlan-id</b>	Enter ERPS configuration mode of the sub-ring

Ruijie(config-erps)# tc-propagation enable	sub-ring	Enable sub-ring topology change propagation
---	----------	---

To disable sub-ring topology change propagation, execute "**no sub-ring tc propagation**" command in the erps configuration mode.

Configuration example:

# Enter privilege mode.

```
Ruijie# configure terminal
```

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

# Configure Ethernet major-ring.

```
Ruijie(config)# interface fastEthernet 0/1
```

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

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

```
Ruijie(config)# interface fastEthernet 0/2
```

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

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

```
Ruijie(config)# erps raps-vlan 4093
```

```
Ruijie(config-erps4093)# ring-port west fastEthernet 0/1 east fastEthernet 0/2
```

# Configure Ethernet sub-ring.

```
Ruijie(config)# interface fastEthernet 0/3
```

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

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

```
Ruijie(config)# erps raps-vlan 100
```

```
Ruijie(config-erps100)# ring-port west fastEthernet 0/3 east virtual-channel
```

# Associate sub-ring with other Ethernet rings.

```
Ruijie(config-erps100)# sub-ring associate raps-vlan 4093
```

# Enable sub-ring topology change propagation.

```
Ruijie(config-erps100)# sub-ring tc-propagation enable
```



#### Caution

You only need to configure this command at the interconnection node of intersecting rings. When the sub-ring is deleted, these configurations will be deleted automatically.



## Configure Timers

The user can configure ERPS protocol timers on the device. Enter privilege mode and execute the following steps to configure protocol timers:

Command	Function
Ruijie# <b>configure terminal</b>	Enter global configuration mode
Ruijie(config)# <b>erps raps-vlan</b> <i>vlan-id</i>	Enter ERPS configuration mode
Ruijie(config-erps)# <b>timer</b> { <b>holdoff-time</b> <i>interval1</i>   <b>guard-time</b> <i>interval2</i>   <b>wtr-time</b> <i>interval3</i> }	Configure protocol timers: <b>Holdoff</b> timer: unit: 100ms; default: 0; scope: 0-100; <b>Guard</b> timer: unit: 10ms; default: 50; scope: 1-200; <b>WTR</b> timer: unit: minute; default: 5; scope: 5-12.

To restore to default values, execute "**no raps-vlan** *vlan-id* **timer { holdoff-time | guard-time | wtr-time }**" command in erps configuration mode.

Configuration example:

# Enter privilege mode.

```
Ruijie# configure terminal
```

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

# Enter erps configuration mode.

```
Ruijie(config)# erps raps-vlan 4093
```

# Configure ERPS protocol timers.

```
Ruijie(config-erps4093)# timer holdoff-time 10
```

```
Ruijie(config-erps4093)# timer guard-time 10
```

```
Ruijie(config-erps4093)# timer wtr-time 10
```



### Caution

After configuring holdoff timer, when link fault is detected, ERPS will not switch topology immediately. Instead, it will wait until the timer runs out and then implement topology switching after verifying that the link fault remains. Therefore, this timer will affect the topology convergence time during link failure.

## Configure Load Balancing

By default, the load balancing feature is not configured. Enter privilege mode and execute the following steps to configure load balancing:

Command	Function
Ruijie# <b>configure terminal</b>	Enter global configuration mode

Ruijie(config)# <b>spanning-tree mst configuration</b>	Enter MST configuration mode.
Ruijie(config-mst)# <b>instance</b> <i>instance-id</i> <b>vlan</b> <i>vlan-range</i> Ruijie(config-mst)# <b>exit</b>	Add VLAN group into a MST instance <i>instance-id</i> , scope: 0—64 <i>vlan-range</i> , scope: 1—4094 For example: instance 1 vlan 2-200: add vlans 2-200 into instance 1. instance 1 vlan 2,20,200: add vlan 2, vlan 20 and vlan 200 into instance 1. Meanwhile, you can also use “no” command to delete vlan from the instance; the deleted vlan will automatically get into instance 0.
Ruijie(config)# <b>erps raps-vlan</b> <i>vlan-id</i>	Enter ERPS configuration mode.
Ruijie(config-erps)# <b>protected-instance</b> <i>instance-id-list</i>	Configure protected VLANs of the Ethernet ring (the corresponding VLANs in instance-id-list are the protected VLANs, which are composed of R-APS VLAN of this Ethernet ring and the data VLANs to be protected)

To disable load balancing, execute "**no protected-instance**" command in the erps mode.

We will briefly introduce load balancing configuration by taking Node4 in Figure 3 as an example. Assuming that R-APS VLAN on ERP1 is 100 and the protected data VLANs are 1-99 and 101-2000, and assuming that R-APS VLAN on ERP2 is 4093 and the protected data VLANs are 2001-4092 and 4091, the load balancing configurations are then shown below:

# Enter privilege mode.

```
Ruijie# configure terminal
```

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

# Configure the protected VLANs on ERP1.

```
Ruijie(config)# spanning-tree mst configuration
```

```
Ruijie(config-mst)# instance 1 vlan 100, 1-99, 101-2000
```

```
Ruijie(config-mst)# exit
```

```
Ruijie(config)# erps raps-vlan 100
```

```
Ruijie(config-erps100)# protected-instance 1
```

# Configure the protected VLANs on ERP2.

```
Ruijie(config)# spanning-tree mst configuration
```

```
Ruijie(config-mst)# instance 2 vlan 4093, 2001-4092, 4094
```

```
Ruijie(config-mst)# exit

Ruijie(config)# erps raps-vlan 4093

Ruijie(config-erps4093)# protected-instance 2
```

**Caution**

Please add all VLANs to the VLANs protected by ERPS when configuring load balancing. Otherwise, the unprotected VLANs may cause network loops.

## Configure Link State Monitoring Method

In respect of link state configuration, we can directly monitor the physical state (up or down) of the link or monitor the logic state (unidirectional fault, bidirectional fault or normal) of the link via OAM (Operation, Administration and Maintenance; please refer to OAM configuration manual for details). By default, the physical state of the link will be monitored directly. Enter privilege mode and execute the following steps to switch the link state monitoring method:

Command	Function
Ruijie# <b>configure terminal</b>	Enter global configuration mode
Ruijie(config)# <b>erps monitor link-state by oam</b>	Configure link state monitoring method

To restore to the default setting, execute "**no erps monitor link-state by oam**" command in the global configuration mode.

Configuration example:

# Enter privilege mode.

```
Ruijie# configure terminal
```

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

# Configure link state monitoring method.

```
Ruijie(config)# erps monitor link-state by oam
```

**Caution**

- 1) The aforementioned configuration command will only enable ERPS to implement topology switching according to the result of OAM monitoring. To implement link state monitoring by OAM, OAM must be enabled as well. Please refer to OAM configuration manual for details.
- 2) When monitoring link state by OAM, since OAM is inefficient in link state monitoring, the convergence time may be longer in case of topology changes.

## Display ERPS Configurations

Execute the following command in privilege mode to display ERPS configuration and status:

Command	Function
Ruijie# <b>show erps</b>	Display ERPS configurations and status.

Execute "**show erps**" command to display ERPS configuration and status of the device:

```
Ruijie# show erps
ERPS Information
Global Status           : Enabled
Link monitored by       : Not Oam
-----
R-APS VLAN              : 4093
Ring Status             : Enabled
West Port               : Gi 0/5 (Blocking)
East Port               : Gi 0/7 (Forwarding)
RPL Port                : West Port
Protected VLANs         : ALL
RPL Owner               : Enabled
Holdoff Time            : 0 milliseconds
Guard Time              : 500 milliseconds
WTR Time                : 2 minutes
Current Ring State      : Idle
-----
R-APS VLAN              : 100
Ring Status             : Enabled
West Port               : Virtual Channel
East Port               : Gi 0/10 (Forwarding)
RPL Port                : None
Protected VLANs         : ALL
RPL Owner               : Disabled
Holdoff Time            : 0 milliseconds
Guard Time              : 500 milliseconds
WTR Time                : 2 minutes
Current Ring State      : Idle
-----
R-APS VLAN              : 200
Ring Status             : Enabled
West Port               : Virtual Channel
East Port               : 12 (Forwarding)
RPL Port                : None
Protected VLANs         : ALL
RPL Owner               : Disabled
Holdoff Time            : 0 milliseconds
Guard Time              : 500 milliseconds
WTR Time                : 2 minutes
Current Ring State      : Idle
```

```
Ruijie# show erps raps_vlan 4093 sub_ring
R-APS VLAN: 4093
Sub-Ring R-APS VLANs    TC Propagation State
-----
100                      Enable
200                      Enable
```

**Note**

The ring port state could be "Forwarding", "Blocking" or "Signal Fail":

- 1) Forwarding: can forward data traffic normally;
- 2) Blocking: do not forward data traffic (if load balancing is configured for RPL owner, then the RPL port will not forward only the data traffic of protected VLANs);
- 3) Signal Fail: failure of the link on this port.

## Typical ERPS Configuration Example

### Single Ring Configuration Example

#### Networking requirements

- Node1, Node2, Node3 and Node4 form a single ring topology;
- The R-APS VLAN of the ring is 4093;
- Node4 is the RPL owner node; the link between Node3 and Node4 is RPL.

#### Network topology

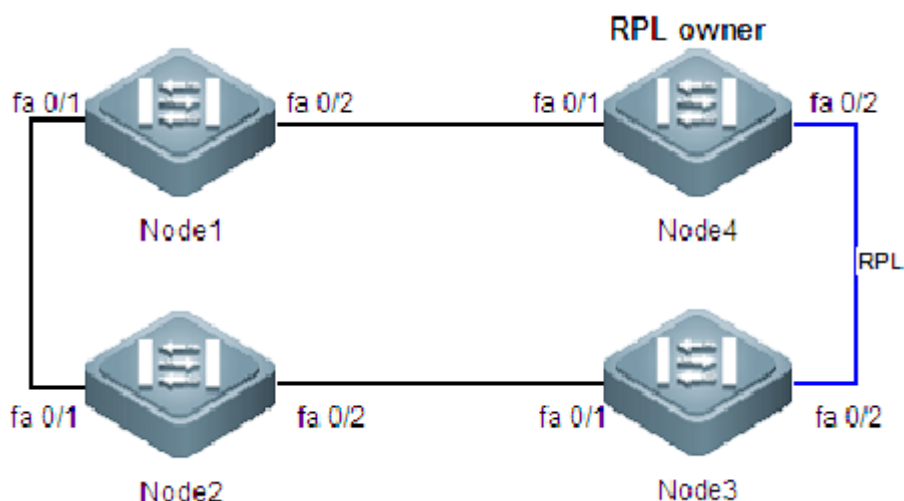


Fig 7 Single ring configuration example

## Configuration tips

You must and can configure only one RPL owner node and only one RPL, while all nodes must have the same R-APS VLAN.

## Configuration steps

### Configure Node1

# Enter privilege mode.

```
Ruijie# configure terminal
```

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

# Configure R-APS VLAN

```
Ruijie(config)# erps raps-vlan 4093
```

```
Ruijie(config-erps4093)# exit
```

# Configure the link mode of the Ethernet ring port.

```
Ruijie(config)# interface fastEthernet 0/1
```

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

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

```
Ruijie(config)# interface fastEthernet 0/2
```

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

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

# Enter erps configuration mode.

```
Ruijie(config)# erps raps-vlan 4093
```

# Configure the port to join Ethernet ring and participate in ERPS protocol computation.

```
Ruijie(config-erps4093)# ring-port west fastEthernet 0/1 east fastEthernet 0/2
```

# Enable ERPS on the specific ring.

```
Ruijie(config-erps4093)# state enable
```

# Enable ERPS globally.

```
Ruijie(config-erps4093)# exit
```

```
Ruijie(config)# erps enable
```

### Configure Node2

# The configurations of Node2 are the same as that of Node1.

### Configure Node3

# Apart from the commands used in Node1 configuration (excluding the command to enable ERPS on the specific ring), Node3 must be further configured with the following commands:

# Enter privilege mode.

```
Ruijie# configure terminal
```

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

# Enter erps configuration mode.

```
Ruijie(config)# erps raps-vlan 4093
```

# Specify the port that the RPL link is on.

```
Ruijie(config-erps4093)# rpl-port east
```

# Enable ERPS on the specific ring

```
Ruijie(config-erps4093)# state enable
```

## Configure Node4

# Apart from the commands used in Node1 configuration (excluding the command to enable ERPS on the specific ring), Node4 must be further configured with the following commands:

# Enter privilege mode.

```
Ruijie# configure terminal
```

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

# Enter erps configuration mode.

```
Ruijie(config)# erps raps-vlan 4093
```

# Specify the connected port and RPL owner of RPL link.

```
Ruijie(config-erps4093)# rpl-port east rpl-owner
```

# Enable ERPS on the specific ring

```
Ruijie(config-erps4093)# state enable
```

## Verification

# Execute "**show erps**" command at respective nodes to verify the configuration. Taking Node4 as an example:

```
Ruijie# show erps
ERPS Information
Global Status           : Enabled
Link monitored by       : Not Oam
-----
R-APS VLAN              : 4093
Ring Status             : Enabled
West Port               : Fa 0/1 (Forwardin)
East Port               : Fa 0/2 (Blocking)
RPL Port                : East Port
Protected VLANs         : ALL
RPL Owner               : Enabled
```

Holdoff Time	: 0 milliseconds
Guard Time	: 500 milliseconds
WTR Time	: 2 minutes
Current Ring State	: Idle

## Tangent Rings Configuration Example

### Networking requirements

- Node1, Node2, Node3 and Node4 form an Ethernet ring of ERP1, while Node3, Node5 and Node6 form another Ethernet ring of ERP2.
- The R-APS VLAN on ERP1 is 4093; the R-APS VLAN on ERP2 is 100.
- Node4 is the RPL owner node, and the link between Node3 and Node4 is the RPL of ERP1; Node 6 is the RPL owner node, and the link between Node5 and Node6 is the RPL of ERP2.

### Network topology

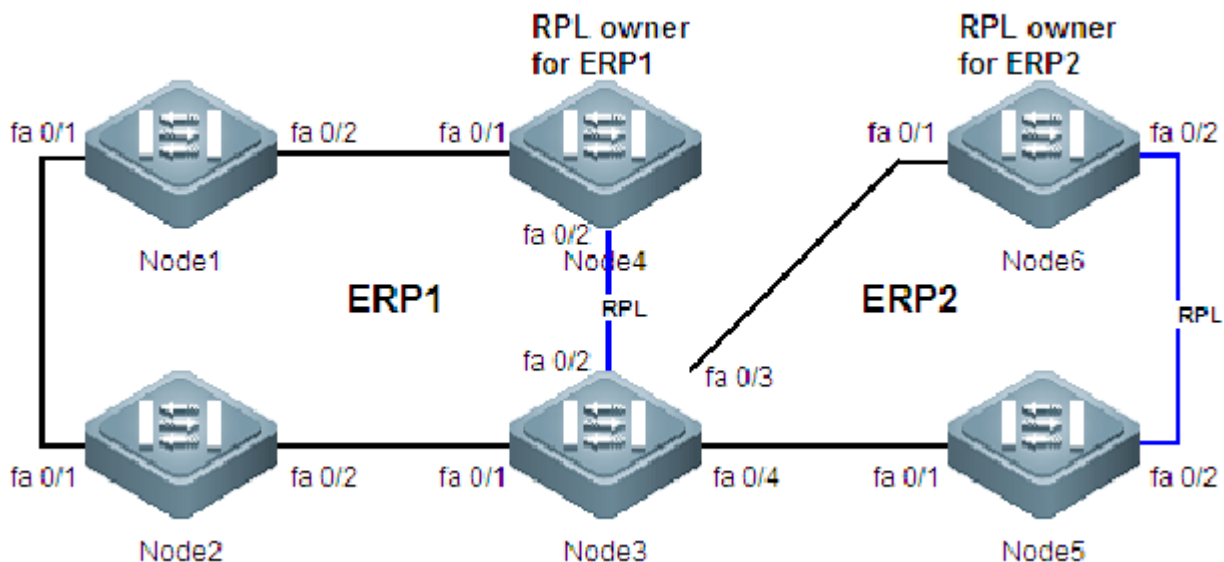


Fig 8 Tangent rings configuration example

### Configuration tips

You must and can configure only one RPL owner node and one RPL for ERP1 and ERP2 respectively; all nodes of ERP1 must have the same R-APS VLAN, and all nodes of ERP2 must have the same R-APS VLAN.

### Configuration steps

#### Configure Node1

# Enter privilege mode.

```
Ruijie# configure terminal
```

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



## # Configure R-APS VLAN

```
Ruijie(config)# erps raps-vlan 4093  
  
Ruijie(config-erps4093)# exit
```

## # Configure the link mode of the Ethernet ring port.

```
Ruijie(config)# interface fastEthernet 0/1  
  
Ruijie(config-if)# switchport mode trunk  
  
Ruijie(config-if)# exit  
  
Ruijie(config)# interface fastEthernet 0/2  
  
Ruijie(config-if)# switchport mode trunk  
  
Ruijie(config-if)# exit
```

## # Enter erps configuration mode.

```
Ruijie(config)# erps raps-vlan 4093
```

## # Configure the port to join Ethernet ring and participate in ERPS protocol computation.

```
Ruijie(config-erps4093)# ring-port west fastEthernet 0/1 east fastEthernet 0/2
```

## # Enable ERPS on the specific ring

```
Ruijie(config-erps4093)# state enable
```

## # Enable ERPS globally.

```
Ruijie(config-erps4093)# exit  
  
Ruijie(config)# erps enable
```

## Configure Node2

# The configurations of Node2 are the same as that of Node1.

## Configure Node3

# Apart from the commands used in Node1 configuration (excluding the command to enable ERPS on the specific ring), Node3 must be further configured with the following commands:

## # Enter privilege mode.

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

## # Enter erps configuration mode.

```
Ruijie(config)# erps raps-vlan 4093
```

## # Specify the port that the RPL link is on.

```
Ruijie(config-erps4093)# rpl-port east
```

## # Enable ERPS on the specific ring.

```
Ruijie(config-erps4093)# state enable
```

### # Configure R-APS VLAN for ERP2.

```
Ruijie(config-erps4093)# exit

Ruijie(config)# erps raps-vlan 100

Ruijie(config-erps100)# exit
```

### # Configure the link mode of ERP2 ring port.

```
Ruijie(config)# interface fastEthernet 0/3

Ruijie(config-if)# switchport mode trunk

Ruijie(config-if)# exit

Ruijie(config)# interface fastEthernet 0/4

Ruijie(config-if)# switchport mode trunk

Ruijie(config-if)# exit
```

### # Enter erps configuration mode.

```
Ruijie(config)# erps raps-vlan 100
```

### # Configure the port to join Ethernet ring and participate in ERPS protocol computation.

```
Ruijie(config-erps100)# ring-port west fastEthernet 0/3 east fastEthernet 0/4
```

### # Enable ERPS on ERP2.

```
Ruijie(config-erps100)# state enable
```

## Configure Node4

# Apart from the commands used in Node1 configuration (excluding the command to enable ERPS on the specific ring), Node4 must be further configured with the following commands:

### # Enter privilege mode.

```
Ruijie# configure terminal

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

### # Enter erps configuration mode.

```
Ruijie(config)# erps raps-vlan 4093
```

### # Specify the connected port and RPL owner of RPL link.

```
Ruijie(config-erps4093)# rpl-port east rpl-owner
```

### # Enable ERPS on the specific ring.

```
Ruijie(config-erps4093)# state enable
```

## Configure Node5

### # Enter privilege mode.

```
Ruijie# configure terminal
```

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

### # Configure R-APS VLAN

```
Ruijie(config)# erps raps-vlan 100

Ruijie(config-erps100)# exit
```

### # Configure the link mode of the Ethernet ring port.

```
Ruijie(config)# interface fastEthernet 0/1

Ruijie(config-if)# switchport mode trunk

Ruijie(config-if)# exit

Ruijie(config)# interface fastEthernet 0/2

Ruijie(config-if)# switchport mode trunk

Ruijie(config-if)# exit
```

### # Enter erps configuration mode.

```
Ruijie(config)# erps raps-vlan 100
```

### # Configure the port to join Ethernet ring and participate in ERPS protocol computation.

```
Ruijie(config-erps100)# ring-port west fastEthernet 0/1 east fastEthernet 0/2
```

### # Specify the port that the RPL link is on.

```
Ruijie(config-erps100)# rpl-port east
```

### # Enable ERPS on the specific ring.

```
Ruijie(config-erps100)# state enable
```

### # Enable ERPS globally.

```
Ruijie(config-erps100)# exit

Ruijie(config)# erps enable
```

## Configure Node6

# The configurations of Node6 are basically the same as that of Node5. You only need to change "rpl-port east" command into "rpl-port east rpl-owner".

## Verification

# Execute "**show erps**" command at respective nodes to verify the configuration. Taking Node3 as an example:

```
Ruijie# show erps

ERPS Information

Global Status                : Enabled
Link monitored by            : Not Oam
-----

R-APS VLAN                   : 100
Ring Status                  : Enabled
```

```

West Port          : Fa 0/3 (Forwarding)
East Port          : Fa 0/4 (Forwarding)
RPL Port           : None
Protected VLANs    : ALL
RPL Owner          : Disabled
Holdoff Time       : 0 milliseconds
Guard Time         : 500 milliseconds
WTR Time           : 2 minutes
Current Ring State : Idle

```

```

-----
R-APS VLAN         : 4093
Ring Status        : Enabled
West Port          : Fa 0/1 (Forwarding)
East Port          : Fa 0/2 (Forwarding)
RPL Port           : East Port
Protected VLANs    : ALL
RPL Owner          : Disabled
Holdoff Time       : 0 milliseconds
Guard Time         : 500 milliseconds
WTR Time           : 2 minutes
Current Ring State : Idle

```

## IntersectingRing Configuration Example

### Networking requirements

- Node1, Node2, Node3 and Node4 form the Ethernet major-ring of ERP1; Node3, Node5 and Node4 form the Ethernet sub-ring of ERP2; Node3, Node6 and Node4 form the Ethernet sub-ring of ERP3; Node1, Node4 and Node7 form the Ethernet sub-ring of ERP4.
- The R-APS VLAN on ERP1 is 4093; the R-APS VLAN on ERP2 is 100; the R-APS VLAN on ERP3 is 200; the R-APS VLAN on ERP4 is 300.
- Node4 is the RPL owner node, and the link between Node1 and Node4 is the RPL of ERP1; Node 5 is the RPL owner node, and the link between Node3 and Node5 is the RPL of ERP2; Node6 is the RPL owner node, and the link between Node4 and Node6 is the RPL of ERP1; Node7 is the RPL owner node, and the link between Node7 and Node1 is the RPL of ERP1.

## Network topology

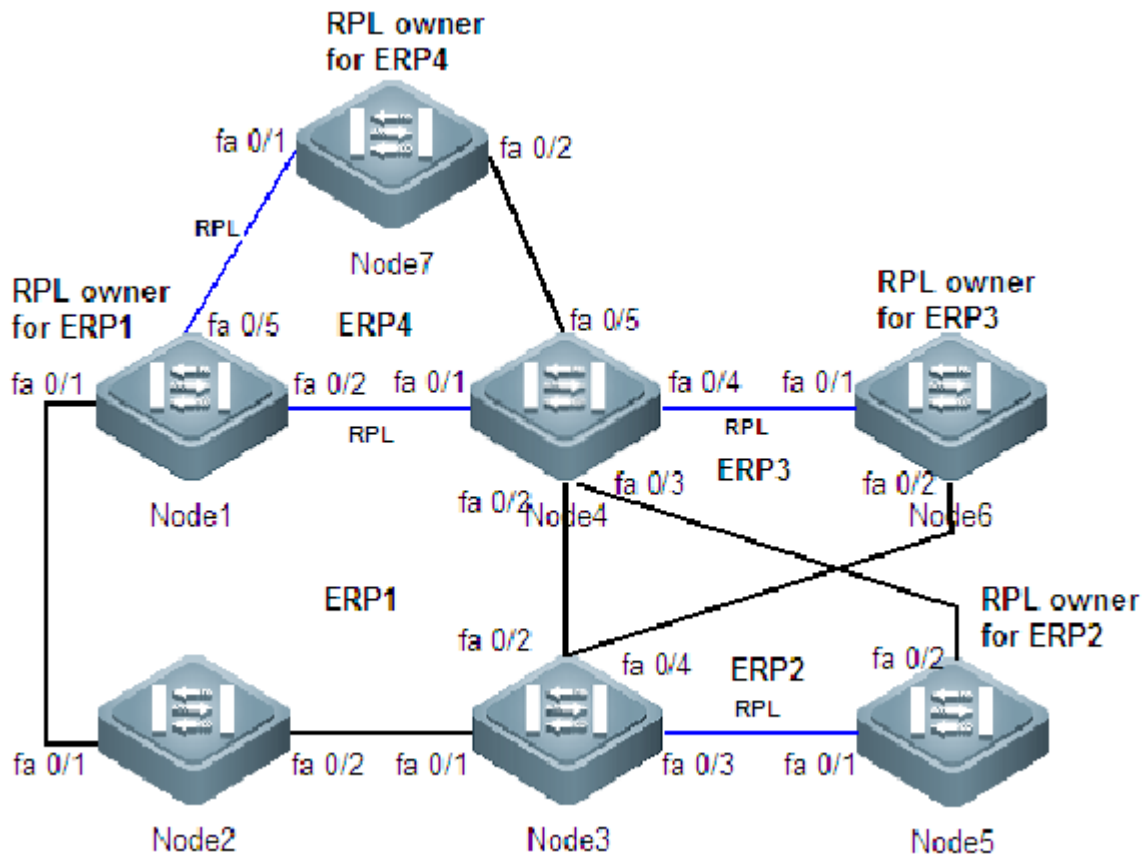


Fig 9 Intersecting rings configuration example

## Configuration tips

You must and can configure only one RPL owner node and one RPL for each ERP ring; all nodes of ERP1 must have the same R-APS VLAN; all nodes of ERP2 must have the same R-APS VLAN; all nodes of ERP3 must have the same R-APS VLAN; all nodes of ERP4 must have the same R-APS VLAN.

## Configuration steps

### Configure Node1

# Enter privilege mode.

```
Ruijie# configure terminal
```

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

# Configure R-APS VLAN to 4093

```
Ruijie(config)# erps raps-vlan 4093
```

```
Ruijie(config-erps4093)# exit
```

# Configure the link mode of the Ethernet ring port.

```
Ruijie(config)# interface fastEthernet 0/1
```

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

```
Ruijie(config-if)# exit

Ruijie(config)# interface fastEthernet 0/2

Ruijie(config-if)# switchport mode trunk

Ruijie(config-if)# exit
```

# Enter erps configuration mode.

```
Ruijie(config)# erps raps-vlan 4093
```

# Configure the port to join Ethernet ring and participate in ERPS protocol computation.

```
Ruijie(config-erps4093)# ring-port west fastEthernet 0/1 east fastEthernet 0/2
```

# Specify the connected port and RPL owner of RPL link.

```
Ruijie(config-erps4093)# rpl-port east rpl-owner
```

# Enable ERPS on the specific ring.

```
Ruijie(config-erps4093)# state enable
```

# Enable ERPS globally.

```
Ruijie(config-erps4093)# exit
```

```
Ruijie(config)# erps enable
```

# Configure R-APS VLAN for sub-ring ERP4.

```
Ruijie(config)# erps raps-vlan 300
```

```
Ruijie(config-erps300)# exit
```

# Configure the link mode of ERP4 ring port.

```
Ruijie(config)# interface fastEthernet 0/5

Ruijie(config-if)# switchport mode trunk

Ruijie(config-if)# exit
```

# Enter erps configuration mode.

```
Ruijie(config)# erps raps-vlan 300
```

# Configure the port to join Ethernet ring and participate in ERPS protocol computation.

```
Ruijie(config-erps300)# ring-port west fastEthernet 0/5 east virtual-channel
```

# Enable ERPS on ERP4.

```
Ruijie(config-erps300)# state enable
```

# Associate ERP1 with ERP4.

```
Ruijie(config-erps300)# exit

Ruijie(config)# erps raps-vlan 4093

Ruijie(config-erps4093)# associate sub-ring raps-vlan 300
```

## Configure Node2

# Enter privilege mode.

```
Ruijie# configure terminal
```

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

# Configure R-APS VLAN to 4093

```
Ruijie(config)# erps raps-vlan 4093
```

```
Ruijie(config-erps4093)# exit
```

# Configure the link mode of the Ethernet ring port.

```
Ruijie(config)# interface fastEthernet 0/1
```

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

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

```
Ruijie(config)# interface fastEthernet 0/2
```

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

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

# Enter erps configuration mode.

```
Ruijie(config)# erps raps-vlan 4093
```

# Configure the port to join Ethernet ring and participate in ERPS protocol computation.

```
Ruijie(config-erps4093)# ring-port west fastEthernet 0/1 east fastEthernet 0/2
```

# Enable ERPS on the specific ring.

```
Ruijie(config-erps4093)# state enable
```

# Enable ERPS globally.

```
Ruijie(config-erps4093)# exit
```

```
Ruijie(config)# erps enable
```

### Configure Node3

# Apart from the commands used in Node2 configuration, Node3 must be further configured with the following commands:

# Enter privilege mode.

```
Ruijie# configure terminal
```

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

# Configure R-APS VLAN for sub-ring ERP2.

```
Ruijie(config)# erps raps-vlan 100
```

```
Ruijie(config-erps100)# exit
```

# Configure the link mode of ERP2 ring port.

```
Ruijie(config)# interface fastEthernet 0/3
```

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

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

# Enter erps configuration mode.

```
Ruijie(config)# erps raps-vlan 100
```

# Configure the port to join Ethernet ring and participate in ERPS protocol computation.

```
Ruijie(config-erps100)# ring-port west virtual-channel east fastEthernet 0/3
```

# Enable ERPS on ERP2.

```
Ruijie(config-erps100)# state enable
```

# Configure R-APS VLAN for sub-ring ERP3.

```
Ruijie(config)# erps raps-vlan 200
```

```
Ruijie(config-erps200)# exit
```

# Configure the link mode of ERP2 ring port.

```
Ruijie(config)# interface fastEthernet 0/3
```

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

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

# Enter erps configuration mode.

```
Ruijie(config)# erps raps-vlan 200
```

# Configure the port to join Ethernet ring and participate in ERPS protocol computation.

```
Ruijie(config-erps200)# ring-port west virtual-channel east fastEthernet 0/3
```

# Enable ERPS on ERP2.

```
Ruijie(config-erps200)# state enable
```

# Associate major-ring ERP1 with sub-ring ERP2 and ERP3.

```
Ruijie(config-erps300)# exit
```

```
Ruijie(config)# erps raps-vlan 4093
```

```
Ruijie(config-erps4093)# associate sub-ring raps-vlan 100,200
```

## Configure Node4

# Apart from the commands used in Node2 configuration (excluding the command to enable ERPS on the specific ring), Node4 must be further configured with the following commands:

# Enter privilege mode.

```
Ruijie# configure terminal
```

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

# Enter erps configuration mode.

```
Ruijie(config)# erps raps-vlan 4093
```

# Specify the connected port and RPL owner of RPL link.

```
Ruijie(config-erps4093)# rpl-port west
```



# Enable ERPS on the specific ring.

```
Ruijie(config-erps4093)# state enable
```

# Configure R-APS VLAN for sub-ring ERP2.

```
Ruijie(config)# erps raps-vlan 100
```

```
Ruijie(config-erps100)# exit
```

# Configure the link mode of ERP2 ring port.

```
Ruijie(config)# interface fastEthernet 0/3
```

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

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

# Enter erps configuration mode.

```
Ruijie(config)# erps raps-vlan 100
```

# Configure the port to join Ethernet ring and participate in ERPS protocol computation.

```
Ruijie(config-erps100)# ring-port west virtual-channel east fastEthernet 0/3
```

# Enable ERPS on ERP2.

```
Ruijie(config-erps100)# state enable
```

# Configure R-APS VLAN for sub-ring ERP3.

```
Ruijie(config)# erps raps-vlan 200
```

```
Ruijie(config-erps200)# exit
```

# Configure the link mode of ERP2 ring port.

```
Ruijie(config)# interface fastEthernet 0/3
```

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

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

# Enter erps configuration mode.

```
Ruijie(config)# erps raps-vlan 200
```

# Configure the port to join Ethernet ring and participate in ERPS protocol computation.

```
Ruijie(config-erps200)# ring-port west virtual-channel east fastEthernet 0/3
```

# Enable ERPS on ERP2.

```
Ruijie(config-erps200)# state enable
```

# Configure R-APS VLAN for sub-ring ERP4.

```
Ruijie(config)# erps raps-vlan 300
```

```
Ruijie(config-erps300)# exit
```

# Configure the link mode of ERP2 ring port.

```
Ruijie(config)# interface fastEthernet 0/3
```

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

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

# Enter erps configuration mode.

```
Ruijie(config)# erps raps-vlan 300
```

# Configure the port to join Ethernet ring and participate in ERPS protocol computation.

```
Ruijie(config-erps300)# ring-port west virtual-channel east fastEthernet 0/5
```

# Enable ERPS on ERP2.

```
Ruijie(config-erps300)# state enable
```

# Associate major-ring ERP1 with sub-ring ERP2 and ERP3.

```
Ruijie(config-erps300)# exit
```

```
Ruijie(config)# erps raps-vlan 4093
```

```
Ruijie(config-erps4093)# associate sub-ring raps-vlan 100,200,300
```

## Configure Node5

# Enter privilege mode.

```
Ruijie# configure terminal
```

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

# Configure R-APS VLAN

```
Ruijie(config)# erps raps-vlan 100
```

```
Ruijie(config-erps100)# end
```

# Configure the link mode of the Ethernet ring port.

```
Ruijie(config)# interface fastEthernet 0/1
```

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

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

```
Ruijie(config)# interface fastEthernet 0/2
```

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

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

# Enter erps configuration mode.

```
Ruijie(config)# erps raps-vlan 100
```

# Configure the port to join Ethernet ring and participate in ERPS protocol computation.

```
Ruijie(config-erps100)# ring-port west fastEthernet 0/1 east fastEthernet 0/2
```

# Specify the connected port and RPL owner of RPL link.

```
Ruijie(config-erps100)# rpl-port east rpl-owner
```

# Enable ERPS on the specific ring.

```
Ruijie(config-erps100)# state enable
```

# Enable ERPS globally.

```
Ruijie(config-erps100)# exit
```

```
Ruijie(config)# erps enable
```

## Configure Node6

# The configurations of Node6 are basically the same as that of Node5. You only need to change "R-APS VLAN" into "VLAN 200".

## Configure Node7

# The configurations of Node7 are basically the same as that of Node5. You only need to change "R-APS VLAN" into "VLAN 300".

## Verification

# Execute "**show erps**" command at respective nodes to verify the configuration. Taking Node3 as an example:

```
Ruijie# show erps
ERPS Information
Global Status           : Enabled
Link monitored by       : Not Oam
-----
R-APS VLAN              : 100
Ring Status             : Enabled
West Port               : Virtual Channel
East Port               : Fa 0/3 (Forwarding)
RPL Port                : None
Protected VLANs         : ALL
RPL Owner                : Disabled
Holdoff Time            : 0 milliseconds
Guard Time              : 500 milliseconds
WTR Time                : 2 minutes
Current Ring State      : Idle
-----
R-APS VLAN              : 200
Ring Status             : Enabled
West Port               : Virtual Channel
East Port               : Fa 0/4 (Forwarding)
RPL Port                : None
Protected VLANs         : ALL
RPL Owner                : Disabled
Holdoff Time            : 0 milliseconds
Guard Time              : 500 milliseconds
WTR Time                : 2 minutes
```

```

Current Ring State      : Idle
-----
R-APS VLAN             : 4093
Ring Status            : Enabled
West Port              : Fa 0/1 (Forwarding)
East Port              : Fa 0/2 (Blocking)
RPL Port               : East Port
Protected VLANs        : ALL
RPL Owner              : Disabled
Holdoff Time           : 0 milliseconds
Guard Time             : 500 milliseconds
WTR Time               : 2 minutes
Current Ring State      : Idle

```

## Load Balancing Configuration Example

### Networking requirements

- Node1, Node2, Node3 and Node4 form the same physical topological ring. This physical topological ring corresponds with two Ethernet rings: ERP1 and ERP2.
- Node1 is the RPL owner of ERP1, and the link between Node1 and Node2 is the RPL link; Node3 is the RPL owner of ERP2, and the link between Node3 and Node4 is the RPL link.
- The R-APS VLAN on ERP1 is 100, and the protected data VLANs are 1-99 and 101-2000. The R-APS VLAN on ERP2 is 4093, and the protected data VLANs are 2001-4092 and 4094.

### Network topology

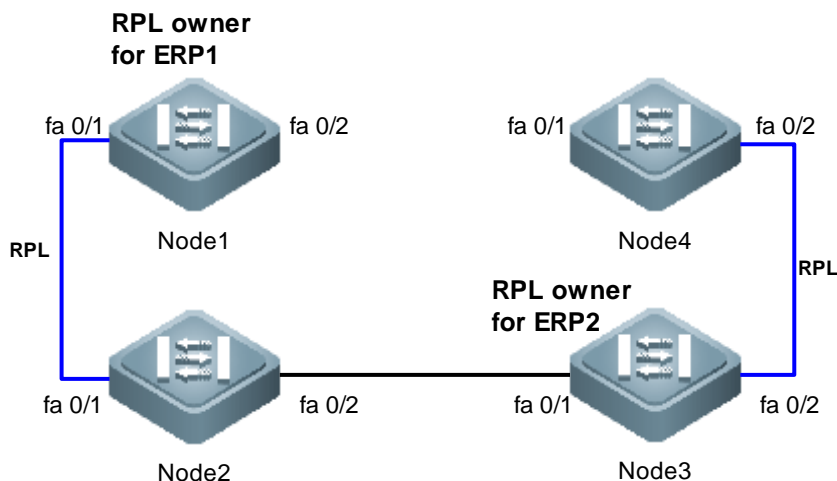


Fig 10 Load balancing configuration example

### Configuration tips

The protected VLANs of Ethernet ring are composed of R-APS VLAN of this Ethernet ring and the data VLANs to be protected.

## Configuration steps

### Configure Node1

# Enter privilege mode.

```
Ruijie# configure terminal
```

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

# Configure Ethernet ring ERP1:

# Configure the link mode of ERP1 ring port.

```
Ruijie(config)# interface fastEthernet 0/1
```

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

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

```
Ruijie(config)# interface fastEthernet 0/2
```

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

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

# Configure the port and RPL of ERP1.

```
Ruijie(config)# erps raps-vlan 100
```

```
Ruijie(config-erps100)# ring-port west fastEthernet 0/1 east fastEthernet 0/2
```

```
Ruijie(config-erps100)# rpl-port west rpl-owner
```

# Configure the protected VLANs on ERP1.

```
Ruijie(config-erps100)# exit
```

```
Ruijie(config)# spanning-tree mst configuration
```

```
Ruijie(config-mst)# instance 1 vlan 1-2000
```

```
Ruijie(config-mst)# exit
```

```
Ruijie(config)# erps raps-vlan 100
```

```
Ruijie(config-erps100)# protected-instance 1
```

# Configure ERP2:

# Configure the port to join ERP1 and participate in ERPS protocol computation.

```
Ruijie(config)# erps raps-vlan 4093
```

```
Ruijie(config-erps4093)# ring-port west fastEthernet 0/1 east fastEthernet 0/2
```

# Configure the protected VLANs on ERP1.

```
Ruijie(config-erps4093)# exit
```

```
Ruijie(config)# spanning-tree mst configuration
```

```
Ruijie(config-mst)# instance 2 vlan 2001-4094
```

```
Ruijie(config-mst)# exit
```

```
Ruijie(config)# erps raps-vlan 4093
```

```
Ruijie(config-erps4093)# protected-instance 2
```

# Enable ERPS on the specific ring and enable ERPS globally.

```
Ruijie(config-erps4093)# state enable
```

```
Ruijie(config-erps4093)# exit
```

```
Ruijie(config)# erps enable
```

## Configure Node2

# Except for RPL configuration command, other configurations of Node2 are the same as that of Node1.

# Configure the RPL of ERP1 at Node2:

```
Ruijie(config)# erps raps-vlan 100
```

```
Ruijie(config-erps100)# rpl-port west
```

## Configure Node3

# Except for RPL configuration command, other configurations of Node3 are the same as that of Node1.

# At Node3, we don't configure the RPL of ERP1; instead, we configure the RPL of ERP2.

```
Ruijie(config)# erps raps-vlan 4093
```

```
Ruijie(config-erps4093)# rpl-port east rpl-owner
```

## Configure Node4

# Except for RPL configuration command, other configurations of Node4 are the same as that of Node3.

# Configure the RPL of ERP2 at Node4:

```
Ruijie(config)# erps raps-vlan 100
```

```
Ruijie(config-erps100)# rpl-port east
```

## Verification

# Execute "**show erps**" command at respective nodes to verify the configuration. Taking Node1 as an example:

```
Ruijie# show erps
ERPS Information
Global Status           : Enabled
Link monitored by       : Not Oam
-----
R-APS VLAN              : 200
Ring Status             : Enabled
West Port               : Gi 0/1 (Blocking)
East Port               : Gi 0/2 (Forwarding)
RPL Port                : West Port
Protected VLANs         : 1-2000
RPL Owner               : Enabled
```

```

Holdoff Time           : 0 milliseconds
Guard Time             : 500 milliseconds
WTR Time               : 2 minutes
Current Ring State     : Idle
-----
R-APS VLAN             : 4093
Ring Status            : Enabled
West Port              : Gi 0/1 (Forwarding)
East Port              : Gi 0/2 (Blocking)
RPL Port               : West Port
Protected VLANs        : 2001-4094
RPL Owner              : Enabled
Holdoff Time           : 0 milliseconds
Guard Time             : 500 milliseconds
WTR Time               : 2 minutes
Current Ring State     : Idle

```

## ERPS Configuration Modification Example

### Networking requirements

- The R-APS Vlan of the ring is changed to 4094 from 4093.
- Node 1 requires changes to the topology. Fa 0/2 is changed to fa 0/3 (or AP port Ag 1 should be changed to Ag 2). The configuration is modifies as well.
- Node 4 requires changes to the WTR time (or other timer time).

### Network topology

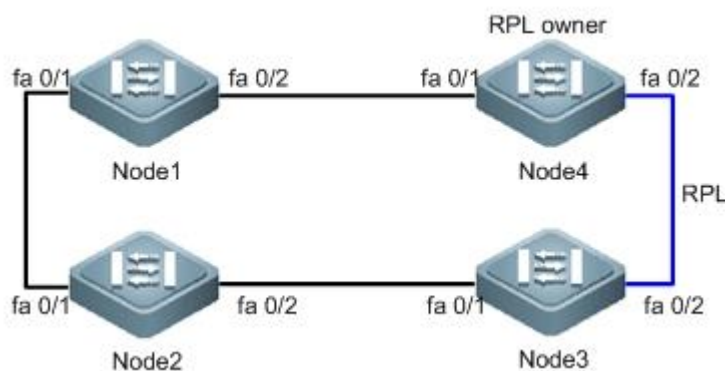


Fig 19 Configuration modification example

### Configuration steps

2) Change the R-APS VLAN from 4093 to 4094.

#### ■ Configure Node 1

# Enter privilege mode

```
Ruijie# configure terminal
```

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

**# Enter interface mode. Shutdown a link on the ring to avoid the loop.**

```
Ruijie(config)# interface fastEthernet 0/1
```

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

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

**# Delete the R-APS VLAN.**

```
Ruijie(config)# no erps raps-vlan 4093
```

#### ■ Configure Node 2

**# Enter privilege mode**

```
Ruijie# configure terminal
```

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

**# Delete the R-APS VLAN**

```
Ruijie(config)# no erps raps-vlan 4093
```

#### ■ Configure Node 3

**# The configuration is the same as that of Node 2.**

#### ■ Configure Node 4

**# The configuration is the same as that of Node 2.**

#### ■ Configure Node 1, Node 2, Node 3 and Node 4

**# The configuration is the same as the single ring configuration example.**

#### ■ Configure Node 1

**# Enter interface mode. Resume the port that was shutdown.**

```
Ruijie(config)# interface fastEthernet 0/1
```

```
Ruijie(config-if)# no shutdown
```

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

3) Node 1 requires changes to the topology, Change Fa 0/2 to fa 0/3 (or change AP port Ag1 to Ag2 ) and modify the configuration.

#### ■ Configure Node 4

**# Enter privilege mode.**

```
Ruijie# configure terminal
```

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

**# Enter interface mode. Shutdown fastEthernet 0/1.**

```
Ruijie(config)# interface fastEthernet 0/1
```

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

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

#### ■ Configure Node 1

**# Enter privilege mode.**

```
Ruijie# configure terminal
```

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

**# Enter ERPS configuration mode.**



```
Ruijie(config)# erps raps-vlan 4093
```

# Disable the ERPS function of the ring.

```
Ruijie(config-erps4093)# no state enable
```

# Delete the ring configuration.

```
Ruijie(config-erps4093)# no ring-port
```

# Reconfigure the port involved in the ERPS protocol.

```
Ruijie(config-erps4093)# ring-port west fastEthernet 0/1 east fastEthernet 0/3
```

# Enable the RRPS function of the ring.

```
Ruijie(config-erps4093)# state enable
```

#### ■ Configure Node 4

# Enter interface mode. Resume port fastEthernet 0/1.

```
Ruijie(config)# interface fastEthernet 0/1
```

```
Ruijie(config-if)# no shutdown
```

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

4) Node 4 requires changes to the time of the WTR timer ( or other timers).

#### ■ Configure Node 1

# Enter privilege mode.

```
Ruijie# configure terminal
```

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

# Enter ERPS configuration mode and change the time.

```
Ruijie(config)# erps raps-vlan 4093
```

```
Ruijie(config-erps4093)# timer holdoff-time 10
```



#### Caution

Please shutdown an ERPS port on the ring when modifying the ERPS configuration to avoid loop. After the modification is complete, change the port status to no shutdown. If you want to change ERPS time only, refer to step 3 for modification.

---

## Verification

# Run the **show erps** command on each node and confirm the configuration, Take Node 4 as an example:

```
Ruijie# show erps

ERPS Information

Global Status                : Enabled

Link monitored by            : Not Oam

-----

R-APS VLAN                   : 4094

Ring Status                  : Enabled

West Port                    : Fa 0/1 (Forwardin)
```

Configuration Guide

---

East Port	: Fa 0/3 (Blocking)
RPL Port	: East Port
Protected VLANs	: ALL
RPL Owner	: Enabled
Holdoff Time	: 0 milliseconds
Guard Time	: 500 milliseconds
WTR Time	: 10 minutes
Current Ring State	: Idle

# IP Address and Application Configuration

---

1. IP Address and Service Configuration
2. IPv6 Configuration
3. DHCP Configuration
4. DHCPv6 Configuration
5. DNS Configuration
6. FTP Client Configuration
7. FTP Server Configuration
8. Network Communication Detection Tools Configuration
9. TCP Configuration Configuration
10. IPv4 Express Forwarding Configuration

# IP Address and Service Configuration

## IP Address Configuration

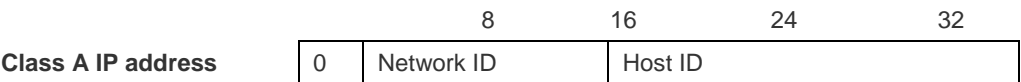
### IP Address Overview

IP address is made up of 32 binary bits and expressed in the dotted decimal format for the convenience of writing and description. In the dotted decimal format, the 32 binary bits are broken into four octets (1 octet equals to 8 bits). Each octet is separated by a period (dot) in the range from 0 to 255. For example, 192.168.1.1 is an IP address in the dotted decimal format.

An IP address is an address that IP protocols use to connect one another. A 32-bit IP address consists of two parts: network address and local address. According to the first several bits of the network address of an IP address, an IP address is divided into four categories.

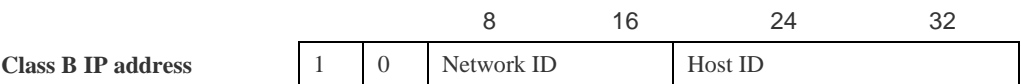
Class A: Total of 128 class-A IP addresses. The highest bit is 0 followed by seven bits identifying Network ID, and the remaining 24 bits identify Host ID.

Figure 1



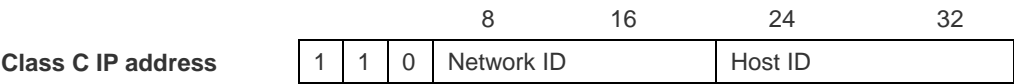
Class B: Total of 16,384 class B IP addresses. The highest two bits are 10 followed by 14 bits identifying Network ID, and the remaining 16 bits identify Host ID.

Figure 1



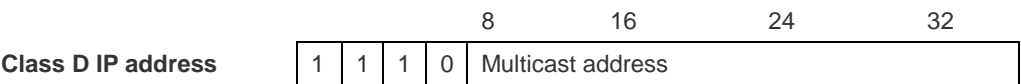
Class C: Totaol of 2,097,152 class C IP addresses. The highest three bits are 110 followed by 21 bits identifying Network ID, and the remaining eight addresses identify Host ID.

Figure 1



Class D: The highest four bits are 1110 and other bits are multicast IP address..

Figure 1



Note

An IP address whose highest four bits are 1111 is prohibited. This type of IP address, also called Class E IP address, is reserved.

When you build up a network, you should execute IP addressing according to the real network environment. To make the network connect to the Internet, you need apply for IP addresses from a central authority, for example, the China Internet Network Information Center (CNNIC) in China. It is the Internet Corporation for Assigned Names and Numbers (ICANN) that is responsible for IP address allocation. However, a private network does not require the application of IP addresses. It is recommended to assign private IP addresses for them.

The following table lists those reserved and available addresses by class.

Class	Address Range	Status
Class A	0.0.0.0	Reserved
	1.0.0.0 to 126.0.0.0	Available
	127.0.0.0	Reserved
Class B	128.0.0.0 to 191.254.0.0	Available
	191.255.0.0	Reserved
Class C	192.0.0.0	Reserved
	192.0.1.0 to 223.255.254.0	Available
	223.255.255.0	Reserved
Class D	224.0.0.0 to 239.255.255.255	Multicast
Class E	240.0.0.0 to 255.255.255.254	Reserved
	255.255.255.255	Broadcast

There are three blocks of IP addresses reserved for private networks that are not used in the Internet. Address translation is required for a private network using one of these IP addresses to access the Internet. The following table details these addresses, which are defined in RFC 1918.

Class	IP Address Range	Network Numbers
Class A	10.0.0.0 to 10.255.255.255	1
Class B	172.16.0.0 to 172.31.255.255	16
Class C	192.168.0.0 to 192.168.255.255	256

For the information on the assignment of IP address, TCP/UDP port and other codes, please refer to RFC 1166.

## IP Address Configuration Task List

The IP address configuration task list includes the following tasks, only the first one is required, others are optional depending on your network requirements.

- Assigning IP Addresses to Network Interfaces (Required)
- Configuring Address Resolution Protocol (ARP) (Optional)
- Configuring IP address to WAN Address Translation (Optional)
- Disabling IP Routing (Optional)
- Handling Broadcast Packets (Optional)

## Assigning IP Addresses to Network Interfaces

Only a host has an IP address configured can it receive and send IP packets. If an interface is configured with an IP address, this means that the interface supports running the IP protocol.

To assign an IP address to an interface, execute the following commands in the interface configuration mode:

Command	Function
Ruijie(config-if)# <b>ip address</b> <i>ip-address mask</i>	Assign an IP address for the interface.
Ruijie(config-if)# <b>no ip address</b>	Remove the IP address configuration for the interface.

A 32-bit mask identifies the network part of an IP address. In a mask, the IP address bit corresponding to 1 represents network ID and the IP address bit corresponding to 0 represents host ID. For example, the mask corresponding a Class A IP address is 255.0.0.0. You can partition a network into multiple segments with a mask. The goal of network partition is to use some bits of the host address of an IP address as the network address to reduce hosts and increase networks. At this point, the mask is called subnet mask.

**Note**

Theoretically, any bit of the host address of an IP address can be used as the subnet mask.



Ruijie product only supports continuous subnet masks from left to right starting from the network ID.

## Assigning multiple IP addresses to an interface

Ruijie product supports assigning multiple IP addresses for an interface with one being the primary IP address and others being the secondary addresses. Theoretically, you can configure secondary addresses up your mind. A secondary IP address can reside in the same or different network with the primary IP address. The secondary IP address will be used frequently during the building of a network, for example, in the following cases:

- There may not enough host addresses for a network. For example, a LAN requires a Class C IP address to support up to 254 hosts. However, when there are more than 254 hosts in the LAN, another Class C IP address is necessary. Therefore, a host needs to connect two networks and thus needs configuring multiple IP addresses.
- Many older networks were built based on layer 2 bridges without partition. The use of secondary IP addresses makes them easy to upgrade to IP-based routing networks. An IP address is assigned for every device in a subnet.
- Two subnets of a network might otherwise be separated by another network. By creating a subnet in each separated subnets, you can connect the two separated subnets together by assigning secondary IP addresses. One subnet cannot appear on two or more interfaces in a device.

**Caution**

Before configuring a secondary IP addresses, you need to confirm that the primary IP address has been configured. If a secondary IP address is configured on one device of the network, you need to configure the secondary IP addresses for other devices of the network. If IP addresses are not assigned to other devices at first, configure the secondary IP address as the main IP address for other devices. All the devices in a network should have the same secondary IP address. If you assign a secondary IP address to a device but do not assign IP addresses for other devices, you can set it to the primary IP address for them.

To assign a secondary IP address to an interface, execute the following command in the interface configuration mode:

Command	Function
Ruijie(config-if)# <b>ip address</b> <i>ip-address mask secondary</i>	Assign a secondary IP address to the interface.
Ruijie(config-if)# <b>no ip address</b> <i>ip-address mask secondary</i>	Remove the secondary IP address configuration for the interface.

### Configuring management IP and gateway

The Ruijie layer-2 switches allow you to configure management IP and gateway in the same command. Generally, the layer-2 switches provide "**ip default-gateway**" command to configure a default gateway. Sometimes, the layer-2 switch is subject to remote management via telnet, and the management IP and default gateway of the layer-2 switch must be modified. In such a case, configuring either **IP address** or **IP default-gateway** will prevent you from configuring another command (as the configuration has changed and this device can no longer be accessed via network). Therefore, we can use the **gateway** keyword of **IP address** command to modify the management IP and default gateway. To configure management IP and gateway at the same time, execute the following commands in interface configuration mode:

Command	Function
Ruijie(config-if)# <b>ip address</b> <i>ip-address mask gateway ip-address</i>	Configure management IP and gateway.
Ruijie(config-if)# <b>no ip address</b> <i>ip-address mask gateway</i>	Remove management IP and gateway configuration.

### Configuring Address Resolution Protocol (ARP)

Every device in a LAN has two addresses: local address and network address. Local address is contained in the header of the frames on the data link layer. Disputably, the correct term is data link layer address. Since this local address is handled in the MAC sub-layer of the data link layer, it is normally called MAC address representing an IP network device in a network. Network address represents a device in the Internet and indicates the network to which the device belongs.

For inter-communication, a device in a LAN must know the 48-bit MAC address of another device. The ARP can resolve the MAC address upon an IP address and the reversed ARP (RARP) can resolve the IP address upon a MAC address. You can resolve the MAC address in two ways: ARP and Proxy ARP. For the information on ARP, Proxy ARP and RARP, refer to RFC 826, RFC 1027, and RFC 903.

ARP binds the IP and MAC Address. It can resolve the MAC address upon an IP address. Then, the relationship between the IP address and the MAC address is stored in the ARP cache. With the MAC address, a device can encapsulate the frames of the data link layer and send them to the LAN in the Ethernet II-type by default. However the frames can also be encapsulated into other types of Ethernet frame (for example, SNAP).

The principle of RARP is similar to ARP. RARP resolves the IP address upon a MAC address. RARP is configured on non-disk workstation in general.

Normally, a device can work without any special address resolution configuration. Ruijie product can manage address resolution by.

## Configuring ARP Statically

The ARP offers dynamic IP address to MAC address mapping. It is not necessary to configure ARP statically in most cases. By configuring ARP Sstatically, Ruijie product can respond to the ARP request from other IP addresses.

To configure static ARP, execute the following command in the global configuration mode:

Command	Function
Ruijie(config)# <b>arp</b> <i>ip-address mac-address arp-type</i>	Define static ARP. Only arpa type is supported for arp-type.
Ruijie(config)# <b>no arp</b> <i>ip-address</i>	Remove static ARP

## Setting ARP Encapsulations

So far Ruijie products only support Ethernet II type ARP encapsulations, also known as ARPA keyword.

## ARP Timeout Setting

ARP timeout takes effect for only the dynamically learned IP address to MAC address mapping. The shorter the timeout, the truer the mapping table saved in the ARP cache is , but the more network bandwidth the ARP occupies. Hence the advantages and disadvantages should be weighted. Generally it is not necessary to configure the ARP timeout time unless there is a special requirement.

To configure ARP timeout time, execute the following command in the interface configuration mode:

Command	Function
Ruijie(config-if)# <b>arp timeout</b> <i>seconds</i>	Configure the ARP timeout time in the range from 0 to 2147483, with 0 not being aged.
Ruijie(config-if)# <b>no arp timeout</b>	Remove the configuration.

By default, timeout time is 3600 seconds, that is, 1 hour.

## Disabling IP Routing

IP routing feature is enabled by default. Do not execute this command unless you sure that IP routing is not needed. Disabling IP routing will make the equipment lose all the routes and the route forwarding function.

To disable IP routing, execute the following commands in the global configuration mode:

Command	Function
Ruijie(config)# <b>no ip routing</b>	Disable IP routing.
Ruijie(config)# <b>ip routing</b>	Enable IP routing

## Handling Broadcast Packets

A broadcast packet is destined for all hosts in a physical network. Ruijie product supports two kinds of broadcast packets: directed broadcast and flooding. A directed broadcast packet is sent to all the hosts in a specific network that the host IDs of their IP addresses are all set to 1. While a flooding broadcast packet is sent to all the hosts whose IP addresses are all



set to 1. Broadcast packets are heavily used by some protocols, including the Internet protocol. Therefore, it is the basic responsibility for a network administrator to manage and control broadcast packets.

Forwarding flooding broadcast packets may make the network overburden and thus influencing network operation. This is known as broadcast storm. There are some ways to suppress and restrict broadcast storm in the local network. However, layer 2 network devices like bridges and switches will forward and propagate broadcast storm.

The best solution to solve the broadcast storm problem is to specify a broadcast address for each network, that is, directed broadcast. This requires the IP protocol to use directed broadcast instead of flooding broadcast if possible.

For detailed description about broadcast, refer to RFC 919 and RFC 922.

## Establishing an IP Broadcast Address

Currently, the most popular way is the destination address consisting of all 1s (255.255.255.255). Ruijie product can be configured to generate any form of IP broadcast address and receive any form of IP broadcast packets.

To set a broadcast IP address other than 255.255.255.255, execute the following command in the interface configuration mode:

Command	Function
Ruijie(config-if)# <b>ip broadcast-address</b> <i>ip-address</i>	Create a broadcast address.
Ruijie(config-if)# <b>no ip broadcast-address</b>	Remove the configuration.

## Enabling Directed Broadcast-to-Physical Broadcast Translation

A directed broadcast IP packet is the one destined to the broadcast address of an IP subnet. For instance, the packet destined to 172.16.16.255 is a directed broadcast packet. However, the node that generates this packet is not a member of the destination subnet.

Upon the receipt of directed broadcast IP packets, the device indirectly connecting the destination subnet will forward the packets in the same way as forwarding unicast packets. After the directed broadcast IP packets arrive the device directly connecting the subnet, the device transforms them into flooding broadcast IP packets (whose destination address is all 1s in general), and then send them to all the hosts within the subnet by means of broadcast on the link layer.

Enabling directed broadcast to physical broadcast translation on an interface allows the interface to forward the directed broadcast IP packets to the directly connected network. This command will only affect the transmission of the directed broadcast IP packets to the final destination subnet, not other directed broadcasts.

You can forward directed broadcast IP packets as required on an interface by defining ACLs. Only those IP packets matching the ACLs are translated from directed broadcasts to physical broadcasts.

To configure the directed broadcast-to-physical broadcast translation, execute the following command in the interface configuration mode:

Command	Function
Ruijie(config-if)# <b>ip directed-broadcast</b> [ <i>access-list-number</i> ]	Enable directed broadcast to physical broadcast translation on the interface.
Ruijie(config-if)# <b>no ip directed-broadcast</b>	Disable the translation.

## Monitoring and Maintaining IP Address

### Clearing Caches and Table Contents

You can remove all contents of a particular cache, table, or database, including: 1) Clearing ARP cache;

- Clearing the hostname;
- IP address mapping table;
- Clearing the routing tables.

Command	Function
Ruijie# <b>clear arp-cache</b>	Clear the ARP cache.
Ruijie# <b>clear ip route</b> {network [mask]   *}	Clear the routing table.

### Displaying System and Network Status

You can show the contents of the IP routing table, cache, and database. Such information is very helpful in troubleshooting the network. You also can display information about reachability of local network and discover the routing path that the packets of your device are taking through the network.

To display system and network status, execute the following commands in the privileged EXEC mode :

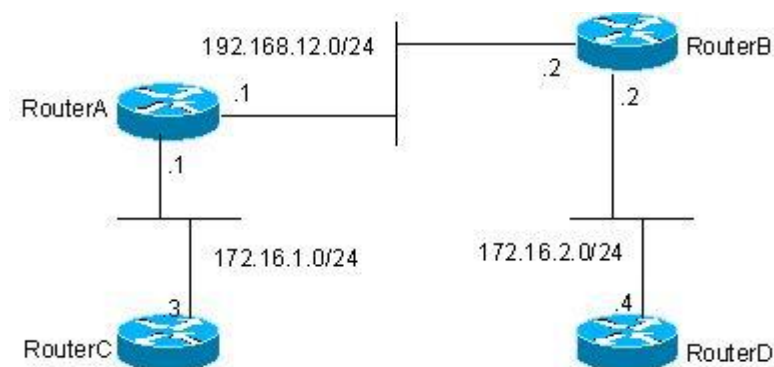
Command	Function
Ruijie# <b>show arp</b>	Show the ARP table.
Ruijie# <b>show ip arp</b>	Show the IP ARP table.
Ruijie# <b>show ip interface</b> [interface-type interface-number]	Show the interface information.
Ruijie# <b>show ip route</b> [network [mask] ]	Show the routing table.
Ruijie# <b>show ip route</b>	Show the brief information of the routing table.
Ruijie# <b>ping</b> ip-address [length bytes] [ntimes times] [timeout seconds]	Test network reachability.

## IP Address Configuration Examples

### Configuration requirements:

The following figure shows IP address assignment and network device connections.

Figure 1-5 Examples of configuring secondary IP addresses.



Configure RIPv1. You can see the routes of 172.16.2.0/24 on router C and the routes of 172.16.1.0/24 on router D.

## Configuration of the Routers:

RIPv1 does not support classless-based routes. This means masks are not carried with routing advertisement. 172.16.1.0/24 and 172.16.2.0/24 that belong to the same network are separated by the Class C network 192.168.12.0/24. Generally, router C and router D cannot route from each other. According to one feature of RIP, the mask of the route to be received should be set to the same value as that of the interface network if the route and the interface network belong to the same network. By configuring routers A and B, you can build a secondary network 172.16.3.0/24 on the network 192.168.12.0/24 to link the two separated subnets. The following presents a configuration description of routers A and B.

Router A:

```
interface FastEthernet 0/0
ip address 172.16.3.1 255.255.255.0 secondary
ip address 192.168.12.1 255.255.255.0
!
interface FastEthernet 0/1
ip address 172.16.1.1 255.255.255.0
!
router rip
network 172.16.0.0
network 192.168.12.0
```

Router B:

```
interface FastEthernet 0/0
ip address 172.16.3.2 255.255.255.0 secondary
ip address 192.168.12.2 255.255.255.0
!
interface FastEthernet 0/1
ip address 172.16.2.1 255.255.255.0
!
router rip
network 172.16.0.0
network 192.168.12.0
```

## IP Service Configuration

### Configuring the Default Gateway



Run the command only on L2 devices.

If no destination IP address to which the packets will be sent is specified, those packets will be sent to the default gateway by default. Use the **show ip redirects** command to view the settings.

To set the default gateway, execute the following command in the global configuration mode. Use the **no** form of this command to remove the default gateway:

Command	Function
<b>ip default-gateway</b> <i>ip-address</i>	Disable the ICMP protocol unreachable and host

Command	Function
	unreachable messages.

To view the configured default gateway, execute the following command:

Command	Function
<b>show ip redirects</b>	Display the default gateway.

## Managing IP Connections

The IP protocol stack offers a number of services to control and manage IP connections. Internet Control Message Protocol (ICMP) provides many of these services. Once a network problem occurs, a router or access server will send an ICMP message to the host or other routers. For detailed information on ICMP, see RFC 792.

### Enabling the ICMP Protocol Unreachable Message

When a router receives a non-broadcast packet destined to it, and this packet uses an IP protocol that it cannot handle, it will return an ICMP protocol unreachable message to the source address. Similarly, if the router is unable to forward the packet because it knows of no route to the destination address, it sends an ICMP host unreachable message. This feature is enabled by default.

To enable this service, execute the following command in the interface configuration mode:

Command	Function
Ruijie(config-if)# <b>ip unreachable</b>	Enable the ICMP protocol unreachable and host unreachable messages.
Ruijie(config-if)# <b>no ip unreachable</b>	Disable the ICMP protocol unreachable and host unreachable messages.

### Enabling the ICMP Redirect Message

Routes are sometimes less than optimal. For example, it is possible for the device to be forced to resend a packet through the same interface on which it was received. If the device resends a packet through the same interface on which it was received, it sends an ICMP redirect message to the originator of the packet telling the originator that the gateway to this destination address is another device in the same subnet. Therefore the originator will transmit the packets based on the optimized path afterwards. This feature is enabled by default.

To enable the ICMP redirect message, execute the following command in the interface configuration mode:

Command	Function
Ruijie(config-if)# <b>ip redirects</b>	Enable the ICMP redirect message. It is enabled by default.
Ruijie(config-if)# <b>no ip redirects</b>	Disable the ICMP redirect message.

## Enabling the ICMP Mask Reply Message

Occasionally, a network device needs to know the mask of a subnetwork in the Internet. To obtain this information, the device can send the ICMP mask request message. The receiving device will send the ICMP mask reply message. Ruijie product can respond the ICMP mask request message. This function is enabled by default.

To enable the ICMP mask reply message, execute the following command in the interface configuration mode:

Command	Function
Ruijie(config-if)# <b>ip mask-reply</b>	Enable the ICMP mask reply message.
Ruijie(config-if)# <b>no ip mask-reply</b>	Disable the ICMP mask reply message.

## Setting the IP MTU

All interfaces have a default MTU (Maximum Transmission Unit) value. All the packets which are larger than the MTU have to be fragmented before sending. Otherwise it is unable to be forwarded on the interface.

Ruijie product allows you to adjust the MTU on an interface. Changing the MTU value can affect the IP MTU value, and the IP MTU value will be modified automatically to match the new MTU. However, changing the IP MTU value has no effect on the value of MTU.

The interfaces of a device in a physical network should have the same MTU for a protocol.

To set the IP MTU, execute the following command in the interface configuration mode:

Command	Function
Ruijie(config-if)# <b>ip mtu bytes</b>	Set the MTU in the range 68 to 1500 bytes.
Ruijie(config-if)# <b>no ip mtu</b>	Restore the setting to the default.

## Configuring IP Source Routing

Ruijie product supports IP source routing. Upon receiving an IP packet, the device will check its IP header like strict source route, loose source route and recorded route, which are defined in RFC 791. If one of these options is enabled, the device performs appropriate action. Otherwise, it sends an ICMP error message to the source and then discards the packet. Our product supports IP source routing by default.

To enable IP source routing, execute the following command in the interface configuration mode:

Command	Function
Ruijie(config)# <b>ip source-route</b>	Enable IP source routing.
Ruijie(config)# <b>no ip source-route</b>	Disable IP source routing.

Confidentiality: Controlled
Document Property: Configuration Guide
Document owner: Wang Xiaofeng

Change History

Date	Changed By	Description

# IPv6 Configuration

## IPv6 Overview

---

As the Internet is growing rapidly and the IPv4 address space is exhausting, the limitation of the IPv4 is more obvious. The research and practice of the next generation of the Internet Protocol becomes popular. Furthermore, the IPng workgroup of the IETF determines the protocol specification of IPng referred to as IPv6. Refer to RFC2460 for details.

### Key Features of Ipv6:

#### ■ More Address Space

The length of address will be extended to 128 bits from the 32 bits of Ipv4. Namely, there are  $2^{128}-1$  addresses for IPv6. The IPv6 adopts the hierarchical address mode and supports multiple-level IP address assignment, for example, from the Internet backbone network to the internal subnet of enterprises.

#### ■ Simplified Format of Packet Header

The design principle of new IPv6 packet header is to minimize the overhead. For this reason, some non-critical fields and optional fields are removed from the packet header and placed into the extended packet header. The length of the IPv6 address is 4 times of IPv4 address; its packet header is only 2 times of IPv4 header. The improved IPv6 packet header is more efficient for forwarding, for instance, there is no checksum in the IPv6 packet header and it is not necessary for the IPv6 router to process the fragment during forwarding (the fragment is completed by the originator).

#### ■ High-efficient hierarchical Addressing and Routing Structure

The IPv6 adopts the aggregation mechanism and defines flexible hierarchical addressing and routing structure, and several networks at the same level is presented as a unified network prefix at the higher level of routers. So it obviously reduces the entries that the router must maintain and greatly minimizes the routing and storage overhead.

#### ■ Simple Management: Plug and Play

Simplify the management and maintenance of the network node by the implementation of a series of auto-discovery and auto-configuration functions. Such as the Neighbor Discovery, the MTU Discovery, the Router Advertisement, the Router Solicitation and the Auto-configuration technologies provide related service for the plug and play. It should be mentioned that the IPv6 supports such address configuration methods as the stateful and the stateless. In the IPv4, the dynamical host configuration protocol (DHCP) implements the automatic setting of the host IP address and related configuration, while the IPv6 inherits this auto-configuration service of the IPv4 and refers to it as the Stateful Auto-configuration. Furthermore, the IPv6 also adopts an auto-configuration service, referred to as the Stateless Auto-configuration. During the stateless auto-configuration, the host obtains the local address of the link, the address prefix of local device and some other related configuration information automatically.

#### ■ Security

The IPsec is an optional extended protocol of the IPv4, while it is only a component of the IPv6 used to provide security. At present, the IPv6 implements the Authentication Header (AH) and Encapsulated Security Payload (ESP) mechanisms. Where, the former authenticates the integrity of the data and the source of the IP packet to ensure that the packet does come from the node marked by the source address, while the latter provides the data encryption function to implement the end-to-end encryption.

### ■ More Excellent QoS Support

The new field in the IPv6 packet header defines how to identify and process the data flow. The Flow Label field in the IPv6 packet header is used to identify the data flow ID, by which the IPv6 allows users to put forward the requirement for the QoS of communication. The router can identify all packets of some specified data flow by this field and provide special processing for these packet on demand.

### ■ Neighbor Nodes Interaction-specific New Protocol

The Neighbor Discovery Protocol of the IPv6 uses a series of IPv6 control information message (ICMPv6) to carry out the interactive management of the neighbor nodes (the nodes of the same link). The Neighbor Discovery Protocol and high-efficient multicast and unicast Neighbor Discovery message replace previous broadcast-based address resolution protocol (ARP) and the ICMPv4 router discovery message.

### ■ Extensibility

The IPv6 provides powerful extensibility and the new features can be added to the extended packet header after the IPv6 packet header. Unlike the IPv4, the packet header can only support the option of up to 40 bytes, while the size of the IPv6 extended packet header is only limited by the maximum bytes of the whole IPv6 packet.

The IPv6 supports the following features:

- IPv6 Protocol
- IPv6 Address Format
- Type of IPv6 Address
- ICMPv6
- IPv6 Neighbor Discovery
- Path MTU Discovery
- ICMPv6 Redirection
- Address Conflict Detection
- IPv6 Stateless Auto-configuration
- IPv6 Address Configuration
- IPv6 Route Forwarding (supporting static route configuration)
- Configuration of various IPv6 parameters
- Diagnosis Tool Ping IPv6

## IPv6 Address Format

The basic format of an IPv6 address is X : X : X : X : X : X : X : X, where X is a 4 hex integers (16 bits). Each digit contains 4 bits of information, each integer contains 4 hex digits and each address contains 8 integers, so it is total for 128 bits. Some legal IPv6 addresses are as follows:

2001:ABCD:1234:5678:AAAA:BBBB:1200:2100

800 : 0 : 0 : 0 : 0 : 0 : 0 : 1

1080 : 0 : 0 : 0 : 8 : 800 : 200C : 417A

These integers are hex integers, where A to F denote 10 to 15 respectively. Each integer in the address must be denoted and the starting 0 needs not be denoted. Some IPv6 address may contain a series of 0s (such as the examples



2 and 3). Once this condition occurs, the “:” is allowed to denote this series of 0s. Namely, the address 800:0:0:0:0:0:0:1 can be denoted as: 800 :: 1.

These two colons denote that this address can be extended to the complete 128-bit address. In this way, the 16-bit group can be replaced with two colons only when they are all 0s and the two colons can only present for one time.

In the mixture environment of IPv4 and IPv6, there is a mixture denotation method. The lowest 32 bits in an IPv6 address can be used to denote an IPv4 address. The address can be expressed in a mixture mode, i.e., X: X: X: X: X: X: d: d: d: d: d. Where, the X denotes a 16-bit integer, while d denotes an 8-bit decimal integer. For instance, the address 0:0:0:0:0:0:192.168.20:1 is a legal IPv6 address. After the abbreviated expression method is used, this address can be denoted as follows: ::192.168.20.1. One of the typical example is the IPv4-compatible IPv6 address, which is expressed in the “::A.B.C.D” mode, i.e., “::1.1.1.1”; the other typical example is the IPv4-mapped IPv6 address, which is expressed in the “::FFFF:A.B.C.D” and used to invert the IPv4 address to the IPv6 address, i.e., map the IPv4 address “1.1.1.1” to the IPv6 address “::FFFF:1.1.1.1”.

For the IPv6 address is divided into two parts such as the subnet prefix and the interface identifier, it can be denoted as an address with additional numeric value by the method like the CIDR address. Where, this numeric value indicates how many bits represent the network part (the network prefix). Namely the IPv6 node address indicates the length of the prefix, and the length is differentiated from the IPv6 address by the slash. For instance: 12AB::CD30:0:0:0/60, The length of the prefix used for routing in this address is 60 bits.

## Type of IPv6 Address

In RFC4291, there are the following three defined types of IPv6 addresses:

- Unicast: Identifier of a single interface. The packet to be sent to a unicast address will be transmitted to the interface identified by this address.
- Anycast: Identifiers of a set of interfaces. The packet to be sent to an anycast address will be transmitted to one of the interfaces identified by this address (select the nearest one according to the routing protocol).
- Multicast: Identifiers of a set of interfaces (In general, they are of different nodes). The packet to be sent to a Multicast address will be transmitted to all the interfaces which are added to this multicast address.



**Caution** The broadcast address is not defined in the IPv6.

---

The following will introduce these types of addresses one-by-one:

### Unicast Addresses

The unicast address is divided into unspecified address, loopback address, link-level local address, site-level local address and global unicast address. Now the site-level local address has been repealed, the unicast addresses excepting for the unspecified address, loopback address and the link-level local address are all global unicast addresses.

#### 1) Unspecified Address

The unspecified address is 0:0:0:0:0:0:0:0, generally abbreviated as ::.

- If there is no unicast address when the host is rebooting, use the unspecified address as the source address, send the router request and obtain the prefix information from the gateway to auto-generate the unicast address.
- When configuring the IPv6 address for the host, check whether the IPv6 address conflicts with the address for other hosts in the same network segment or not. If so, use the unspecified address as the source address to send the neighbor request message, same as free ARP.

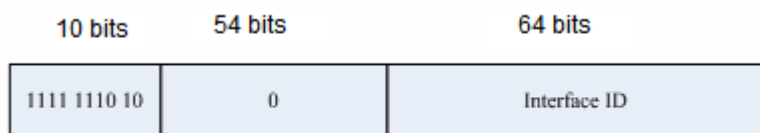
## 2) Loopback Address

The loopback address is 0:0:0:0:0:0:1, abbreviated as ::1, which is equal to the IPv4 address 127.0.0.1 and used when the node sends the packets to itself.

## 3) Link-level Local Address

The format of link-level local address:

Figure 1

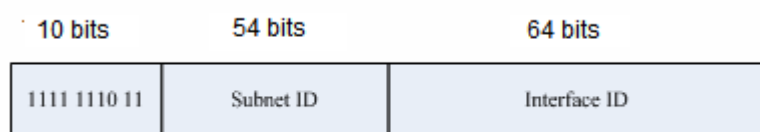


The link-level local address is used to number the host on the single network link. The address of former 10-bit identification for the prefix is the link-level local address. The router will not forward the message of the source address or the destination address with the link-level local address forever. The intermediate 54-bit of this address is 0. The latter 64 indicates the interface identifier, this part allows the single network to connect to up to  $2^{64}-1$  hosts.

## 4) Site-level Local Address

The format of site-level local address:

Figure 2

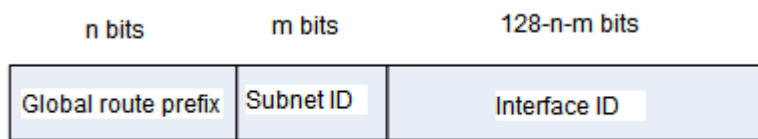


The site-level local address can be taken to transmit the data within the site, and the router will not forward the message of the source address or the destination address with the site-level local address to Internet. Namely, such packet can only be forwarded within the site, but cannot be forwarded to out of the site. Suppose that the site is the LAN for a company, the site-level local address is similar to the IPv4 private address, i.e., 192.168.0.0/16. The RFC3879 has repealed the site-level local address.

## 5) Global Unicast Address

The format of global unicast address:

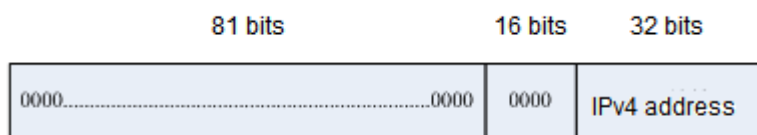
Figure 3



One class of the global unicast address is the IPv6 address embedded with IPv4 address, which is used to interconnect the IPv4 nodes and the IPv6 nodes and divided into IPv4-compatible IPv6 address and the IPv4-mapped IPv6 address.

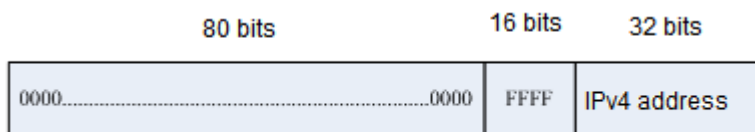
The format of IPv4-compatible IPv6 address:

Figure 4



The format of IPv4-mapped IPv6 address:

Figure 5



The IPv4-compatible IPv6 address is mainly used to the automatic tunneling, which supports both the IPv4 and IPv6. The IPv4-compatible IPv6 address will transmit the IPv6 packet via the IPv4 router in the tunneling way. Now the IPv4-compatible IPv6 address has been repealed. The IPv6 address of an IPv4 mapping is used to access the nodes that only support IPv4 by IPv6 nodes. For example, when one IPv6 application of the IPv4/IPv6 host requests the resolution of a host name (the host only supports IPv4), the name server will internally generate the IPv6 addresses of the IPv4 mapping dynamically and return them to the IPv6 application.

## Multicast Addresses

The format of the IPv6 multicast address is shown as follows:



The first byte of the address format is full 1, which denote a multicast address.

#### ■ Flag field:

It consists of 4 bits. At present, only the fourth bit is specified. The bit is used to indicate whether the address is a known multicast address specified by Internet Number Constitution or a temporary multicast address used in a specific condition. If this flag bit is 0, it indicates this address is a known multicast address. If this bit is 1, it indicates that this address is a temporary one. Other 3 flag bits are reserved for future use.

#### ■ Range field:

Composed of 4 bits and used to denote the range of multicast. Namely, whether the multicast group contains the local node, the local link and the local site or any position nodes in the IPv6 global address space.

#### ■ Group Identifier field:

112 bits long and used to identify a multicast group. Depending on whether a multicast address is temporary or known and the range of the address, a multicast identifier can denote different groups.

The multicast address of the IPv6 is this type of address taking FF00::/8 as the prefix. One multicast address of an IPv6 usually identifies the interfaces of a serial of different nodes. When one message is sent to one multicast address, this message will be distributed to the interfaces of each node with this multicast address. One node (host or router) should add the following multicast:

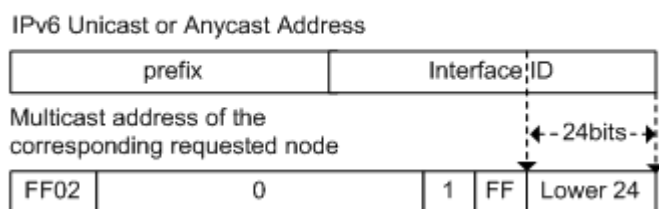
- The multicast address of all nodes for the local link is FF02::1
- The prefix of the multicast address for the solicited node is FF02:0:0:0:1:FF00:0000/104

If they are routers, it is necessary to add the multicast address FF02::2 of all routers for the local link.

The multicast address of the solicited node corresponds to the IPv6 unicast and anycast address, so it is necessary for the IPv6 node to add corresponding multicast address of the solicited node for each configured unicast address and anycast address. The prefix of the multicast address for the solicited node is FF02:0:0:0:1:FF00:0000/104, another 24 bits are comprised of the unicast address or the lower 24 bits of the anycast address, for instance, the multicast address of the solicited node corresponding to the FE80::2AA:FF:FE21:1234 is FF02::1:FF21:1234,

The multicast address of solicited node is usually used to the neighbor solicitation (NS) message. The format of the solicited node is shown as follows:

Figure 6



## Anycast Addresses

The anycast address is similar with the multicast address as more than one node shares an anycast address. The difference is that only one node expects to receive the data packet of the anycast address, while all nodes of the multicast address members expect to receive all packets sending to this address. The anycast address is assigned to

normal IPv6 unicast address space, so the anycast address cannot be differentiated from the unicast address from the style. For this reason, each member of all anycast addresses has to be configured explicitly to identify the anycast address.



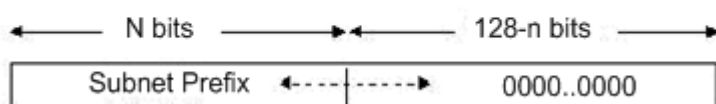
**Caution** The anycast address can only be assigned to the router, but cannot be assigned to the host. Furthermore, the anycast address cannot be taken as the source address of the message.

The RFC2373 predefines an anycast address, referred to as the anycast address of the subnet router. The following diagram shows the anycast address format of the subnet router, which consists of the subnet prefix followed by a series of 0s (as the interface identifier).

Where, the subnet prefix identifies a specified link (subnet) and the packet to be sent to the anycast address of the subnet router will be distributed to a router of this subnet. The anycast address of the subnet router is usually used for some node which needs to communicate with one router of the remote subnet.

Figure 7

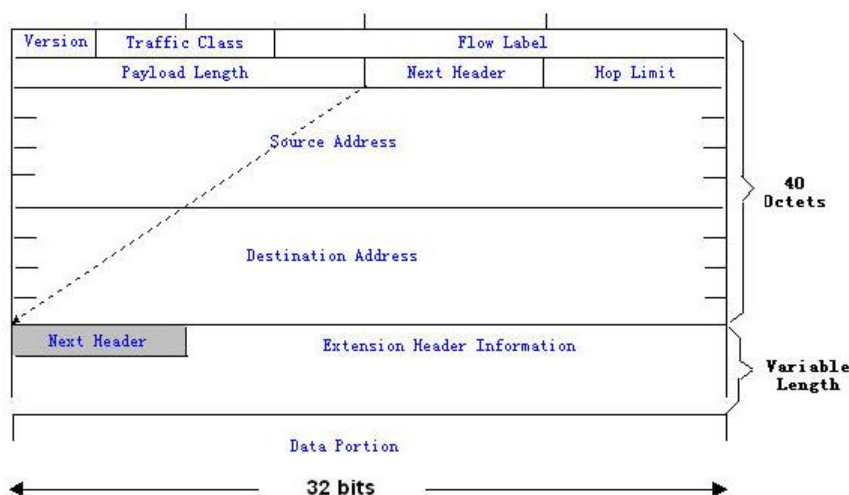
Anycast Address Format of Subnet Router



### IPv6 Packet Header Structure

The format of the IPv6 packet header is shown as the figure below:

Figure 8



The IPv4 packet header takes 4 bytes as the unit; the IPv6 packet header takes 8 bytes as the unit and the total length of the packet header is 40 bytes. In the IPv6 packet header, the following fields are defined:

- Version:

The length is 4 bits. For IPv6, the field must be 6.

■ Traffic Class:

The length is 8 bits. It indicates a type of service provided to the packet and is equal to the “TOS” in the IPv4.

■ Flow Label:

The length is 20 bits used to identify the packets of the same service flow. One node can be taken as the sending source of several service flows. Flow label and source node IP address identify a service flow uniquely.

■ Payload Length:

The length is 16 bits, including the byte length of payload and the length of various IPv6 extension options (if any). In other words, it includes the length of an IPv6 packet except for the IPv6 header itself.

■ Next Header:

This field indicates the protocol type in the header field following the IPv6 header. Similar to the IPv4 protocol field, the Next Header field can be used to indicate whether the upper level is TCP or UDP. It can also be used to indicate whether an extended IPv6 header exists.

■ Hop Limit:

The length is 8 bits. When one router forwards the packet for one time, this field will reduce 1. If this field is 0, this packet will be discarded. It is similar to the life span field in the IPv4 packet header.

■ Source Address (Source Address):

The length is 128 bits. It indicates the sender address of an IPv6 packet.

■ Destination Address (Destination Address):

The length is 128 bits. It indicates the receiver address of an IPv6 packet.

At present, the following extended headers are defined for the IPv6:

■ Hop-by-Hop Options:

This extended header must directly follow an IPv6 header. It contains the option data that must be checked by each node along the path.

■ Routing Header (Routing (Type 0)):

This extended header indicates the nodes that a packet will go through before reaching the destination. It contains the address table of various nodes that the packet goes through. The initial destination address of the IPv6 header is the first one of a series of addresses in the routing header, other than the final destination address of the packet. After receiving this packet, the node of this address will process the IPv6 header and the routing header, and send the packet to the second address of the routing header list. It repeats this step until the packet reaches the final destination.

■ Fragment Header (Fragment):

This extended header is used to fragment the packets longer than the MTU of the path between the source node and destination node.

■ Destination Option Header (Destination Options):

This extended header replaces the IPv4 option field. At present, the only defined destination option is to fill the option with an integer multiple of 64 bits (8 bytes) when necessary. This extended header can be used to carry the information checked by the destination node.

■ Upper-layer Extended Header (Upper-layer header):

It indicates the the upper layer transmission protocol, such as TCP(6) and UDP(17).

Furthermore, the extended header of the Authentication and the Encapsulating Security Payload will be described in the IPSec section. At present, the IPv6 implemented by us cannot support the IPSec.

### IPv6 Path MTU Discovery

As with the path MTU discovery of the IPv4, the path MTU discovery of the IPv6 allows one host to discover and adjust the size of the MTU in the data transmission path.

Furthermore, when the data packet to be sent is larger than the MTU of the data transmission path, the host will fragment the packets by itself. This behavior makes it not necessary for the router to process the fragment, and thus save resources and improve the efficiency of the IPv6 network.



#### Caution

The minimum link MTU is 68 bytes in the IPv4, indicating that the links along the path over which the packets are transmitted should support at least the link MTU of 68 bytes. The minimum link MTU is 1280 bytes in the IPv6. It is strongly recommended to use the link MTU of 1500 bytes for the link in the IPv6.

---

### IPv6 Neighbor Discovery

The main functions of the IPv6 Neighbor discovery protocol include Router Discovery, Prefix Discovery, Parameter Discovery, Address Auto-configuration, Address Resolution(ARP), Next-hop Confirmation, Neighbor Unreachability Check, Address Conflict Check and Redirection. Neighbor discovery defines 5 types of ICMP message, which are Router Solicitation(ICMP type133), Router Advertisement(ICMP type134), Neighbor Solicitation or ARP request (ICMP type135), Neighbor Advertisement or APR response(ICMP type136) and ICMP redirection message(ICMP type137).

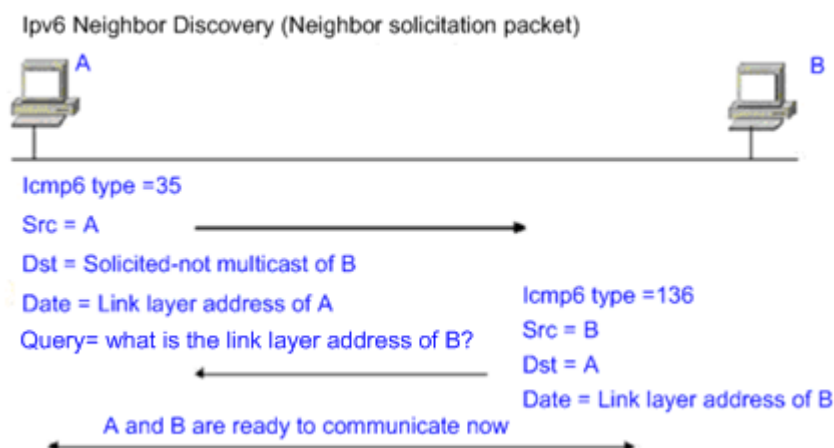
The following describes the neighbor discovery function in detail:

#### Address Resolution

A node must get the link layer address of another node before communicating with it. At this time, it should send the neighbor solicitation (NS) message to the solicited multicast address of the IPv6 address of the destination node. The NS message also contains the link layer address of itself. After receiving this NS message, the destination node responds with a message, referred to as neighbor advertisement (NA), with its link layer address. After receiving the response message, the source node can communicate with the destination node.

The following is the neighbor solicitation procedure:

Figure 9



## Neighbor Unreachability Detection

Enabling the Neighbor Unreachability Detection function to send the IPv6 unicast packet to the neighbor whose reachable time expires.

Neighbor Unreachability Detection and sending the IPv6 packet to the neighbor can be co-processed. During the detection, it continues to forward the IPv6 packet to the neighbor.

## Address Conflict Detection

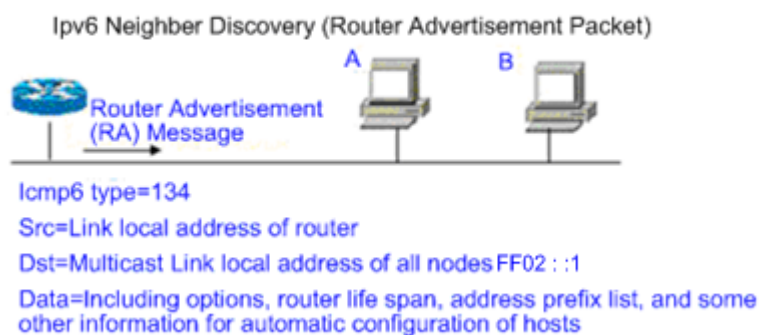
After configuring the IPv6 address to the host, enabling the address conflict detection function to check whether the IPv6 address in the link is sole or not.

## Router, Prefix and Parameter Advertisement

The router sends the Router Advertisement (RA) to all the local nodes of the link periodically.

The following figure shows the process of sending the Router Advertisement (RA):

Figure 10



In general, the Router Advertisement (RA) contains the contents below:

- One or more IPv6 address prefixes used for the on-link confirmation or the stateless address auto-configuration.



- Effective period of the IPv6 address prefix.
- Usage of the host auto-configuration (Stateful or stateless).
- Information for the default router (namely, determine whether this router is taken as the default router. If yes, it will announce the time as the default router itself).
- Other information for configuration such as the hop limit, the MTU and the neighbor solicitation retransmission interval.

The Router Advertisement (RA) is also used to respond to the Router Solicitation (RS) message sent by the host. The Router Solicitation (RS) message allows the host to obtain the auto-configuration information immediately without waiting for the router to send the Router Advertisement (RA). If there is no unicast address when the host is activated, the Router Solicitation (RS) message sent by the host will use the unassigned address (0:0:0:0:0:0:0:0) as the source address of the solicitation message. Otherwise, the existing unicast address is taken as the source address, while the Router Solicitation (RS) message uses the multicast address (FF02::2) of all routers for the local link as the destination address. As the response router solicitation (RS) message, the Router Advertisement (RA) message will use the source address of the solicitation message as the destination address (if the source address is the unassigned address, it will use the multicast address FF02::1) of all nodes for the local link.

The following parameters can be configured in the Router Advertisement (RA) message:

Ra-interval: Interval of sending the Router Advertisement (RA).

Ra-lifetime: Router lifetime, namely whether the device is acted as the default router of the local link and the time as this role.

Prefix: IPv6 address prefix of the local link, which can be used for the on-link confirmation or the stateless address auto-configuration, including the configuration of other parameters for the prefix.

Rs-interval: Interval of sending the neighbor solicitation message.

Reachabletime: Time maintained after considering the neighbor reachable.

We configure the above parameters in the IPv6 interface property.



### Caution

1. By default, no Router Advertisement (RA) message is sent actively on the interface. To do so, you can use the command **no ipv6 nd suppress-ra** in the interface configuration mode.
  2. In order to make the stateless address auto-configuration of the node work normally, the length of the prefix for the router advertisement (RA) message should be 64 bits.
- 

## Redirection

After receiving the IPv6 packets, the router discovers the better next-hop and sends the ICMP redirection message to notify the host of the better next-hop. Next time the host sends the IPv6 packets to the better next-hop directly.

## IPv6 Configuration

---

The following will introduce the configuration of various function modules of the IPv6 respectively:

## Configuring IPv6 Address

This section describes how to configure an IPv6 address on an interface. By default, no IPv6 address is configured.



### Caution

Once an interface is created and its link status is UP, the system will automatically generate the local link address for the interface. At present, the IPv6 doesn't support anycast address..

To configure an IPv6 address, execute the following commands in the global configuration mode:

Command	Meaning
Ruijie# <b>configure terminal</b>	Enter the global configuration mode.
Ruijie(config)# <b>interface</b> <i>interface-id</i>	Enter the interface configuration mode. Note that the <b>no switchport</b> command shall be used to switchover the layer-2 port to the layer-3 interface.
Ruijie(config-if)# <b>ipv6 enable</b>	Enable the IPv6 protocol on an interface. If this command is not run, the system automatically enables the IPv6 protocol when you configure an IPv6 address for an interface.
Ruijie(config-if)# <b>ipv6 address</b> <i>ipv6-address/prefix-length</i>  Ruijie(config-if)# <b>ipv6 address</b> <i>ipv6-prefix/prefix-length [eui-64]</i>	Configure the IPv6 unicast address for this interface. The key word <b>Eui-64</b> indicates the generated IPv6 address consists of the configured address prefix and the 64-bit interface ID. Note: Whether the key word <b>eui-64</b> is used, it is necessary to enter the complete address format to delete an IPv6 address (Prefix + interface ID/prefix length). When you configure an IPv6 address on an interface, then the IPv6 protocol is automatically enabled on the interface. Even if you use no <b>ipv6 enable</b> , you cannot disable the IPv6 protocol.
Ruijie(config-if)# <b>end</b>	Return to the privileged EXEC mode.
Ruijie# <b>show ipv6 interface</b> <i>interface-id</i>	View the IPv6 interface information.
Ruijie# <b>copy running-config startup-config</b>	Save the configuration.

Use the **no ipv6 address** *ipv6-prefix/prefix-length [eui-64]* command to delete the configured IPv6 address.

The following is an example of the configuration of the IPv6 address:

```
Ruijie(config)# interface GigabitEthernet 0/1
Ruijie(config-if)# ipv6 enable
Ruijie(config-if)# ipv6 address fec0:0:0:1::1/64
Ruijie(config-if)# end
Ruijie(config-if)# show ipv6 interface GigabitEthernet 0/1
Interface GigabitEthernet 0/1 is Up, ifindex: 1
address(es):
Mac Address: 00:00:00:00:00:01
INET6: fe80::200:ff:fe00:1 , subnet is fe80::/64
INET6: fec0:0:0:1::1 , subnet is fec0:0:0:1::/64
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 100 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<160--240>
ND router advertisements live for 1800 seconds

```

## Configuring ICMPv6 Redirection

This section will describe how to configure the ICMPv6 redirection function on the interface. By default, the redirection function of the IPv6 on the interface is enabled. The router needs to send the redirection message to the source during packet forwarding in the following cases:

- The destination address of the message is not a multicast address;
- The destination address of the message is not the router itself;
- The output interface of the next hop determined by the device for this message is the same as the interface this message received, namely, the next hop and the originator is of the same link;
- The node identified by the source IP address of the packet is a neighbor of the local router. Namely, this node exists in the router's neighbor table.



### Caution

The router other than the host can generate the redirection message, and the router will not update its routing table when it receives the redirection message.

To enable redirection on the interface, execute the following commands in the global configuration mode:

Command	Meaning
Ruijie# <b>configure terminal</b>	Enter the global configuration mode.
Ruijie(config)# <b>interface</b> <i>interface-id</i>	Enter the interface configuration mode. Note that the <b>no switchport</b> command shall be used to switchover the layer-2 port to the layer-3 interface.
Ruijie(config-if)# <b>ipv6 redirects</b>	Enable the IPv6 redirection function.
Ruijie(config-if)# <b>end</b>	Return to the privileged EXEC mode.
Ruijie# <b>show ipv6 interface</b> <i>interface-id</i>	Show the interface configuration.
Ruijie# <b>copy running-config startup-config</b>	Save the configuration.

Use the **no ipv6 redirects** command to disable the redirection function. The following is an example to configure the redirection function:

```
Ruijie(config)# interface GigabitEthernet 0/1
Ruijie (config-if)# ipv6 redirects
Ruijie (config-if)# end
Ruijie # show ipv6 interface GigabitEthernet 0/1
Interface GigabitEthernet 0/1 is Up, ifindex: 1
address(es):
Mac Address: 00:d0:f8:00:00:01
INET6: fe80::2d0:f8ff:fe00:1 , subnet is fe80::/64
INET6: fec0:0:0:1::1 , subnet is fec0:0:0:1::/64
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<160--240>
ND router advertisements live for 1800 seconds
```

## Configuring Static Neighbor

This section will describe how to configure a static neighbor. By default, the static neighbor is not configured. In general, a neighbor learns and maintains its status by the Neighbor Discovery Protocol (NDP) dynamically. Moreover, you can configure the static neighbor manually.

To configure the static neighbor, execute the following commands in the global configuration mode.

Command	Meaning
Ruijie#configure terminal	Enter the global configuration mode.
Ruijie(config)# <b>ipv6 neighbor</b> <i>ipv6-address</i> <i>interface-id hardware-address</i>	Configure a static neighbor on the interface.
Ruijie(config)#end	Return to the privileged EXEC mode.
Ruijie#show ipv6 neighbors	View the neighbor list.
Ruijie#copy running-config startup-config	Save the configuration.

Use the **no ipv6 neighbor** *ipv6-address interface-id* command to delete the specified neighbor. The following is an example to configure a static neighbor on GigabitEthernet 0/1:

```

Ruijie(config)# ipv6 neighbor fec0:0:0:1::100 GigabitEthernet 0/1 00d0.f811.1234
Ruijie (config)# end
Ruijie# show ipv6 neighbors verbose fec0:0:0:1::100
IPv6 Address      Linklayer Addr  Interface
fec0:0:0:1::100   00d0.f811.1234  GigabitEthernet 0/1
State: REACH/H Age: - asked: 0

```



### Caution

When you configure a static neighbor, the configuration takes effect only when the neighbor prefix matches the interface. Specifically, the configured static neighbor prefix belongs to the network segment of an address configured for the interface, and does not conflict with the address. An invalid static neighbor stays in the **inactive** state. Data sent to the destination is not sent to the MAC address specified by the static neighbor, but the MAC address is learnt based on routes in dynamic learning mode. To view the validation status of a static neighbor, run the **show ipv6 neighbor static** command.

## Configuring Address Conflict Detection

This section describes how to configure address conflict detection times. Address conflict detection is mandatory to assign unicast addresses to interfaces. The goal is to detect the uniqueness of an address. The address conflict detection should be carried out for the manual configuration address, the stateless auto-configuration address or the statefull auto-configuration address. However, it is not necessary to carry out the address conflict detection under the following two conditions:

- The management prohibits the address conflict detection, namely, the number of the neighbor solicitation messages sent for the address conflict detection is set to 0.
- The configured anycast address can not be applied to the address conflict detection.

Furthermore, if the address conflict detection function is not disabled on the interface, the system will enable the address conflict detection process for the configured address when the interface changes to the Up status from the Down status.

The following is the configuration procedure of the quantity of the neighbor solicitation message sent for the address conflict detection:

Command	Meaning
Ruijie# <b>configure terminal</b>	Enter the global configuration mode.
Ruijie(config)# <b>interface</b> <i>interface-id</i>	Enter the interface configuration mode. Note that the <b>no switchport</b> command shall be used to switchover the layer-2 port to the layer-3 interface.
Ruijie(config-if)# <b>ipv6 nd dad attempts</b> <i>attempts</i>	The quantity of the neighbor solicitation message sent for the address conflict detection. When it is configured to 0, any neighbor solicitation message is denied. Enable the address conflict detection function on the interface.
Ruijie(config-if)# <b>end</b>	Return to the privileged EXEC mode.

Ruijie# <b>show ipv6 interface vlan 1</b>	View the IPv6 information on the interface.
Ruijie# <b>copy running-config startup-config</b>	Save the configuration.

Use the **no ipv6 nd dad attempts** command to restore the default value. The following is an example to configure the times of the neighbor solicitation (NS) message sent for the address conflict detection on the SVI1:

```
Ruijie(config)# interface GigabitEthernet 0/1
Ruijie(config-if)# ipv6 nd dad attempts 3
Ruijie(config-if)# end
Ruijie# show ipv6 interface GigabitEthernet 0/1
Ruijie(config)# interface vlan 1
Ruijie(config-if)# ipv6 nd dad attempts 3
Ruijie(config-if)# end
Ruijie# show ipv6 interface vlan 1
Interface GigabitEthernet 0/1 is Up, ifindex: 1
address(es):
Mac Address: 00:d0:f8:00:00:01
INET6: fe80::2d0:f8ff:fe00:1 , subnet is fe80::/64
INET6: fec0:0:0:1::1 , subnet is fec0:0:0:1::/64
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: 3
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<160--240>
ND router advertisements live for 1800 seconds
```

## Configuring the IPv6 MTU of the Interface

Every interface of the device has a default MTU value. If one IPv6 packet exceeds the IPv6 MTU, the RGOS software will disassemble the packet. For the interconnection interfaces of devices on the same physical network segment, the IPv6 MTU values are consistent.

For device interfaces on the same physical network segment, the MTU values of the same protocol must be consistent.

To set the IPv6 MTU value, run the following commands in the interface configuration mode.

Command	Function
---------	----------

Ruijie(config-if)# <b>ipv6 mtu bytes</b>	Set the MTU value within the range 1280–1500..
Ruijie(config-if)# <b>no ipv6 mtu</b>	Restore the default value.

## Configuring Other Interface Parameters

The IPv6 parameters on an interface fall into 2 parts, one is used to control the behavior of the router itself, the other is used to control the contents of the router advertisement (RA) sent by the router to determine what action should be taken by the host when it receives this router advertisement (RA).

The following will introduce these commands one by one:

Command	Meaning
Ruijie# <b>configure terminal</b>	Enter the global configuration mode.
Ruijie(config)# <b>interface interface-id</b>	Enter the interface configuration mode. Note that the <b>no switchport</b> command shall be used to switchover the layer-2 port to the layer-3 interface.
Ruijie(config-if)# <b>ipv6 enable</b>	Enable the IPv6 function.
Ruijie(config-if)# <b>ipv6 nd ns-interval milliseconds</b>	(Optional) Define the retransmission interval of the neighbor solicitation message, in ms, the default value is 1000ms.
Ruijie(config-if)# <b>ipv6 nd reachable-time milliseconds</b>	(Optional) Define the time when the neighbor is considered to be reachable, in ms, the default value is 30000ms. Note: as specified in RFC4861, the reachable time of a neighbor should be increased or decreased at random on the basis of the configured time in the range of 0.5 to 1.5 of the configured time.
Ruijie(config-if)# <b>ipv6 nd prefix</b> {ipv6-prefix/prefix-length   <b>default</b> } [ [ valid-lifetime preferred-lifetime ]   [ <b>at</b> valid-date preferred-date ]   [ <b>infinite</b> {infinite   preferred-lifetime}]] [ <b>no-advertise</b> ]   [[ <b>off-link</b> ] [ <b>no-autoconfig</b> ]]	(Optional) Set the address prefix to be advertised in the router advertisement (RA) message.
Ruijie(config-if)# <b>ipv6 nd ra-lifetime seconds</b>	(Optional) Set the TTL of the router in the router advertisement (RA) message, namely the time as the default router. 0, indicates that the router will not act as the default router of the direct-connected network. The default value is 1800s.
Ruijie(config-if)# <b>ipv6 nd ra-interval {seconds min-max min_value max_value}</b>	(Optional) Set the time interval for the router to send the router advertisement (RA) message periodically, in second, and the default value is 200s. With the <b>min-max</b> specified, the actual interval of the message sending is a random value between the minimum and maximum value. Without the <b>min-max</b> specified, the actual interval of the message sending is approximately 1.2/0.8*the configured value.
Ruijie(config-if)# <b>ipv6 nd managed-config-flag</b>	(Optional) Set the “managed address configuration” flag bit of the router advertisement (RA) message, and determine whether the host will use the stateful auto-configuration to obtain the address when it receives this router advertisement (RA).

Command	Meaning
	By default, the flag bit is not configured for the router advertisement (RA) message.
Ruijie(config-if)# <b>ipv6 nd other-config-flag</b>	(Optional) Set the “other stateful configuration” flag bit of the router advertisement (RA) message, and determine whether the host will use the stateful auto-configuration to obtain other information other than the address when it receives this router advertisement (RA). By default, the flag bit is not configured for the router advertisement (RA) message.
Ruijie(config-if)# <b>ipv6 nd suppress-ra</b>	(Optional) Set whether suppress the router advertisement (RA) message in this interface. By default, the flag bit is not configured for the router advertisement (RA) message.
Ruijie(config-if)# <b>end</b>	Return to the privileged EXEC mode.
Ruijie# <b>show ipv6 interface</b> [ <i>interface-id</i> ] <b>[ra-info]</b>	Show the ipv6 interface of the interface or the information of RA sent by this interface.
Ruijie# <b>copy running-config startup-config</b>	(Optional) Save the configuration.

The **no** command of above commands can be used to restore the default value. For details, refer to *IPv6 Command Reference*.

## IPv6 Monitoring and Maintenance

It is mainly used to provide related command to show some internal information of the IPv6 protocol, such as the ipv6 information, the neighbor table and the route table information of the interface.

Command	Meaning
<b>show ipv6 interface</b> [ <i>interface-id</i> ] <b>[ra-info]</b>	Show the IPv6 information of the interface.
<b>Show ipv6 neighbors</b> [ <b>verbose</b> ] [ <i>interface-id</i> ] <i>[ipv6-address]</i>	Show the neighbor information.
<b>Show ipv6 route</b> [ <b>static   local   connected   bgp   rip   ospf   isis</b> ]	Show the information of the IPv6 routing table.

- View the IPv6 information of an interface.

```
Ruijie# show ipv6 interface
interface GigabitEthernet 0/1 is Down, ifindex: 1
address(es):
Mac Address: 00:d0:f8:00:00:01
INET6: fe80::2d0:f8ff:fe00:1 , subnet is fe80::/64
INET6: fec0:1:1:1::1 , subnet is fec0:1:1:1::/64
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<160--240>
ND router advertisements live for 1800 seconds
```

■ View the information of the router advertisement (RA) message to be sent of an interface

```
Ruijie# show ipv6 interface ra-info
GigabitEthernet 0/1: DOWN
RA timer is stopped
waits: 0, initcount: 3
statistics: RA(out/in/inconsistent): 4/0/0, RS(input): 0
Link-layer address: 00:00:00:00:00:01
Physical MTU: 1500
ND router advertisements live for 1800 seconds
ND router advertisements are sent every 200 seconds<160--240>
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)
```

■ View the neighbor table information of the IPv6.

```
Ruijie# show ipv6 neighbors
IPv6 Address                Linklayer Addr  Interface
fe80::200:ff:fe00:1          0000.0000.0001 GigabitEthernet 0/1
State: REACH/H Age: - asked: 0
fec0:1:1:1::1                0000.0000.0001 GigabitEthernet 0/1 State: REACH/H Age: - asked: 0
```

# DHCP Configuration

## Introduction to DHCP

The DHCP (Dynamic Host Configuration Protocol), specified in RFC 2131, provides configuration parameters for hosts over the Internet. The DHCP works in the client/server mode. The DHCP server assigns IP addresses for the hosts dynamically and provides configuration parameters.

The DHCP assigns IP address in three ways:

- 1) Assign IP addresses automatically. The DHCP server assigns permanent IP addresses to the clients;
- 2) Assign IP addresses dynamically. The DHCP server assigns IP addresses that will expire after a period of time to the clients (or the clients can release the addresses by themselves);
- 3) Configure IP addresses manually. Network administrators specify IP addresses and send the specified IP addresses to the clients through the DHCP.

Among the above mentioned three methods, only dynamic assignment allows reuse of the IP address that the client does not need any more.

The format of DHCP message is based on that of BOOTP (Bootstrap Protocol) message. Hence, it is necessary for the device to be able to act as the BOOTP relay agent and interact with the BOOTP client and the DHCP server. The function of BOOTP relay agent eliminates the need of deploying a DHCP server in every physical network. The DHCP is detailed in RFC 2131 and RFC 2132.

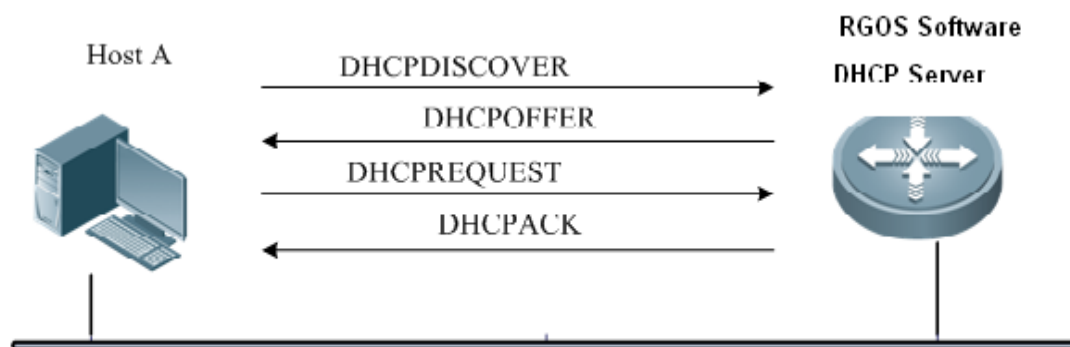
## DHCP Working Principles

The DHCP protocol is widely used to dynamically assign reusable network resources, for example, IP addresses. A DHCP client sends DISCOVER broadcast packets to a DHCP server. After receiving the DISCOVER packets, the DHCP server will assign resources, e.g. IP addresses, by a certain policy in OFFER packets sent to the client. Once receiving the OFFER packets, the DHCP client verifies the availability of the resource. If the resource is available, it will send a REQUEST packet; otherwise, it will re-send the DISCOVER packet. Once the server receives the REQUEST packet, it will verify whether the IP address or other limited resource can be assigned. If so, the server will send an ACK packet; otherwise, it will send a NAK packet. Once the DHCP client receives the ACK packet, it will start using the resource assigned by the server; if the NAK packet is received, the client may re-send the DISCOVER packet.

## Introduction to the DHCP Server

As specified in RFC2131, the DHCP server of Ruijie is implemented to assign and manage IP addresses for the DHCP clients. The DHCP operation process is shown in the following figure.

Fig 1-1 DHCP process



Process of requesting an IP address:

- 1) The host broadcasts a DHCPDISCOVER packet in the network to locate the DHCP server;
- 2) The DHCP server sends a DHCPOFFER packet in unicast form to the host, including IP address, MAC address, domain name and address lease period;
- 3) The host sends a DHCPREQUEST packet in broadcast form to formally request the server to assign the provided IP address;
- 4) The DHCP server sends a DHCPACK packet in unicast form to the host to confirm the request.

**Note**

The DHCP client may receive the DHCPOFFER packets from multiple DHCP servers, and accept any DHCPOFFER packet. However, the DHCP client usually accepts the first received DHCPOFFER packet only.

**Note**

The address specified in the DHCPOFFER packet from the DHCP server is not necessarily the finally assigned address. Generally, the DHCP server reserves this address until the client sends a formal request.

The DHCPREQUEST that requests the DHCP server to assign an address is a broadcast packet with the server address in order to enable all other DHCP servers that send DHCPOFFER response packets to receive the packet. Other DHCP servers are unable to find that the client has received the DHCPOFFER packet from just the DHCPREQUEST packet, so they will not release the IP addresses offered (pre-assigned) to the clients and will enable the IP addresses corresponding to the unaccepted OFFER lease to be reused through the timing mechanism.

If the DHCPOFFER packet sent to the DHCP client contains invalid parameters, the DHCP client sends the DHCPDECLINE packet to refuse the assigned configuration.

The advantages of using the DHCP server of Ruijie for network construction are:

- Decrease network access cost. Generally, dynamic address assignment costs less than static address assignment.
- Simplify configuration tasks and reduce network construction cost. Dynamic address assignment significantly simplifies equipment configuration, and even reduces deployment cost if devices are deployed in the places where there are no professionals.

- Centralized management. During configuration management on several subnets, any configuration parameter can be changed simply by modifying and updating configurations in the DHCP server.

## Introduction to the DHCP Client

The DHCP client can obtain IP addresses and other configuration parameters from the DHCP server automatically. The DHCP client brings the following advantages:

- Save device configuration and deployment time.
- Reduce the possibility of configuration errors.
- Centrally manage IP address assignment.

☒ The DHCP Client is supported on the Ethernet interface, FR, PPP, HDLC interfaces.

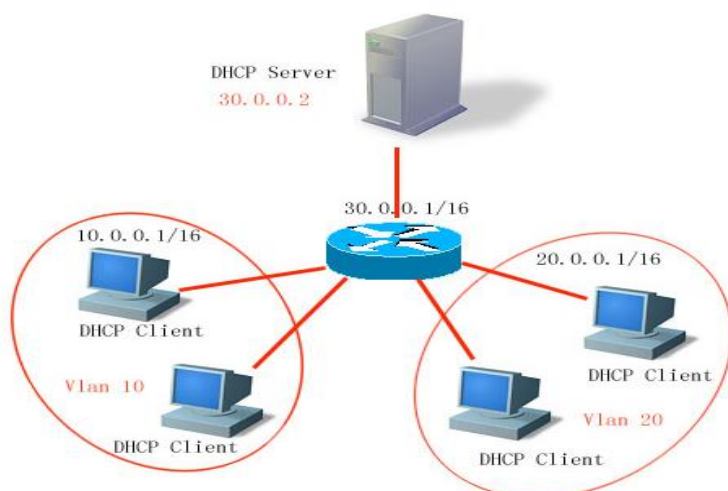
## Introduction to the DHCP Relay Agent

The DHCP relay agent forwards DHCP packets between the DHCP server and the DHCP clients. When the DHCP clients and the server are not located in the same subnet, a DHCP relay agent must be available for forwarding the DHCP request and response messages. Data forwarding by the DHCP relay agent is different from general forwarding. In general forwarding, IP packets are unaltered and the transmission is transparent. However, upon receiving a DHCP message, the DHCP relay agent regenerates and forwards a DHCP message.

From the perspective of the DHCP client, the DHCP relay agent works like a DHCP server. From the perspective of the DHCP server, the DHCP relay agent works like a DHCP client.

The DHCP relay forwards the DHCP request packet received in the form of unicast to the DHCP server, at the same time, forwards the DHCP response packet received to the DHCP client. The DHCP relay serves as a forwarding station, responsible for the communication between the DHCP clients and the DHCP servers at different network segments. In this way, only one DHCP server can dynamically manage IP addresses at multiple segments, that is, the DHCP dynamic IP management in the Client-Relay-Server mode, as shown below:

Figure 1-2



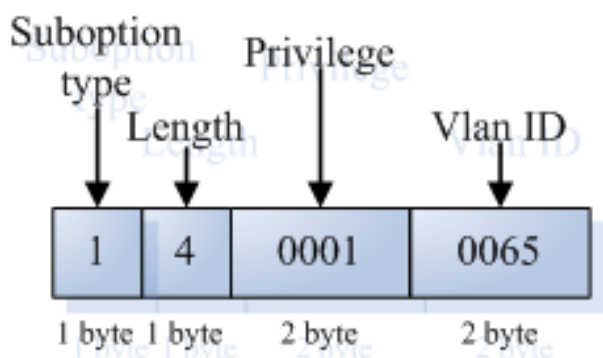
VLAN 10 and VLAN 20 correspond to the networks of 10.0.0.1/16 and 20.0.0.1/16 respectively while the DHCP server is at 30.0.0.1/16. To enable the DHCP server at 30.0.0.2 to dynamically manage the IP addresses at 10.0.0.1/16 and 20.0.0.1/16, just enable the DHCP relay function on the device which serves as a gateway and configure 30.0.0.2 as the IP address of the DHCP server.

## Understanding DHCP Relay Agent Information (option 82)

According to the definition of RFC3046, when a relay performs the DHCP relay, by adding an option, you can show in details some network information about the DHCP client so as to enable the server to assign users IP addresses with different privileges based on more accurate information. According to the definition of RFC3046, the number of the option used is 82, hence the option is called option 82. Currently, there are three application solutions of the relay agent information realized by Ruijie Network, which are described below:

- relay agent information option dot1x: this application requires the support from 802.1x authentication and Ruijie's network product RG-SAM. The DHCP relay integrates the sub-option of Circuit ID based on the IP privilege issued by the RG-SAM during the 802.1x authentication and the vid of the DHCP client. The format of the option is shown below:

Figure 1-3



- relay agent information option82: this application can run without the support from other protocol modules. The DHCP relay integrates the option 82 based on the physical port receiving the DHCP request packets and its own physical address information. The format of the option is shown in Figure 1-4 below:

Figure 1-4 Agent Circuit ID

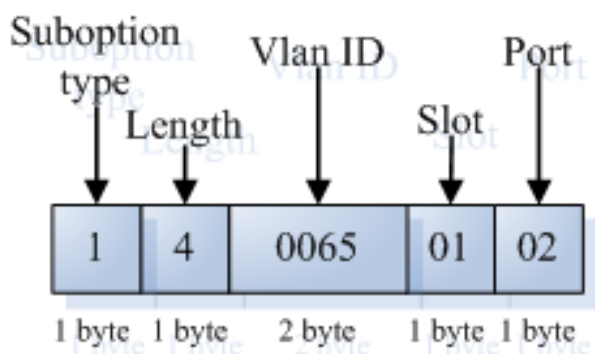
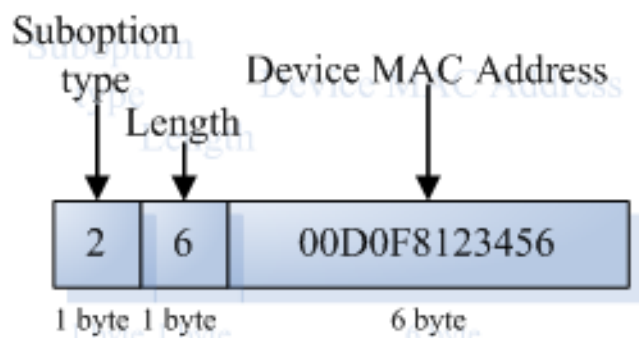


Figure 1-5 Agent Remote ID



## Understanding the Function of DHCP relay Check Server-id

In the application environment of DHCP, each network is usually provided with several DHCP servers for backup to ensure the availability of the network even when a server is not working properly. In the four interactions of DHCP acquirement, if a DHCP client has selected a server when sending the DHCP REQUEST, the request packet will carry an option of server-id. In some special application scenarios, in order to relieve the pressure on the network server, the relay needs to enable this option to send the request packet to the DHCP server under this option instead of every DHCP server configured. This is the function of DHCP relay check server-id.

## Configuring DHCP

To configure DHCP, perform the following tasks, of which the first three tasks are mandatory.

- Enabling the DHCP Server and the DHCP Relay Agent (required)
- Configuring DHCP Excluded Addresses (required)
- Configuring DHCP Address Pool (required)
- Configuring CLASS (Optional)
- Configuring database binding for storage (optional)
- Binding Address Manually (optional)
- Configuring the Ping Times (optional)
- Configuring Ping Packet Timeout (optional)

## Enabling the DHCP Server

To enable the DHCP server, execute the following commands in global configuration mode:

Command	Function
Ruijie(config)# <b>service dhcp</b>	Enable the DHCP server and the DHCP relay agent.
Ruijie(config)# <b>no service dhcp</b>	Disable the DHCP server and the DHCP relay agent.

- 
- ☒ By default, in v10.1 and later, the command **service dhcp** can be used for both DHCP server and DHCP relay, which are two mutually-exclusive functions. The switchover of those two functions depends on whether the DHCP address pool is configured or not.
-

- ✓ However, for the product in the version prior to v10.1(excluding v10.1), the command **service dhcp** is not supported by both DHCP server and DHCP relay. You can use the command **service dhcp** to enable the DHCP service or the DHCP server.
- ✓ For some product in v10.1 and later, DHCP may conflict with some functions. For the details, see the prompting message of specific product.

## Configuring DHCP Excluded Addresses

Unless configured particularly, the DHCP server tries to assign all the subnet addresses defined in the address pool to the DHCP clients. If you want to reserve some addresses, such as those that have been assigned to servers or devices, you must define clearly that these addresses cannot be assigned to the DHCP clients.

To configure the addresses that cannot be assigned to the DHCP clients, execute the following commands in global configuration mode:

Command	Function
Ruijie(config)# <b>ip dhcp excluded-address</b> <i>low-ip-address [ high-ip-address ]</i>	Define a range of IP addresses that the DHCP server will not assign to the DHCP clients.
Ruijie(config)# <b>no ip dhcp excluded-address</b> <i>low-ip-address [ high-ip-address ]</i>	Remove the configuration.



### Note

A good practice in configuring the DHCP server is to prohibit the DHCP server from assigning any address that has been assigned specifically. This provides two advantages: 1) No address conflict will occur; 2) When DHCP assigns addresses, the time for detection is shortened and thus DHCP will perform assignment more efficiently.

## Configuring DHCP Address Pool

Both DHCP Address assignment and DHCP parameters sent to the client should be defined in the DHCP address pool. If no DHCP address pool is configured, addresses cannot be assigned to the DHCP clients even though the DHCP server has been enabled. However, if the DHCP server has been enabled, the DHCP relay agent is always working regardless of the DHCP address pool.

You can give a meaningful name that can be memorized easily to the DHCP address pool. The name of address pool contains characters and digits. Ruijie product allows you to define multiple address pools. The IP address of the DHCP relay agent in the DHCP request packet is used to determine which address pool is used for address assignment.

- If a DHCP request packet contains no IP address of relay agent, the address will be assigned according to the segment range of the interface receiving request packets. The logic of assignment is that, if an address pool of a large segment scope is configured, addresses can be assigned for the request packets received by the small segment interfaces within the large address pool segment scope. For example, if the large address pool configured is 192.168.0.0/16, it can be used for assigning addresses to the DHCP requests arriving at the small segment interfaces of 192.168.1.0/24, 192.168.2.0/24 and 192.168.4.0/24. If multiple address pools of small segments are configured, these pools can assign addresses to the request packets arriving at the large segment interface covering the small segments. For example, the two small address pools: 192.168.1.0/24 and

192.168.3.0/24, can assign addresses to the DHCP requests arriving at the interface of 192.168.0.0/16. If the minimum match between the segment range of the interface receiving request packets and the segment range of the address pool is unsuccessful, the address assignment fails.

- If the DHCP request packet contains the IP address of the DHCP relay agent, the address that is in the same subnet or network as this address is assigned to the DHCP client. If no address pool is defined for this network segment, address assignment fails.

To configure a DHCP address pool, perform the following tasks as appropriate, of which the first three tasks are mandatory:

- Configure an address pool name and enter its configuration mode (required)
- Configure a subnet and its mask for the address pool (required)
- Configure the default gateway for the DHCP client (required)
- Configure the address lease period (optional)
- Configure the startup server and file of the client (optional)
- Configure the domain name of the DHCP client (optional)
- Configuring the domain name server (optional)
- Configure the NetBIOS WINS server (optional)
- Configure the NetBIOS node type for the DHCP client (optional)
- Configure the address pool to assign addresses as per Option 82 (optional)
- Configure the alarm threshold of the address pool utilization (optional)

### Configuring an Address Pool Name and Enter Its Configuration Mode

To configure an address pool name and enter address pool configuration mode, execute the following command in global configuration mode:

Command	Function
Ruijie(config)# <b>ip dhcp pool</b> <i>dhcp-pool</i>	Configuring an address pool name and enter address pool configuration mode
Ruijie(config)# <b>no ip dhcp pool</b> <i>dhcp-pool</i>	Deleting the configured address pool named dhcp-pool

### Configuring the Address Pool Network Number and Mask

To configure dynamic address binding, the subnet and its mask of the new address pool must be configured to provide the DHCP server with an address space that can be assigned to clients. Unless there is address exclusion configuration, the addresses in all the address pools can be assigned to clients. DHCP assigns addresses in the address pool in order. If an address exists in the DHCP binding table or is detected to have existed in the segment, the next address will be checked until a valid address is assigned.

Execute the following commands in address pool configuration mode to configure the subnet and mask of an address pool:

Command	Function
Ruijie(dhcp-config)# <b>network</b> <i>network-number mask</i>	Configure the network number and mask of a DHCP address pool



## Configuring the Default Gateway for the DHCP Client

When Ruijie's devices assign DHCP addresses, default gateways to be issued to clients can be either specified manually or assigned dynamically.

- If the default gateway of the address pool is specified manually, the gateway address manually specified is the default gateway of the client when a lease is obtained from the corresponding address pool.
- If no default gateway is configured, the default address type dynamically assigned is determined based on whether the VRRP address is configured to the interface that receives packets. If the VRRP address has been configured, the gateway is selected based on whether the request packets carry the field "relay". If the request packet is forwarded by the relay, the segment of the field "relay" is used as the default gateway to issue; otherwise, the interface address selected by the longest match principle is the gateway to be issued.

To configure the default gateway for the DHCP client, execute the following command in address pool configuration mode:

Command	Function
Ruijie(dhcp-config)# <b>default-router</b> <i>address</i> [ <i>address2...address8</i> ]	Configure the default gateway.

## Configuring the Address Lease Period

The lease period of the addresses assigned to clients by the DHCP server is infinite for static address pools, and 1 day for other address pools, by default. The client should request to renew when the lease period is going to expire. Otherwise, it cannot use this address when the lease period expires.

To configure the address lease period, execute the following command in address pool configuration mode:

Command	Function
Ruijie(dhcp-config)# <b>lease</b> { <i>days</i> [ <i>hours</i> ] [ <i>minutes</i> ]   <b>infinite</b> }	Configure the address lease period.

Configure the startup server and boot file of the client The client startup file is the boot image file that is used for client startup. Usually, after obtaining an IP address from the DHCP server, the DHCP client will download the boot image file from the startup server (usually the TFTP server) and initialize the device using the obtained configuration file. If no configuration file information is obtained, the device will be started up with the empty configuration.

Execute the following commands in address pool configuration mode to configure the download server and boot file of a client:

Command	Function
Ruijie (dhcp-config)# <b>next-server</b> <i>address</i> [ <i>address2...address8</i> ]	Configure the download server address for client startup
Ruijie (dhcp-config)# <b>bootfile</b> <i>filename</i>	Configure the client boot file name

## Configuring the Domain Name of the DHCP Client

The domain name of the DHCP client can be specified. In this way, the domain name suffix will be automatically added to the incomplete host name to form a complete host name when the DHCP client accesses the network resources using the host name.

To configure the domain name of the DHCP client, execute the following command in address pool configuration mode:

Command	Function
Ruijie(dhcp-config)# <b>domain-name</b> <i>domain</i>	Configure the domain name.

## Configuring the Domain Name Server

A DNS server should be specified for domain name resolution when the DHCP client accesses the network resources using a host name. To configure a domain name server for the DHCP client, execute the following command in address pool configuration mode:

Command	Function
Ruijie(dhcp-config)# <b>dns-server</b> <i>address</i> [ <i>address2...address8</i> ]	Configure a DNS server.

## Configuring the NetBIOS WINS Server

WINS is a domain name resolution service from Microsoft that the TCP/IP network uses to resolve a NetBIOS name to an IP addresses. The WINS server runs in Windows NT. After started, the WINS server will receive a registration request from the WINS client. When the WINS client is being shut down, it will send a name release message to the WINS server to guarantee the consistency of available computers between the WINS database and the network.

To configure a NetBIOS WINS server for the DHCP client, execute the following command in address pool configuration mode:

Command	Function
Ruijie(dhcp-config)# <b>netbios-name-server</b> <i>address</i> [ <i>address2...address8</i> ]	Configure a DNS server.

## Configuring the NetBIOS Node Type for the DHCP Client

There are four types of NetBIOS nodes for Microsoft DHCP client: Broadcast. The NetBIOS name is resolved in the broadcast mode; Peer-to-peer. The WINS server is asked directly to resolve the NetBIOS name; Mixed. First, the name is resolved in the broadcast mode, and then the WINS server is connected to resolve the name; Hybrid. First the WINS server is asked directly to resolve the NetBIOS name. If there is no response, the NetBIOS name is resolved in the broadcast mode.

By default, the Windows operation systems support broadcast or hybrid type NetBIOS nodes. If no WINS server is configured, the node is of broadcast type. If a WINS server is configured, the node is of hybrid type.

To configure the NetBIOS node type for the DHCP client, execute the following command in address pool configuration mode:

Command	Function
---------	----------

Command	Function
Ruijie(dhcp-config)# <b>netbios-node-type</b> <i>type</i>	Configure the NetBIOS node type.

## Configuring DHCP Address Pool to Allocate Address as per Option82

Generally, the DHCP relay agent will insert an option of "Option 82" to carry relevant information about the client during the process of packet forwarding (such as the VLAN to which the client belongs, slot number, port number or user's 1X class). Upon receipt of such packets, the DHCP server will allocate addresses according to the specific information about clients by analyzing Option 82 information. For example, Option 82 can be utilized to allocate a certain range of IP addresses to clients belonging to a certain VLAN or user class. This feature can be used when it is needed to allocate a specific range of IP addresses according to user's network allocation information (such as VLAN, slot number or port number) or user's priority.

Each DHCP address pool can allocate addresses using Option 82 information. Option 82 information will be matched and classified, and we can specify the allocable address range for the corresponding class. One DHCP address pool can be associated with multiple classes, and different address ranges can be specified for each class.

During the process of address allocation, we can first determine the allocable address pool according to the network segment to which the client belongs, and then further determine its CLASS according to Option 82 information, so as to allocate IP address from the address range corresponding to the CLASS. When a request packet matches multiple classes in the address pool, address will be allocated from the address ranges corresponding to these classes in the order that the classes are configured in the address pool. If the class has not allocable address, the address range for next matching class will be used, and the like. Each class corresponds to one address range, and the addresses must be allocated from low to high. Multiple classes can be configured with the same address range. If the CLASS associated with the address pool is specified, but the segment range of the CLASS is not configured, the DHCP clients of this CLASS cannot be assigned addresses..

To configure the CLASS associated with address pool and the address range corresponding to the class, execute the following commands in address pool configuration mode:

Command	Function
Ruijie(dhcp-config)# <b>class</b> <i>class-name</i>	Configure the name of associated class, and enter class configuration mode of address pool.
Ruijie(config-dhcp-pool-class)# <b>address range</b> <i>low-ip-address high-ip-address</i>	Configure the corresponding address range.



### Note

When the class configured cannot be found in global class, a global class will be created automatically; The associated class configured in the address pool may conflict with the static manual binding, and therefore must not be configured at the same time. Up to 5 classes can be configured for each address pool

## Configuring the alarm threshold of the address pool utilization

You can configure the generation of the SYSLOG alarm information when the highest IP address utilization reaches the threshold on the DHCP server. The IP utilization is the ratio of the number of assigned addresses to the total addresses in the current address pool that can be assigned. If the number of assigned addresses keeps above the alarm threshold,

the alarm information will be generated every five minutes. When the IP utilization of the address pool is one hundred percent, meaning that the current address pool has been used up, the DHCP server will send the Trap message on the use-up of address pool to the gateway server. When the address pool is no longer in the status of use-up, the Trap message on removing the use-up information of address pool will be sent so that the network administrator can know the use of the address pool in time.

Execute the following commands in address pool configuration mode to configure the alarm function of address pool:

Command	Function
Ruijie(dhcp-config)# <b>lease-threshold</b> <i>percentage</i>	Configuring the alarm threshold of address pool Percentage: 60-100; 90 by default.



#### Note

The factors affecting the total addresses in the current address pool that can be assigned include: the segment range dependent on the network number of the address pool and its mask; the excluded addresses configured by the network administrator that belong to the current address pool; and the IP address that is configured as an interface address.



#### Note

To enable the DHCP server to send the Trap message on the use-up of address pool to the gateway server, the Trap-related functions must be enabled first.

## Configuring Class

### Configuring Option82 Matching Information for CLASS

The specific Option82 matching information corresponding to each CLASS can be configured after entering CLASS configuration mode in global mode. One CLASS can match multiple Option 82 information, and it is considered matched if the packet matches any information. If no matching information is configured for CLASS, then this CLASS can match any request packets carrying Option 82 information. The address can only be allocated from the corresponding address pool after the request packet matches a specific CLASS.

To configure global CLASS and the Option 82 information corresponding to the CLASS, execute the following commands in global configuration mode:

Command	Function
Ruijie(config)# <b>ip dhcp class</b> <i>class-name</i>	Configure CLASS name and enter global CLASS configuration mode.
Ruijie(config-dhcp-class)# <b>relay agent information</b>	Enter Option 82 matching information configuration mode.
Ruijie(config-dhcp-class-relayinfo)# <b>relay-information</b> <b>hex</b> <i>aabb.ccdd.eeff... [*]</i>	Configure specific Option 82 matching information. Aabb.ccdd.eeff.. is a hexadecimal number * means imperfect matching mode. It is considered matched if the information before * is matched.



#### Note

Global CLASS can have up to 20 matches.

## Configuring Remark Information for CLASS

To configure remark information to describe the meaning of CLASS, execute the following commands in global configuration mode:

Command	Function
Ruijie(config)# <b>ip dhcp class</b> <i>class-name</i>	Configure CLASS name and enter CLASS configuration mode.
Ruijie(config-dhcp-class)# <b>remark</b> <i>used in #1 building</i>	Configure remark information.

## Configuring whether or not to use CLASS Allocation

To configure address allocation using CLASS, execute the following commands in global configuration mode:

Command	Function
Ruijie(config)# <b>ip dhcp use class</b>	Configure address allocation using CLASS.



**Caution** This command is enabled by default. Execute NO command to disable address allocation using CLASS.

## Configuring Binding Database Storage

### Configuring to periodically Save Binding Database into FLASH

To avoid the loss of binding database (lease information) on DHCP server due to power failure or reboot of device, you can configure the delay time to write the database into FLASH. The time is 0 by default, namely the database will be written into FLASH at variable intervals.

To periodically write the binding database into the FLASH, execute the following command in global configuration mode:

Command	Function
Ruijie(config)# <b>[no] ip dhcp database write-delay</b> <i>[time]</i>	Configure DHCP delay time to write into FLASH. <i>Time:600s--86400s (default: 0)</i>



**Caution** Since frequent FLASH reading and writing will shorten the service life of FLASH, we shall pay attention to the delay time configured. Short delay time will enable efficient storage of device information, while long delay time can reduce the frequency of FLASH reading and writing, thus providing a longer service life.

### Configuring to manually Save Binding Database into FLASH

To avoid the loss of DHCP binding database (lease information) due to power failure or reboot of device, you can also manually write the existing binding database information into the FLASH as needed besides configuring the delay time for FLASH writing.

To manually write the binding database into the FLASH, execute the following command in global configuration mode:

Command	Function
Ruijie(config)# <b>ip dhcp database write-to-flash</b>	Write DHCP binding database information into the FLASH

## Manual Address Binding

Address binding refers to the IP address to MAC address mapping for the DHCP clients. You can bind addresses in two ways. 1 Manual binding: Configure the static IP address to MAC address mapping for the DHCP client on the DHCP server manually. Manual binding actually offers a special address pool; 2 Dynamic binding: Upon receiving a DHCP request from the DHCP client, the DHCP server dynamically assigns an IP address from the DHCP address pool to the DHCP client, and thus mapping the IP address to the MAC address for the DHCP client.

To define manual address binding, you first need to define a host address pool for each manual binding, and then define the IP address and hardware address (MAC address) or ID for the DHCP client. Generally, a client ID instead of a MAC address, is defined for the Microsoft clients. The client ID contains media type and MAC address. For the codes of media types, refer to Address Resolution Protocol Parameters in RFC 1700. The code of Ethernet type is "01".

To configure the manual address binding, execute the following commands in address pool configuration mode:

Command	Function
Ruijie(config)# <b>ip dhcp pool</b> <i>name</i>	Define the name of the DHCP address pool and enter DHCP configuration mode.
Ruijie(dhcp-config)# <b>host</b> <i>address</i> [ <i>netmask</i> ]	Define an IP address for the DHCP client.
Ruijie(dhcp-config)# <b>hardware-address</b> <i>hardware-address type</i> or: Ruijie(dhcp-config)# <b>client-identifier</b> <i>unique-identifier</i>	Define a hardware address for the DHCP client, such as aabb.bbbb.bb88 type is the type of client media.  Define an ID for the DHCP client, such as 01aa.bbbb.bbbb.88
Ruijie(dhcp-config)# <b>client-name</b> <i>name</i>	(Optional) Define the client name using standard ASCII characters. Don't include domain name in the client name. For example, if you define the mary host name, do not define as mary.rg.com



### Caution

Before configuring the reserved manually bound addresses, set the pre-configured addresses as excluded addresses to ensure that these addresses will not be dynamically assigned.

## Configuring Ping Times

By default, when trying to assign an IP address from the DHCP address pool to a DHCP client, the DHCP server will ping the IP address twice (one packet for each time). If there is no response, the DHCP server considers this address an idle address and assigns it to the DHCP client. If there is a response, the DHCP server considers that this address is in use and tries to assign another address to the DHCP client until an address is assigned successfully.

To configure the number of Ping packets, execute the following commands in global configuration mode:

Command	Function
Ruijie(config)# <b>ip dhcp ping packets</b> <i>number</i>	Configure the number of Ping packets before the DHCP server assigns an address. If it is set to 0, the Ping operation is not performed. The default value is 2.

## Configuring Ping Packet Timeout

By default, the DHCP server considers the IP address inexistent if it has not received a response within 500 milliseconds after pinging an IP address. You can adjust the Ping packet timeout.

To configure the Ping packet timeout, execute the following commands in global configuration mode:

Command	Function
Ruijie(config)# <b>ip dhcp ping timeout</b> <i>milliseconds</i>	Configure the Ping packet timeout for the DHCP server. The default value is 500ms.

## Configuring the forcible NAK sending

Whenever the device starts up, the DHCP client checks the IP address used previously and sends the DHCPREQUEST packet for renewal, expecting to use the IP address again. As per the RFC2131 protocol, if the IP address has timed out or is unavailable (e.g. the client segment has changed or the IP address has been configured as an excluded address), the DHCP server shall respond with an NAK to make the DHCP client send a DHCPDISCOVER packet, applying for a new IP address.

Execute the following commands in global configuration mode to configure the forcible NAK sending:

Command	Function
Ruijie(config)# <b>ip dhcp force-send-nak</b>	Enable the forcible NAK packet sending
Ruijie(config)# <b>no ip dhcp force-send-nak</b>	Disable the forcible NAK packet sending



### Caution

The function of forcible NAK sending is mainly applied in the wireless deployment scenario. As the movement of users often causes segment switch in such scenario, the function will accelerate the application for a new segment IP address.



### Caution

When there are more than one DHCP servers in the network, this function must be used cautiously. When four packet interactions for DHCP to obtain an address is at the DHCPREQUEST stage, if another DHCP server that is not selected in DHCP OFFER receives a broadcast REQUEST, sending NAK forcibly will disturb the normal address acquisition of the DHCP client and lead to failure of the address assignment.

## Configuring the VRRP status monitoring

In the scenario of VRRP (Virtual Router Redundancy Protocol) application, DHCP provides configuration commands to determine whether to monitor the VRRP status of the current interface. For an interface configured with a VRRP

address, when the VRRP status monitoring is configured, the DHCP server will only process the DHCP client request packets from the device interfaces in the MASTER status, and discard the request packets from the interfaces in the BACKUP status. For an interface not configured with a VRRP address, the DHCP server will not monitor the VRRP status and all the DHCP request packets will be processed. The command of VRRP monitoring can only be configured on a layer-3 interface. The VRRP monitoring function is enabled by default.

Execute the following commands in layer-3 interface configuration mode to configure the function of VRRP status monitoring by the DHCP:

Command	Function
Ruijie(config-if)# <b>[no] ip dhcp monitor-vrrp-state</b>	Configure the packet processing based on the VRRP status. The function is enabled by default.

## Configuring the DHCP Client

Ruijie's products currently allows to configure the DHCP client on Ethernet interfaces, and FR, PPP and HDLC encapsulation links to acquire IP addresses and other configuration parameters from the DHCP server automatically.

- Configuring the DHCP client on the Ethernet interface (optional)
- Configuring the DHCP client on the PPP encapsulation link (optional)
- Configuring the DHCP client on the FR encapsulation link (optional)
- Configuring the DHCP client on the HDLC encapsulation link (optional)
- Configuring the DHCP client in the wireless application environment (optional)

### Configuring the DHCP Client on the Ethernet Interface

- 
- ☒ Ruijie products support obtaining the IP address dynamically assigned by the DHCP server on an Ethernet interface.
- 

To configure the DHCP client on the Ethernet port, execute the following command in interface configuration mode:

Command	Function
Ruijie(config-if)# <b>ip address dhcp</b>	Obtain an IP address through DHCP.

### Configuring the DHCP Client in the PPP Encapsulation Link

Ruijie products support obtaining the IP addresses dynamically assigned by the DHCP server on a PPP encapsulation interface.

To configure the DHCP client, execute the following command in interface configuration mode:

Command	Function
Ruijie(config-if)# <b>ip address dhcp</b>	Obtain an IP address through DHCP.

### Configuring the DHCP Client in the FR Encapsulation Link

- 
- ☒ Ruijie products support obtaining the IP addresses dynamically assigned by the DHCP server on an FR encapsulation interface.
- 

To configure the DHCP client, execute the following command in interface configuration mode:



Command	Function
Ruijie(config-if)# <b>ip address dhcp</b>	Obtain an IP address through DHCP.

## Configuring the DHCP Client in the HDLC Encapsulation Link

- ☒ Ruijie products support obtaining the IP address dynamically assigned by the DHCP server on an HDLC encapsulation interface.

To configure the DHCP client, execute the following command in interface configuration mode:

Command	Function
Ruijie(config-if)# <b>ip address dhcp</b>	Obtain an IP address through DHCP.

- ☒ For some product in v10.1, DHCP client supports obtaining the IP address assigned by the DHCP server in the point-to-point link of PPP, HDLC, FR encapsulation.

## Configuring the DHCP client in the wireless application environment (optional)

Ruijie's wireless products allow an AP to obtain the IP address of an AC device through the DHCP option by configuring the DHCP option mode on the AC device. The supported DHCP option modes include the standard and the private modes. By default, the standard mode is adopted. The standard modes uses the options of CAPWAP AC DHCPv4(Option 138) and CAPWAP AC DHCPv6(Option 52); and the private modes uses Option 43 (Vendor Specific Information) and Option 60 (Vendor class identifier).

Perform the following steps to configure the DHCP option modes:

Command	Function
Ruijie(config)# <b>ap-config AP0001</b>	Enter AP0001 Configuration Mode
Ruijie(config-ap)# <b>ip dhcp capwap option private</b>	Enable AP001 to use the private DHCP option mode to obtain an AC address
Ruijie(config-ap)# <b>ip dhcp capwap option standard</b>	Enable AP001 to use the standard DHCP option mode to obtain an AC address



### Note

Refer to the definition of RFC 5417 for the format definitions of Option 138 and Option 52.



### Note

Refer to the definition of RFC 2132 for the format definitions of Option 43 and Option 60.



### Note

Ruijie's wireless AP products can analyze the Option 43 returned by the server in the TLV format as shown below:

Type --- 0xf1

Length --- number of IP addresses of the AC \* 4

Value --- IP address list of the AC, which is saved by the hexadecimal system

**Note**

By default, the standard mode is adopted to obtain the AC address.

**Note**

For external DHCP servers (i.e. Windows/Linux/SunOS's own DHCP server), only the private mode is supported for the DHCP client to obtain the AC address. For built-in DHCP servers (i.e. enabled DHCP server function on the network devices from network vendors), both the standard and the private modes are supported for the DHCP client to obtain the AC address by configuring customized options.



The above configuration is only supported by Ruijie's wireless products.

## Configuring the DHCP Relay

### Enabling the DHCP relay agent

Perform the following steps in global configuration mode to configure the DHCP relay agent:

Command	Function
Ruijie (config)# <b>service dhcp</b>	Enable the DHCP agent
Ruijie(config)# <b>no service dhcp</b>	Disable the DHCP agent

### Configuring the IP address of the DHCP server

After the IP address of a DHCP server is configured, the device will forward the DHCP request packets to the server, at the same time, it will forward the DHCP server's response packets to the DHCP client.

The IP address of the DHCP server can be configured globally or on a layer-3 interface. Up to 20 DHCP server addresses can be configured globally or on each layer-3 interface. When a DHCP request packet is received on an interface, the DHCP server list on the interface will be used first; if no DHCP server list is configured on the interface, the DHCP server list configured globally will be used.

Perform the following steps to configure a DHCP server address:

Command	Function
Ruijie(config)# <b>ip helper-address [global] A.B.C.D</b>	Add a global DHCP server address to display the VPN.
Ruijie(config-if)# <b>ip helper-address [global] A.B.C.D</b>	Add a DHCP server address of an interface. This command must be configured on a layer-3 interface. to display the VPN or the global space the specified server belongs to. By default, it shares the VPN or global space with the current interface.
Ruijie(config)# <b>no ip helper-address [global] A.B.C.D</b>	Delete a global DHCP server address
Ruijie(config-if)# <b>no ip helper-address [global] A.B.C.D</b>	Delete a DHCP server address of an interface

## Configuring the DHCP option dot1x

According to the description of the DHCP Relay Agent Information, when IPs of different privileges are assigned to users based on their different privileges, the function of option dot1x of the DHCP relay can be enabled with the command **ip dhcp relay information option dot1x**. When a device forwards the DHCP request packet as a DHCP relay, it adds the option information in the DHCP request packet with the support of 802.1x. This function is performed in combination of the function of dot1x.

Perform the following steps in global configuration mode to configure the DHCP option dot1x:

Command	Function
Ruijie(config)# <b>ip dhcp relay information option dot1x</b>	Enable the function of DHCP option dot1x
Ruijie(config)# <b>no ip dhcp relay information option dot1x</b>	Disable the function of DHCP option dot1x

## Configuring DHCP option dot1x access-group

In the application of the option dot1x, the device needs to limit the privilege of unauthenticated or low-privilege IPs to access some specific IP addresses, and restrict the mutual access between low-privilege users. This can be achieved through the command **ip dhcp relay information option dot1x access-group acl-name**. The ACL defined by *acl-name* must be pre-configured to filter some contents, mainly, to prohibit the mutual access between unauthenticated users. In addition, the ACL associated is applied to all the ports, and the ACL has no default ACE and does not conflict with the ACLs associated with other interfaces. For example:

Assign a category of IP addresses to all unauthenticated users, which is 192.168.3.2-192.168.3.254, 192.168.4.2-192.168.4.254, 192.168.5.2-192.168.5.254; and 192.168.3.1, 192.168.4.1 and 192.168.5.1 are used as gateway addresses and not assigned to users. Then users use 192.168.3.x-5.x to access the web portal to download the client software. Therefore, the configuration on the device is required as follows:

```
Ruijie# configure terminal
Ruijie(config)# ip access-list extended DenyAccessEachOtherOfUnauthrize
Ruijie(config-ext-nacl)# permit ip any host 192.168.3.1
```

// permit the packets sent to the gateway

```
Ruijie(config-ext-nacl)# permit ip any host 192.168.4.1
Ruijie(config-ext-nacl)# permit ip any host 192.168.5.1
Ruijie(config-ext-nacl)# permit ip host 192.168.3.1 any
```

// permit the packets sent from the gateway

```
Ruijie(config-ext-nacl)# permit ip host 192.168.4.1 any
Ruijie(config-ext-nacl)# permit ip host 192.168.5.1 any
Ruijie(config-ext-nacl)# deny ip 192.168.3.0 0.0.0.255 192.168.3.0 0.0.0.255
```

// prohibit mutual access between unauthenticated users

```
Ruijie(config-ext-nacl)# deny ip 192.168.3.0 0.0.0.255 192.168.4.0 0.0.0.255
Ruijie(config-ext-nacl)# deny ip 192.168.3.0 0.0.0.255 192.168.5.0 0.0.0.255
Ruijie(config-ext-nacl)# deny ip 192.168.4.0 0.0.0.255 192.168.4.0 0.0.0.255
```

```
Ruijie(config-ext-nacl)# deny ip 192.168.4.0 0.0.0.255 192.168.5.0 0.0.0.255
Ruijie(config-ext-nacl)# deny ip 192.168.5.0 0.0.0.255 192.168.5.0 0.0.0.255
Ruijie(config-ext-nacl)# deny ip 192.168.5.0 0.0.0.255 192.168.3.0 0.0.0.255
Ruijie(config-ext-nacl)# deny ip 192.168.5.0 0.0.0.255 192.168.4.0 0.0.0.255
Ruijie(config-ext-nacl)# exit
```

Apply the command **ip dhcp relay information option dot1x access-group DenyAccessEachOtherOfUnauthorize** to the global interface. Perform the following steps in global configuration mode to configure the **DHCP option dot1x access-group**:

Command	Function
Ruijie(config)# <b>ip dhcp relay information option dot1x access-group</b> <i>acl-name</i>	Apply the DHCP option dot1x acl
Ruijie(config)# <b>no ip dhcp relay information option dot1x access-group</b> <i>acl-name</i>	Undo the application of the DHCP option dot1x acl

## Configuring the DHCP option 82

When configuring the command **ip dhcp relay information option82**, the device serves as a DHCP relay to add the option information in the DHCP request packet when forwarding such packet.

Perform the following steps in global configuration mode to configure the DHCP option82:

Command	Function
Ruijie(config)# <b>ip dhcp relay information option82</b>	Enable the function of DHCP option 82
Ruijie(config)# <b>no ip dhcp relay information option82</b>	Disable the function of DHCP option 82

## Configuring the DHCP relay check server-id

After the command **ip dhcp relay check server-id** is configured, the DHCP relay will only forward the DHCP request packets to the server specified in option server-id. If the command is not configured, the DHCP relay will forward the DHCP request packets to all configured DHCP servers.

Perform the following steps in global configuration mode to configure the **DHCP relay check server-id**:

Command	Function
Ruijie(config)# <b>ip dhcp relay check server-id</b>	Enable the function of DHCP relay check server-id
Ruijie(config)# <b>no ip dhcp relay check server-id</b>	Disable the function of DHCP relay check server-id

## Configuring the DHCP relay suppression

After the command **ip dhcp relay suppression** is configured on a specified interface, the DHCP request packets received on the interface will be blocked; and the DHCP request packets received on other interfaces will be forwarded.

Perform the following steps in global configuration mode to configure the **ip dhcp relay suppression**:

Command	Function
Ruijie(config-if)# <b>ip dhcp relay suppression</b>	Enable the function of DHCP relay suppression
Ruijie(config-if)# <b>no ip dhcp relay suppression</b>	Disable the function of DHCP relay suppression

---

## Other cautions for configuring the DHCP relay

---

**Note**

For layer-2 network devices, one of the functions of option dot1x, dynamic address binding or option 82 must be enabled if the cross-segment management of VLAN's DHCP relay can be performed; otherwise, only the management of VLAN's relay can be performed on the layer-2 devices.

---

## Cautions for configuring the DHCP option dot1x

---

**Caution**

This command will only take effect when the AAA/802.1x-related configuration is correct.

**Caution**

The IP authorization of in DHCP mode of the 802.1x must be enabled if this solution is applied.

**Caution**

This command and the DHCP option 82 are mutually excluded, thus cannot be used simultaneously.

**Caution**

Where the IP authorization in the DHCP mode of the 802.1x, the MAC + IP binding is set as well, then it cannot be enabled when the DHCP dynamic binding is enabled at the same time.

---

## Cautions for configuring the DHCP option 82

---

**Caution**

The functions of DHCP option 82 and dhcp option dot1x are mutually excluded, thus cannot be used simultaneously.

---

## DHCP configuration examples

The following commands enable the function of DHCP relay and add two sets of server addresses:

```
Ruijie# configure terminal
Ruijie(config)# service dhcp           // enable the DHCP relay
Ruijie(config)# ip dhcp relay information option82 // enable the DHCP option82
Ruijie(config)# ip helper-address 192.18.100.1 // add a global server address
Ruijie(config)# ip helper-address 192.18.100.2
Ruijie(config)# interface GigabitEthernet 0/3
Ruijie(config)# ip helper-address 192.18.100.1 // add an interface server address
Ruijie(config-if)# ip helper-address 192.18.200.2
Ruijie(config-if)# end
```

## Monitoring and Maintenance Information

---

### Displaying the DHCP configuration

Use the command **show running-config** in the privileged mode to display the DHCP configuration.

```
Ruijie# show running-config
Building configuration...
Current configuration : 1464 bytes
version RGOS 10.1.00(1), Release(11758) (Fri Mar 30 12:53:11 CST 2007 -nprd
hostname Ruijie
vlan 1
ip helper-address 192.18.100.1
ip helper-address 192.18.100.2
ip dhcp relay information option dot1x
interface GigabitEthernet 0/1
interface GigabitEthernet 0/2
interface GigabitEthernet 0/3
no switchport
ip helper-address 192.168.200.1
ip helper-address 192.168.200.2
interface VLAN 1
ip address 192.168.193.91 255.255.255.0
line con 0
exec-timeout 0 0
line vty 0
exec-timeout 0 0
login
password 7 0137
line vty 1 2
```

```
login
password 7 0137
line vty 3 4
login
end
```

## Monitoring and Maintaining the DHCP Server

Three types of commands are available for monitoring and maintaining the DHCP server:

1. Clear commands, used to clear such information as DHCP address binding, address conflict and server statistics;
2. Debug commands, used to output necessary debugging information. Such commands are mainly used to diagnose and fix faults;
3. Show commands, used to show information about DHCP.

Ruijie products provide three clear commands. To clear information, execute the following commands in the command execution mode:

Command	Function
Ruijie# <b>clear ip dhcp binding</b> { address   * }	Clear the DHCP address binding information.
Ruijie# <b>clear ip dhcp conflict</b> { address   * }	Clear the DHCP address conflict information.
Ruijie# <b>clear ip dhcp server statistics</b>	Clear the DHCP server statistics.

To debug the DHCP server, execute the following command in the command execution mode:

Command	Function
Ruijie# <b>debug ip dhcp server</b> [events   packet]	Debug the DHCP server.

To show the working status of the DHCP server, execute the following commands in the command execution mode:

Command	Function
Ruijie# <b>show ip dhcp binding</b> [address]	Show the DHCP address binding information.
Ruijie# <b>show ip dhcp conflict</b>	Show the DHCP address conflict information.
Ruijie# <b>show ip dhcp server statistics</b>	Show the DHCP server statistics.

## Monitoring and Maintaining the DHCP Client

There are two types of commands for monitoring and maintaining the DHCP client. The following operations can be performed on the DHCP client:

1. Debug commands, used to output necessary debugging information. Such commands are mainly used to diagnose and clear faults.
2. Show commands, used to show information about DHCP.

To debug the DHCP client, execute the following command in the command execution mode:

Command	Function
Ruijie# <b>debug ip dhcp client</b>	Debug the DHCP client.

To show information about the lease that the DHCP client obtains, execute the following command in the command execution mode:

Command	Function
<code>show dhcp lease</code>	Show the information about DHCP lease.

## DHCP Configuration Examples

### Example of Configuring Address Pool to Support Option82

In the following example, an address pool of "net82" is defined; the address pool is in the network segment of 172.16.1.0/24, and the associated classes include class1, class2, class3 and class4. Class1 will allocate addresses from the range of 172.16.1.1-172.16.1.8; class2 will allocate addresses from the range of 172.16.1.9-172.16.1.18; class3 will allocate addresses from the range of 172.16.1.19-172.16.1.28; class4 has no defined address range, and will allocate addresses from the range of entire network segment. Configure class1 to match Option 82 information of 0100002120, class2 to match 0106020145, class3 to match 06020506\*, and class4 to match any information.

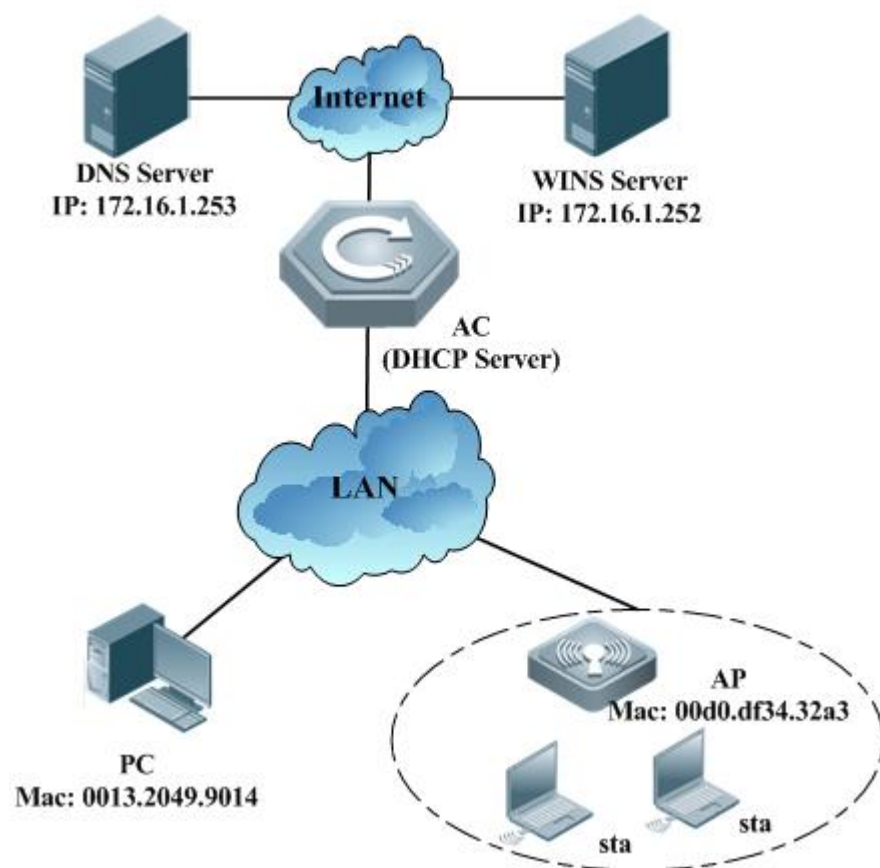
```
!  
ip dhcp class class1  
  relay agent information  
    relay-information hex 0100002120  
!  
ip dhcp class class2  
  relay agent information  
    relay-information hex 0106020145  
!  
ip dhcp class class3  
  relay agent information  
    relay-information hex 06020506*  
!  
ip dhcp class class4  
!  
ip dhcp pool net82  
network 172.16.1.0 255.255.255.0  
class class1  
address range 172.16.1.1 172.16.1.8  
class class2  
address range 172.16.1.9 172.16.1.18  
class class3  
address range 172.16.1.19 172.16.1.28  
class class4
```



## Typical DHCP Configuration Example

### Topological Diagram

Fig 1-6 Diagram of DHCP example



### Application Requirements

- An AC can serve as the DHCP server to assign dynamic IP addresses to some client users. The segment for IP address assignment is 172.16.1.0/24; the default gateway is 172.16.1.254; the domain name is ruijie.com; the domain name server is 172.16.1.253; the WINS server is 172.16.1.252; the NetBIOS node type is compound; and the address lease period is one day. Except the addresses of 172.16.1.2~172.16.1.100 in the address segment, all the other addresses can be assigned.
- The AC assigns fixed IP addresses to some client users. The IP address assigned to the fit AP (DHCP client) with the MAC address of 00d0.df34.32a3 is 172.16.1.101; the mask is 255.255.255.0; the domain name is admin; the default gateway is 172.16.1.254; the domain name server is 172.16.1.253; the WINS server is 172.16.1.252; and the NetBIOS node type is compound.
- The AP is configured as the fit mode; the DHCP auto-assign address is configured on the device interface FastEthernet 0/1; the capwap tunnel Sta is established with the AC to associate the AP; the addresses are assigned dynamically on the DHCP server of the AC.

## Configuration Tips

- Enable the function of DHCP server on the AC and create an address pool to dynamically assign IP addresses. And create another address pool to manually bind IP addresses. Specify the address of the domain name server in the corresponding address pool (in this example, the addresses of the DNS server and WINS server) and the domain name of the client.
- The AP is configured as the fit mode. It automatically obtains an address through the DHCP and establishes the capwap connection with the AC.

## Configuration Steps

Step 1: Create a new DHCP address pool and configure dynamic IP address allocation on the AC.

! Configure the name of address pool as "dynamic" and enter DHCP configuration mode.

```
AC# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
AC(config)# ip dhcp pool dynamic
```

! In DHCP configuration mode, configure an IP address network allocable to clients and configure the default gateway of this network segment. And set the lease period to two days.

```
AC(dhcp-config)# network 172.16.1.0 255.255.255.0
AC(dhcp-config)# default-router 172.16.1.254
AC(dhcp-config)# lease 2
```

Step 2: Specify the DNS Server of "dynamic" address pool and configure the domain name of client.

! Assuming that the IP address of DNS Server is 192.168.1.2, configure Domain Name Server in the address pool and configure the domain name of client as ruijie.com.

```
AC(dhcp-config)# dns-server 172.16.1.253
AC(dhcp-config)# domain-name ruijie.com
```

Step 3: Specify the WINS Server of "dynamic" address pool and configure the NetBIOS node type of client.

! Assuming that the IP address of WIN Server is 172.16.1.252, configure NetBIOS WINS server in the address pool and configure the NetBIOS node type as Hybrid.

```
AC(dhcp-config)# netbios-name-server 172.16.1.252
AC(dhcp-config)# netbios-node-type h-node
```

Step 4: Configure excluded addresses in global mode.

! As shown above, IP addresses of 172.16.1.254, 172.16.1.253 and 172.16.1.252 have been allocated to the gateway, DNS server and WINS server, and the address range of 172.16.1.2~172.16.1.100 are not allowed to be assigned. By configuring excluded addresses, these addresses won't be allocated to clients.

```
AC(dhcp-config)# exit
AC(config)# ip dhcp excluded-address 172.16.1.252 172.16.1.254
AC(config)# ip dhcp excluded-address 172.16.1.2 172.16.1.100
```

Step 5: Create another address pool and manually bind the IP address.

! Configure the name of address pool as "static" and enter DHCP configuration mode.

```
AC(config)# ip dhcp pool static
```

! Manually bind the IP address of 172.16.1.101/24 to the MAC address of 00d0.df34.32a3, with client name being "admin". Note: The identifier for identifying the client shall indicate the network media type ("01" for Ethernet), namely the identifier of the client corresponding to the manually bound MAC address shall be 0100.d0df.3432.a3.

```
AC(dhcp-config)# host 172.16.1.101 255.255.255.0
AC(dhcp-config)# client-identifier 0100.d0df.3432.a3
AC(dhcp-config)# client-name admin
```

Step 6: Specify the gateway address corresponding to the "static" address pool.

! Configure gateway address as 172.16.1.254.

```
AC(dhcp-config)# default-router 172.16.1.254
```

Step 7: Specify the DNS Server of "static" address pool and configure the domain name of client.

! Assuming that the IP address of DNS Server is 172.16.1.253, configure Domain Name Server in the address pool and configure the domain name of client as ruijie.com.

```
AC(dhcp-config)# dns-server 172.16.1.253
AC(dhcp-config)# domain-name ruijie.com
```

Step 8: Specify the WINS Server of "static" address pool and configure the NetBIOS node type of client.

! Assuming that the IP address of WIN Server is 172.16.1.252, configure NetBIOS WINS server in the address pool and configure the NetBIOS node type as Hybrid.

```
AC(dhcp-config)# netbios-name-server 172.16.1.252
AC(dhcp-config)# netbios-node-type h-node
AC(dhcp-config)# exit
```

Step 9: Enable DHCP Server on AC.

```
AC(dhcp-config)# exit
AC(config)# service dhcp
```

## Verification

Step 1: View the configuration information on the AC.

```
AC# show running-config
!
service dhcp
!
ip dhcp excluded-address 172.16.1.252 172.16.1.254
ip dhcp excluded-address 172.16.1.2 172.16.1.100
!
!
```

```

ip dhcp pool dynamic
 netbios-node-type H-node
 netbios-name-server 172.16.1.252
 domain-name ruijie.com
 lease 2 0 0
 network 172.16.1.0 255.255.255.0
 dns-server 172.16.1.253
 default-router 172.16.1.254
!
ip dhcp pool static
 client-name admin
 client-identifier 0100.d0df.3432.a3
 host 172.16.1.101 255.255.255.0
 netbios-node-type h-node
 netbios-name-server 172.16.1.252
 domain-name ruijie.com
 dns-server 172.16.1.253
 default-router 172.16.1.254
!

```

Step 2: View the configuration information on the AP.

```

Ruijie# show running-config
!
interface GigabitEthernet0/1
ip address dhcp

```

Step 3: Connect a PC with the MAC address of 0013.2049.9014, and view the IP address information assigned by the DHCP server on the AC.

```

Ruijie#show ip dhcp binding
IP address      Client-Identifier/      Lease expiration      Type
                Hardware address
172.16.1.101    0100.d0.df34.32a347.    000 days 23 hours 45 mins Manual
                6967.6162.6974.4574.
                6865.726e.6574.302f.
                31
172.16.1.102    0100.1320.4990.14      000 days 23 hours 48 mins Automatic

```

Step 4: Associate the STA with the MAC address of 0100.e04c.70b7.e2 with the AP, dynamically assign addresses from the DHCP server on the AC, and view the IP address information assigned by the DHCP server on the AC.

```

Ruijie#show ip dhcp binding
IP address      Client-Identifier/      Lease expiration      Type
                Hardware address
172.16.1.101    0100.d0.df34.32a347.    000 days 23 hours 45 mins Manual
                6967.6162.6974.4574.

```

```

6865.726e.6574.302f.
31
172.16.1.102 0100.1320.4990.14 000 days 23 hours 48 mins Automatic
172.16.1.103 0100.e04c.70b7.e2 000 days 23 hours 55 mins Automatic

```

## Examples of Typical DHCP Relay Configuration

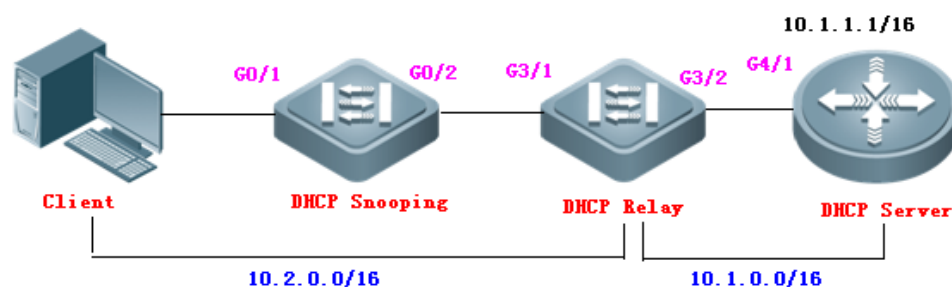
### Cross-segment users applying for IPs for Internet access

#### Configuration Requirements

1. Users can obtain IP addresses for Internet access across segments;
2. Illegal users are prevented from setting IP addresses themselves for Internet access.

#### Network Topology

Figure 1-7



#### Demand analysis

The switch port connecting the DHCP snooping switch and the DHCP relay is an ordinary access port. It is required that clients can automatically obtain IP addresses for Internet access across segments. To achieve this purpose, the DHCP relay is required. There are two approaches to preventing users from setting IP addresses themselves for Internet access. One is enabling DAI (dynamic ARP detection) in the global mode; the other is configuring port address binding in the interface mode in combination with the function of arp-check to prevent illegal users from access the Internet. In this example, the first approach is taken.

#### Configuration Procedure

Create an environment according to the above topology and perform the following steps of configuration:

##### ■ Configuration of the DHCP snooping:

# Enable the DHCP snooping

```
Ruijie(config)# ip dhcp snooping
```

# Configure the Gi0/2 connected to the server as a trusted port

```

Ruijie(config)# interface gigabitEthernet 0/2
Ruijie(config-if)# ip dhcp snooping trust

```

# Configure the Gi0/2 as the trusted port of the ARP detection

```
Ruijie(config-if)# ip arp inspection trust
Ruijie(config-if)# exit
```

# Enable the DAI packet check of the specified VLAN

```
Ruijie(config)# ip arp inspection vlan 1
```

# Configure the IP address of the device (SVI1)

```
Ruijie(config)# interface vlan 1
Ruijie(config-if)# ip address 10.2.0.1 255.255.0.0
```

# Configure the static route to another segment (10.1.0.0/16)

```
Ruijie(config)# ip route 10.1.0.0 255.255.0.0 10.2.1.1
```

#### ■ Configuration of the DHCP relay

# Enable the DHCP relay agent

```
Ruijie(config)# server dhcp
```

# Add a global DHCP server address

```
Ruijie(config)# ip helper-address 10.1.1.1
```

# Configure the IP address of the port connected to the Snooping device

```
Ruijie(config)# interface gigabitEthernet 3/1
Ruijie(config-if)# no switchport
Ruijie(config-if)# ip address 10.2.1.1 255.255.0.0
```

# Configure the IP address of the port connected to the Server

```
Ruijie(config)# interface gigabitEthernet 3/2
Ruijie(config-if)# no switchport
Ruijie(config-if)# ip address 10.1.0.1 255.255.0.0
```

#### ■ Configuration on the DHCP server:

# Configure the IP address of the port connected to the Relay

```
Ruijie(config)# interface gigabitEthernet 4/1
Ruijie(config-if)# no switchport
Ruijie(config-if)# ip address 10.1.1.1 255.255.0.0
```

# Enable the DHCP server

```
Ruijie(config)# service dhcp
```

# Configure the DHCP excluded addresses, which will not be assigned to the clients

```
Ruijie(config)# ip dhcp excluded-address 10.1.1.1 10.1.1.10
```

# Configure the address pool name and enter address pool configuration mode

```
Ruijie(config)# ip dhcp pool linwei
```

# Configure the default client gateway

```
Ruijie(dhcp-config)# default-router 10.2.1.1
```

# Configure the network number and mask of the DHCP address pool

```
Ruijie(dhcp-config)# network 10.2.0.0 255.255.0.0
```

# Configure the static route to another segment (10.2.0.0/16)

```
Ruijie(config)# ip route 10.2.0.0 255.255.0.0 10.1.0.1
```

# DHCPv6 Configuration

## DHCPv6 Overview

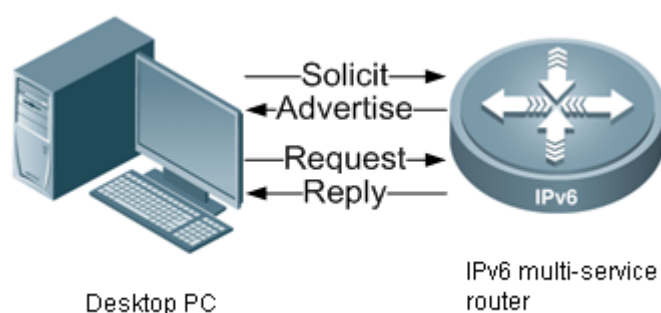
Along with the development of IPv6 network, IPv6-based network is being applied more and more widely. As the framework proposed at the beginning of IPv6 design, the automatic configuration of network nodes has become a key feature of IPv6 network. In the new network framework, the concepts of stateless configuration and stateful configuration were brought forward. Through stateless auto-configuration, the new nodes in the network can complete all configurations via Route Advertisement; while in stateful auto-configuration, the network nodes need interact with relevant configuration server in the network in order to complete the configuration of network address and other parameters. As the only stateful configuration model developed at the present time, DHCPv6 is fully described in RFC3315.

Comparatively complete description on the application model of DHCPv6 has been given in RFC3315 (Dynamic Host Configuration Protocol for IPv6). Similar to the framework of sDHCPv4, the application model of DHCPv6 is composed of the DHCP server, DHCP clients and DHCP relay. The configuration parameters can be obtained through the interaction between DHCP clients and DHCP server, while the DHCP relay can link the DHCP clients with the DHCP server outside the local link. The message interaction and parameter maintenance basically follow the practices of DHCPv4, but DHCPv6 do give proper consideration to the message structure and process according to the new network.

In IPv6 network, the auto-configuration of network nodes can be divided into:

- Stateless auto-configuration: Network nodes will acquire configuration parameters from route advertisement.
- Stateful auto-configuration: Network nodes will acquire configuration parameters from the DHCPv6 server.

Fig -1 DHCPv6 stateful auto-configuration



As shown in the above figure, the new network node (host or interface) will send a multicast message (Solicit) to all the DHCPv6 servers and DHCPv6 relays in the local link (address: FF02::1:2; port: 547), and the DHCPv6 servers will send the unicast Advertise reply message after receiving such message. After selecting the DHCP server, the DHCP clients will send the Request message to solicit for configuration information, and the DHCP server will send Reply message after completing the allocation of parameters.

As mentioned above, such a 4-message interaction is very similar to the 4-message interaction in DHCPv4 (Discover - Offer - Request - Ack). Certainly, DHCPv6 has made further modifications and expansions.



- Multicast is used instead of broadcast because broadcast has been abolished in the IPv6 network.
- By utilizing the option of Rapid Commit, the 4-message interaction can be simplified into 2-message interaction (Solicit - Reply).
- New DHCP message structure, DHCPv6 has made huge modifications to the original DHCPv4 message, and has removed optional parameters in the header of DHCP message. Only few fields to be used in all interactions are preserved. Other optional fields are all encapsulated in the option field of the DHCP message. During the interaction with the DHCP server and the DHCP relay, the DHCP message sent by the DHCP client to the DHCP server will be wholly encapsulated in the DHCP relay message as an option.
- New address parameters. As mentioned above, in DHCPv6, the address field is deleted from the fixed header of the DHCP message, and the entire address parameters and relevant time parameters are encapsulated in an option called IA (Identity Association). Each DHCPv6 client is associated with one IA, and each IA can contain multiple addresses and relevant time information. The corresponding IA can be generated in accordance with the type of address, such as IA\_NA (Identity association for non-temporary addresses) and IA\_TA (Identity association for temporary addresses).
- New DHCP client/server identifier, namely DUID (DHCP Unique Identifier).
- Stateless DHCPv6 auto-configuration. During the auto-configuration of network nodes, the address configuration is independent from parameter configuration, and each corresponding configuration can be acquired via the DHCP protocol, which means network nodes can acquire other non-address parameters from the DHCPv6 server. Compared with the allocation method used in DHCPv4, this is a critical change. Relevant information is detailed in RFC3736.
- Prefix delegation. Apart from IPv6 address, network prefix can also be delegated via DHCPv6. This also accredits to the definition of IA in DHCPv6. A prefix can be delegated to the client in the form of address (or time parameter, etc) only by expanding the type of IA. Such a new type of IA is called IA\_PD (Identity Association for Prefix Delegation), and it is detailed in RFC3633.

## Introduction to the DHCPv6 Server

### IPv6 address allocation method

In the IPv6 network, a 128-bit IPv6 address is usually written in the hexadecimal format, making it difficult to allocate addresses manually. As the IPv6 address format is inconvenient for people to identify, the automatic allocation method for IPv6 addresses is a key part in network planning. To allocate addresses without or with minimum man-made interference, many applications have been developed to handle addresses and parameters allocated to IPv6 hosts. Several IPv6 address allocation methods are described as follows:

- Manual allocation

The method is to configure an IPv6 address statically through manual allocation. The method is applicable to configuration of router interfaces and static network parameters. Manual allocation method may lead to many errors.

- Stateless automatic address allocation

The stateless address auto-configuration is to allocate addresses to IPv6 nodes without man-made interference. If this method is applied on one IPv6 node, this node must be connected with at least one IPv6 router through the network. The IPv6 router is configured by the administrator to send Router Advertisement messages on the link. Such messages

will be received by the IPv6 node connected to the router and the node will configure the IPv6 address and routing parameters.

#### ■ State DHCPv6 method

The Dynamic Host Configuration Protocol for IPv6 (DHCPv6) defined by RFC3315 enables DHCP Server to send configuration parameters such as IPv6 address to IPv6 nodes. The protocol enables adding network addresses flexibly and using them repeatedly.

#### ■ DHCPv6-PD method

The DHCPv6 Prefix Delegation (DHCPv6-PD) method defined by RFC3633 is developed based on DHCPv6. In the typical DHCPv6 method, DHCPv6 Server allocates state IPv6 addresses to DHCPv6 Client. Developed based on DHCPv6, the DHCPv6-PD method enables the DHCPv6-PD Server to allocate a complete subnet and other network and interface parameters to DHCPv6-PD Client by allocating Prefix Delegation information.

#### ■ Stateless DHCPv6 method

The stateless DHCPv6 method combines characteristics of the stateless automatic address allocation and state DHCPv6 method. The device can use the stateless automatic address allocation method to obtain the IPv6 address and use DHCPv6 to obtain other parameters, which cannot be obtained by using the stateless automatic address allocation method. The device can use the information to complete the configuration.



#### Note

In network planning, the above-mentioned IPv6 address and parameter allocation methods can be used concurrently.

---

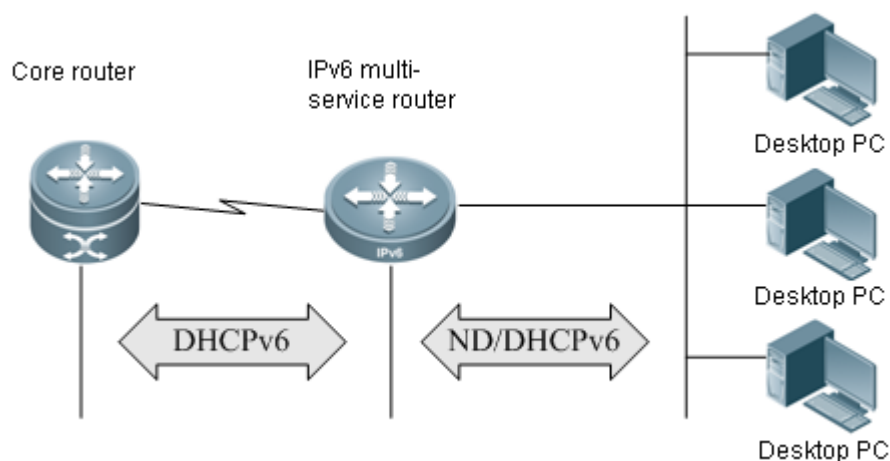
Ruijie DHCPv6 Server supports IPv6 address and prefix allocation. The IPv6 address allocation is to allocate IPv6 addresses automatically to DHCPv6 Client. The prefix allocation realizes flexible and automatic site-level configuration to control the site address space flexibly. Network terminals such as PCs can use stateless or state automatic configuration to realize automatic configuration of addresses and other network parameters.

Ruijie DHCPv6 Server also supports DHCPv6-PD Server. DHCPv6 Server and DHCPv6-PD Server are collectively referred to as DHCPv6 Server.

## Application of DHCPv6

The DHCPv6 server realizes the allocation of IAPD and IANA. The allocation of IANA refers to the automatic allocation of IPv6 address to the DHCP client, which is similar to DHCPv4. The allocation of IAPD allows flexible site-level auto-configuration to control the address range of sites. Terminal devices (such as PC) can realize auto-configuration of address via stateless auto-configuration or stateful auto-configuration.

Fig 1-- Prefix-based DHCPv6 application

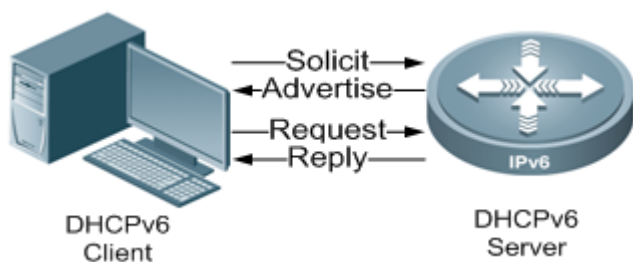


The above figure illustrates the application of prefix-based DHCPv6 in IPv6 network.

- Core router runs prefix delegation (PD) based DHCPv6 server.
- IPv6 multi-service router runs the DHCPv6 client on the interface connecting to the core router, acquiring prefix space from the core router and storing it in the global prefix pool of IPv6.
- IPv6 multi-service router enables auto-configuration on the interface connecting to the desktop computer and runs interface-based router advertisement or address assignment (NA) based DHCPv6 server.
- The desktop computer completes address and parameter configuration via ND or address assignment (NA) based DHCPv6 client.
- In the above model, DHCPv6 fulfils the following functions:
- The DHCP client (host, node) sends out prefix delegation (PD) based multicast solicit message within the link to look for DHCPv6 servers.
- The DHCP servers will send unicast advertisement message to the DHCP client after receiving such solicitation message.
- The DHCP client will select one server and send a multicast request message.
- The DHCP server will then send a unicast reply message to complete address assignment.

In the IPv6 network, DHCPv6 can be applied to enable user terminals to obtain IPv6 addresses and related parameters automatically.

Figure 1-3 DHCPv6 communication process



A typical DHCPv6 communication process:

- 1) DHCPv6 client sends a Solicit packet with the destination address of FF02::1:2 and destination UDP port of 547 to demand the DHCP service. All the DHCPv6 servers in the network segment will receive the packet.
- 2) After receiving the Solicit packet, each DHCPv6 server will send an Advertise packet in reply through unicast to state that it can provide the DHCP service.
- 3) The DHCPv6 client will choose a server among those that have sent the Advertise packets to it, and send a Request packet with the destination address of FF02::1:2 and destination UDP port of 547 to announce the server that has been chosen by it. All the DHCPv6 servers in the network segment will receive the packet.
- 4) After the DHCPv6 server that has been chosen receives the Request packet, it will send a Reply packet through unicast to announce the IP address allocated for the DHCPv6 client and other information.



**Note** FF02::1:2 is used to identify all the DHCPv6 servers and relays in the same network segment.



**Note** The Solicit and Request packets use this address as the destination address. The packets are only transmitted within the network segment.

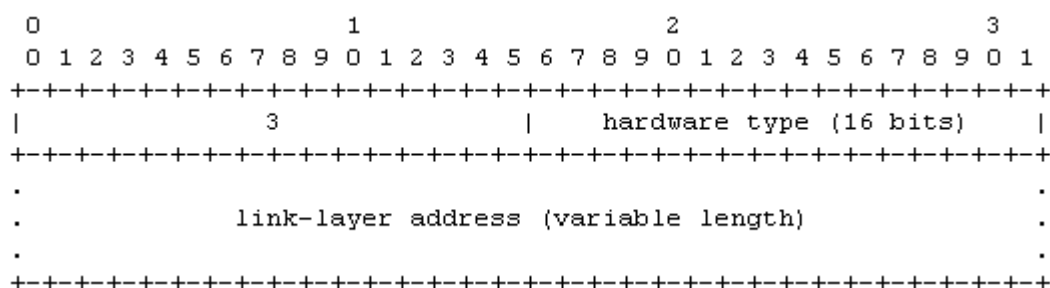
## DUID Overview

DUID means the DHCP Unique Identifier. The RFC3315 defines that each DHCPv6 device (including the client, relay and server) must have a DHCPv6 unique identifier for identification during the exchange of DHCPv6 messages between devices. DUID cannot be used for any other purposes. For all DHCPv6 devices, DUID must be designed as unrepeatable and fixed for any devices. For example, a device's DUID must remain the same when any part of the device is replaced. A DUID has a maximum length of 128 bytes. The protocol provides three types of DUID definitions:

- DUID based on link-layer address plus time, DUID-LLT;
- DUID assigned by vendor based on enterprise number, DUID-EN; and
- link-layer address, DUID-LL

Currently, Ruijie DHCPv6 devices apply DUID-LL. The structure of the DUID-LL is as follows:

Figure 1-4



In the structure, the DUID type is DUID, DUID-LL type value is 0x0003; the Hardware type is hardware, the hardware type supported by the device is Ethernet, the value is 0x0001; Link layer address is the address of the link layer, and the value is the device's MAC address.

## DHCPv6 address allocation

Unlike DHCPv4, Server in DHCPv6 allocates an identity association (IA) rather than an address to each Client. DHCPv6 Server will allocate addresses on the IA basis and each IA has an IAID unique identifier. The identity association identifier (IAID) is generated by DHCPv6 Client. Each IA is only corresponding to one Client and can contain multiple addresses. The Client can allocate addresses in the IA to other interfaces on the device. Addresses contained in an IA can be divided into the following three types:

- Non-temporary address (NA), globally unique address;
- Temporary address (TA), with few related applications;
- Prefix delegation (PD);

According to the types of addresses contained in IAs, IAs can be divided into three types, namely IA\_NA, IA\_TA and IA\_PD. Ruijie DHCPv6 Server supports IA\_NA and IA\_PD, but not IA\_TA.

## DHCPv6 Bindings

The DHCPv6 Bindings is a group of manageable address information structures. The binding is based on the IA and can be identified by Server and Clients. The binding data on Server records the IA allocated to each Client and other configuration information. Each Client can apply for several bindings. Binding data on the Server is managed in the binding table and can be searched by DUID, IA-Type and IAID.

## DHCPv6 packet type

RFC3315 provides that DHCPv6 can use UDP546 and 547 ports to send and receive packets. The DHCPv6 Client uses port 546 to receive packets, while DHCPv6 Server and Relay use port 547 to receive packets. RFC3315 defines that packets of the following types can be exchanged among DHCPv6 Server, Client and Relay:

- Types of packets that can be sent by Client to Service: Solicit, Request, Confirm, Renew, Rebind, Release, Decline and Information-request;
- Types of packets that can be sent by Server to Client: Advertise, Reply and Reconfigure;
- Types of packets that can be sent by Relay to Relay or Server: Relay-forward;
- Types of packets that can be sent by Server or Relay to Relay: Relay-reply;

To simplify the DHCP communication process, not all types of packets are used. Users can decide which type of packets should be used based on the DHCPv6 options carried by packets. The DHCP data also vary with the options chosen. In terms of packet types and functions, DHCPv6 is similar with DHCPv4. Although DHCPv6 packets are adjusted to new networks and processes, some packet types in DHCPv6 are corresponding to those in DHCPv4. The following table outlines the corresponding relationship between packet types of DHCPv6 and DHCPv4:

DHCPv6 packet type	DHCPv4 packet type
Solicit (1)	DHCPDISCOVER
Advertise (2)	DHCPOFFER
Request (3), Renew (5), Rebind (6)	DHCPREQUEST
Reply (7)	DHCPACK / DHCPNAK
Release (8)	DHCPRELEASE
Information-request (11)	DHCPINFORM

Decline (9)	DHCPDECLINE
Confirm (4)	None
Reconfigure (10)	DHCPFORCERENEW
Relay-forward (12), Relay-reply (13)	None

**Caution**

The Reconfigure type of packets is not supported by Ruijie DHCPv6 Server. Please refer to the Guide for DHCP Configuration chapter for information about DHCPv4.

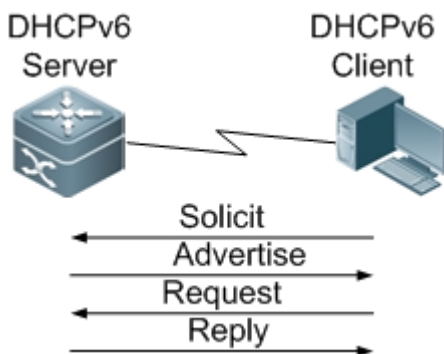
## Working principle of DHCPv6 Server

The application mode of DHCPv6 is generally developed based on the framework of DHCPv4. The application mode of DHCPv6 comprises Server, Client and Relay. Configuration parameters are obtained through communication between Client and Server. Relay can connect Client with Server that is not on the local link. In terms of the exchange of packets and maintenance of parameters, DHCPv6 is generally similar with DHCPv4. However, it has adjusted the packet structure and handling process to new networks. Comparison between DHCPv6 and DHCPv4

- DHCPv6 applies a new packet structure. Original DHCPv4 packets have been largely modified. Optional parameters in DHCPv4 packet heads are removed, with only a few fields required for exchange of all packets left. Other optional fields are encapsulated as options in the option domain of packets.
- DHCPv6 applies new address parameters. As mentioned above, the address field in the fixed packet head in DHCPv4 is removed in DHCPv6. All the address parameters and related time parameters are encapsulated in the IA option. Each DHCPv6 Client is associated with an IA and each IA may contain several addresses and related time information; the corresponding type of IA, such as IA\_NA, IA\_TA or IA\_PD, will be generated according to the address type;
- DHCPv6 adopts a new client service-end identifier, namely DUID;
- DHCPv6 supports the stateless automatic DHCPv6 configuration, which means that when automatic configuration is being performed on a network node, the address and parameters can be configured separately, and each configuration can be obtained through the DHCP method. Therefore, network nodes can obtain parameters in addition to addresses through a DHCPv6 server. This is a substantial difference from the allocation mode of DHCPv4.
- DHCPv6 supports prefix-based allocation so that in addition to IPv6 addresses, network prefixes can also be allocated through DHCPv6.

DHCPv6's basic application mode is shown in the following figure:

Figure 1-5 Typical DHCPv6 address allocation

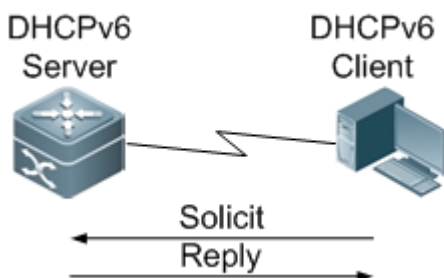


A typical DHCPv6 address allocation process is shown in the following figure:

- 1) DHCPv6 Client sends a multicast Solicit packet with the destination address of FF02::1:2 and destination UDP port of 547 on the local link. All the DHCPv6 Servers and Relays on the local link will receive the packet.
- 2) After DHCPv6 Servers receive the packet, they will send unicast Advertise packets in reply;
- 3) After DHCPv6 Client chooses a Server, it will send a multicast Request packet with the destination address of FF02::1:2 and destination UDP port of 547 on the local link.
- 4) After the DHCPv6 Server receives the Request packet, it will send an unicast Reply packet in reply and the configuration process completes.

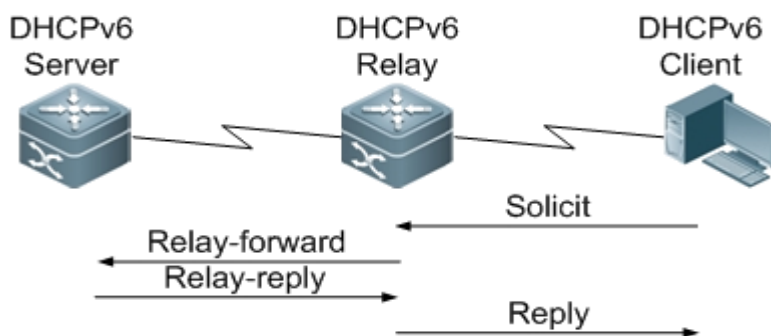
The DHCPv6 communication process involves four packets and is similar with the DHCPv4 communication process, which also involves four packets (Discover, Offer, Request and Ack). The special option Rapid Commit can be used to shorten the communication process to involve only two packets (Solicit and Reply). The Client can add this option into the Solicit packet. The Server will send the Reply packet after receiving the packet. The shortened process is shown as follows:

Figure 1-6 Shortened 2-packet communication



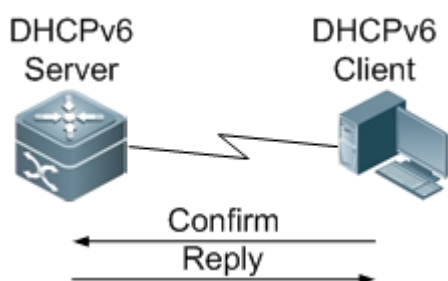
A Relay can be added between Server and Client to perform the address allocation between Client and Server on different network segments. The request packet sent by Client will be encapsulated as an option in the Relay-forward packet and sent to Server. After the request is obtained by Server from the request message, the reply message will be encapsulated in the Relay message option of the Relay-reply packet and the Relay-reply packet will be sent to Relay. The reply message will be forwarded to Client after being obtained. The process is shown as follows:

Figure 1-7 Communication between Server, Relay and Client



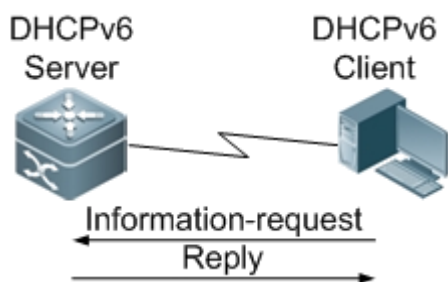
When the Client's network connection changes, Client will send the Confirm packet to Server to inquire whether the resource allocated by Server previously is available. After Server receives the packet, it will send a Reply packet to Client. The process is shown as follows:

Figure 1-8 Server replies to a Confirm packet



If Client adopts the stateless address configuration but obtains other parameters through the DHCP method, the Client will send a Information-request packet to Server. After Server receives the packet, it will send a Reply packet to Client. The process is shown as follows:

Figure 1-9 Server replies to an Information-request packet



### Protocol specification

- See RFC3315 for the DHCPv6 protocol specification;
- See RFC3633 for the DHCPv6-PD protocol specification;

### Introduction to the DHCPv6 Client

The DHCPv6 client can automatically acquire prefix space and other configuration parameters from the DHCPv6 server. After obtaining the prefix space, the DHCP client will store it in the global prefix space pool of IPv6, and then such prefix space can be assigned to other interfaces via prefix partition for prefix advertisement.



The DHCPv6 client gets relevant parameters based on interface, such as Domain Name Server, SNTP server. Relevant parameters configurations depend on the validity of interface.

## Introduction to the DHCPv6 Relay

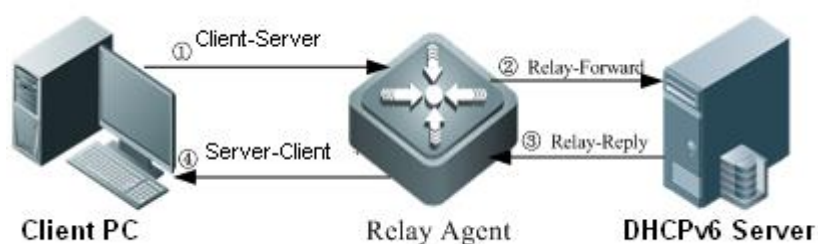
The DHCPv6 relay forwards DHCPv6 messages between the DHCPv6 server and the DHCP client. When the DHCP server and the DHCP client are not in the same physical network, the DHCP relay is responsible for forwarding the DHCP solicit and reply messages. The forwarding process is different from routing forwarding, which features transparent transmission. Generally, the router will not modify the contents of IP packets. Upon receiving the DHCP message, the DHCP relay will regenerate and forward another one.

The DHCP relay is just like a DHCP server for the DHCP clients and a DHCP client for the DHCP server.

## Functions of DHCPv6 Relay Agent

With the help of DHCPv6 Relay Agent, the DHCPv6 server can provide services for DHCPv6 clients in other network segments; without DHCPv6 Relay Agent, the DHCPv6 server can only provide services for DHCPv6 clients in the same network segment.

Figure 1-10 Functions of DHCPv6 Relay Agent



Functions of DHCPv6 Relay Agent are described as follows (corresponding to the numbers in the figure):

- 1) It enables the DHCPv6 relay, the gateway that has enabled DHCPv6 Relay Agent, to receive packets sent by the DHCPv6 client to the DHCPv6 server.
- 2) It enables the DHCPv6 relay to encapsulate packets received (sent by the DHCPv6 client to DHCPv6 server) in the Relay-Forward packet and send it in the unicast manner to the specified DHCPv6 server.
- 3) It enables the DHCPv6 server to encapsulate the reply in the Relay-Reply packet after it receives the Relay-Forward packet and send it to the DHCPv6 relay in the unicast manner.
- 4) It enables the DHCPv6 relay to restore the packet (sent by the DHCPv6 server to the DHCPv6 client) after it receives the Relay-Reply packet and send it to the DHCPv6 client in the unicast manner.



### Note

In the address lease renewal, rebinding and release processes on a DHCPv6 client and the configuration refreshing process on a server, the DHCPv6 Relay Agent plays a similar role.

## Protocol specification

- RFC3315 Dynamic Host Configuration Protocol for IPv6 (DHCPv6)

## DHCPv6 Configuration

### Configure the DHCPv6 Server

#### Default configuration

The following table outlines the default configuration of the DHCPv6 Server.

Function and feature	Default setting
DHCPv6 Server function	Disabled
DHCPv6 configuration information pool	Not configured

#### Configuring the DHCPv6 Server function

This task involves how to create and configure a DHCPv6 configuration information pool, and how to associate this pool with the DHCPv6 server on the interface.

To configure the DHCPv6 server, run the following commands:

Command	Function
Ruijie# <b>configure terminal</b>	Enter global configuration mode.
Ruijie(config)# <b>ipv6 dhcp pool</b> <i>poolname</i>	Configure the DHCPv6 configuration information pool and enter pool configuration mode.
Ruijie(config-dhcp)# <b>domain-name</b> <i>domain</i>	Configure a domain name that can be assigned to the DHCPv6 client.
Ruijie(config-dhcp)# <b>dns-server</b> <i>ipv6-address</i>	Configure a DNS server that can be assigned to the DHCPv6 client.
Ruijie(config-dhcp)# <b>prefix-delegation</b> <i>ipv6-prefix/prefix-length client-DUID [lifetime]</i>	Configure an address prefix that can be assigned to the IAPD of a specific DHCP client.
Ruijie(config-dhcp)# <b>prefix-delegation pool</b> <i>poolname</i> <b>[lifetime</b> { <i>valid-lifetime</i>   <i>preferred-lifetime</i> }]	Configure a prefix pool for the DHCPv6 server, and address prefix can be delegated to the DHCP clients from this prefix pool.
Ruijie(config-dhcp)# <b>iana-address prefix</b> <i>ipv6-prefix/prefix-length [lifetime {valid-lifetime   preferred-lifetime}]</i>	Configure an IANA address prefix for the DHCPv6 server, and IANA address can be assigned to the DHCP clients within the scope of addresses designated by this prefix.
Ruijie(config-dhcp)# <b>exit</b>	Exit DHCPv6 pool configuration mode.
Ruijie(config)# <b>interface</b> <i>type number</i>	Enter interface configuration mode.
Ruijie(config-if)# <b>ipv6 dhcp server</b> <i>poolname [rapid-commit] [preference value]</i>	Enable the DHCPv6 server on this interface.

For example:

# Configure a configuration information pool named pool 1 and configure the domain name, DNS Server, IA\_NA, IA\_PD and etc. Enable the DHCPv6 Server function on the FastEthernet 0/1 interface.

```
Ruijie# configure terminal
Ruijie(config)# ipv6 local pool client-prefix-pool 2008:10::/64 78
Ruijie(config)# ipv6 dhcp pool pool1
Ruijie(config-dhcp)# domain-name example.com
Ruijie(config-dhcp)# dns-server 2008:1::1
Ruijie(config-dhcp)# prefix-delegation 2008:2::/64
0003000100d0f82233ac
Ruijie(config-dhcp)# prefix-delegation pool client-prefix-pool lifetime 2000 1000
Ruijie(config-dhcp)# iana-address prefix 2008:50::/64
Ruijie(config-dhcp)# exit
Ruijie(config)# interface fastethernet 0/1
Ruijie(config-if)# ipv6 dhcp server pool1
```

**Note**

DHCPv6 Server does not support allocation of gateway addresses for clients. To do this, the RA notification function `Ruijie(config-if)# no ipv6 nd suppress-ra` must be enabled on the device.

**Note**

The flag bit "managed address configuration" in the Router Announcement (RA) packet should also be set to decide whether the host that receives the RA should use the stateful automatic configuration to obtain the addresses. By default, the flag bit in the RA packet is not set:

`Ruijie(config-if)# ipv6 nd managed-config-flag`

**Note**

The flag bit "other stateful configuration" in the RA packet is set to decide whether the host that receives the RA should use the stateful automatic configuration to obtain information other than the addresses. By default, the flag bit in the RA packet is not set by `Ruijie(config-if)# ipv6 nd other-config-flag`

**Note**

Finally, disable the prefix notification function: `Ruijie(config-if)# ipv6 nd prefix ipv6-prefix/prefix-length no-advertise`

**Caution**

When the address pool prefix or prefix mask in the address pool information is revised, the lease information of the corresponding address pool will be deleted. In this case, DHCPv6 Server may allocate an address or address prefix that has been allocated previously to a new request to trigger an address conflict. Please note that generally, after an address pool is created to allocate addresses or prefixes, the address pool's prefix or prefix mask should be revised unless it is necessary to do so.

## Configuring the stateless DHCPv6 Server function

The stateless DHCPv6 Server does not need to configure the prefix pool. Given that the Client has obtained the address through RA, the Server only needs to provide the Client with other configuration information. The configuration process is described as follows:

Command	Function
Ruijie# <b>configure terminal</b>	Enter global configuration mode.
Ruijie(config)# <b>ipv6 dhcp pool</b> <i>poolname</i>	Configure the DHCPv6 configuration information pool and enter pool configuration mode.
Ruijie(config-dhcp)# <b>domain-name</b> <i>domain</i>	Configure a domain-name that can be allocated to DHCPv6 Client.
Ruijie(config-dhcp)# <b>dns-server</b> <i>ipv6-address</i>	Configure the DNS Server that can be provided to the DHCPv6 Client.
Ruijie(config-dhcp)# <b>exit</b>	Exit DHCPv6 pool configuration mode.
Ruijie(config)# <b>interface</b> <i>interface-name</i>	Enter interface configuration mode.
Ruijie(config-if)# <b>ipv6 dhcp server</b> <i>poolname</i> <b>[rapid-commit] [preference value]</b>	Enable the DHCPv6 Server on the interface.
Ruijie(config-if)# <b>ipv6 nd other-config-flag</b>	Set the flag bit "other stateful configuration" in IPv6 RA.

Example:

# Configure a configuration information pool named pool1 and configure the domain name, DNS Server and etc. Enable the DHCPv6 Server function on the FastEthernet 0/1 interface, and set the flag bit in IPv6 RA.

```
Ruijie# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Ruijie(config)# ipv6 dhcp pool pool1
Ruijie(config-dhcp)# domain-name example.com
Ruijie(config-dhcp)# dns-server 2008:1::1
Ruijie(config-dhcp)# exit
Ruijie(config)# interface fastethernet 0/1
Ruijie(config-if)# ipv6 dhcp server pool1
Ruijie(config-if)# ipv6 nd other-config-flag
```



### Note

DHCPv6 Server does not support allocation of gateway addresses for clients. To do this, the RA notification function `Ruijie(config-if)# no ipv6 nd suppress-ra` must be enabled on the device.

## Showing the DHCPv6 Server configuration

Use the following commands to show information about DHCPv6 Server configuration and state:

Command	Function
<b>show ipv6 dhcp</b>	Show the device's DUID information.

<b>show ipv6 dhcp binding</b>	Show the DHCPv6 server's address binding information.
<b>show ipv6 dhcp conflict</b>	Show the DHCPv6 server's address conflict information.
<b>show ipv6 dhcp interface</b>	Show the DHCPv6 interface information.
<b>show ipv6 dhcp pool</b>	Show the DHCPv6 pool information.
<b>show ipv6 dhcp server statistics</b>	Show the DHCPv6 statistics.

# Example:

```
Ruijie# show ipv6 dhcp
This device's DHCPv6 unique identifier(DUID): 00:03:00:01:00:d0:f8:22:33:b0
```

```
Ruijie# show ipv6 dhcp binding
Client DUID: 00:03:00:01:00:d0:f8:22:33:ac
IAPD: iaaid 0, T1 1800, T2 2880
Prefix: 2001:20::/72
        preferred lifetime 3600, valid lifetime 3600
        expires at Jan 1 2008 2:23 (3600 seconds)
```

```
Ruijie# show ipv6 dhcp interface
VLAN 1 is in server mode
Server pool dhcp-pool
Rapid-Commit: disable
```

```
Ruijie# show ipv6 dhcp pool
DHCPv6 pool: dhcp-pool
DNS server: 2011:1::1
DNS server: 2011:1::2
Domain name: example.com
```

```
Ruijie# show ipv6 dhcp server static
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

```

## Configure the DHCPv6 Client

This task involves how to enable DHCPv6 client function and prefix solicitation on the interface.

To configure the DHCPv6 Client, run the following commands:

Command	Function
Ruijie# <b>configure terminal</b>	Enter global configuration mode.
Ruijie (config)# <b>interface</b> <i>type number</i>	Enter interface configuration mode.
Ruijie (config-if)# <b>ipv6 dhcp client pd</b> <i>prefix-name</i> [ <i>rapid-commit</i> ]	Enable the DHCPv6 client and prefix solicitation on the interface.

For example:

```

Ruijie# configure terminal
Ruijie(config)# interface fastethernet 0/1
Ruijie(config-if)# ipv6 dhcp client pd pd_name

```

## Configuring stateless DHCPv6 Client

The configuration process is described as follows:

Command	Function
Ruijie# <b>configure terminal</b>	Enter global configuration mode.
Ruijie(config)# <b>interface</b> <i>type number</i>	Enter interface configuration mode.
Ruijie(config-if)# <b>ipv6 enable</b>	Enable the IPv6 function on the interface.

Example:

```

Ruijie# configure terminal

```

```
Ruijie(config)# interface fastethernet 0/1
Ruijie(config-if)# ipv6 enable
```

## Re-enable the DHCPv6 Client on the interface.

The task explains how to re-enable DHCPv6 Client on an interface.

The configuration process is described as follows:

Command	Function
Ruijie# <b>clear ipv6 dhcp client interface-type interface-number</b>	Re-enable the DHCPv6 Client on the interface.

Example:

```
Ruijie# clear ipv6 dhcp client fastethernet 0/1
```

## Configure the DHCPv6 Relay Agent

### Default configuration

Function and feature	Default setting
DHCPv6 Relay Agent function	Disabled
DHCPv6 Relay Agent server address	Unspecified

### Configuring the DHCPv6 Relay function

This task enables the DHCPv6 relay function on the interface, and configures the address used for relay forwarding.

To configure the DHCPv6 relay, run the following commands:

Command	Function
Ruijie# <b>configure terminal</b>	Enter global configuration mode.
Ruijie(config)# <b>interface type number</b>	Enter interface configuration mode.
Ruijie(config-if)# <b>ipv6 dhcp relay destination ipv6-address [interface-type interface-number]</b>	Enable the DHCPv6 relay on the interface, and designate the address for relay forwarding.
Ruijie(config-if)# <b>end</b>	Exit from the interface mode.

Use the following command to show the destination address of the DHCPv6 Relay:

```
show ipv6 dhcp relay destination { all | interface interface-type interface-number }
```

Use the following command to delete the destination address of the DHCPv6 Relay:

```
no ipv6 dhcp relay destination ipv6-address [ interface-type interface-number ]
```

Example: Enable the DHCPv6 Relay Agent function with the destination address of 3001::2 on the interface VLAN 1.

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

```
Ruijie(config)#interface vlan 1
Ruijie(config-if)#ipv6 dhcp relay destination 3001::2
Ruijie(config-if)#end
```



**Caution** The IPv6 DHCP Relay Destination command can only be used on the layer-3 interface;



**Caution** One device can be configured with 20 Relay Agent Destinations at most;



**Caution** When Destination configures multicast addresses, the interface numbers must be specified behind the addresses.

## Showing/clearing DHCPv6 Relay information

Command	Function
<b>show ipv6 dhcp relay destination { all   interface interface-type interface-number }</b>	Show the DHCPv6 Relay's destination address.
<b>show ipv6 dhcp relay statistics</b>	Show the DHCPv6 Relay Agent's packet statistics.
<b>clear ipv6 dhcp relay statistics</b>	Clear the DHCPv6 Relay Agent's packet statistics.

Example: Show the DHCPv6 Relay's destination address.

```
Ruijie# show ipv6 dhcp relay destination all
Interface: Vlan1
Destination address(es)          Output Interface
3001::2
```

Example: Show the DHCPv6 Relay Agent's statistics.

```
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

## Typical configuration examples

### Typical DHCPv6 Server configuration example

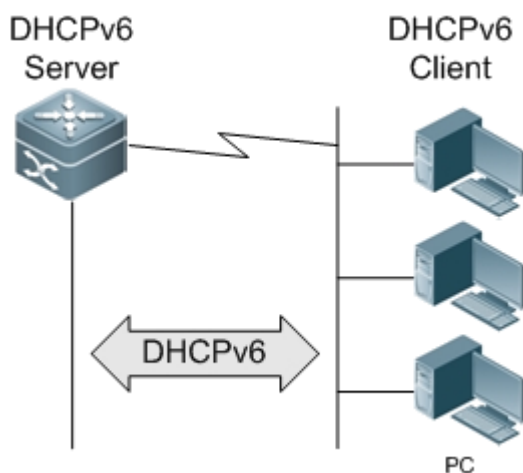
#### Networking demand

In the user environment, the most common practice is to deploy DHCPv6 Server in the core or convergent position of the network to allocate the entire subnet's IP addresses and manage the allocation.

#### Networking topology

As shown in the following figure, enable the DHCPv6 Server function on the convergent device to allocate IPv6 address and other network configuration information for PCs in the subnet. The range of IA\_NA addresses that can be allocated is configured on the Server. When a PC sends a request for address allocation, the Server will calculate an available address in the IA\_NA address range and allocate it to the PC after it receives the request. In addition, the Server provides other information including DNS Server addresses and domain names. To ensure that the DHCPv6 Server function takes effect, the IP address in the same network segment with the IA\_NA should be configured on the layer-3 interface where the Server function is enabled.

Figure 1-11 DHCPv6 Server networking topology



#### Key points

If the core device serves as the DHCPv6 Server, the device's CPU and memory occupancy rates will rise. When Clients increase, the pressure on the Server will rise. Therefore, a high-performance or separate device should be used as the DHCPv6 Server.

#### Configuration process



```
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
```

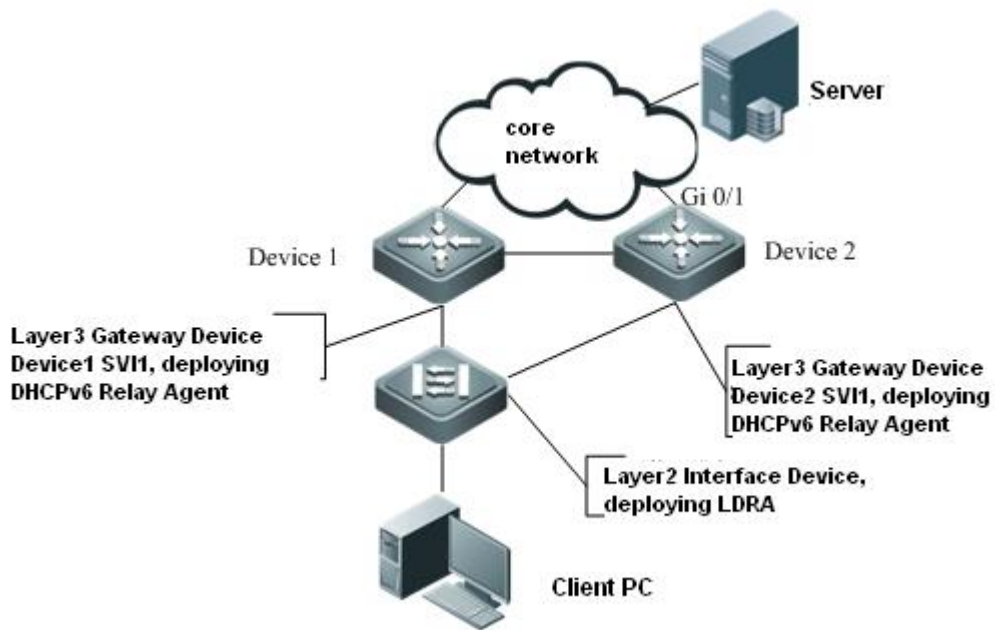
## Typical DHCPv6 Relay configuration example

### Networking demand

Device1 enables the DHCPv6 Relay Agent with the destination address of 3001::2; Device2 enables the DHCPv6 Relay Agent with the destination address of FF02::1:2 (for all Server and Relay multicast packets) to continue relaying the packet to other servers. The layer-3 interface whose egress interface is specified as the upper destination address is gi 0/1.

### Networking topology

Figure 1-12 DHCPv6 Relay Agent networking topology



## Key configuration points

Enable the DHCPv6 Relay Agent function on the gateway and designate the known server address or next-level Relay address as the destination.

## Configuration process

- Enable the DHCPv6 Relay Agent function on the convergence gateway device Device1 with the destination address of 3001::2:

```
Ruijie#config
Enter configuration commands, one per line. End with CNTL/Z
Ruijie(config)#interface vlan 1
Ruijie(config-if)# ipv6 dhcp relay destination 3001::2
```

- Enable the DHCPv6 Relay Agent function on the convergence gateway device Device2 with the destination address of FF02::1:2:

```
Ruijie#config
Enter configuration commands, one per line. End with CNTL/Z
Ruijie(config)#interface vlan 1
Ruijie(config-if)#ipv6 dhcp relay destination FF02::1:2 interface gi 0/1
```

## Checking the configuration effect

- Show the configuration of DHCPv6 Relay Agent on Device 1.

```
Ruijie# show ipv6 dhcp relay destination all
Interface: Interface vlan 1
Server address(es)                Output Interface
3001::2
```

- Show the configuration of DHCPv6 Relay Agent on Device 2.

```
Ruijie# show ipv6 dhcp relay destination all
Interface: Interface vlan 1
Server address(es)                Output Interface
FF02::1:2                        gi0/1
```

# DNS Configuration

## DNS Overview

Each IP address may present a host name consisting of one or more strings separated by the decimal. Then, all you need to do is to remember the host name rather than IP address. This is the function of the DNS protocol.

There are two methods to map from the host name to the IP address: 1) Static Mapping: A device maintains its host name to IP address mapping table and uses it only by itself. 2) Dynamic Mapping: The host name to IP address mapping table is maintained on the DNS server. In order for a device to communicate with others by its host name, it needs to search its corresponding IP address on the DNS server.

The domain name resolution (or host name resolution) is the process that the device obtains IP address which corresponds to the host name by the host name. The Ruijie switches support the host name resolution locally or by the DNS. During the resolution of domain name, you can firstly adopt the static method. If it fails, use the dynamic method instead. Some frequently used domain names can be put into the resolution list of static domain names. In this way, the efficiency of domain name resolution can be increased considerably.

## Configuring Domain Name Resolution

### Default DNS Configuration

The default configurations of DNS are as follows:

Attribute	Default Value
Enable/disable the DNS resolution service	Enable
IP address of DNS server	None
Static Host List	None
Maximum number of DNS servers	6

### Enabling DNS Resolution Service

This section describes how to enable the DNS resolution service.

Command	Function
Ruijie(config)# <b>ip domain-lookup</b>	Enable DNS.

The command **no ip domain-lookup** is used to disable DNS.

```
Ruijie(config)# ip domain-lookup
```

### Configuring the DNS Server

This section describes how to configure the DNS server. The dynamic domain name resolution can be carried out only when the DNS Server is configured.

The **no ip name-server** [*ip-address*] command can be used to remove the DNS server. Where, the **ip-address**

parameter indicates the specified DNS server to be removed. If this parameter is omitted, all the DNS servers will be removed.

Command	Function
Ruijie(config)# <b>ip name-server</b> <i>ip-address</i>	Add the IP address of the DNS Server. The switch will add a DNS Server when this command is executed every time. If the domain name can't be obtained from the first DNS Server, the switch will send the DNS request to the subsequent several servers until the correct response is received. The system can support six DNS servers at most.

## Configuring the Host Name to IP/IPv6 Address Mapping Statically

This section describes how to configure the host name to IP/IPv6 address mapping. The switch maintains a host name to IP/IPv6 address corresponding table, which is also referred to as the host name to IP/IPv6 address mapping table. You can obtain the mapping table in two ways: manual configuration and dynamic learning.

Command	Function
Ruijie(config)# <b>ip host</b> <i>host-name ip-address</i>	Configure the host name to IP address mapping manually.
Ruijie(config)# <b>ipv6 host</b> <i>host-name ip-address</i>	Configure the host name to IPv6 address mapping manually.

This command with the parameter **no** can be used to remove the mapping between the host name and IP/IPv6 address.

## Clearing the Dynamic Buffer Table of Host Names

This section describes how to clear the dynamic buffer table of host names. If the command **clear host** or **clear host \*** is entered, the dynamic buffer table will be cleared. Otherwise, only the entries of specified domain names will be cleared.

Command	Function
Ruijie# <b>clear host</b> [ <i>host-name</i> ]	Clear the dynamic buffer table of host names. The host names configured statically will not be removed.

## Showing Domain Name Resolution Information

This section describes how to display the DNS configuration.

Command	Function
Ruijie# <b>show hosts</b>	Show the DNS configuration.

```
Ruijie# show hosts
Name servers are:
192.168.5.134 static
```

Host	type	Address	TTL(sec)
www.163.com	static	192.168.5.243	---

## Typical DNS Configuration Examples

### Example of Static DNS Configuration

#### Topological Diagram



Figure1 Network topology for static DNS configuration

#### Application Requirements

Since the network device Ruijie-A will frequently access the host of destination.com, we can use static DNS to access the host of IP 1.1.1.20 through the domain name of destination.com, so as to enhance the efficiency of domain resolution.

#### Configuration Tips

1. Make sure the route between device and host is reachable.
2. The mapping between host name and IP address is correct.

#### Configuration Steps

Manually configure the mapping between host name and IP address. In this example, configure the host name to "destination.com" and the corresponding IP address to 1.1.1.20.

```
Ruijie-A(config)#ip host destination.com 1.1.1.20
```

#### Verifications

Step 1: View DNS information. Key point: the mapping between host and IP address shall be correct.

```
Ruijie-A #show host
Name servers are:
```



Host	type	Address	TTL(sec)
destination.com	static	1.1.1.20	---

Step 2: Execute "ping destination.com" command to verify the result.

```
Ruijie-A #ping destination.com
Translating "destination.com"...[OK]
Sending 5, 100-byte ICMP Echoes to 1.1.1.20, timeout is 2 seconds:
< press Ctrl+C to break >
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
```

From the above information, we can learn that Ruijie-A has successfully accessed the host with IP address being 1.1.1.20 through the host name of destination.com by means of static DNS.

## Example of Dynamic DNS Configuration

### Topological Diagram

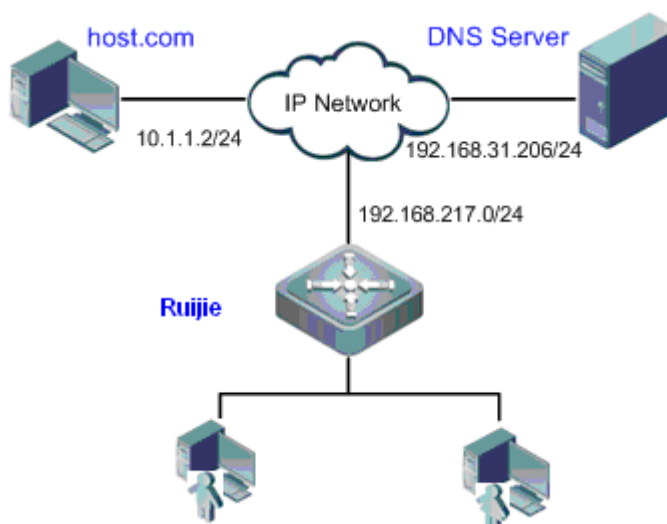


Figure2 Network topology for dynamic DNS configuration

### Application Requirements

1. The IP address of DNS server is 192.168.31.206/24.
2. The network device is the DNS client and can access the host of 10.1.1.2 through the host name of host.com by means of dynamic DNS.

### Configuration Tips

1. The route between DNS client, DNS server and access PC shall be reachable.
2. DNS shall be enabled. The DNS feature is enabled by default.
3. The IP address of DNS server has been correctly configured.

## Configuration Steps

---

### Step 1: Configure DNS server

Different DNS servers need to be configured differently. Please configure DNS server according to the actual conditions.

Configure the mapping between host and IP address on DNS server. In this example, configure host name as "host.com" and IP address as 10.1.1.2/24.

### Step 2: Configure DNS client

The route between DNS client, DNS server and access PC shall be reachable. The interface IP configurations are shown in the topological diagram.

! DNS shall be enabled. The DNS feature is enabled by default.

```
Ruijie(config)#ip domain-lookup
```

! Configure the IP address of DNS server as 192.168.31.206

```
Ruijie(config)#ip name-server 192.168.31.206
```

## Verifications

---

### Step 1: Execute "ping host.com" command to verify the result.

```
Ruijie#ping host.com
```

```
Translating " host.com "...[OK]
```

```
Sending 5, 100-byte ICMP Echoes to 10.1.1.2, timeout is 2 seconds:
```

```
< press Ctrl+C to break >
```

```
!!!!
```

```
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
```

From the above information, we can learn that the client device can ping the host, and the corresponding destination IP is 10.1.1.2. Through dynamic DNS, the host with IP address being 10.1.1.2 can be accessed through the host name of host.com.

### Step 2: View DNS information. Key point: the host name and IP address.

```
Ruijie#show host
```

```
Name servers are:
```

```
192.168.31.206 static
```

Host	type	Address	TTL(sec)
<b>host.com</b>	<b>dynamic</b>	10.1.1.2	3503

From the above information, we can learn that the mapping between host name and host IP is correct.

## FTP Client Configuration

FTP Client provides users with the feature of file transfer with remote FTP server through FTP protocol.

### Introduction to FTP

FTP (File Transfer Protocol) is a concrete application of TCP/IP for establishing connection-oriented and reliable TCP session between FTP client and server. The user can access a remote computer running FTP server program. After the user issues commands to the server, the server will respond to such commands and return the execution results to the client. Through such command interaction, the user can view files under the server directories and copy such files from remote computer to the local device, or transfer the local files to the remote computer. FTP protocol is detailed in RFC 959.

### FTP Connection Mode

FTP maintains two TCP connections:

- Control link (also referred to command link) for transferring command between FTP client and server.
- Data link for uploading or downloading data.

(1) Control connection: For certain simple connections, only the control connection is needed. The client sends commands to the server, which will then respond to these commands. The process is shown below:

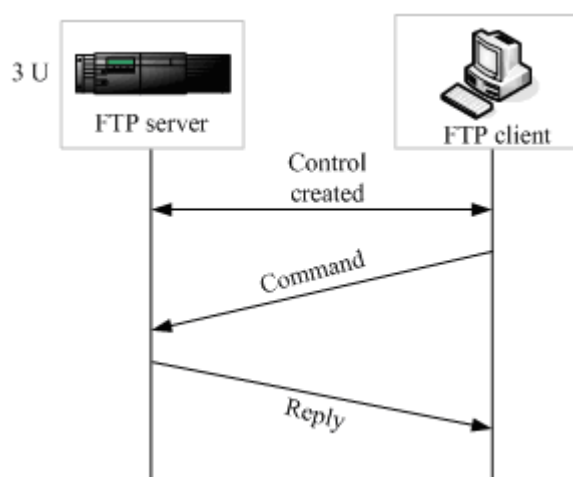


Figure 1 Control Connection

(2) Control connection and data connection: When the client needs to upload or download data, the data connection must be established in addition to the control connection.

FTP features two types of data connections: active (PORT) mode and passive (PASV) mode. The key difference between them is the mode of data connection establishment, yet they are basically the same in terms of control connection establishment.

## Active Mode

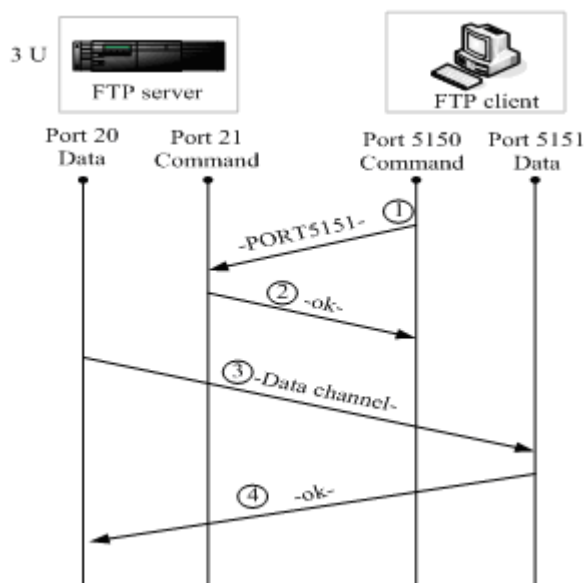


Figure 2 Port (active) Mode

In this mode, FTP server actively establishes data connection with FTP client through the following four steps:

1. The client uses the source port 5150 to communicate with the port 21 of server. The client requests to establish connection and notify the server that it is using the port 5151.
2. Upon receipt of the request, the server responds with OK (ACK) message. The client and server then exchange control signals through the control port.
3. The server opens the port 20 as the source port for sending data to the port 5151 of client.
4. The client replies and the transfer process ends.

## Passive Mode

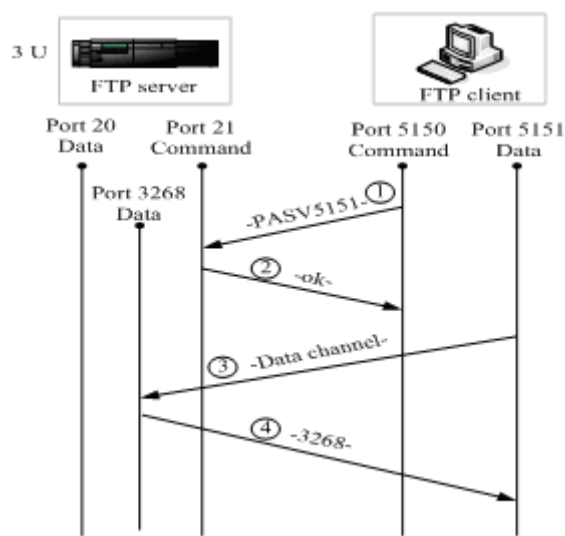


Figure 3 PASV (passive) Mode

This mode is generally configured through **passive** command. Since FTP server is passively connected to FTP client, it is referred to as passive connection. This process involves the following four steps:

1. In passive mode, the client initializes the control signal connection and uses the source port 5150 to establish connection with port 21 of server. The client uses the **passive** command to request the server to enter passive mode.
2. The server agrees to enter PASV mode, randomly selects a port number greater than 1024 and notifies the client.
3. Upon receipt of such message, the client will use the port 5151 to carry out data communication with the port 3268 as provided by the server. Here, 5151 is the source port and 3268 is the destination port.
4. Upon receipt of message, the server will transfer data and reply with ACK (OK).

When data connection is established between client and server, data upload and download can be performed, while the client can also carry out certain file system operation on the server.

**Note**

The control connection for transferring commands and replies exists all along, and the data connection is only established when needed. The application of PASV mode or PORT mode is determined only by FTP client, which will send relevant commands to use different modes of data connection. By default, Ruijie FTP client uses passive mode.

---

## FTP Transfer Mode

---

There are two FTP transfer modes: text (ASCII) transfer mode and binary (BINARY) data transfer mode. Currently, Ruijie FTP Client supports both modes, and the default mode is BINARY.

### Text Mode

---

The difference between ASCII mode and BINARY mode is the handling of new line. In ASCII mode, the new line is converted to the carriage return character of local device, such as `\n` for Unix, `\r\n` for Windows and `\r` for Mac.

### Binary Mode

---

BINARY mode can be used to transfer executable files, compressed files and image files without any data processing. Taking the example of transferring text file from Unix to Windows, the BINARY mode will not convert the new-line character from `\r` (Unix) to `\r\n`, and thus there is no line shifting when this file is viewed on Windows (you can only see black boxes). Since there is no new-line processing, the BINARY mode is faster than text mode, and all ASCII values can be transferred without error.

**Note**

If text format conversion is needed, such as the conversion between Unix-formatted text and Dos-formatted text, there are many tools available. Therefore, the Binary mode is generally the default mode of FTP.

---

## Introduction to FTP Client

---

Instead of any standard FTP client using interactive commands, Ruijie FTP Client uses the **copy** command to complete the steps of open, user and pass. After control connection is established, it will

enter file transfer process and establish data connection, allowing file upload or download.

**Note**

Our former products support TFTP, yet TFTP is only used for the transfer of small files. FTP protocol supports the transfer of large files. Implementing FTP allows the file transfer between local device and remote client and server.

## Configuring FTP Client

### Configuring Connection Mode

The default connection mode is passive (PASV) mode. To configure the device to use active mode, execute the following command in global configuration mode:

Command	Function
<b>configure terminal</b>	Enter global configuration mode
<b>ftp-client port</b>	Configure FTP to use active connection mode

To configure the device to use passive mode, execute the following command in global configuration mode:

Command	Function
<b>configure terminal</b>	Enter global configuration mode
<b>no ftp-client port</b>	Configure FTP to use passive connection mode

### Configuring Transfer Mode

The default transfer mode is BINARY mode. To configure the device to use ASCII mode, execute the following command in global configuration mode:

Command	Function
<b>configure terminal</b>	Enter global configuration mode
<b>ftp-client ascii</b>	Configure FTP to use text transfer mode

To configure the device to use BINARY transfer mode, execute the following commands in global configuration mode:

Command	Function
<b>configure terminal</b>	Enter global configuration mode
<b>no ftp-client ascii</b>	Configure FTP to use binary transfer mode

### Configuring Source IP Address

FTP Client can bind the source IP address of the client communicating with the server. Execute the following command in global configuration mode to configure the source IP address:

Command	Function
<b>configure terminal</b>	Enter global configuration mode
<b>ftp-client source-address</b> { <i>ip-address</i> / <i>ipv6-address</i> }	Configure the source IP address of FTP client (supporting IPv4 and IPv6)
To disable source IP address binding of the client, execute the following command:	
Command	Function
<b>configure terminal</b>	Enter global configuration mode
<b>no ftp-client source-address</b>	Disable source IP address binding of the client

## Restoring Default Settings

To restore default settings, execute the following command in global configuration mode:

Command	Function
<b>configure terminal</b>	Enter global configuration mode
<b>default ftp-client</b>	Restore FTP client to default settings: data connection to passive mode, file transfer to binary mode, and source IP binding removed.

## Downloading File

In CLI command mode, execute the following steps to complete file download:

Before downloading, launch FTP Server program on the host and then log into the device. In privileged EXEC mode, execute the following command to download file.

Command	Function
Ruijie# <b>copy</b> <b>ftp://username:password@dest-address[/remote-directory]/remote-file</b> <b>flash:[/local-directory]/local-file</b>	Download the file specified in URL to the device. The filename can be reset.

The key word "username" in FTP URL specifies the username for logging into the FTP Server, and must not exceed 32 bytes or include such characters as ":", "@", "/" or space, nor can it be omitted. The key word "password" specifies the password for logging into FTP Server, and is subject to the same constraints of username. The key word "dest-address" specifies the IP address of FTP Server, and the optional key word "remote-directory" specifies the directory on Server. The key word "remote file" specifies the target filename on the Server. The optional key word "local-directory" in Flash URL specifies the directory on device, or implies the current directory if not specified. The key word "local-file" specifies the target local filename.



### Caution

If Flash URL contains the "directory" field, the user must ensure that such directory has been created on the device. Automatic directory creation is not supported by this download command.

## Example of File Download

Using username of "user" and password of "pass" to download a file named "remote-file" from the directory "root" on FTP Server with IP address being 192.168.23.69 to directory "home" on the local device, and change the name to "local-file".

```
Ruijie# copy ftp://user:pass@192.168.23.69/root/remote-file flash: home/local-file
```

## Uploading File

In CLI command mode, execute the following steps to complete file upload:

Before uploading, launch FTP Server program on the host and then log into the device. In privileged EXEC mode, execute the following command to upload file. The key word "dest-address" specifies the IP address of FTP Server.

Command	Function
Ruijie# <b>copy</b> <b>flash:</b> <i>[local-directory]/local-file</i> <b>ftp:</b> <i>//username:password@dest-address[/remote-directory]/remote-file</i>	Upload the file specified in Flash URL to the host. The filename can be reset.

Please refer to the previous command for descriptions of key words and parameters.

## Example of File Upload

Using username of "user" and password of "pass" to upload a file named "local-file" from the directory "home" on the device to directory "root" on FTP Server, and change the name to "remote-file".

```
Ruijie# copy flash: home/local-file ftp://user:pass@192.168.23.69/root/remote-file
```



# FTP Server Configuration

## Overview

You can set a device as the FTP server. Then you can connect to the FTP server through a FTP client and upload or download documents through the FTP protocol.

FTP server enables you to get documents from devices like Syslog file. You can also copy documents to the file system of devices directly.

## FTP Commands Supported

Upon receiving a FTP connection request, the FTP server requires the FTP client offer login user name and password for authentication.

The FTP client can run commands only when it passes authentication. Not all FTP client commands are supported at present. The following table shows the FTP client commands supported:

ascii	delete	mdelete	mput	quit	send
bin	dir	mdir	nlist	recv	size
bye	disconnection	mget	open	rename	system
cd	get	mkdir	passive	rhel	type
cdup	image	mls	put	rmdir	user
close	ls	modtime	pwd	rstatus	

For the method to use above mentioned FTP client commands, refer to FTP client software document. In addition, many FTP client tools, for instance, CuteFTP and FlashFXP have graphic operation interface. Users no longer need to use FTP commands.

## Configure the FTP Server

### Enable or Disable the FTP Server

By default, the FTP Server is disabled. To enable the FTP server, run the **ftp-server enable** command in the global configuration mode. It should be noted that the FTP client cannot access the FTP server before you configure the top directory, login user name and password of the FTP server. So it is recommended to refer to the later sections to configure the top directory, login user name and password before enabling the FTP Server for the first time.

To disable the FTP server, run the **no ftp-server enable** command in the global configuration mode.

Command	Function
---------	----------

Ruijie(config)# <b>ftp-server enable</b>	Enable the FTP Server.
Ruijie(config)# <b>no ftp-server enable</b>	Disable the FTP Server.

**Caution**

In real network, only one client is allowed to access the FTP server at a time. Before the client currently in service is disconnected, no other clients can connect to the FTP server.

## Configure the Top Directory

The function limits the range that the FTP client can access. (For the details on how to view and manage the directories on the device, refer to *File System Configuration Guide*.) For instance, you can set the top directory to the “/syslog” directory. After logging in the FTP Server, the FTP client can access only the files and folders under the “/syslog” directory.

To configure the top directory, run the **ftp-server topdir** command in the global configuration mode. The **no** form of this command removes the top directory configuration and prohibits the FTP client to access any files on the FTP server.

Command	Function
Ruijie(config)# <b>ftp-server topdir</b> <i>directory</i>	Configures the top directory of the FTP Server.
Ruijie(config)# <b>no ftp-server topdir</b>	Removes the top directory configuration and prohibits the FTP client to access any files on the FTP server.

Assume that log files are stored under the “/syslog” directory. To download log files from a device through the FTP client on the management PC while prohibiting the FTP client from accessing the files other than the “/syslog” directory, configure the top directory as below:

```
Ruijie(config)# ftp-server topdir /syslog
```

After configuration, the FTP client can only access the files and sub directories under the “/syslog” directory. Given the limit of the top directory, the FTP client cannot back to the parent directory of the “/syslog” directory.

## Configure Session Idle Time Out

The FTP Server does not support parallel connections. When a user logs in to the FTP Server, the FTP Server may maintain this connection in case of abnormal abortion. Consequently, the FTP Server occupies this connection for a long period of time and cannot respond the login requests of other users.

Session idle timeout can be used to solve this problem. When the FTP Server does not interact with one user within a specific period of time, the FTP Server considers that the connection is not available and automatically disconnects the connection. The session idle timeout is 30 minutes by default.

To configure session idle timeout, run the **ftp-server timeout** command in the global configuration mode.

Command	Function
Ruijie(config)# <b>ftp-server timeout</b> <i>time</i>	Sets the session idle timeout. time: idle timeout in the range of 1-3600 minutes

Ruijie(config)# <b>no ftp-server timeout</b>	Restores the idle timeout to the default value (30 minutes)
--	---

The following example sets the session idle timeout to 5 minutes:

```
Ruijie(config)# ftp-server timeout 5
```

If the FTP client has not executed any operation within five minutes, the FTP Server automatically disconnects the connection and then begins to respond other connection requests.



**Caution** The session idle timeout refers to the time period between two operations in a FTP session. The FTP Server starts to calculate the session idle time from 0 after completing a command (for instance, transferring a file) and stops calculation before executing a new command. Consequently, this configuration will not influence some time-consuming file transmission.

## Configure Login User Name and Password

The FTP Server uses login user name and password to authentication clients. By default, the login user name and password are null.

Anonymous user and null password are not supported on the FTP Server. To configure valid login user name and password in the global configuration mode, run the **ftp-server username** and **ftp-server password** commands in the global configuration mode. Only one user name and password can be configured on the FTP Server.

Command	Function
Ruijie(config)# <b>ftp-server username</b> <i>username</i>	Sets user name.
Ruijie(config)# <b>no ftp-server username</b>	Removes the user name configuration.
Ruijie(config)# <b>ftp-server password</b> [ <i>type</i> ] <i>password</i>	Sets a password.
Ruijie(config)# <b>no ftp-server password</b>	Removes the password configuration.

A user name consists of up to 64 characters, including English letter, half-width numeral and half-width symbol, not blank space.

A password consists of letters or numerals. Blank space is allowed behind and in front of the password, but it will be ignored. The length of a password in plain text mode ranges from 1 to 25 characters and a password in cipher text mode ranges from 4 to 52 characters.

The following example sets the user name to “admin” and password to “letmein”.

```
Ruijie(config)# ftp-server username admin
Ruijie(config)# ftp-server password letmein
```

## View Status and Debugging Information

To view status and debugging information, run the **show ftp-server** and **debug ftpserver** command in the privileged EXEC configuration mode.

Command	Function
Ruijie# <b>show ftp-server</b>	Shows the status of the FTP Server.
Ruijie# <b>debug ftpserver</b>	Turns on the debugging of the FTP Server.
Ruijie# <b>no debug ftpserver</b>	Turns off the debugging of the FTP Server.

The following example shows the status information of the FTP Server:

```
Ruijie# show ftp-server
ftp-server information
=====
enable : Y
topdir : /
timeout: 20min
username config : Y
password config : Y
type: BINARY
control connect : Y
ftp-server: ip=192.167.201.245 port=21
ftp-client: ip=192.167.201.82 port=4978
port data connect : Y
ftp-server: ip=192.167.201.245 port=22
ftp-client: ip=192.167.201.82 port=4982
passive data connect : N
```

The following example turns on the debugging of the FTP Server:

```
Ruijie# debug ftpserver
FTPSRV_DEBUG:(RECV) SYST
FTPSRV_DEBUG:(REPLY) 215 RGOS Type: L8
FTPSRV_DEBUG:(RECV) PORT 192,167,201,82,7,120
FTPSRV_DEBUG:(REPLY) 200 PORT Command okay.
```

The following example turns off the debugging of the FTP Server:

```
Ruijie# no debug ftpserver
```

## Typical FTP Server configuration Example

### Networking Requirements

The logs of a device (Switch A in the following figure) are stored in the directory of "/syslog". By configuring the FTP Server, the following requirements must be met:

- The client can login FTP server with username of "admin" and password of "ruijie".
- After successful login, the FTP client on the management PC can directly download logs from the device, but the FTP client is not allowed to access files in directories other than "/syslog".
- If the current client carries out no operation within 5 minutes, the FTP server will be disconnected automatically. After disconnection, the FTP server can respond to the new access requests.

### Network Topology

Figure 1-1 Diagram for typical FTP application



### Configuration Tips

To meet the above requirements, execute the following steps:

- 1) Configure the username and password for server login as "admin" and "ruijie" respectively;
- 2) Configure session timeout timer as 5 minutes;
- 3) Configure the top directory of server as "/syslog";
- 4) Enable FTP server;

### Configuration Steps

# Configure SwitchA as the FTP Server

Step 1: Configure the username and password for server login as "admin" and "ruijie" respectively

```
Ruijie#configure
Enter configuration commands, one per line. End with CNTL/Z.
Ruijie(config)#ftp-server username admin
Ruijie(config)#ftp-server password ruijie
```

Step 2: Configure session timeout timer as 5 minutes

```
Ruijie(config)#ftp-server timeout 5
```

Step 3: Configure the top directory of server as "/syslog";

```
Ruijie(config)#ftp-server topdir /syslog
```

Step 4: Enable FTP server

```
Ruijie(config)#ftp-server enable
```

## Verification

Step 1: Display the relevant state of FTP server:

```
Ruijie(config)#show ftp-server
      ftp-server information
=====
enable : Y
topdir : /syslog
timeout: 5min
username config : Y
password config : Y
transfer type: ASCII
control connection : N
port data connection : N
passive data connection : N
```

Step 2: Debug the FTP server

```
Ruijie# debug ftpserver
FTPSRV_DEBUG:(RECV)  SYST
FTPSRV_DEBUG:(REPLY) 215 RGOS Type: L8
FTPSRV_DEBUG:(RECV)  PORT 192,167,201,82,7,120
FTPSRV_DEBUG:(REPLY) 200 PORT Command okay.
```

# Network Communication Detection Tools Configuration

## Ping Connectivity Test

To test the connectivity of a network, many network devices support the **Echo** protocol. The protocol sends a special packet to a specified network address and waits for a response. This allows you to evaluate the connectivity, delay and reliability of a network. The ping tool provided by RGOS can effectively help users diagnose and locate the connectivity problems in a network.

The **Ping** command runs in the user EXEC mode and privileged EXEC mode. In the user EXEC mode, only basic ping functions are available. However, in the privileged EXEC mode, extended ping functions are available.

Command	Function
Ruijie# <b>ping</b> [ip] [address [length length] [ntimes times] [data data] [source source] [timeout seconds] [df-bit] [validate] ]	Test the network connectivity.

The basic ping function can be performed in either the user EXEC mode or the privileged EXEC mode. By default, this command sends five 100-byte packets to the specified IP address. If the system receives a response within the specified time (2 seconds by default), it shows "!" . Otherwise, it shows ".". Finally, the system shows statistics. This is a normal ping example:

```
Ruijie# ping 192.168.5.1
Sending 5, 100-byte ICMP Echoes to 192.168.5.1, timeout is 2 seconds:
< press Ctrl+C to break >
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/10 ms
```

The extended ping function can be performed in the privileged EXEC mode only. This function allows you specify the number of packets, packet length, and timeout. As with the basic ping function, the extended ping also shows statistics. The following is an example of the extended ping:

```
Ruijie ping 192.168.5.197 length 1500 ntimes 100 data ffff source 192.168.4.190 timeout 3
Sending 100, 1000-byte ICMP Echoes to 192.168.5.197, timeout is 3 seconds:
< press Ctrl+C to break >
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!
Success rate is 100 percent (100/100), round-trip min/avg/max = 2/2/3 ms
Ruijie#
```

## Ping IPv6 Connectivity Test

To test the connectivity of a network, many network devices support the **Echo** protocol. The protocol sends a special packet to a specified network address and waits for a response. This allows you to evaluate the connectivity, delay and reliability of a network. The ping tool provided by RGOS can effectively help users diagnose and locate the connectivity problems in a network.

The **Ping ipv6** command runs in the user EXEC mode and privileged EXEC mode. In the user EXEC mode, only basic **ping IPv6** functions are available. However, in the privileged EXEC mode, extended **ping IPv6** functions are available.

Command	Function
Ruijie# <b>ping ipv6</b> [ <i>address</i> [ <b>length</b> <i>length</i> ] [ <b>ntimes</b> <i>times</i> ] [ <b>data</b> <i>data</i> ][ <b>source</b> <i>source</i> ] [ <b>timeout</b> <i>seconds</i> ]	Test the network connectivity.

The basic ping function can be performed in either the user EXEC mode or the privileged EXEC mode. By default, this command sends five 100-byte packets to the specified IP address. If the system receives a response within the specified time (2 seconds by default), it shows "!". Otherwise, it shows ".". If the response does not match the request, the system shows "C" and outputs statistics. This is a normal ping example:

```
Ruijie# ping ipv6 2000::1
Sending 5, 100-byte ICMP Echoes to 2000::1, timeout is 2 seconds:
< press Ctrl+C to break >
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/10 ms
```

The extended ping function can be performed in the privileged EXEC mode only. This function allows you specify the number of packets, packet length, and timeout. As with the basic ping function, the extended ping also shows statistics. The following is an example of the extended ping:

```
Ruijie# ping ipv6 2000::1 length 1500 ntimes 100 data ffff source 2000::2 timeout 3
Sending 100, 1000-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
```

## Traceroute Connectivity Test

The **Traceroute** command is mainly used to check the network connectivity. It shows all the gateways that a packet passes through from the source to the destination and exactly locates the fault when the network fails.

One of the network transmission rules is that the number in the TTL field in the packet will decrease by 1 every time when a packet passes through a gateway. When the number in the TTL field is 0, the gateway will discard this packet and send a TTL overtime error message back to the source. According to this rule, the execution of the **traceroute** command is as follows: At first, the source sends a packet whose TTL is 1 to the destination address. The first gateway sends an ICMP error message back, indicating that this packet cannot be forwarded for TTL timeout. Then, the first gateway re-sends the packet after the TTL domain adds 1. Likewise, the second gateway returns a TTL timeout error and the process lasts until the packet reaches the destination address. By recording every address returning the ICMP TTL timeout message, you can draw the entire path passed by the IP packet from the source address to the destination address.

The **traceroute** command can run in the user EXEC mode and the privileged EXEC mode. The command format is as follows:

Command	Function
---------	----------



Command	Function
Ruijie# <b>traceroute</b> [ <i>protocol</i> ] [ <i>address</i> ] [ <b>probe</b> <i>probe</i> ] [ <i>t</i> <b>tl</b> <i>minimum</i> <i>maximum</i> ] [ <b>s</b> <i>source</i> <i>source</i> ] [ <i>t</i> <b>imeout</b> <i>seconds</i> ]]	Trace the path that a packet passes through.

The following are two examples that apply **traceroute**. In one example, network connectivity is good. In another example, some gateways in a network are not connected.

■ **traceroute** example where network connectivity is good:

```
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  202.101.143.130   4 msec  16 msec   8 msec
 6  202.101.143.154  12 msec   8 msec  24 msec
 7  61.154.22.36     12 msec   8 msec  22 msec
```

As you can see, to access the host with an IP address of 61.154.22.36, the network packet passes through gateways 1 to 6 from the source address. Meanwhile, you can know the time that the network packet spends to reach a gateway. This is very useful for network analysis.

■ **traceroute** example where some gateways in a network are not connected:

```
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
```

As you can see, to access the host with an IP address of 202.108.37.42, the network packet passes through gateways 1 to 17 from the source address and the gateway 4 does not reply to ICMP packet.

## Traceroute IPv6 Connectivity Test

The **Traceroute ipv6** command is mainly used to check the network connectivity. It shows all the gateways that a packet passes through from the source to the destination and exactly locates the fault when the network fails.

For network **transmission**, refer to the previous section.

The **traceroute ipv6** command can run in the user EXEC mode and the privileged EXEC mode. The command format is as follows:

Command	Function
Ruijie# <b>traceroute ipv6</b> [ <i>address</i> [ <i>probe probe</i> ] [ <i>ttl minimum maximum</i> ] [ <i>timeout seconds</i> ]]	Trace the path that a packet passes through.

The following are two examples that apply **traceroute ipv6**. In one example, network connectivity is good. In another example, some gateways in a network are not connected.

### ■ **traceroute ipv6** example where network connectivity is good:

```
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
```

As you can see, to access the host with an IP address of *3004::1*, the network packet passes through gateways 1 to 3 from the source address. Meanwhile, you can know the time that the network packet spends to reach a gateway. This is very useful for network analysis.

### ■ **traceroute ipv6** example where some gateways in a network are not connected:

```
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
```

As you can see, to access the host with an IP address of *3004::1*, the network packet passes through gateways 1 to 4 from the source address and the gateway 4 does not reply to ICMP packet.

# TCP Configuration Configuration

## overview

---

TCP module provides a reliable and connective IP-based transmission layer protocol for the application layer.

The application layer sends data streams represented in 8-bit bytes for Internet transmission to the TCP layer, which separates the data streams into packet segments with proper size. The maximum segment size (MSS) is generally limited by the maximum transmission unit (MTU) of the data link layer of the network to which the computer is connected. After that, TCP transmits the result packets to the IP layer, which will then transmit the said packets through the network to the TCP layer of receiving terminal.

To ensure no packet loss, TCP assigns a sequence number to each byte, and the sequence number also ensures that packets transmitted to the receiving terminal are received in sequence. The receiving terminal will then reply with an ACK to confirm the receipt of each byte. If no ACK is received within the reasonable Round Trip Time (RTT), then the corresponding byte (assumed lost) will be retransmitted by the sender.

- With regard to data accuracy and validity, TCP uses a checksum function to verify the data. The checksum must be calculated while the data is sent or received. In the meantime, MD5 authentication can also be utilized to encrypt the data.
- To ensure reliability, TCP applies the mechanisms of timeout retransmission and piggybacking.
- The sliding window protocol is applied to implement flow control. According to the protocol, all unconfirmed packets within the window will be retransmitted.
- The widely recognized TCP congestion control algorithm (also called AIMD algorithm) is applied to implement congestion control. This algorithm mainly involves: 1) additive increase, multiplicative decrease; 2) slow start; 3) response to timeouts.

## Configuring TCP

---

### Changing the Timeout for Establishing TCP Session

Establishing TCP session requires a three-way handshake: the local end sends a SYN packet, the remote end responds with a SYN+ACK packet, and then the local end responds with an ACK.


- After the local end sends SYN, if the remote end doesn't respond with SYN+ACK, the local end will continuously retransmit SYN packets until a specified number of retransmissions are reached or until the timeout timer expires.
- After the local end sends SYN and the remote end responds with SYN+ACK, if the local end no longer responds with ACK, the remote end will retransmit continuously until a specified number of retransmissions is reached or until the timeout timer expires. (Such as SYN attack).

Execute the following command to configure the timeout value for SYN packet (the maximum time from SYN transmission to successful three-way handshake), namely the timeout for establishing TCP session.

Command	Function
Ruijie(config)# <b>ip tcp syntime-out</b> <i>seconds</i>	Change the timeout value for establishing TCP session. Range: 5-300 seconds; default: 20

Use the **no ip tcp syntime-out** command to restore the default value.

---

 This command only applies to IPv4 TCP.

---


## Changing Window Size

The TCP receiving buffer is utilized to buffer the data received from the peer end. These data will be subsequently read by the application program. Generally, the window size of TCP packets implies the size of free space in the receiving buffer. For sessions featuring greater bandwidth ratio and excess data, increasing the size of receiving buffer will provide notable TCP transmission performance. The sending buffer is utilized to buffer the data of application program. Each byte in the buffer has its sequence number, and byte with sequence number acknowledged will be removed from the sending buffer. Increasing the sending buffer will improve the interaction between TCP and application program and thus enhance the performance. However, increasing the receiving buffer and sending buffer will result in more memory consumption of TCP.

Command	Function
Ruijie(config)# <b>ip tcp window-size</b> <i>size</i>	Change the size of receiving buffer and sending buffer for TCP session. Range: 0-65535 bytes; default: 4096.

Use the **no ip tcp window-size** command to restore the default value.

---

 This command only applies to IPv4 TCP.

---



**Note** This command doesn't apply to the existing TCP session; it only applies to the newly established TCP session.



**Note** This command will apply to both the receiving buffer and sending buffer.

---

## Prohibiting the Reset Packet When the Port is Unreachable

When the TCP module distributes TCP packets, if the TCP session to which such packets belong cannot be found, a reset packet will be replied to the peer end to terminate the TCP session. The attacker may initiate attacks by sending excess port-unreachable TCP packets.

Execute the following command to prohibit/restore the reset packet sent when the port-unreachable TCP packet is received.

Command	Function
Ruijie(config)# <b>ip tcp not-send-rst</b>	Prohibit sending reset packet when the port-unreachable TCP packet is received.

Use the **no ip tcp not-send-rst** command to restore default setting.



This command only applies to IPv4 TCP.

## Limiting the Maximum Segment Size of TCP Session

MSS (Maximum Segment Size) refers to the maximum size of the payload of a TCP packet, excluding TCP options.

During the three-way handshake for establishing a TCP session, one important job is to carry out MSS negotiation. Both sides will insert MSS option into the SYN packet to indicate the maximum size of segment that can be received by the local end, namely the maximum size of segment that can be sent by the remote end. Both sides will take the lower of the MSS value sent locally and that received from the remote end as the maximum segment size of this session.

The methods for calculating the value of MSS option while sending SYN packet are shown below:

- Non-directly connected network:  $mss = \text{default value of } 536$ .
- Directly connected network:  $mss = \text{egress interface MTU corresponding to the peer IP address} - 20\text{-byte ip header} - 20\text{ byte TCP header}$ .  
Generally speaking, if mtu is affected by certain application configured on the egress interface, such application will configure the mtu accordingly, such as tunnel port, vpn port and etc.



**Note** In release 10.4(3), in the syn+ack packet replied by the remote end of a directly connected network, the mss option is not calculated through mtu. Instead, the default value of 536 is used.



**Note** The mss calculated cannot exceed the size of receiving buffer or the ip tcp mss configured by the user. Otherwise, the lower of them will be used.



**Note** If certain options are supported by this session, then the size obtained after 4-byte alignment of the option must be subtracted from mss. For example, the size of MD5 option is 18 bytes, and 20 bytes will be obtained after alignment.

The rmss value obtained here is the value of mss option in the syn packet sent. For example, BGP adjacency is generally established in the directly connected network, and the mss of such session is  $1500 - 20 - 20 - 20 = 1440$ .

The function of IP TCP MSS is to limit the MSS of the pending TCP session. The negotiated MSS cannot exceed the value configured.

Command	Function
Ruijie(config)# <b>ip tcp mss</b> <i>max-segment-size</i>	Limit the maximum segment size of TCP session. Range: 68-10000 bytes.

Use the **no ip tcp mss** command to disable such limit.

☒ This command only applies to IPv4 TCP.

## Enabling PMTU Discovery

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.

Command	Function
Ruijie(config)# <b>ip tcp path-mtu-discovery</b> [ <b>age-timer</b> <i>minutes</i>   <b>age-timer infinite</b> ]	Enable PMTU discovery. <b>age-timer</b> <i>minutes</i> : The time interval for further discovery after discovering PMTU. Range: 10-30 minutes. Default: 10. <b>age-timer infinite</b> : No further discovery after discovering PMTU.

According to RFC1191, after discovering PMTU, TCP can use greater MSS to discover new PMTU, and the time interval thereof is specified with the parameter **age-timer**. When the PMTU discovered by the device is smaller than the MSS negotiated, the device will try to discover greater PMTU as per the aforementioned time interval. Such discovery process will not end until PMTU reaches the value of MSS or until user stop this timer. To turn off the timer, use the parameter **age-timer infinite**.

Use the **no ip tcp path-mtu-discovery** command to disable PMTU discovery.

☒ This command applies to both IPv4 TCP and IPv6 TCP.



**Note** This command doesn't apply to the existing TCP session; it only applies to the newly established TCP session.

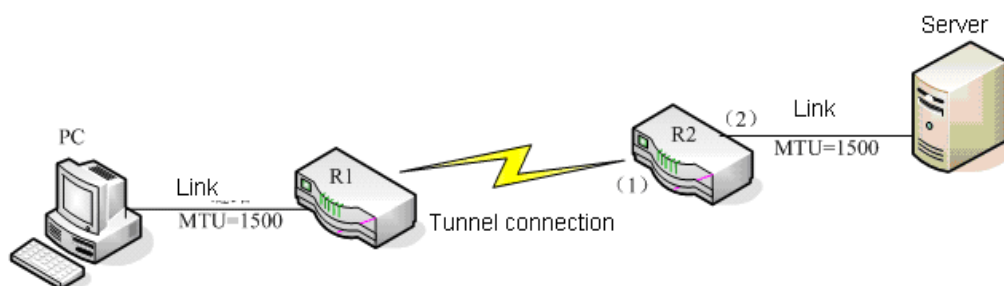
## Configuring the MSS Option Value of SYN Packets Sent and Received on the Interface

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 session, it negotiates the maximum payload of TCP packets through the MSS option field of TCP SYN packet. The MSS value of client's SYN packet implies the maximum payload of TCP packets sent by the server, and vice versa.

As shown below, PC may fail to access the server through http, because the MSS of 1460 will be negotiated between PC and server, but such MSS cannot pass R1 and R2 (R1 and R2 are connected through tunnel, with MTU lower than 1500).

Figure 1-1



In such a case, we can configure the following command on port (1) and port (2) of R2 to change the MSS option value of SYN packet, so as to change the MSS value negotiated for the TCP session going through port (1) and port (2).

Command	Function
Ruijie(config-if)# <b>ip tcp adjust-mss</b> <i>max-segment-size</i>	Configure the MSS option value of SYN packets sent and received on the interface. Range: 500-1460 bytes.

Use the **no ip tcp adjust-mss** command to remove the configuration. In such a case, the MSS option value of packets won't be changed when the interface sends and receives SYN packets.

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. It is suggested to configure the same value on the ingress interface and egress interface, or else the MSS option of SYN packets going through the device will be changed to the lower of two values configured.



This command only applies to IPv4 TCP and only supports router products.

## Monitoring and Maintenance

Command	Function
Ruijie# <b>show tcp connect</b>	Display basic information about the current TCP sessions.
Ruijie# <b>show tcp pmtu</b>	Display information about TCP PMTU.
Ruijie# <b>show tcp port</b>	Display information about the current TCP port.

# IPv4 Express Forwarding Configuration

## Overview

---

To adapt to the needs of high-end devices, currently we are using "Prefix Tree + Adjacency" Express Forwarding model to achieve fast forwarding. In case the device only caches partial information of the core routing table, the central CPU will have to add cache entries again if the cache fails. Express Forwarding maintains a mirror image of the entire core routing table in order to relieve CPU load and guarantee the stability of routing performance.

Express Forwarding uses the following two components to create the mirror image of routing table:

### ■ Prefix Tree

This is an IP prefix tree organized as per the longest matching principle to look up adjacent nodes. In practice, the data structure for constructing Prefix Tree is generally different from the Radix Tree of core routing table. A data structure called M-Tries Tree is used to realize faster lookup. The Prefix Tree created by M-Tries Tree will consume more memory than Radix Tree, and the update of Prefix and node information will be comparatively time-consuming, but higher lookup performance can be realized.

### ■ Adjacency

Adjacent node, including the output interface information of routed packets, such as next hop list, next processing unit, link-layer output encapsulation and etc. When packets matches with such adjacent node, the packets will be encapsulated and forwarded by calling the transmit function of this node. To facilitate lookup and update, the adjacent nodes will generally form a hash table. To support router load balancing, the next-hop entries of adjacent nodes are organized into a load balancing table. Adjacent node may not include next-hop information, or may include the index number of next processing unit (such as other line cards, multi-service card and etc).

Express Forwarding comprises three steps:

1. Express Forwarding to de-encapsulate packets;
2. Use Prefix Tree to look up the next-hop adjacent node of packet route;
3. After matching to the next-hop adjacent node, the final egress interface of packets will be determined according to the information of adjacent node, and packets will be encapsulated according to the type of egress interface.

## Configuring Express Forwarding Load Balancing Policy

---

Fast forwarding supports load balancing of packets, and currently two IP address based load balancing policies are supported. In EF model, when route prefix IP/MASK is associated with multiple next hops (multipath routing), this route will be associated with a load balancing table and achieve load balancing according to its weight. When IP packets match with this load balancing table as per the longest prefix, Express Forwarding will



select one of the paths to forward packets according to the hash IP address of packets.

1. Perform load balancing as per the destination IP of IP packets and include destination address of packets in the hash; path with greater weight value will be selected. The policy is used by default.
2. Perform load balancing as per the destination IP and source IP of IP packets and include destination IP and source IP of packets in the hash; path with greater weight value will be selected.

## Flooding

Express forwarding obtains the MAC address corresponding to next hop of route from the ARP table, and obtains the corresponding physical port from the MAC address table. If no physical port is found in the MAC address table, how will the chip process packets matching this route (broadcast in VLAN or discard)? Broadcom chip doesn't support flooding, but Marvell chip does. By default, the chip will discard such packets. After executing this flooding command, the chip will broadcast packets on the VLAN.

To configure load balancing policy, execute the following commands in global configuration mode:

Command	Function
Ruijie(config)# <b>ip ref broadcast-in-vlan</b>	Enable flooding, namely if no physical port is found in the MAC address table, the chip will broadcast these packets in VLAN.

## Express Forwarding table Maintenance and Monitoring

The express forwarding module only passively receives and maintains the external routing information, and will not actively insert or delete any routing information. Therefore, express forwarding mainly provides the statistics of existing routes.

To monitor and maintain the express forwarding table, the following commands are provided:

- Global statistics
- Adjacency table
- Packet forwarding path
- Routes in express forwarding table
- Synchronize express forwarding table to hardware forwarding table

### Global Statistics

Global statistics refers to the data structure related information in the existing fast forwarding table, including the number of existing routes, the number of adjacent nodes, the number of load balancing tables and the number of weighted nodes.

Command	Function
Ruijie# <b>show ip ref</b>	Display statistics in the existing express forwarding table.

## Adjacency Table

In the express forwarding table, adjacency list is one of the important data structure. Execute the following commands to view existing adjacency information:

Command	Function
Ruijie# <b>show ip ref adjacency [glean   local   ip   (interface <i>interface_type</i> <i>interface_number</i>) ]</b>	Display the glean adjacency, local adjacency, IP-specific adjacency, interface-specific adjacency and all adjacent nodes.

In the event of the following cases, the adjacency table will be used to forward packets.

1. Direct route, such as 1.1.0.0/16 vlan1
2. A route with longer mask than the direct route, such as 1.1.1.0/24 vlan2 2.2.2.2
3. Neighbor with direct route, such as 1.1.1.1.

Packets with destination IP address being 1.1.1.1 will be forwarded according to the information of adjacency 1.1.1.1, as 1.1.1.1/32 is the longest match route.

## Packet Forwarding Path

The router forwarding of packets is performed based on the IP address of packets. If the source IP address and destination IP address of packets are specified, then the forwarding path of such packets will be definitive. Executing the following command and specifying the source IP and destination IP of packets will display the actual forwarding path of such packets, such as packet discarding, CPU submission or forwarding. The interface through which the packets are forwarded can also be learned.

Command	Function
Ruijie# <b>show ip ref exact-route</b> <i>source-ipaddress dest_ipaddress</i>	Display the actual forwarding path for specific packets



### Caution

The above commands are router-specific commands.

## Routes in Express Forwarding Table

Express forwarding receives external route advertisement and maintains its own express forwarding table, which is a mirror image of core routing table sharing same routing information. Execute the following commands to display relevant routing information in the express forwarding table.

Command	Function
---------	----------

Ruijie# <b>show ip ref route [default   (ip mask)]</b>	Display the default routing information in the existing express forwarding table. If no default route is specified, all routing information in the express forwarding table will be displayed, including routes, default route and ordinary gateway routes.
--	---

## Synchronizing Express Forwarding Table to Hardware Forwarding Table

On a layer-3 switch, the hardware forwarding table and software forwarding table may be inconsistent due to the case that the total number of routes in software forwarding table exceeds the capacity of hardware forwarding table or the conflict between hardware and hash bucket. If the total number of routes in software forwarding table exceeds the capacity of hardware forwarding table, the user shall manage to reduce the number of routes and then execute "ip ref synchronize all" command in privilege mode to synchronize the software forwarding table to hardware forwarding table, yet there is no solution to the conflict between hardware and hash bucket.

Command	Function
Ruijie# <b>ip ref synchronize all</b>	When software forwarding table and hardware forwarding table are inconsistent, execute this command to synchronize.

In case the capacity of hardware forwarding table is insufficient or there is a conflict between hardware and hash bucket, such event will be printed in logs in the format of: EFHW-4-(TBL\_NO\_RESOURCE): DESCRIPTION.

# IP Routing Configuration

---

## 1. IP Routing Configuration

# IP Routing Configuration

## Enabling IP Routing

By default, the IPv4 or IPv6 routing function is enabled.

Command	Function
Ruijie(config)# <b>ip routing</b>	Enable the IPv4 routing function.
Ruijie(config)# <b>ipv6 unicast-routing</b>	Enable the IPv6 routing function.

Use the **no** form of this command to disable the IPv4 or IPv6 routing function.



### Note

The IS2700G series products support only the IPv4 or IPv6 static routes, and IPv4 or IPv6 directly connected route.



### Note

Configure the static route to obtain the IPv4 or IPv6 static route.



### Note

Configure the IP address of the SVI to obtain the IPv4 or IPv6 directly connected route.

For the example of configuring static routes, see “Example of Dynamic Routes Overriding Static Routes” in this chapter.

If they are not deleted, Ruijie product will always retain the static routes. However, you can replace the static routes with the better routes learned by the dynamic routing protocols. Better routes mean that they have smaller distances. All routes including the static ones carry the parameters of the management distance. The following table shows the management distances of various sources of Ruijie product:

## Configuring Static Routes

Static routes are manually configured so that the packets can be sent to the specified destination network go through the specified route. Multiple static routes can be configured. The new route cannot be added if the number of the configured static routes reaches the upper limit.

Command	Function
Ruijie(config)# <b>ip route</b> <i>network net-mask</i> { <i>ip-address</i>   <i>interface</i> [ <i>ip-address</i> ] } [ <i>distance</i> ] [ <b>tag</b> <i>tag</i> ] [ <b>permanent</b> ] [ <b>disable</b>   <b>enable</b> ]	Configure the IPv4 static route.
Ruijie(config)# <b>ipv6 route</b> <i>ipv6-prefix / prefix-length</i> { <i>ipv6-address</i>   <i>interface</i> [ <i>ipv6-address</i> ] } [ <i>distance</i> ]	Configure the IPv6 static route.
Ruijie(config)# <b>ip static route-limit</b> <i>number</i>	Configure the upper limit of the IPv4 static route.

Ruijie(config)# <b>ipv6 static route-limit</b> <i>number</i>	Configure the upper limit of the IPv6 static route.
--	---

When a port is “down”, all routes to that port will disappear from the routing table. In addition, when Ruijie product fails to find the forwarding route to the next-hop address, the static route will also disappear from the routing table.

**Note**

The IS2700G series products support up to 32 IPv4 static routes and 16 IPv6 static routes.

**Note**

The IPv4 static route supports only the default route with the mask being 0, and the host route with the mask being 32.

**Note**

The IPv6 static route supports only the default route with the mask being 0, and the host route with the mask being 128.

## Displaying the Routing Table

Use the following commands in privileged EXEC mode, global configuration mode or interface configuration mode to display the routing table.

Command	Function
<b>show ip route</b> [ <i>network</i> [ <i>mask</i> ]   <b>count</b>   <b>summary</b> ]	Display the IPv4 routing table.
<b>show ipv6 route</b> [ <i>network prefix-length</i>   <b>summary</b> ]	Display the IPv6 routing table.

## Multicast Configuration

---

1. IGMP Snooping Configuration
2. MLD Snooping Configuration
3. Multicast Forwarding Control Configuration

# IGMP Snooping Configuration

## Overview

### Understanding IGMP Snooping

Internet Group Management Protocol, abbreviated as IGMP Snooping, is an IP multicast flow mechanism running in the VLAN, and used to manage and control the IP multicast flow forwarding in the VLAN and belongs to the Layer2 multicast function. The IGMP Snooping function described below is in the VLAN, and the related ports are the member ports in the VLAN.

The device running IGMP Snooping sets up the mapping for the port and the multicast address by analyzing the received IGMP packets, and forwards the IP multicast packets based on the mapping. As shown in the Figure-1, with IGMP Snooping enabled, the IP multicast packets are broadcasted in the VLAN; while without IGMP Snooping enabled, the known IP multicast packets are not broadcasted in the VLAN but sent to the specified recipient.

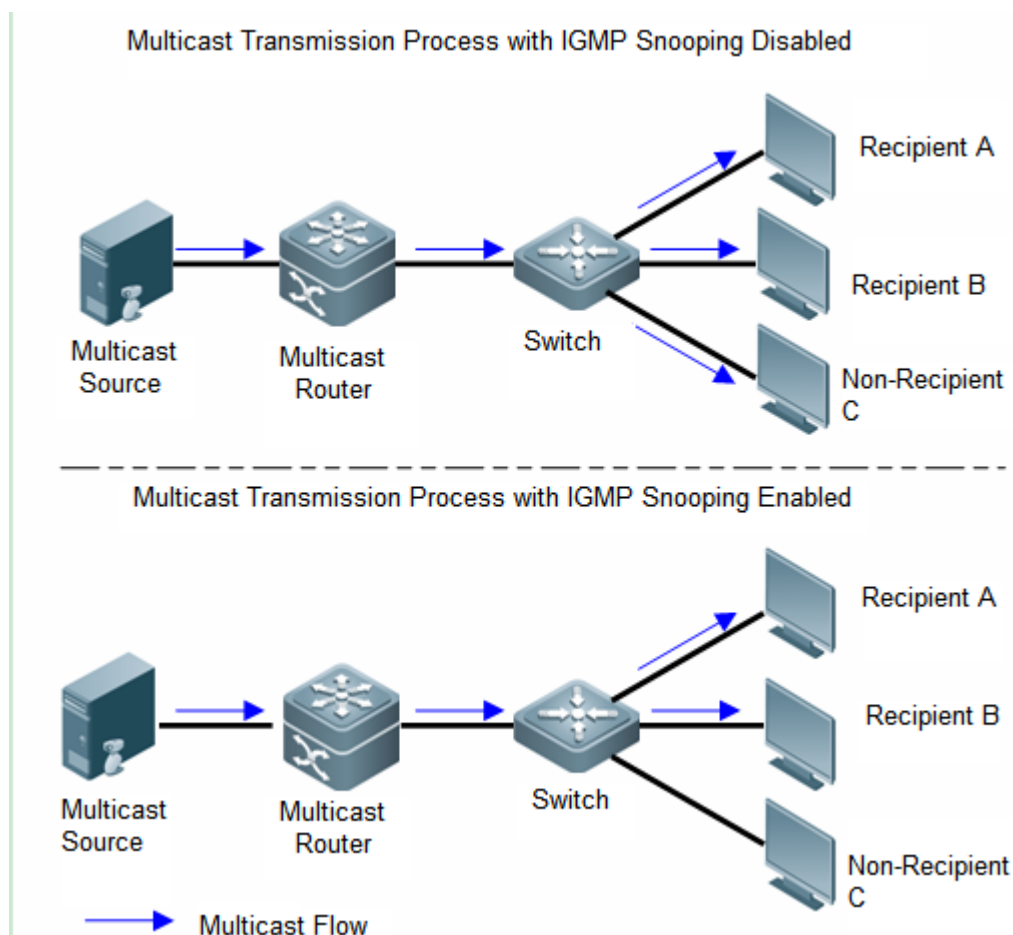


Figure 1

Ruijie multicast products support both the layer 2 multicast(IGMP Snooping) function and the layer 3 multicast(Multicast-routing) function. That is to say, to realize better packet forwarding function, Ruijie device supports not only the layer 3 multicast route forwarding, but also the snooping in the VLAN.



## Understanding the Type of IGMP Snooping Ports

As shown in the Figure 2, the Router is connected with the multicast source. The IGMP Snooping is enabled on the SwitchA. HostA and HostC are receives (that is, the IP multicast group member)

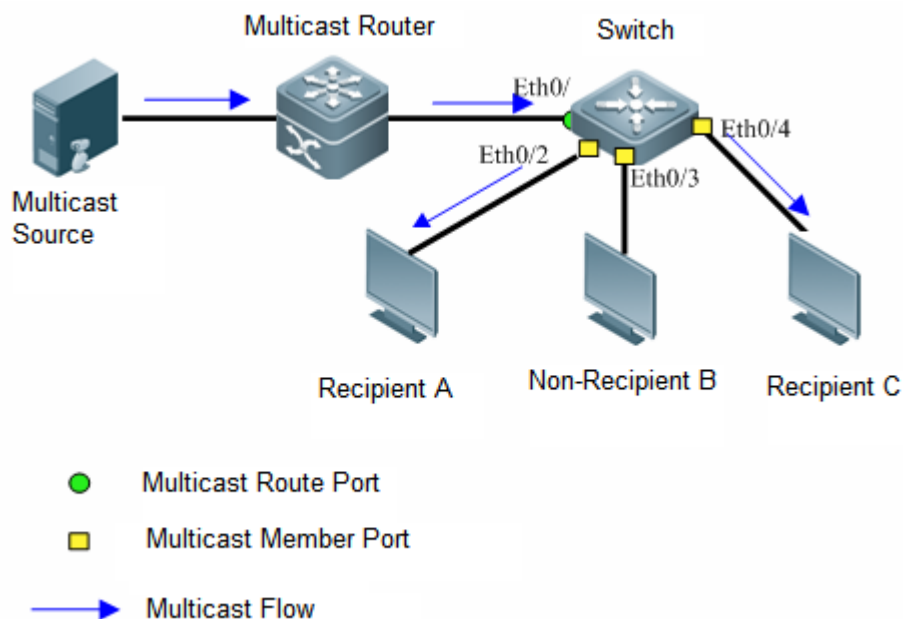


Figure 2 IGMP Snooping Port Type

**Multicast Router Port:** the switch is connected with the multicast router(the Layer3 multicast device), take the SwitchA interface Eth0/1 for example. All router ports on the switch(including the dynamic and static ports) are recorded in the router port list. By default, the router port corresponds to the recipient of the multicast data in the VLAN, and can also be added to the IGMP Snooping forwarding list.

**Member Port:** the abbreviation of the IP multicast group member port, also named Listener Port, representing the port connected with the IP multicast group member on the switch, take the SwitchA interface Eth0/2, Eth0/3 and Eth0/4 for example. All member ports on the switch(including the dynamic and static ports) are recorded in the IGMP Snooping forwarding list.

## Understanding the Aging Timer of Dynamic Port

Table-1 Aging timer of dynamic port

Type	Description	Events triggering timer	Activity after timeout
Aging timer for the dynamic router port	Enable a timer for each dynamic router port. The timeout time is the aging time of the dynamic router port.	Receive the IGMP general query packet or the IP PIM Hello packet.	Remove the port from the router port list.
Aging timer for the dynamic member port	Enable a timer for each dynamic member port. The timeout time is the aging time of the	Receive the IGMP query packet.	Remove the port from the IGMP Snooping multicast group forwarding list.

	dynamic member port.		
--	----------------------	--	--

## Understanding Operation Mechanism of IGMP Snooping

### General Group Query and Specific Group Query

IGMP querier sends the general query packets to all hosts and routers(with the address: 224.0.0.1) in the local network segment periodically to query for the IP multicast group member in the network segment. Upon receiving the IGMP general query packets, the switch forwards those query packets to all ports in this VLAN, and processes the packet-receiving port as follows:

- If this port has already been in the router port list, reset the aging timer.
- If this port has not been in the router port list, add the port to the list and enable the aging timer.
- After receiving the IGMP general query packets, the multicast device enable the aging timer for all member ports. Set the aging time as the maximum respond time of the IGMP query packets. When the aging time is 0, no member port receives the multicast flow and the port will be removed from the IGMP Snooping forwarding list.

After receiving the IGMP specific-group query packets, the multicast device enable the aging timer for all member ports in the specific group. Set the aging time as the maximum respond time of the IGMP query packets. When the aging time is 0, no member port receives the multicast flow and the port will be removed from the IGMP Snooping forwarding.

For the IGMP specific-group source query packets, it is no need to update the aging timer.

### Membership Report

In the following circumstances, the host sends the IGMP membership report to the IGMP querier:

- After receiving the IGMP query(general or specific-group query) packets, the IP multicast group member host responds to the received packets.
- If the host wants to join in an IP multicast group, it will take the initiative to send the IGMP membership report to the IGMP querier and claim to join in the IP multicast group.

Upon receiving the IGMP membership report message, the switch forwards the message through all router ports in the VLAN, analyzes the IP multicast group address from the message to add to the host, and deals with the packet-receiving port as follows:

If the corresponding forwarding entry of IP multicast group is inexistent, create a forwarding entry, add the dynamic member port to the outgoing port list, and enable the aging timer.

If the corresponding forwarding entry of IP multicast group exists but the outgoing port list excludes the port, add the dynamic member port to the outgoing port list, and enable the aging timer.

If the corresponding forwarding entry of IP multicast group exists and the outgoing port list includes the port, reset the aging timer.

### Leaving the Multicast Group

When leaving the IP multicast group, the host notifies the multicast router of the leave event by sending the IGMP leave group packets. Upon receiving the IGMP leave group packets on a dynamic member

port, the switch forwards those packets to the router ports.

## Understanding IGMP Profiles

IGMP Profiles is the group filtering actually, defines a series of multicast address range and the access to those multicast addresses(permit/deny), including “Multicast address range in the SVGL mode”, “Filtering multicast data range of router port”, “IGMP Filtering range”.

## Understanding Working Modes of IGMP Snooping

**DISABLE:** The IGMP Snooping does not work in this mode. That is, the switch does not snoop the IGMP messages between the host and the router. Multicast frames are forwarded in the VLAN in the broadcast form.

**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.

**SVGL(Shared VLAN Group Learning):** In this mode, the hosts in different VLANs share the same multicast flow. A host can request multicast flows across VLANs. By designating a Shared VLAN, you can only forward the multicast flows received in this Shared VLAN to other member ports in different VLANs. In the SVGL mode, IGMP Profile must be used to divide the multicast address range, within which the multicast flow can be forwarded across VLANs. By default, all group range is not within the SVGL range and all multicast flows are dropped. As shown in Figure-3:

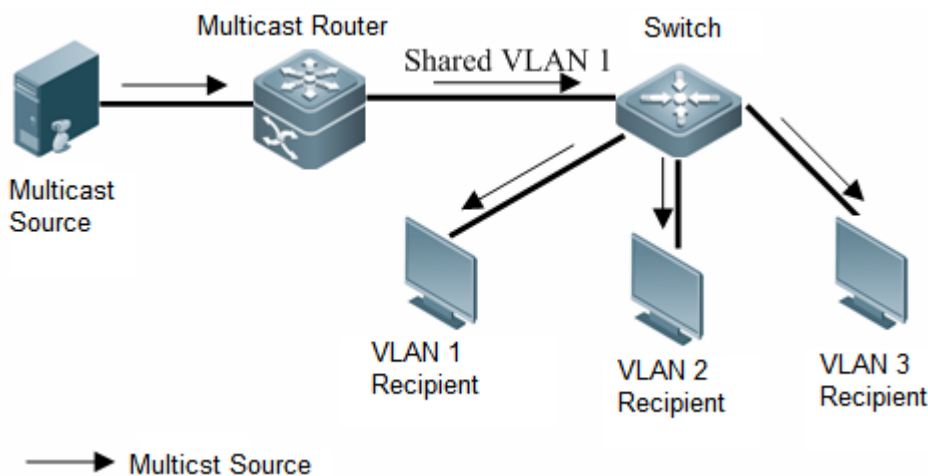


Figure-3 Multicast Flow in the Shared VLAN forwarding across VLANs

**Promiscuous mode:** also known as IVGL-SVGL mode. In this mode, the IVGL mode and the SVGL mode can co-exist. Use IGMP Profile to divide a set of multicast address range to the SVGL, within which the member port of the multicast forwarding entry can be forwarded across VLANs and without which the member ports are forwarded in the same VLAN.

## Understanding Relationship between IGMP Snooping and QinQ

After IGMP Snooping is enabled and dot1q-tunnel port is configured on the device, IGMP packets received from dot1q-tunnel port will be handled in two ways through IGMP Snooping:

- a) 1st way: Create multicast entries on the VLAN to which IMGP packets belong, and forward IMGP packets on such VLAN. For example: It is assumed that IGMP

Snooping has been enabled on the device; port A is a dot1q-tunnel port; the default VLAN of port A is VLAN 1, and packets from VLAN 1 and VLAN 10 can pass through port A. When multicast requests of VLAN 10 are sent to port A, IGMP Snooping will create the multicast entry of VLAN 10 and forward the multicast requests to the router port of VLAN 10.

- b) 2nd way: Create multicast entries on the default VLAN to which dot1q-tunnel belong, and forward multicast packets on the default VLAN of dot1q-tunnel port after inserting the VLAN Tag of the default VLAN of dot1q-tunnel port. For example: It is assumed that IGMP Snooping has been enabled on the device; port A is a dot1q-tunnel port; the default VLAN of port A is VLAN 1, and packets from VLAN 1 and VLAN 10 can pass through port A. When multicast requests of VLAN 10 are sent to port A, IGMP Snooping will create the multicast entry of VLAN 1 and insert the VLAN Tag of VLAN 1 into multicast requests before forwarding the multicast requests to the router port of VLAN 1.

By default, the 2nd way is used.

## Understanding IGMP Snooping Querier

In a multicast network running IGMP, a Layer-3 multicast device acting as the IGMP querier is responsible for sending IGMP general queries, so that all Layer-3 multicast devices can establish and maintain multicast forwarding entries, thus to forward multicast traffic correctly at the network layer.

However, in a network without layer-3 multicast device, a layer-2 multicast device does not support IGMP, and therefore cannot realize the relevant functions of IGMP querier. By enabling IGMP snooping on a layer-2 device, the layer-2 device can establish and maintain multicast forwarding entries at the data link layer, thus to forward multicast traffic correctly at the data link layer.

## Understanding Multicast VLAN

As shown in Figure 3, in the traditional multicast programs-on-demand mode, when hosts, Host A, Host B and Host C, belonging to different VLANs require multicast programs-on-demand service, the multicast router needs to copy the multicast traffic in each VLAN as multicast snooping is only carried out in the VLAN. This results in not only waste of network bandwidth but also extra burden on the Layer 3 device.

To solve this problem, we can configure multicast VLAN feature on the switch (namely IGMP Snooping will be running in SVGL mode or hybrid mode), which means that the VLANs to which these hosts belong will be configured as the sub-VLANs of a multicast VLAN. In this way, the multicast router needs to replicate the multicast traffic only in the multicast VLAN instead of making a separate copy of the multicast traffic in each user VLAN. This lessens the burden of the Layer 3 device.

When running on the multicast VLAN, the master multicast VLAN (namely SVGL VLAN) and the multicast address of multicast VLAN must be specified for the devices. Meanwhile, the sub-VLANs associated with the multicast VLAN may also need to be specified. Only the traffic from master multicast VLAN can be forwarded to the sub-VLANs needing to receive the multicast traffic.



### Caution

If sub-VLAN is not specified, all VLANs can receive the multicast traffic from multicast VLAN.

## Understanding Multicast Security Control

### Understanding Multicast Access Control

IGMP itself cannot control whether or not a user can join a specific multicast group. Since the multicast traffic is replicated at the access node, it is important to control whether or not a user can obtain a multicast video stream at the access node as it can guarantee the security of video data and benefit of the carrier and avoid illegal users. Currently, the customized Profile can be preconfigured on the user port through the feature of device management, so as to permit or deny user joining, control multicast service and avoid illegal users from occupying network resources when controlling the access to one or multiple multicast programs. Through similar functions, precise control of user access to multicast programs can also be realized at the access node, such as multicast preview. We can also control the number of programs accessible to a specific user, thus effectively protecting the network bandwidth resources.

The multicast devices released by Ruijie can realize diversified control of users:

- ◆ Port-based control of user access to multicast traffic

Under certain circumstances, you may need to control user's access to multicast traffic on the port. By this time, you can configure the port-based multicast filter. Detailed configurations are described in the section of "Configure port filter".

- ◆ VLAN-based control of user access to multicast traffic

Under certain circumstances, you may need to control VLAN's access to multicast traffic. By this time, you can configure the VLAN-based multicast filter. Detailed configurations are described in the section of "Configure VLAN filter".

- ◆ Port-based control of the amount of multicast traffic accessible to user

If the user requests multiple multicast programs on the same port, it will impose great pressure on network bandwidth. By configuring the number of multicast programs allowed on the port, we can effectively control the multicast programs that can be requested by the user. Detailed configurations are given in the section of "Configure IGMP Filtering".

- ◆ Multicast preview

For certain multicast video streams, if the user doesn't have access to such video streams but the service provider wants the user to preview such video streams within the preview interval, the device shall be able to support user-based multicast preview.

### Understanding Source IP Check

Among the multicast devices released by Ruijie, certain products support IGMP SNOOPING source IP check, further enhancing network security.

IGMP SNOOPING source IP check is intended to limit the source IP address of IGMP multicast traffic. When IGMP Snooping source IP check is disabled, all incoming video streams are considered valid, the layer-2 multicast device will forward them to registered member ports as per IGMP Snooping forwarding table. When IGMP Snooping source IP check is enabled, only the multicast traffic with the configured source IP address will be considered valid, and the multicast device will then forward them to the registered ports. Multicast traffic with other source IP addresses will be considered invalid and discarded.

## Configuring IGMP Snooping

We will describe how to configure IGMP snooping in the following sections

Function Configuration		Description
Configure Basic IGMP Snooping Function	Enable IGMP Snooping	Required
	Set the aging timer for the dynamic port	Optional
	Set the maximum respond time of the IGMP Query Packet	Optional
Configure IGMP Snooping Port Function	Set the router port.	Optional
	Set the member port.	Optional
	Set the port fast-leave	Optional
	Set the IGMP membership report packet suppression.	Optional
Configure the IP Multicast Group Policy on the Port	Set the IP multicast group filtering	Optional
	Set the source IP check.	Optional

### Enabling IGMP Snooping

By default, when enabling IGMP Snooping, the IGMP Snooping working mode(IVGL,SVGL and IVGL-SVGL) must be specified.



**Caution**

The Layer2 multicast device does not support IGMP Snooping if the device works in the private VLAN mode.

### Configuring IVGL Mode

In the global configuration mode, run the following commands to configure the IGMP Snooping IVGL mode:

Command	Function
Ruijie(config)# <b>ip igmp snooping ivgl</b>	Enable the IGMP Snooping IVGL mode. By default, the IGMP Snooping is disabled.
Ruijie (config)# <b>show ip igmp snooping</b>	Verify the configuration.
Ruijie(config)# <b>no ip igmp snooping</b>	Disable the IGMP Snooping function.

This example sets the IGMP Snooping IVGL mode:

```
Ruijie# configure terminal
Ruijie(config)# ip igmp snooping ivgl
```

```

Ruijie(config)# show ip igmp snooping
IGMP Snooping running mode: IVGL
SVGL vlan: 1
SVGL profile number: 0
Source port check: Disable
Source ip check: Disable
IGMP Fast-Leave: Disable
IGMP Report suppress: Disable

```

## Configuring SVGL Mode

In the global configuration mode, run the following commands to configure the IGMP Snooping SVGL mode:

Command	Function
Ruijie(config)# <b>ip igmp snooping svgl</b>	Enable the IGMP Snooping SVGL mode. By default, the IGMP Snooping is disabled.
Ruijie (config)# <b>show ip igmp snooping</b>	Verify the configuration.
Ruijie(config)# <b>no ip igmp snooping</b>	Disable the IGMP Snooping function.

This example sets the IGMP Snooping SVGL mode:

```

Ruijie# configure terminal
Ruijie(config)# ip igmp snooping svgl
Ruijie(config)# show ip igmp snooping
IGMP Snooping running mode: SVGL
SVGL vlan: 1
SVGL profile number: 11
Source port check: Disable
Source ip check: Disable
IGMP Fast-Leave: Disable
IGMP Report suppress: Disable

```



### Note

In the SVGL mode, an IGMP Profile must be associated to specify the multicast address range in the SVGL mode, or the configuration related to the SVGL mode will not take effect. For the details, see the chapter of “Configuring the Multicast Address Range in the SVGL mode”.

The layer 3 multicast-routing function cannot be enabled, or the command **ip multicast-routing** cannot be executed when the running mode is SVGL. Similarly, you cannot enter the SVGL mode when the layer 3 multicast-routing function has been enabled.

## Configuring IVGL-SVGL Mode

In the global configuration mode, run the following commands to configure the IGMP Snooping

IVGL-SVGL mode:

Command	Function
Ruijie(config)# <b>ip igmp snooping ivgl-svgl</b>	Enable the IGMP Snooping IVGL-SVGL mode. By default, the IGMP Snooping is disabled.
Ruijie (config)# <b>show ip igmp snooping</b>	Verify the configuration.
Ruijie(config)# <b>no ip igmp snooping</b>	Disable the IGMP Snooping function.

This example sets the IGMP Snooping IVGL-SVGL mode:

```
Ruijie# configure terminal
Ruijie(config)# ip igmp snooping ivgl-svgl
Ruijie(config)# show ip igmp snooping
IGMP Snooping running mode: IVGL SVGL
SVGL vlan: 1
SVGL profile number: 11
Source port check: Disable
Source ip check: Disable
IGMP Fast-Leave: Disable
IGMP Report suppress: Disable
```



#### Note

In the SVGL mode, an IGMP Profile must be associated to specify the multicast address range in the SVGL mode, or the configuration related to the SVGL mode will not take effect. For the details, see the chapter of “Configuring the Multicast Address Range in the SVGL mode”.

The layer 3 multicast-routing function cannot be enabled, or the command **ip multicast-routing** cannot be executed when the running mode is SVGL. Similarly, you cannot enter the SVGL mode when the layer 3 multicast-routing function has been enabled.

## Disabling IGMP Snooping

In the global configuration mode, run the following command to disable IGMP Snooping:

Command	Function
Ruijie(config)# <b>no ip igmp snooping</b>	Disable the IGMP Snooping function.
Ruijie (config)# <b>show ip igmp snooping</b>	Verify the configuration.

This example disables the IGMP Snooping:

```
Ruijie# configure terminal
Ruijie(config)# no ip igmp snooping svgl
Ruijie(config)# show ip igmp snooping
IGMP Snooping running mode: DISABLE
```



```

SVGL vlan: 1
SVGL profile number: 11
Source port check: Disable
Source ip check: Disable
IGMP Fast-Leave: Disable
IGMP Report suppress: Disable

```

## Enabling IGMP Snooping in the Specific VLAN

By default, with IGMP Snooping globally enabled, the IGMP Snooping function is auto-enabled in all VLANs. To disable the IGMP Snooping in the specified VLAN, run the following command.

In the global configuration mode, run the following command to disable IGMP Snooping:

Command	Function
Ruijie(config)# <b>no ip igmp snooping vlan num</b>	Disable the IGMP Snooping in the specified VLAN. By default, the IGMP Snooping in the VLAN is enabled.
Ruijie (config)# <b>ip igmp snooping vlan num</b>	Enable the IGMP Snooping in the specified VLAN.

This example disables the IGMP Snooping in the VLAN3:

```

Ruijie# configure terminal
Ruijie(config)# no ip igmp snooping vlan 3
Ruijie(config)# show ip igmp snooping
IGMP Snooping running mode: IVGL
SVGL vlan: 1
SVGL profile number: 11
Source port check: Disable
Source ip check: Disable
IGMP Fast-Leave: Disable
IGMP Report suppress: Disable

vlan 1
-----
IGMP Snooping                :Enabled
Multicast router learning mode :pim-dvmrp
IGMPv2 immediate leave       :Disabled

vlan 2
-----
IGMP Snooping                :Enabled
Multicast router learning mode :pim-dvmrp
IGMPv2 immediate leave       :Disabled

vlan 3
-----
IGMP Snooping                :Disabled

```

```
Multicast router learning mode :pim-dvmrp
IGMPv2 immediate leave       :Disabled
```

```
vlan 4
```

```
-----
IGMP Snooping                :Enabled
Multicast router learning mode :pim-dvmrp
IGMPv2 immediate leave       :Disabled
```

**Note**

With the IGMP Snooping enabled in the VLAN, the MLD Snooping function must also be enabled if the IPv6 multicast is applied in the VLAN.

## Configuring the Aging Time for the Dynamic Route Port

If no IGMP general query packets or PIM Hello packets are received on the dynamic router port within the aging time, the router port will be deleted.

To configure the aging time for the dynamic router port, execute the following commands in the global configuration mode.

Command	Function
Ruijie(config)# <b>ip igmp snooping dyn-mr-aging-time</b> <i>time</i>	Configure the aging time for the dynamic router port. <i>Time</i> : aging time in the range of 1 to 3600s. Default value: 300s.
Ruijie(config)# <b>no ip igmp snooping dyn-mr-aging-time</b>	Return the aging time to the default value.

The following example configures the aging time of the dynamically learned router interface to 100s:

```
Ruijie# configure terminal
Ruijie (config) # ip igmp snooping dyn-mr-aging-time 100
```

## Configuring the Maximum Response Time of the IGMP Query Message

The multicast router periodically sends an IGMP Query message to query whether a multicast member exists or not. If the multicast router has not received the IGMP Report message from a host within a period of time, the switch will think this port no longer receives multicast frames, and delete this port from the multicast forwarding table. The default time is 10 seconds.

To configure the maximum response time of the IGMP Query message, execute the following commands in the global configuration mode:

Command	Function
Ruijie(config)# <b>ip igmp Snooping query-max-response-time</b> <i>seconds</i>	Set the maximum response time of the IGMP Query message in the range of 1 to 65535 seconds. The default time is 10 seconds.

Command	Function
Ruijie(config)# <b>no ip igmp Snooping query-max-response-time</b>	Restore the maximum response time to the default value.

The following example configures the maximum response time of the IGMP Query message to 15s:

```
Ruijie# configure terminal
Ruijie (config) # ip igmp snooping query-max-response-time 15
```

## Configuring IGMP Profiles

An IGMP Profile entry defines a set of multicast address range and permit/deny activity for the functions like multicast address range for SVGL mode, multicast data range filtered on the router interface, and IGMP Filtering range. Note that modifying an IGMP Profile after associating it with a function will influence the multicast forwarding table generated by the function.

To configure an IGMP profile, execute the following commands:

Command	Function
Ruijie(config)# <b>ip igmp profile</b> <i>profile-number</i>	Enter the IGMP Profile mode. Assign a number in the range of 1 to 1024 to identify. By default, no profile is configured.
Ruijie (config-profile)# <b>permit   deny</b>	(Optional) Permit or deny this range of multicast addresses while deny or permit other multicast addresses. The default value is deny.
Ruijie(config-profile)# <b>range ip</b> <i>multicast-address</i>	Add one or more multicast address ranges.
Ruijie# <b>end</b>	Return to the privileged EXEC mode.

To delete an IGMP Profile, use **no ip igmp profile** *profile-number*.

To delete a range of the IGMP Profile, use **no range ip** *multicast address*.

This example shows the IGMP Profile configuration process:

```
Ruijie(config)# ip igmp profile 1
Ruijie (config-profile) # permit
Ruijie (config-profile) # range 224.0.1.0 239.255.255.255
Ruijie (config-profile) # end
Ruijie# show ip igmp profile 1
IGMP Profile 1
permit
range 224.0.1.0 239.255.255.255
```

As you can see, the rule of the IGMP Profile is to permit the multicast addresses from 224.0.1.0 to 239.255.255.255, while all other multicast addresses are denied.

## Configuring the Ports of IGMP Snooping

### Configuring the Route Port

By default, the router port is dynamically learned in the VLAN. Use the **no** option of the command to disable the dynamic learning function for the router interface in the VLAN and clear all router ports learned dynamically.

Use the command to set the switch port as the static router port.

To configure a router port, execute the following command:

Command	Function
Ruijie(config)# <b>ip igmp snooping</b> <b>vlan</b> <i>vlan-id</i> <b>mrouter interface</b> <i>interface-id</i>	Set the interface as the static router interface.
Ruijie(config)# <b>no ip igmp snooping</b> <b>vlan</b> <i>vlan-id</i> <b>mrouter interface</b> <i>interface-id</i>	Cancel the static router interface setting.
Ruijie(config)# <b>ip igmp snooping</b> <b>vlan</b> <i>vlan-id</i> <b>mrouter learn</b> <b>pim-dvmrp</b>	Enable the dynamic learning function for the router interface in the VLAN. By default, the dynamic learning function is enabled.
Ruijie(config)# <b>no ip igmp snooping</b> <b>vlan</b> <i>vlan-id</i> <b>mrouter learn</b> <b>pim-dvmrp</b>	Disable the dynamic learning function for the router interface in the VLAN and clear all router ports learned dynamically.

This example sets GigabitEthernet 1/1 as the router port and enables dynamic learning function in the VLAN1:

```
Ruijie# configure terminal
Ruijie(config)# ip igmp snooping vlan 1 mrouter interface gigabitEthernet 0/7
Ruijie(config)# ip igmp snooping vlan 1 mrouter learn pim-dvmrp
Ruijie(config)# end
Ruijie# show ip igmp snooping mrouter
Vlan      Interface          State      IGMP profile
----      -
1  GigabitEthernet 0/7  static      0
1  GigabitEthernet 0/12 dynamic      0
Ruijie# show ip igmp snooping mrouter learn
Vlan      learn method
----      -
1          pim-dvmrp
```

## Configuring Static Member Port

When IGMP Snooping is enabled, you can statically configure a port to receive a specific multicast flow in disregard of various IGMP packets.

To configure a static member port of IGMP Snooping, execute the following commands in the global configuration mode:

Command	Function
Ruijie(config)# <b>ip igmp Snooping ivgl</b>	Enable IGMP Snooping and set it as the IVGL mode.

Command	Function
Ruijie(config)# <b>ip igmp snooping</b> <b>vlan <i>vlan-id</i> static <i>ip-addr</i> interface</b> <i>[interface-id]</i>	Statically configure a port to receive a certain multicast flow. <ul style="list-style-type: none"> <li>• <i>vlan-id</i>: vid of multicast flow</li> <li>• <i>ip-addr</i>: multicast group address</li> <li>• <i>interface-id</i>: Interface ID</li> </ul>
Ruijie(config)# <b>no ip igmp snooping</b> <b>vlan <i>vlan-id</i> static <i>ip-addr</i> interface</b> <i>[interface-id]</i>	Remove a static member port. <ul style="list-style-type: none"> <li>• <i>vlan-id</i>: vid of multicast flow</li> <li>• <i>ip-addr</i>: multicast group address</li> <li>• <i>interface-id</i>: Interface ID</li> </ul>

Use **no ip igmp snooping vlan *vlan-id* static *ip-addr* interface *interface-id*** to delete the static member of IGMP Snooping.

This example configures a static member port of IGMP snooping:

```
Ruijie# configure terminal
Ruijie(config)# ip igmp snooping vlan 1 static 233.3.3.4 interface GigabitEthernet 0/7
Ruijie(config)# end
Ruijie(config)# show ip igmp snooping gda
Abbr: M - mrouter
      D - dynamic
      S - static
VLAN  Address                Member ports
-----
1      233.3.3.4              GigabitEthernet 0/7(S)
```

## Configuring Fast-Leave

According to the IGMP protocol, a port cannot leave a multicast group immediately after the host sends the IGMP Leave message. Instead, the multicast router should first send an IGMP Query packet and lets a port leave the group only when the host does not respond. However, in specific environments (for example, one port is connected to only one multicast user), the port can immediately leave the multicast group after the multicast router receives the IGMP Leave message, a mechanism known as Fast Leave. To enable fast-leave, execute the following commands in the global configuration mode:

Command	Function
Ruijie(config)# <b>ip igmp snooping</b> <b>fast-leave enable</b>	Enable the fast-leave function.
Ruijie(config)# <b>no ip igmp snooping</b> <b>fast-leave enable</b>	Disable the fast-leave function.

The following example enables the fast-leave function:

```
Ruijie# configure terminal
Ruijie(config)# ip igmp snooping fast-leave enable
Ruijie(config)# end
```

## Configuring IGMP Snooping Suppression

For IGMP Snooping-enabled devices, a multicast group address may have multiple IGMP users. When a user joins the multicast group and receives the IGMP Query message, he or she will send an IGMP Report message. Ruijie switches will forward every IGMP Query message to the multicast router. In this way, the multicast router will receive multiple IGMP Report messages when it sends an IGMP Query message to the ports on the IGMP Snooping-enabled devices.

To reduce the pressure of the server on processing the IGMP Report messages, the switch only forwards the first received IGMP Report message to the router port while suppressing other IGMP Report messages. This is called IGMP Snooping Suppression.

To enable IGMP Snooping suppression, execute the following commands in the global configuration mode:

Command	Function
Ruijie(config)# <b>ip igmp snooping suppression enable</b>	Enable IGMP Snooping suppression. By default, this function is enabled.
Ruijie(config)# <b>no ip igmp snooping suppression enable</b>	Disable IGMP Snooping suppression.

The following example enables the IGMP Snooping suppression function:

```
Ruijie# configure terminal
Ruijie(config)# ip igmp snooping suppression enable
Ruijie(config)# end
```

## Configuring the Multicast Security Control

### Configuring Source IP Check

Source IP check corresponds to two commands: 1) configuration of default source IP address of valid multicast traffic for all multicast groups; 2) configuration of the source IP address of valid multicast traffic for a specific multicast group belonging to specific VLAN. The source IP address of valid multicast server can only be configured for a specific group after enabling default source IP check of all groups.

In global configuration mode, execute the following steps to enable IGMP Snooping source IP check:

Command	Function
Ruijie(config)# <b>ip igmp snooping source-check default-server</b> <i>address</i>	Enable source IP check and configure the default source IP address of valid multicast traffic for all groups. This feature is disabled by default.
Ruijie(config)# <b>no ip igmp snooping source-check default-server</b>	Disable source IP check.
Ruijie(config)# <b>ip igmp snooping limit-ipmc vlan</b> <i>vid address address server address</i>	Configure the source IP address of valid multicast traffic for specific group address. By default, the source IP address of the valid multicast traffic for this group address is the same as the IP address of default-server.

```
Ruijie(config)# no ip igmp snooping
limit-ipmc vlan vid address address
```

Remove the configuration of limit-ipmc.

The following example shows how to enable source IP check and configure the default source IP to 1.1.1.1, and how to configure the source IP address of valid multicast traffic for group 233.3.3.3 belonging to VLAN1 to 1.1.1.2.

```
Ruijie# configure terminal
```

```
Ruijie(config)# ip igmp snooping source-check default-server 1.1.1.1
```

```
Ruijie(config)# ip igmp snooping limit-ipmc vlan 1 address 233.3.3.3 server 1.1.1.2
```



#### Caution

IGMP Snooping source IP check cannot be shared with layer-3 multicasting, which means layer-3 multicast forwarding will be compromised after enabling layer-3 multicasting and source IP check at the same time.

## Configuring Port Filter

Under certain circumstances, you may need to control a specific port to only receive a group of specific multicast traffic and control the maximum number of groups that can be joined on this port. IGMP Filtering well meets such needs.

You can apply an IMGP Profile to a port. If IMGP Report packets are received on the port, the layer-2 multicast device will verify whether the multicast address to be joined by this port falls within the range permitted by IGMP Profile. If yes, the port will join and process subsequently.

You can also configure the maximum number of groups that can be joined by the port. If the threshold is exceeded, the layer-2 multicast device will no longer receive and process IGMP Report packets.

In global configuration mode, execute the following steps to configure IGMP Filtering:

Command	Function
Ruijie(config)# <b>interface</b> <i>interface-id</i>	Enter the interface to be configured.
Ruijie(config-if)# <b>ip igmp snooping filter</b> <i>profile-number</i>	(Optional) Apply Profile to this interface. The range of profile number is 1-1024. By default, a port is not associated with any profile.
Ruijie(config-if)# <b>no ip igmp snooping filter</b>	(Optional) Delete the profile associated to the interface, which will then permit all groups.
Ruijie(config-if)# <b>ip igmp snooping max-groups</b> <i>number</i>	(Optional) Configure the maximum number (0-1024) of groups that can be joined on this port. The number is not restricted by default.

The following example shows how to configure the filter:

```
Ruijie# configure terminal
Ruijie(config)# interface fastEthernet 0/1
Ruijie(config-if)# ip igmp snooping filter 1
Ruijie(config-if)# ip igmp snooping max-groups 1000
Ruijie(config-if)# end
Ruijie# show ip igmp snooping interface fastEthernet 0/1
```

Interface	Filter profile number	max-group
FastEthernet 0/1	1	1000

## Configuring VLAN Filter

Under certain circumstances, you may need to control the reception of multicast traffic on the egress of specific VLAN. VLAN-based filter well meets such need.

You can apply an IMGP Profile to a VLAN. If IMGP Report packets are received on the port belong to this VLAN, the layer-2 multicast device will verify whether the multicast address to be joined by this port falls within the range permitted by IGMP Profile. If yes, the port will join and process subsequently.

In global configuration mode, execute the following steps to configure IGMP Filtering:

Command	Function
Ruijie(config)# <b>ip igmp snooping vlan num filter profile-number</b>	(Optional) Apply Profile to this VLAN. The range of profile number if 1-1024. By default, a VLAN is not associated with any profile.
Ruijie(config-if)# <b>no ip igmp snooping vlan num filter</b>	(Optional) Delete the profile associated to the VLAN, which will then permit all groups.

The following example shows how to configure the VLAN filter:

```
Ruijie# configure terminal
Ruijie(config)# interface fastEthernet 0/1
Ruijie(config-if)# ip igmp snooping vlan 2 filter 1
```

## Configuring Multicast Preview

To configure multicast preview, the following information must be configured: the multicast group that can be previewed, and the preview interval.

In global configuration mode, execute the following steps to configure multicast preview:

Command	Function
---------	----------



Ruijie(config)# <b>ip igmp snooping preview profile-number</b>	(Optional) Apply Profile to this preview. The range of profile number is 1-1024. By default, a multicast traffic can be previewed.
Ruijie(config)# <b>ip igmp snooping preview interval num</b>	(Optional) Configure preview interval. The range of num is 1-300, and the default value is 60 seconds.
Ruijie(config)# <b>no ip igmp snooping preview</b>	(Optional) No preview.

The following example shows how to configure multicast preview. Multicast traffic failing to match profiles1 but matching profiles2 can be previewed.

```
Ruijie# configure terminal
Ruijie(config)# ip igmp snooping preview 2
Ruijie(config)# int fa 0/1
Ruijie(config-if)# ip igmp snooping filter 1
```

## Configuring the Relationship Between IGMP Snooping and QinQ

By default, IGMP Passthrough is disabled. In global configuration mode, execute the following steps to configure the relationship between IGMP Snooping and QinQ:

Command	Function
Ruijie# <b>configure terminal</b>	Enter global configuration mode
Ruijie(config)# <b>ip igmp snooping tunnel</b>	<p>Enable IGMP Passthrough:</p> <p>After IGMP Snooping is enabled and dot1q-tunnel port is configured on the device, create multicast entries on the VLAN to which IMGP packets belong, and forward IMGP packets on such VLAN.</p> <p>For example: It is assumed that IGMP Snooping has been enabled on the device; port A is a dot1q-tunnel port; the default VLAN of port A is VLAN 1, and packets from VLAN 1 and VLAN 10 can pass through port A. When multicast requests of VLAN 10 are sent to port A, IGMP Snooping will create the multicast entry of VLAN 10 and forward the multicast requests to the router port of VLAN 10.</p> <p>By default, IGMP Passthrough is disabled.</p>

Ruijie(config)# <b>no ip igmp snooping tunnel</b>	<p>Disable IGMP Passthrough.</p> <p>After IGMP Snooping is enabled and dot1q-tunnel port is configured on the device, create multicast entries on the default VLAN to which dot1q-tunnel belong, and forward multicast packets on the default VLAN of dot1q-tunnel port after inserting the VLAN Tag of the default VLAN of dot1q-tunnel port.</p> <p>For example: It is assumed that IGMP Snooping has been enabled on the device; port A is a dot1q-tunnel port; the default VLAN of port A is VLAN 1, and packets from VLAN 1 and VLAN 10 can pass through port A. When multicast requests of VLAN 10 are sent to port A, IGMP Snooping will create the multicast entry of VLAN 1 and insert the VLAN Tag of VLAN 1 into multicast requests before forwarding the multicast requests to the router port of VLAN 1.</p>
---	---

The following example shows how to enable IGMP Passthrough:

```
Ruijie# configure terminal
Ruijie(config)# ip igmp snooping tunnel
```

## Configuring IGMP Snooping Querier

### Globally Enabling Querier

In global configuration mode, execute the following steps to enable global querier:

Command	Function
Ruijie(config)# <b>ip igmp snooping querier</b>	Globally enable IGMP querier.
Ruijie(config)# <b>no ip igmp snooping querier</b>	Globally disable IGMP querier.

The following example shows how to globally enable IGMP querier:

```
Ruijie# configure terminal
Ruijie(config)# ip igmp snooping querier
```

### Globally Configuring Querier Source IP

In global configuration mode, execute the following steps to globally configure the source IP address of queries:

Command	Function
Ruijie(config)# <b>ip igmp snooping querier address a.b.c.d</b>	Globally configure querier source IP.
Ruijie(config)# <b>no ip igmp snooping querier address</b>	Globally disable querier source IP.

The following example shows how to globally configure the source IP address of IGMP querier:

```
Ruijie# configure terminal
Ruijie(config)# ip igmp snooping querier address 192.168.2.2
```

### Globally Configuring the Maximum Response Time to Queries

In global configuration mode, execute the following steps to configure the maximum response time to queries:

Command	Function
Ruijie(config)# <b>ip igmp snooping querier max-response-time num</b>	Globally configure the maximum response time to queries. The default value is 10 seconds.
Ruijie(config)# <b>no ip igmp snooping querier max-response-time</b>	Globally restore the maximum response time to queries to default value.

The following example shows how to configure the maximum response time to queries:

```
Ruijie# configure terminal
Ruijie(config)# ip igmp snooping querier 20
```

### Globally Configuring the Query Interval

In global configuration mode, execute the following steps to configure the interval for periodically sending queries:

Command	Function
Ruijie(config)# <b>ip igmp snooping querier query-interval num</b>	Globally configure the interval for periodically sending IGMP queries. The default value is 60 seconds.
Ruijie(config)# <b>no ip igmp snooping querier query-interval</b>	Globally restore the interval for periodically sending IGMP queries to default value.

The following example shows how to globally configure the query interval:

```
Ruijie# configure terminal
Ruijie(config)# ip igmp snooping querier query-interval 300
```

### Globally Configuring Querier Expiration Timer

In global configuration mode, execute the following steps to configure querier expiration timer:

Command	Function
Ruijie(config)# <b>ip igmp snooping querier timer expiry num</b>	Globally configure querier expiration timer.
Ruijie(config)# <b>no ip igmp snooping querier timer expiry</b>	Globally configure querier expiration timer to the default value.

The following example shows how to globally configure querier expiration timer:

```
Ruijie# configure terminal
Ruijie(config)# ip igmp snooping querier timer expiry 70
```

## Globally Configuring IGMP Version Number

In global configuration mode, execute the following steps to globally configure IGMP version number:

Command	Function
Ruijie(config)# <b>ip igmp snooping querier version num</b>	Globally configure IGMP version number (1-2). Default value: 2.
Ruijie(config)# <b>no ip igmp snooping querier version</b>	Globally restore IGMP version number to the default value.

The following example shows how to globally configure IGMP version number:

```
Ruijie# configure terminal
Ruijie(config)# ip igmp snooping querier version 1
```

## Globally Configuring Querier Function on VLAN

In global configuration mode, execute the following steps to enable querier function on VLAN:

Command	Function
Ruijie(config)# <b>ip igmp snooping vlan num querier</b>	Enable IGMP querier function on VLAN.
Ruijie(config)# <b>no ip igmp snooping vlan num querier</b>	Disable IGMP querier function on VLAN.

The following example shows how to enable IGMP querier on VLAN:

```
Ruijie# configure terminal
Ruijie(config)# ip igmp snooping vlan 2 querier
```

## Globally Configuring Source IP for Querier on VLAN

In global configuration mode, execute the following steps to globally configure the source IP address of queries on VLAN:

Command	Function
---------	----------

Ruijie(config)# <b>ip igmp snooping vlan num querier address a.b.c.d</b>	Configure the source IP of querier on VLAN.
Ruijie(config)# <b>no ip igmp snooping vlan num querier address</b>	Remove the source IP of querier on VLAN.

The following example shows how to globally configure the source IP address of IGMP querier:

```
Ruijie# configure terminal
Ruijie(config)# ip igmp snooping vlan 2 querier address 192.168.2.2
```

## Globally Configuring the Maximum Response Time to Queries on VLAN

In global configuration mode, execute the following steps to configure the maximum response time to queries:

Command	Function
Ruijie(config)# <b>ip igmp snooping vlan num querier max-response-time num</b>	Configure the maximum response time to queries on VLAN. The default value is 10 seconds.
Ruijie(config)# <b>no ip igmp snooping vlan num querier max-response-time</b>	Restore the maximum response time to queries on VLAN to default value.

The following example shows how to configure the maximum response time to queries:

```
Ruijie# configure terminal
Ruijie(config)# ip igmp snooping vlan 2 querier 20
```

## Globally Configuring the Query Interval on VLAN

In global configuration mode, execute the following steps to configure the interval for periodically sending queries:

Command	Function
Ruijie(config)# <b>ip igmp snooping vlan num querier query-interval num</b>	Configure the interval for periodically sending IGMP queries on VLAN. The default value is 60 seconds.
Ruijie(config)# <b>no ip igmp snooping vlan num querier query-interval</b>	Restore the interval for periodically sending IGMP queries on VLAN to default value.

The following example shows how to configure the query interval on VLAN:

```
Ruijie# configure terminal
Ruijie(config)# ip igmp snooping vlan 2 querier query-interval 300
```

## Globally Configuring Querier Expiration Timer on VLAN

In global configuration mode, execute the following steps to configure querier expiration timer:

Command	Function
Ruijie(config)# <b>ip igmp snooping vlan num querier timer expiry num</b>	Configure querier expiration timer on VLAN.
Ruijie(config)# <b>no ip igmp snooping vlan num querier timer expiry</b>	Configure querier expiration timer on VLAN to default value.

The following example shows how to configure querier expiration timer on VLAN:

```
Ruijie# configure terminal
Ruijie(config)# ip igmp snooping vlan 2 querier timer expiry 70
```

## Globally Configuring IGMP Version Number on VLAN

In global configuration mode, execute the following steps to configure IGMP version number on VLAN:

Command	Function
Ruijie(config)# <b>ip igmp snooping vlan num querier version num</b>	Configure IGMP version number (1-2) on VLAN. Default value: 2.
Ruijie(config)# <b>no ip igmp snooping vlan num querier version</b>	Restore IGMP version number to the default value on VLAN.

The following example shows how to configure IGMP version number on VLAN:

```
Ruijie# configure terminal
Ruijie(config)# ip igmp snooping vlan 2 querier version 1
```

## Configuring Multicast VLAN

### Enabling SVGL mode

In global configuration mode, execute the following steps to enable SVGL mode of IGMP Snooping:

Command	Function
Ruijie(config)# <b>ip igmp snooping svgl</b>	Enable SVGL mode of IGMP Snooping.
Ruijie(config)# <b>ip igmp snooping ivgl-svgl</b>	Enable IVGL-SVGL mode of IGMP Snooping.
Ruijie(config)# <b>no ip igmp snooping</b>	Disable IGMP Snooping.

The following example shows how to globally enable IGMP querier:

```
Ruijie# configure terminal
Ruijie(config)# ip igmp snooping svgl
```

## Configuring the Master VLAN of Multicast VLAN

In global configuration mode, execute the following steps to configure the master VLAN of multicast

VLAN:

Command	Function
Ruijie(config)# <b>ip igmp snooping svgl</b> <b>vlan num</b>	Configure the master VLAN of multicast VLAN.
Ruijie(config)# <b>no ip igmp snooping svgl</b> <b>vlan</b>	Configure the default VLAN of multicast VLAN.

The following example shows how to globally configure the master VLAN of multicast VLAN to VLAN 2:

```
Ruijie# configure terminal
Ruijie(config)# ip igmp snooping svgl vlan 2
```



#### Caution

By default, the master VLAN of multicast VLAN is VLAN 1. After enabling multicast VLAN, the multicast traffic falling into the group address range of multicast VLAN can only be received and processed if entering from multicast VLAN; traffic entering from other VLANs won't be received and processed.

## Configuring the Sub-VLANs of Multicast VLAN

In global configuration mode, execute the following steps to configure the sub-VLANs of multicast VLAN:

Command	Function
Ruijie(config)# <b>ip igmp snooping svgl</b> <b>subvlan num</b>	Configure the sub-VLANs of multicast VLAN.
Ruijie(config)# <b>no ip igmp snooping svgl</b> <b>subvlan</b>	Remove the sub-VLANs of multicast VLAN.

The following example shows how to globally configure the sub-VLANs of multicast VLAN to VLAN 3 and VLAN 6:

```
Ruijie# configure terminal
Ruijie(config)# ip igmp snooping svgl subvlan 3,6
```

```
IGMP Snooping running mode: IVGL-SVGL
SVGL vlan: 1
SVGL profile number: 1
IGMP Snooping SVGL subvlan 3,6
IGMP Fast-Leave: Disable
IGMP Report suppress: Disable
IGMP Globle Querier: Disable
Dynamic Mroute Aging Time : 300(Seconds)
```

```
vlan 1
-----
IGMP Snooping state: Enabled
Multicast router learning mode: pim-dvmrp
```

```

IGMPv2 immediate leave: Disabled
IGMP VLAN querier: Disable

vlan 3
-----
IGMP Snooping state: Enabled
Multicast router learning mode: pim-dvmrp
IGMPv2 immediate leave: Disabled
IGMP VLAN querier: Disable

vlan 4
-----
IGMP Snooping state: Enabled
Multicast router learning mode: pim-dvmrp
IGMPv2 immediate leave: Disabled
IGMP VLAN querier: Disable

vlan 6
-----
IGMP Snooping state: Enabled
Multicast router learning mode: pim-dvmrp
IGMPv2 immediate leave: Disabled
IGMP VLAN querier: Disable

```

**Caution**

By default, no sub-VLAN of the multicast VLAN is configured on the device. By this time all other VLANs will be able to receive the multicast traffic from master VLAN.

If sub-VLANs are configured, only VLANs falling into the range of sub-VLANs can receive multicast traffic.

## Configuring the Multicast Address range of Multicast VLAN

After configuring the operating mode of IGMP Snooping to SVGL mode or IVGL-SVGL mode, you need to associate SVGL to one profile in order to specify which group addresses can be applied with SVGL mode, namely the member ports of multicast forwarding table entries can forward traffic across VLAN, while the member ports of multicast forwarding table entries corresponding to other multicast address ranges must belong to the same VLAN. By default, no profile is associated, meaning that no multicast group can be applied with SVGL mode.

Command	Function
Ruijie(config)# <b>ip igmp snooping svgl profile</b> <i>profile_num</i>	Configure to associate one profile with SVGL.



Ruijie(config)# <b>no ip igmp snooping svgl profile</b>	Disable SVGL-profile association and restore to the default value of 0.
---	---

The following example shows how to configure the multicast address range applied with SVGL mode:

```
Ruijie# configure terminal
Ruijie(config)# ip igmp snooping ivgl-svgl
Ruijie(config)# ip igmp snooping svgl profile 1
Ruijie(config)# end
Ruijie# show ip igmp snooping
IGMP Snooping running mode: IVGL_SVGL
SVGL vlan: 1
SVGL profile number: 1
Source port check: Disable
Source ip check: Disable
IGMP Fast-Leave: Disable
IGMP Report suppress: Disable
IGMP Globle Querier: Disable
Dynamic Mroute Aging Time : 30000(Seconds)

vlan 1
-----
IGMP Snooping state: Enabled
Multicast router learning mode: pim-dvmrp
IGMPv2 immediate leave: Disabled
IGMP VLAN querier: Disable
```

## Configuring Source IP Check

There are two configuration commands for the source IP check: one command is for the configuration of default source IP addresses of the legal multicast flows in all multicast groups; and the other command is for the configuration of the default source IP address for the legal multicast flows in the specified VLAN group. Only with the default source IP check enabled in all groups, the source IP address of the legal multicast server in a specific group can be set.

To enable source IP check, execute the following commands in the global configuration mode:

Command	Function
Ruijie(config)# <b>ip igmp snooping source-check default-server</b> <i>address</i>	Enable source IP check and configure the default source IP address of the legal multicast flows in all multicast groups. By default, this function is disabled.
Ruijie(config)# <b>no ip igmp snooping source-check default-server</b>	Disable source IP check.

Command	Function
Ruijie(config)# <b>ip igmp snooping limit-ipmc vlan</b> <i>vid address address server address</i>	Add the source IP address of the legal multicast flow to a specified multicast group addresses. By default, the source IP address of the legal multicast flow is the IP address of the default-server.
Ruijie(config)# <b>no ip igmp snooping limit-ipmc vlan</b> <i>vid address address</i>	Cancel a limit-ipmc configuration.

The following example enables source IP check and set the default source IP address to 1.1.1.1. In the example, a multicast group address-source IP address entry is added, where vid is 1, group IP address is 233.3.3.3 and source ip address is 1.1.1.2.

```
Ruijie# configure Terminal
Ruijie(config)# ip igmp snooping source-check default-server 1.1.1.1
Ruijie(config)# ip igmp snooping limit-ipmc vlan 1 address 233.3.3.3 server 1.1.1.2
Ruijie(config)# end
```

## Configuring IGMP Filtering

In some cases, you may need to limit a port to receive a specified set of multicast data flows, and control the maximum number of multicast groups that the port is allowed to join dynamically IGMP Filtering can address this requirement.

You can apply one IGMP Profile to a port. If the port receives the IGMP Report message, the switch will check if the IP address of the multicast group that the port wants to join is permitted by the IGMP Profile. If so, the switch allows it to join the multicast group.

You can also configure the maximum number of multicast groups that the port is allowed to join. If the number of the multicast groups that the port joins exceeds the threshold, the switch will no longer receive or handle the IGMP Report message.

To enable IGMP Filtering, execute the following commands in the global configuration mode:

Command	Function
Ruijie(config)# <b>interface</b> <i>interface-id</i>	Enter the interface configuration interface.
Ruijie(config-if)# <b>ip igmp snooping filter</b> <i>profile-number</i>	(Optional) Apply a profile to the interface. The profile number ranges from 1 to 1024.
Ruijie(config-if)# <b>ip igmp snooping max-groups</b> <i>number</i>	(Optional) Specify the maximum number of multicast groups that the interface can join, in the range of 0 to 1024.
Ruijie(config-if)# <b>no ip igmp snooping max-groups</b>	(Optional) Restore the max-groups to the default value.

The example below shows how to configure IGMP Filtering:

```
Ruijie# configure terminal
Ruijie(config)# interface fastEthernet 0/1
Ruijie(config-if)# ip igmp snooping filter 1
Ruijie(config-if)# ip igmp snooping max-groups 1000
```

```

Ruijie (config-if)#end

Ruijie #show ip igmp snooping interface fastEthernet 0/1

Interface                Filter profile number      max-group
-----                -
FastEthernet 0/1         1                          1000

```

## Showing IGMP Snooping Information

### Showing Current Mode

To view the current operation mode and global configuration of IGMP Snooping, execute the following command in the privileged EXEC mode:

Command	Function
Ruijie# <b>show ip igmp snooping</b>	View the current operation mode and global configuration of IGMP Snooping.

The following example uses the **show ip igmp snooping** command to view the IGMP Snooping configuration information:

```

Ruijie# show ip igmp snooping
IGMP-snooping mode      : IVGL
SVGL vlan-id            : 1
SVGL profile number     : 0
Source port check       : Disabled
Source ip check          : Disabled
IGMP Fast-Leave          : Disabled
IGMP Report suppress    : Disable

```

### Showing and Clearing IGMP Snooping Statistics

To view and clear the IGMP Snooping statistics, execute the following commands in the privileged EXEC mode:

Command	Function
Ruijie# <b>show ip igmp snooping statistics [vlan <i>vlan-id</i>]</b>	View the IGMP Snooping statistics
Ruijie# <b>clear ip igmp snooping statistics</b>	Clear the IGMP Snooping statistics

The following example uses the **show ip igmp snooping statistics** command to view the IGMP Snooping statistics:

```

Ruijie# show ip igmp snooping statistics
Current number of Gda-table entries: 1
Configured Statistics database limit: 1024
Current number of IGMP Query packet received : 1957
Current number of IGMPv1/v2 Report packet received: 5
Current number of IGMPv3 Report packet received: 4

```

```
Current number of IGMP Leave packet received: 1
```

```

GROUP  Interface  Last Last  Report  Leave report time reporter  pkts  pkts
-----  -
233.3.3.3  gi1/1  00:02:40  1.1.1.1  3      1

```

## Showing the Route Interface

To view the route interface information of IGMP Snooping, execute the following commands in the privileged EXEC mode:

Command	Function
Ruijie# <b>show ip igmp snooping mrouter</b>	Show the router interface information of IGMP Snooping

The following example uses the **show ip igmp snooping** command to view the router interface information of IGMP Snooping:

```

Ruijie# show ip igmp snooping mrouter
Vlan    Interface          State      IGMP profile number
----    -
1  GigabitEthernet 0/7  static      1
1  GigabitEthernet 0/12 dynamic      0

```

## Showing Dynamic Forwarding Table

To view the forwarding rule of each port in the multicast group, that is, the GDA(Group Destination Address) table, execute the following commands in the privileged EXEC mode:

Command	Function
Ruijie# <b>show ip igmp snooping gda-table</b>	Show the forwarding rule of each port in the multicast group.

This example shows the information on various multicast groups of the GDA table and the information on all the member ports of one multicast group:

```

Ruijie# show ip igmp snooping gda-table
Abbr: M - mrouter
      D - dynamic
      S - static
VLAN  Address          Member ports
-----
1     233.3.3.3      GigabitEthernet 0/7(S)

```

## Clearing Dynamic Forwarding Table

To clear the forwarding rule of each port in the multicast group, that is, the GDA(Group Destination Address) table, execute the following commands in the privileged EXEC mode:

Command	Function
---------	----------

Command	Function
Ruijie# <b>clear ip igmp snooping gda-table</b>	Clear the forwarding rule of each port in the multicast group.

This example clears the information on various multicast groups of the GDA table:

```
Ruijie# clear ip igmp snooping gda-table
```

## Clearing IGMP Snooping Statistics

To clear the forwarding rule of each port in the multicast group, that is, the GDA(Group Destination Address) table, execute the following commands in the privileged EXEC mode:

Command	Function
Ruijie# <b>clear ip igmp snooping statistics</b>	Clear the dynamic statistics of the entry node in the forwarding table.

This example clears the multicast group statistics in the GDA table:

```
Ruijie# clear ip igmp snooping statistics
```

## Showing IGMP Profile

To view the IGMP Profile information, execute the following command in the privileged EXEC mode:

Command	Function
Ruijie# <b>show ip igmp profile</b> <i>profile-number</i>	View the IGMP Profile information.

This example shows the IGMP Profile information:

```
Ruijie# show ip igmp profile 1
Profile      1
    Permit
    range 224.0.1.0, 239.255.255.255
```

## Showing IGMP Filtering

To view the IGMP Filtering information, execute the following command in the privileged EXEC mode:

Command	Function
Ruijie# <b>show ip igmp snooping interface</b> <i>interface-id</i>	View IGMP Filtering information.

The following example views the IGMP Filtering information.

```
Ruijie# show ip igmp snooping interface GigabitEthernet 0/7
Interface      Filter Profile number      max-groups
```

## Showing IGMP Snooping Querier

To view the IGMP Snooping Querier information, execute the following command in the privileged EXEC

mode:

Command	Function
Ruijie# <b>show ip igmp snooping querier</b>	View IGMP Querier information.
Ruijie# <b>show ip igmp snooping querier detail</b>	View the details of IGMP Querier.

The following example views the IGMP Querier information.

```
Ruijie# show ip igmp snooping querier detail
Vlan      IP Address      IGMP Version      Port
-----
Global IGMP switch querier status
-----
admin state           : Enable
admin version         : 2
source IP address     : 1.1.1.1
query-interval (sec)  : 125
max-response-time (sec) : 10
querier-timeout (sec) : 60

Vlan 1:  IGMP switch querier status
-----
admin state           : Enable
admin version         : 2
source IP address     : 1.1.2.2
query-interval (sec)  : 125
max-response-time (sec) : 10
querier-timeout (sec) : 60
operational state     : Disable
operational version   : 2

Vlan 2:  IGMP switch querier status
-----
admin state           : Disable
admin version         : 2
source IP address     : 1.1.1.1
query-interval (sec)  : 125
max-response-time (sec) : 10
querier-timeout (sec) : 60
operational state     : Disable
operational version   : 2
```

## Typical IGMP Snooping Configuration Example

### Example of IVGL mode Configuration

#### Topological Diagram

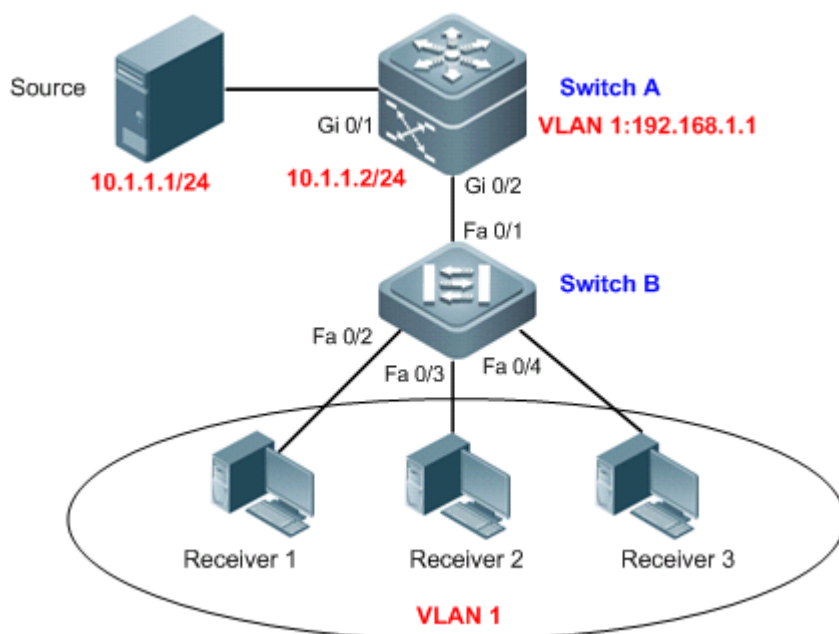


Figure4 Diagram for IVGL mode

#### Application Requirements

As shown above, Switch A is a multicast routing device directly connected with a multicast source, and Switch B is a layer-2 access device connected with multiple multicast receivers which belong to the same VLAN. The primary requirements are shown below:

- ✓ Achieve layer-3 multicast routing on Switch A, and on Switch B, multicast traffic won't be broadcasted on VLAN but sent to the specified receiver.
- ✓ Receiver 1 can receive IP multicast traffic with group address being 224.1.1.1; Receiver 2 can only receive IP multicast traffic with group address falling within 225.1.1.1-226.1.1.1; Receiver 3 can only join 100 IP multicast groups.
- ✓ On Switch B, all access ports can quickly leave a specific IP multicast group.
- ✓ On Switch B, IGMP members are prohibited from forwarding response messages to Switch A, so as to lessen the burden of Switch A.

#### Configuration Tips

1. On the multicast routing device (Switch A), enable multicast routing and forwarding and configure multicast routing protocol on the corresponding layer-3 interface (Gi 0/1 and VLAN 1); on the layer-2 multicast device (Switch B), configure IGMP Snooping to operate in IVGL mode; the router port can be

generated dynamically or configured statically (configure port Fa 0/1 as the static router port).

2. Configure the port directly connected with Receiver 1 (Fa 0/2) as the static member port of corresponding group; configure IGMP Filtering on the port directly connected with Receiver 2 (Fa 0/3); Configure the maximum number of multicast groups that can be joined on the port directly connected with Receiver 3 (Fa 0/4).
3. Enable fast leave on the device running IGMP Snooping (Switch B).
4. Configure IGMP Snooping report suppression on the device running IGMP Snooping (Switch B).

## Configuration Steps

Step 1: Configure multicast routing on the multicast routing device.

! Globally enable multicast routing and forwarding on Switch A.

```
SwitchA#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
SwitchA(config)#ip multicast-routing
```

! Configure port Gi 0/1 of Switch A as a router port for connecting multicast source and configure the multicast routing protocol

```
SwitchA(config)#interface gigabitEthernet 0/1
SwitchA(config-if-GigabitEthernet 0/1)#no switchport
SwitchA(config-if-GigabitEthernet 0/1)#ip address 10.1.1.2 255.255.255.0
SwitchA(config-if-GigabitEthernet 0/1)#ip pim dense-mode
SwitchA(config-if-GigabitEthernet 0/1)#exit
```

! Configure the SVI and VLAN 1 and configure multicast routing protocol on SVI.

```
SwitchA(config)#interface vlan 1
SwitchA(config-if-VLAN 1)#ip address 192.168.1.1 255.255.255.0
SwitchA(config-if-VLAN 1)#ip pim dense-mode
SwitchA(config-if-VLAN 1)#exit
```

! Configure port Gi 0/2 as a trunk port for connecting layer-2 multicast device.

```
SwitchA(config)#interface gigabitEthernet 0/2
SwitchA(config-if-GigabitEthernet 0/2)#switchport mode trunk
SwitchA(config-if-GigabitEthernet 0/2)#exit
```

Step 2: Enable IGMP Snooping on layer-2 multicast device and configure router port.

! On Switch B, globally configure IGMP Snooping to operate in IVGL mode and configure Fa 0/1 as the router port of VLAN 1.

```
SwitchB(config)#ip igmp snooping ivgl
SwitchB(config)#ip igmp snooping vlan 1 mrouter interface fastEthernet 0/1
```

Step 3: Configure the ports connecting with Receiver 1, Receiver 2 and Receiver 3.

! Configure port Fa 0/2 as the static member port of VLAN 1 with group address being 224.1.1.1.



```
SwitchB(config)#ip igmp snooping vlan 1 static 224.1.1.1 interface fastEthernet 0/2
```

**! Configure IGMP Profile1 to receive only the IP multicast traffic with group address falling within 225.1.1.1-226.1.1.1 and apply to port Fa 0/3.**

```
SwitchB(config)#ip igmp profile 1
SwitchB(config-profile)#permit
SwitchB(config-profile)#range 225.1.1.1 226.1.1.1
SwitchB(config-profile)#exit
SwitchB(config)#interface fastEthernet 0/3
SwitchB(config-if-FastEthernet 0/3)#ip igmp snooping filter 1
SwitchB(config-if-FastEthernet 0/3)#exit
```

**! Configure that port Fa 0/4 can be joined by up to 100 multicast groups.**

```
SwitchB(config)#interface fastEthernet 0/4
SwitchB(config-if-FastEthernet 0/4)#ip igmp snooping max-groups 100
SwitchB(config-if-FastEthernet 0/4)#exit
```

**Step 4: On layer-2 device, configure that all access sports can quickly leave a certain IP multicast group and enable IGMP report suppression.**

**! Enable fast leave on Switch B.**

```
SwitchB(config)#ip igmp snooping fast-leave enable
```

**! Enable IGMP Snooping report suppression on Switch B.**

```
SwitchB(config)#ip igmp snooping suppression enable
```

## Verification

**Step 1: Display device configurations**

**! Configurations of Switch A**

```
SwitchA#show running-config
!
ip multicast-routing
!
interface GigabitEthernet 0/1
no switchport
ip pim dense-mode
no ip proxy-arp
ip address 10.1.1.2 255.255.255.0
!
interface GigabitEthernet 0/2
switchport mode trunk
!
interface VLAN 1
ip pim dense-mode
no ip proxy-arp
ip address 192.168.1.1 255.255.255.0
```

## ! Configurations of Switch B

```
SwitchB#show running-config
!
interface FastEthernet 0/3
 ip igmp snooping filter 1
!
interface FastEthernet 0/4
 ip igmp snooping max-group 100
!
ip igmp profile 1
permit
range 225.1.1.1 226.1.1.1
ip igmp snooping ivgl
ip igmp snooping vlan 1 static 224.1.1.1 interface FastEthernet 0/2
ip igmp snooping vlan 1 mrouter interface FastEthernet 0/1
ip igmp snooping fast-leave enable
ip igmp snooping suppression enable
```

### Step 2: Display the IGMP Snooping configurations of Switch B

```
SwitchB#show ip igmp snooping
IGMP Snooping running mode: IVGL
Source port check: Disable
Source ip check: Disable
IGMP Fast-Leave: Enable
IGMP Report suppress: Enable
IGMP Globle Querier: Disable
Dynamic Mroute Aging Time : 300(Seconds)
Tunnel IGMP Packet: Disable

vlan 1
-----
IGMP Snooping state: Enabled
Multicast router learning mode: pim-dvmrp
IGMPv2 fast leave: Disabled
IGMP VLAN querier: Disable
```

### Step 3: Display router port configuration of Switch B

```
SwitchB#show ip igmp snooping mrouter
Multicast Switching Mroute Port
D: DYNAMIC
S: STATIC
(*, *, 1):
VLAN(1) 1 MROUTES:
FastEthernet 0/1 (S)
```

### Step 4: Display interface configurations of IGMP Snooping

```
SwitchB#show ip igmp snooping interfaces
Interface          Filter profile number  max-group
-----
FastEthernet 0/3    1                      4294967294
FastEthernet 0/4    0                      100
```

**Step 5: Send IP multicast traffic with group address being 224.2.2.2 through the Source, and request multicast traffic on port Fa 0/2 of Switch B. Display the group members of Switch A and CDA table of Switch B.**

```
! Switch A
SwitchA#show ip igmp groups
IGMP Connected Group Membership
Group Address Interface Uptime Expires Last Reporter
224.2.2.2      VLAN 1  00:00:51  00:03:55  0.0.0.0
```

**! Switch B**

```
SwitchB#show ip igmp snooping gda-table
Multicast Switching Cache Table
D: DYNAMIC
S: STATIC
M: MROUTE
(*,224.1.1.1, 1):
VLAN(1) 2 OPORTS:
FastEthernet 0/1 (M)
FastEthernet 0/2 (S)
(*,224.2.2.2, 1):
VLAN(1) 2 OPORTS:
FastEthernet 0/1 (M)
FastEthernet 0/2 (D)
```

## Example of IVGL-SVGL mode Configuration

### Topological Diagram

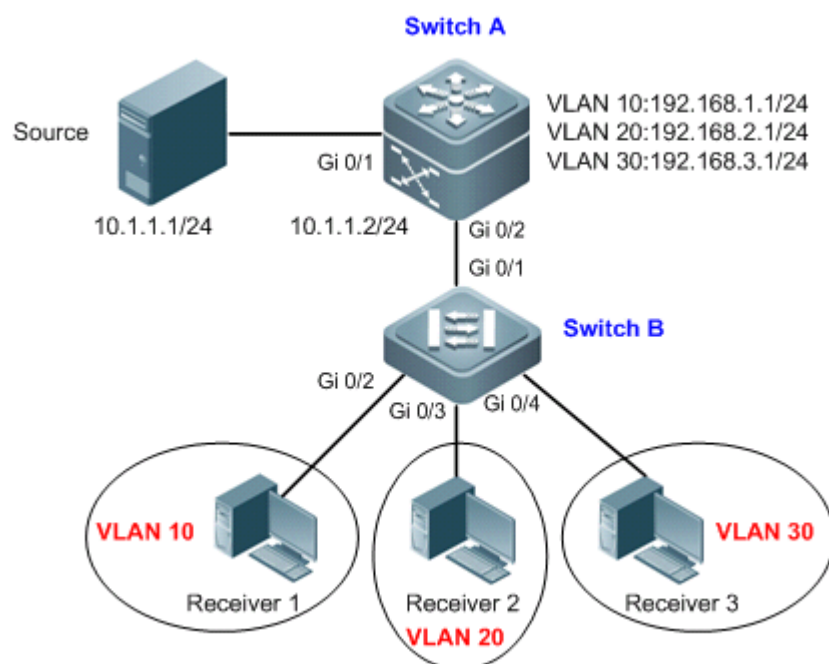


Figure 5 Diagram for IVGL mode

### Application Requirements

As shown above, Switch A is a multicast routing device directly connected with a multicast source, and Switch B is a layer-2 access device connected with multiple multicast receivers which belong to different VLANs. The primary requirements are shown below:

- ✓ Achieve layer-3 multicast routing on Switch A, and on Switch B, multicast traffic won't be broadcasted on VLAN but sent to the specified receiver.
- ✓ On Switch B, specify that IP multicast traffic with multicast address falling within 224.1.1.1-226.1.1.1 can be forwarded across VLAN, while other IP multicast traffic can only be forwarded to the member ports belonging to the same VLAN.
- ✓ On Switch B, only IP multicast traffic received by the router port will be forwarded, and IP multicast traffic received by non-router port will be blocked.

### Configuration Tips

1. On the multicast routing device (Switch A), enable multicast routing and forwarding and configure multicast routing protocol on the corresponding layer-3 interface (Gi 0/1 and VLAN 10, VLAN 20 and VLAN 30); on the layer-2 multicast device (Switch B), configure IGMP Snooping to operate in IVGL-SVGL mode; the router port can be generated dynamically or configured statically (configure port Gi 0/1 as the static router port).

2. On the layer-2 multicast device (Switch B) running IGMP Snooping, specify a VLAN as Share VLAN (VLAN 10) and configure the multicast address range (224.1.1.1-226.1.1.1) of Share VLAN, so that IP multicast traffic falling within this multicast address range can be forwarded across VLAN. By default, IP multicast traffic related to other address ranges can only be forwarded within the same VLAN.

## Configuration Steps

Step 1: Configure multicast routing on the multicast routing device.

! Globally enable multicast routing and forwarding on Switch A.

```
SwitchA#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
SwitchA(config)#ip multicast-routing
```

! Configure port Gi 0/1 of Switch A as a router port for connecting multicast source and configure the multicast routing protocol

```
SwitchA(config)#interface gigabitEthernet 0/1
SwitchA(config-if-GigabitEthernet 0/1)#no switchport
SwitchA(config-if-GigabitEthernet 0/1)#ip address 10.1.1.2 255.255.255.0
SwitchA(config-if-GigabitEthernet 0/1)#ip pim dense-mode
SwitchA(config-if-GigabitEthernet 0/1)#exit
```

! On Switch A, configure the SVI of VLAN 10, VLAN 20 and VLAN 30, and configure multicast routing protocol on SVI.

```
SwitchA(config)#vlan 10
SwitchA(config-vlan)#exit
SwitchA(config)#interface vlan 10
SwitchA(config-if-VLAN 10)#ip address 192.168.1.1 255.255.255.0
SwitchA(config-if-VLAN 10)#ip pim dense-mode
SwitchA(config-if-VLAN 10)#exit
SwitchA(config)#vlan 20
SwitchA(config-vlan)#exit
SwitchA(config)#interface vlan 20
SwitchA(config-if-VLAN 20)#ip address 192.168.2.1 255.255.255.0
SwitchA(config-if-VLAN 20)#ip pim dense-mode
SwitchA(config-if-VLAN 20)#exit
SwitchA(config)#vlan 30
SwitchA(config-vlan)#exit
SwitchA(config)#interface vlan 30
SwitchA(config-if-VLAN 30)#ip address 192.168.3.1 255.255.255.0
SwitchA(config-if-VLAN 30)#ip pim dense-mode
SwitchA(config-if-VLAN 30)#exit
```

! On Switch A, configure port Gi 0/2 as a trunk port for connecting layer-2 multicast device.

```
SwitchA(config)#interface gigabitEthernet 0/2
SwitchA(config-if-GigabitEthernet 0/2)#switchport mode trunk
SwitchA(config-if-GigabitEthernet 0/2)#exit
```

**Step 2: Create VLAN on layer-2 multicast device and configure user ports of corresponding VLANs**

**! On Switch B, create VLAN 10, VLAN 20 and VLAN 30; configure port Gi 0/2 to belong to VLAN 10, Gi 0/3 to belong to VLAN 20, and Gi 0/4 to belong to VLAN 30.**

```
SwitchB#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
SwitchB(config)#interface gigabitEthernet 0/2
SwitchB(config-if-GigabitEthernet 0/2)#switchport access vlan 10
SwitchB(config-if-GigabitEthernet 0/2)#exit
SwitchB(config)#interface gigabitEthernet 0/3
SwitchB(config-if-GigabitEthernet 0/3)#switchport access vlan 20
SwitchB(config-if-GigabitEthernet 0/3)#exit
SwitchB(config)#interface gigabitEthernet 0/4
SwitchB(config-if-GigabitEthernet 0/4)#switchport access vlan 30
SwitchB(config-if-GigabitEthernet 0/4)#exit
```

**! Configure port Gi 0/1 as a trunk port.**

```
SwitchB(config)#interface gigabitEthernet 0/1
SwitchB(config-if-GigabitEthernet 0/1)#switchport mode trunk
SwitchB(config-if-GigabitEthernet 0/1)#exit
```

**Step 3: Enable IGMP Snooping on layer-2 multicast device and configure router port.**

**! On Switch B, globally configure IGMP Snooping to operate in IVGL-SVGL mode and configure Gi 0/1 as the router port of VLAN 10, VLAN 20 and VLAN 30.**

```
SwitchB(config)#ip igmp snooping ivgl-svgl
SwitchB(config)#ip igmp snooping vlan 10 mrouter interface gigabitEthernet 0/1
SwitchB(config)#ip igmp snooping vlan 20 mrouter interface gigabitEthernet 0/1
SwitchB(config)#ip igmp snooping vlan 30 mrouter interface gigabitEthernet 0/1
```

**Step 4: Configure Share VLAN on layer-2 multicast device and specify the multicast address range.**

**! On Switch B, specify VLAN 10 as the Share VLAN.**

```
SwitchB(config)#ip igmp snooping svgl vlan 10
```

**! On Switch B, configure IGMP Profile 1 to permit the IP multicast address range of 224.1.1.1-226.1.1.1 and associate SVGL mode.**

```
SwitchB(config)#ip igmp profile 1
SwitchB<config-profile>#permit
SwitchB<config-profile>#range 224.1.1.1 226.1.1.1
```

```
SwitchB<config-profile>#exit
SwitchB(config)#ip igmp snooping ssvg1 profile 1
Step 5: Configure source port check on layer-2 multicast device.
SwitchB(config)#ip igmp snooping source-check port
```

## Verification

### Step 1: Display device configurations

#### ! Configurations of Switch A

```
SwitchA#show running-config
!
vlan 10
!
vlan 20
!
vlan 30
!
ip multicast-routing
!
interface GigabitEthernet 0/1
 no switchport
 ip pim dense-mode
 no ip proxy-arp
 ip address 10.1.1.2 255.255.255.0
!
interface GigabitEthernet 0/2
 switchport mode trunk
!
interface VLAN 10
 ip pim dense-mode
 no ip proxy-arp
 ip address 192.168.1.1 255.255.255.0
!
interface VLAN 20
 ip pim dense-mode
 no ip proxy-arp
 ip address 192.168.2.1 255.255.255.0
!
interface VLAN 30
 ip pim dense-mode
 no ip proxy-arp
 ip address 192.168.3.1 255.255.255.0
```

#### ! Configurations of Switch B

```
SwitchB#show running-config
!
vlan 10
!
vlan 20
!
vlan 30
!
interface GigabitEthernet 0/1
 switchport mode trunk
!
interface GigabitEthernet 0/2
 switchport access vlan 10
!
interface GigabitEthernet 0/3
 switchport access vlan 20
!
interface GigabitEthernet 0/4
 switchport access vlan 30
!
ip igmp profile 1
permit
range 224.1.1.1 226.1.1.1
ip igmp snooping ivgl-svgl
ip igmp snooping svgl vlan 10
ip igmp snooping svgl profile 1
ip igmp snooping source-check port
ip igmp snooping vlan 10 mrouter interface GigabitEthernet 0/1
ip igmp snooping vlan 20 mrouter interface GigabitEthernet 0/1
ip igmp snooping vlan 30 mrouter interface GigabitEthernet 0/1
```

## Step 2: Display the IGMP Snooping configurations of Switch B

```
SwitchB#show ip igmp snooping
IGMP Snooping running mode: IVGL_SVGL
SVGL vlan: 10
SVGL profile number: 1
Source port check: Enable
Source ip check: Disable
IGMP Fast-Leave: Disable
IGMP Report suppress: Disable
IGMP Globle Querier: Disable
Dynamic Mroute Aging Time : 30000(Seconds)

vlan 1
-----
```



```
IGMP Snooping state: Enabled
Multicast router learning mode: pim-dvmrp
IGMPv2 immediate leave: Disabled
IGMP VLAN querier: Disable

vlan 10
-----
IGMP Snooping state: Enabled
Multicast router learning mode: pim-dvmrp
IGMPv2 immediate leave: Disabled
IGMP VLAN querier: Disable

vlan 20
-----
IGMP Snooping state: Enabled
Multicast router learning mode: pim-dvmrp
IGMPv2 immediate leave: Disabled
IGMP VLAN querier: Disable

vlan 30
-----
IGMP Snooping state: Enabled
Multicast router learning mode: pim-dvmrp
IGMPv2 immediate leave: Disabled
IGMP VLAN querier: Disable
```

### Step 3: Display router port configuration of Switch B

```
SwitchB#show ip igmp snooping mrouter
Multicast Switching Mroute Port
  D: DYNAMIC
  S: STATIC
(*, *, 10):
  VLAN(10) 1 MROUTES:
    GigabitEthernet 0/1(S)

(*, *, 20):
  VLAN(20) 1 MROUTES:
    GigabitEthernet 0/1(S)

(*, *, 30):
  VLAN(30) 1 MROUTES:
    GigabitEthernet 0/1(S)
```

**Step 4: Send IP multicast traffic with group address being 224.1.1.1 through the Source, and request multicast traffic on port Gi 0/3 of Switch B (belonging to VLAN 20 and IP address being 192.168.2.3). Display the group members of Switch A and CDA table of Switch B:**

**! Switch A**

```
SwitchA#show ip igmp groups
IGMP Connected Group Membership
Group Address  Interface Uptime  Expires  Last Reporter
224.1.1.1      VLAN 10  00:00:16  00:04:04  192.168.2.3
```

**! Switch B**

```
SwitchB#show ip igmp snooping gda-table
Multicast Switching Cache Table
D: DYNAMIC
S: STATIC
M: MROUTE
(*,224.1.1.1, 20):
VLAN(1) 2 OPORTS:
GigabitEthernet 0/3(D)
GigabitEthernet 0/1(M)
```

! From the above information, we can learn that the group address range of IP multicast traffic requested by port Gi 0/3 is 224.1.1.1-226.1.1.1, and the traffic is forwarded through Share VLAN 10.

Step 5: Send IP multicast traffic with group address being 228.1.1.1 through the Source, and request multicast traffic on port Gi 0/3 of Switch B (belonging to VLAN 20 and IP address being 192.168.2.3). Display the group members of Switch A and CDA table of Switch B:

**! Switch A**

```
SwitchA#show ip igmp groups
IGMP Connected Group Membership
Group Address Interface Uptime Expires Last Reporter
228.1.1.1      VLAN 20  00:00:14  00:04:06  192.168.2.3
```

**! Switch B**

```
SwitchB#show ip igmp snooping gda-table
Multicast Switching Cache Table
D: DYNAMIC
S: STATIC
M: MROUTE
(*,228.1.1.1, 20):
VLAN(1) 2 OPORTS:
GigabitEthernet 0/3(D)
GigabitEthernet 0/1(M)
```

! From the above information, we can learn that the group address range of IP multicast traffic requested by port Gi 0/3 is outside 224.1.1.1-226.1.1.1, and the traffic is forwarded on VLAN 20.

# MLD Snooping Configuration

## Understanding MLD Snooping

### MLD Snooping Overview

MLD Snooping is the short form of Multicast Listener Discovery Snooping. It is designed to manage and control the transmission of IPv6 multicast stream on layer 2.

By running the MLD Snooping equipment and analyzing the MLD message received, mapping relationship is established for port and MAC multicasting address, and such relationship provides a basis for the transmission of IPv6 multicast data on layer 2. When the MLD Snooping is not running, IPv6 multicast data message is broadcast on layer 2; while after the switch places MLD Snooping into operation, the known multicast data message of IPv6 multicast group will not be broadcast on layer 2, but be exchanged to specified receiver(s) on layer 2.

### Basic Concepts of MLD Snooping

#### Understanding two types of MLD Snooping ports

As shown in Figure 1, Router is connected with multicast source and with the switch to run MLD Snooping, host A and host C become the hosts (or multicast listener) of receiver.

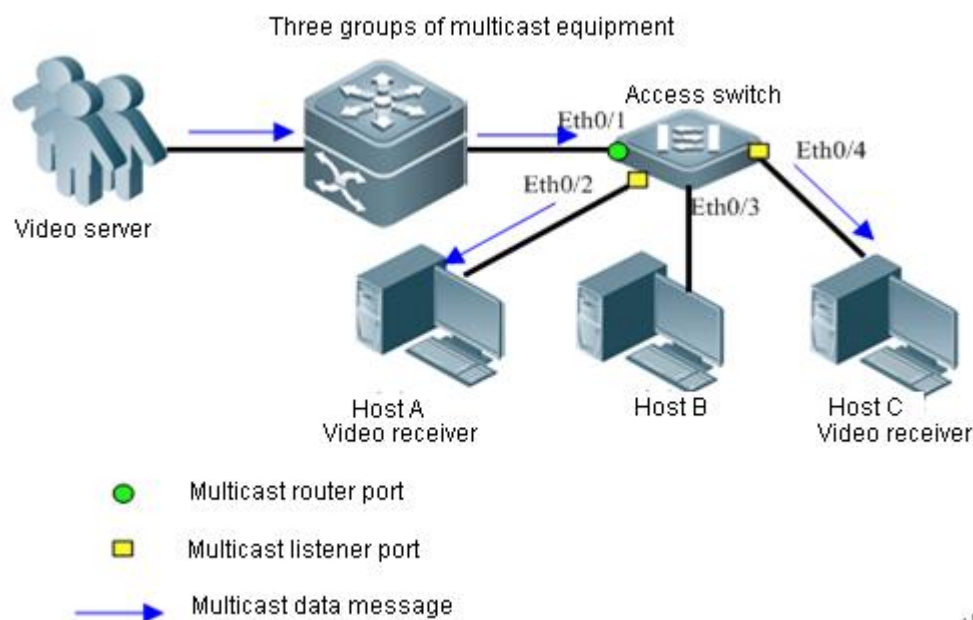


Figure 1 Two types of MLD Snooping ports

**Multicast Router Port:** a multicast device of the switch to connect layer 3, e.g., Eth 0 / 1 port;

**Member Port:** the short form of the IPv6 multicast group member port, also called Listener Port.

For example, the Access Switch Eth0/2, Eth0/3 and Eth0/4 port.

## Understanding MLD Profiles

MLD Profiles are actually some group filters, which can define a series of multicast address ranges, and permit or deny the access of those multicast addresses, providing usage for different functions of the following "multicast address ranges for SVGL mode application", "multicast data area to be filtered by router port", "MLD Filtering range", etc.

## Understanding different kinds of working modes of MLD Snooping

**DISABLE mode:** Under this mode, MLD Snooping is out of function, i.e., layer 2 multicast equipment does not "snoop" the MLD message between hosts and router, and multicast frames are broadcast in VLAN.

**IVGL (Independent VLAN Group Learn) working mode:** Under this mode, multicast stream among all VLANs is inter-independent. A host can only request multicast stream from the router port in the same VLAN where the host is located; switch can only transmit the multicast data flow being received from any VLAN to listener ports in the same VLAN.

**SVGL (Shared VLAN Group Learn) working mode:** Under this mode, hosts of each VLAN share a multicast stream and may request for multicast stream across the VLAN. When specifying a shared VLAN, only the multicast data flow of the VLAN may transmit to other hosts across the VLAN. So long as multicast data flow belongs to Shared VLAN, they can be transmitted to the listener ports of this multicast address, even if some listener ports do not belong to Shared VLAN. Under SVGL mode, it is necessary to use MLD Profile to allocate a number of multicast address ranges to SVGL, within such ranges the listener ports of the multicast forwarding-table may transmit across VLAN. Under default condition, all class ranges are not within the application area of SVGL, and all multicast stream will be discarded.

The two modes of IVGL and SVGL may coexist, you may allocate with MLD Profile a number of multicast addresses ranges to SVGL, within such ranges the listener ports of the multicast forwarding-table may transmit across VLAN. However, the listener ports of the multicast forwarding-tables within other multicast address ranges must belong to the same VLAN.

## Working Principle of MLD Snooping

The switch that runs MLD Snooping processes different MLD messages in the following ways:

### 1. MLD QUERY

Layer 3 multicast equipments regularly send group-general query message to all hosts and routers (address: FF 02::1) within local network segment to find out which listeners of IPv6 multicast group exist in this local network segment. A switch transmits MLD group-general query message being received to all other ports except receive port within VLAN and process the receive port in the following ways:

- If the port is already included in the list of router ports, its aging timer should be reset.
- If the port is not included in the list of router ports, it should be added to the list of

router ports and its aging timer should be enabled.

- Whenever receiving MLD group-general query message, layer 2 multicast equipment will update respective aging timers of all listener ports and demote the timer to configured MLD query-max-response-time. When the timer value is reduced to "0", it is considered that there is no longer any listener of the port receiving multicast stream. Layer 2 multicast equipment will delete the port from MLD Snooping forwarding-table.
- Whenever receiving MLD group-specific query message, layer 2 multicast equipment will update aging timers of all listener ports in the specific group, and demote the timer to configured MLD query-max-response-time. When the timer value is reduced to "0", it is considered that there is no longer any listener of the port receiving multicast stream. Layer 2 multicast equipment will delete the port from MLD Snooping forwarding-table.
- When receiving MLD group-specific source query message, the aforesaid two kinds of timers will not be updated.

## 2. MLD REPORT

A host will send MLD membership report to MLD queriers under following conditions:

- When receiving MLD (group-general or group-specific) query message, the listener hosts of IPv6 multicast group will respond with MLD membership report message.
- When joining certain IPv6 multicast group, a host will actively send MLD membership report message to MLD queriers to announce its joining in this IPv6 multicast group.

A switch transmits through all routers in VLAN the MLD membership report message being received, resolve the IPv6 multicast group addresses which hosts will join, and process the receive port in the following ways:

- If the forwarding-table corresponding to this IPv6 multicast group does not exist, a forwarding-table should be created. And the port should be added as a dynamic listener port to the list of outgoing ports and its aging timer should be enabled.
- If the forwarding-table corresponding to this IPv6 multicast group already exists, but the list of its outgoing ports does not include this port, the port should be added as a dynamic listener port to the list of outgoing ports and its aging timer should be enabled.
- If the forwarding-table corresponding to this IPv6 multicast group already exists, and the list of its outgoing ports includes this dynamic listener port, then its aging timer should be reset.

## 3. MLD LEAVE

When leaving IPv6 multicast group, a host will send MLD leave message to notify the multicast router that it has left certain IPv6 multicast group. A switch will directly forward to router port the MLD leave message it receives from certain dynamic listener port. When the fast-leave function is enabled, the equipment will directly remove relevant ports from the list of ports that transmit corresponding group records.

## Protocol Specification

Relevant Protocol specification:

RFC4541

## Default Configuration

The following table is used to describe the default configuration of MLD Snooping.

Function characteristics	Default value
Global MLD Snooping switch	Disabled
VLAN-based MLD Snooping switch	Enabled
Aging interval of router ports	300s
Max-response-time for MLD query	10s
Function as a dynamic learn router port	Disabled
The function of fast-leave from multicast listener ports	Disabled
The function of restraining MLD report	Disabled
Port-based filtration of unicast group of specific multicast	Disabled
Number of port-based max-restriction multicast group	1024

## Enable Global MLD Snooping

It is necessary to specify the working mode of MLD Snooping when enabled MLD Snooping is set as default. You may assign one of the three modes of IVGL, SVGL and IVGL-SVGL (coexist).



### Caution

After enabling the layer2 multicasting on the Private VLAN and Super VLAN, if the multicast source exists in the Sub-VLAN, one more route entry is needed to be duplicated and the ingress is the Sub-VLAN in which the multicast streams enter as the ingress validity check is required when multicast forwarding, resulting in occupying one more multicast hardware entry with 1 less multicast capacity.

## Configuring IVGL Mode

To enable the MLD Snooping and configure the IVGL mode, run the following commands:

Command	Function
Ruijie(config)# <b>ipv6 mld snooping ivgl</b>	Enable the MLD Snooping and configure the IVGL mode. By default, the MLD Snooping is disabled.

Ruijie(config)# <b>exit</b>	Return to the privilege mode.
Ruijie# <b>show ipv6 mld snooping</b>	Verify the configurations.

The following example shows how to enable the MLD Snooping and configure the IVGL mode:

```
Ruijie# configure terminal
Ruijie(config)# ipv6 mld snooping ivgl
Ruijie(config)# exit
Ruijie# show ipv6 mld snooping
MLD-snooping mode      :IVGL
SVGL VLAN-ID           :1
SVGL profile number     :0
Source check port       :Disable
Query Max Response Time :10 (Seconds)
```

## Configuring SVGL Mode

To enable the MLD Snooping and configure the SVGL mode, run the following commands:

Command	Function
Ruijie(config)# <b>ipv6 mld snooping svgl</b>	Enable the MLD Snooping and configure the SVGL mode. By default, the MLD Snooping is disabled.
Ruijie(config)# <b>exit</b>	Return to the privilege mode.
Ruijie# <b>show ipv6 mld snooping</b>	Verify the configurations.

The following example shows how to enable the MLD Snooping and configure the SVGL mode:

```
Ruijie# configure terminal
Ruijie(config)# ipv6 mld snooping svgl
Ruijie(config)# exit
Ruijie# show ipv6 mld snooping
MLD-snooping mode      :SVGL
SVGL VLAN-ID           :1
SVGL profile number     :0
Source check port       :Disable
Query Max Response Time :10 (Seconds)
```

**Caution**

When configuring the mode as SVGL mode, a profile must be related to assign multicast address range for SVGL mode application, otherwise, the default application of SVGL will not take effect. For the detailed configuration, please refer to the section of *Configuring the multicast address range for SVGL mode application*.

MLD SNOPING SVGL mode and IPV4/V6 layer 3 multicast cannot coexist.

## Configuring IVGL-SVGL Mode

To enable the MLD Snooping and configure the IVGL-SVGL mode, run the following commands:

Command	Function
Ruijie(config)# <b>ipv6 mld snooping ivgl-svgl</b>	Enable the MLD Snooping and configure the IVGL-SVGL mode. By default, the MLD Snooping is disabled.
Ruijie(config)# <b>exit</b>	Return to the privilege mode.
Ruijie# <b>show ipv6 mld snooping</b>	Verify the configurations.

The following example shows how to enable the MLD Snooping and configure the IVGL-SVGL mode:

```
Ruijie# configure terminal
Ruijie(config)# ipv6 mld snooping ivgl-svgl
Ruijie(config)# exit
Ruijie# show ipv6 mld snooping
MLD-snooping mode      :IVGL-SVGL
SVGL VLAN-ID           :1
SVGL profile number     :0
Source check port       :Disable
Query Max Response Time :10 (Seconds)
```

**Caution**

When configuring the mode as IVGL-SVGL mode, a profile must be related to assign multicast address range for SVGL mode application, otherwise, the default application of SVGL will not take effect. During configuring, please refer to the following section of "multicast address range applied in configuring SVGL mode".

MLD SNOPING IVGL-SVGL mode and IPV4/V6 layer 3 multicast cannot coexist.

## Disable Global MLD Snooping

To disable the MLD Snooping function, run the following commands in the global configuration mode:



Command	Function
Ruijie(config)# <b>no ipv6 mld snooping</b>	Disable the MLD Snooping function. By default, the MLD Snooping is disabled.
Ruijie(config)# <b>exit</b>	Return to the privilege mode.
Ruijie# <b>show ipv6 mld snooping</b>	Verify the configurations.

The following example shows how to disable the MLD Snooping function:

```
Ruijie# configure terminal
Ruijie(config)# no ipv6 mld snooping
Ruijie(config)# exit
Ruijie# show ipv6 mld snooping
MLD-snooping mode      :DISABLE
SVGL VLAN-ID           :1
SVGL profile number     :0
Source check port       :Disable
Query Max Response Time :10 (Seconds)
```

## Disable VLAN-based MLD Snooping

To disable the VLAN-based MLD Snooping function, run the following commands in the vlan configuration mode:

Command	Function
Ruijie(config-vlan)# <b>no ipv6 mld snooping</b>	Disable the VLAN-based MLD Snooping function. By default, with the global MLD Snooping enabled, the MLD Snooping function in all VLANs are enabled.
Ruijie(config-vlan)# <b>end</b>	Return to the privilege mode.
Ruijie# <b>show ipv6 mld snooping</b>	Verify the configurations.

The following example shows how to disable the MLD Snooping in vlan 2:

```
Ruijie# configure terminal
Ruijie(config)# vlan 2
Ruijie(config-vlan)# no ipv6 mld snooping
Ruijie(config-vlan)# end
Ruijie# show ipv6 mld snooping
MLD-snooping mode      :IVGL
SVGL VLAN-ID           :1
SVGL profile number     :0
Source check port       :Disable
Query Max Response Time :10 (Seconds)
```

DISABLE VLAN

:2

**Note**

After enabling MLD Snooping within VLAN, users must also enable IGMP Snooping within this VLAN if they make application of IPv4 multicast within this VLAN.

## Configuring the Aging Timer for the Dynamic Route Port

If the dynamic route port has not received MLD group-general query message or IPv6 PIM Hello message before its aging time is out, the switch will delete the port from the list of router ports.

To configure the aging timer for the dynamic route port, run the following command:

Command	Function
Ruijie(config)# <b>ipv6 mld snooping dyn-mr-aging-time</b> <i>time</i>	Configure the aging timer for dynamic route port <i>time</i> : the valid range is 1-3600, and the default value is 300s.

Use the **no IPv6 MLD Snooping dyn-mr-aging-time** command to restore the aging time for the dynamic route port to the default value.

The following example shows how to set the aging time for the dynamic route port as 100s:

```
Ruijie# configure terminal
```

```
Ruijie(config)# ipv6 mld snooping dyn-mr-aging-time 100
```

## Configuring Max-response-time for MLD Query Message

- After receiving MLD group-general query message, layer 2 multicast equipment will enable respective aging timers of all listener ports and timer is set at max-response-time. When the timer value is reduced to "0", it is considered that there is no longer any listener of the port receiving multicast stream. And layer 2 multicast equipment will delete the port from MLD Snooping forwarding-table.
- After receiving MLD group-specific query message, layer 2 multicast equipment will enable respective aging timers of all listener ports in the specific group and timer is set at max-response-time. When the timer value is reduced to "0", it is considered that there is no longer any listener of the port receiving multicast stream. And layer 2 multicast equipment will delete the port from MLD Snooping forwarding-table.
- As for MLD group-specific source query message, timers will not be updated.

Command	Function
---------	----------

Ruijie(config)# <b>ipv6 mld snooping query-max-response-time</b> <i>time</i>	Configure MLD group-general and group-specific query max-response-time within the range of 1-65535, and the default value is 10s.
--	---

The following example shows how to set the max-response-time for the MLD query message as 15s:

```
Ruijie# configure terminal
```

```
Ruijie(config)# ipv6 mld snooping query-max-response-time 15
```

## Configuring Router port

By default, you may enable the dynamic router port learning in a VLAN for the layer 2 multicast device. Use the **no** form of this command to disable dynamic learning and clear all dynamically-learned router port.

You may also configure the switch port as a static router port so that all IPv6 multicast data received by the switch may be transmitted through this port.

To configure the router port, run the following command:

Command	Function
Ruijie(config)# <b>ipv6 mld snooping vlan</b> <i>vlan-id</i> <b>mrouter</b> { <i>interface interface-id</i>   <b>learn</b> }	Set the interface as static router port, by default, the port is not a static router port; set the dynamically-learned router port on the layer 2 multicast device, by default, the dynamic learning is allowed.

The following example shows how to set the Ethernet interface 0/1 as the router port and configure the auto-learning for the router port:

```
Ruijie# configure terminal
```

```
Ruijie(config)# ipv6 mld snooping vlan 1 mrouter interface gigabitEthernet 0/1
```

```
Ruijie(config)# ipv6 mld snooping vlan 1 mrouter learn
```

```
Ruijie(config)# end
```

```
Ruijie# show ipv6 mld snooping mrouter
```

```
VLAN      Interface          State      MLD profile
----      -
1  GigabitEthernet 0/1  static      0
1  GigabitEthernet 0/2  dynamic     0
```

```
Ruijie# show ipv6 mld snooping mrouter learn
```

```
VLAN      learn method
----      -
1          pim
```

## Configuring Static Listener Port

Use this command to set a port joins to the IPv6 multicast group statically to become a static listener port, if the host that connects to the port needs to receive the IPv6 multicast data sent to an IPv6 multicast group in a fixed manner.

To configure the MLD Snooping static listener port, run the following commands:

Command	Function
Ruijie(config)# <b>ipv6 mld snooping ivgl</b>	Enable and set MLD Snooping to IVGL mode.
Ruijie(config)# <b>ipv6 mld snooping vlan <i>vlan-id</i> static <i>ip-addr</i> interface <i>interface-id</i></b>	Statically configure a port to receive certain multicast stream. <ul style="list-style-type: none"> <li>• <i>vlan-id</i>: VID of multicast stream</li> <li>• <i>ip-addr</i>: Multicast address</li> <li>• <i>interface-id</i>: Port number</li> </ul>

Use the **no ipv6 mld snooping vlan *vlan-id* static *ip-addr* interface *interface-id*** command to delete the static configuration of the multicast listeners.

The following example shows how to set the MLD Snooping static listener port:

```
Ruijie# configure terminal
Ruijie(config)# ipv6 mld snooping vlan 1 static FF88::1234 interface GigabitEthernet 0/7
Ruijie(config)# end
Ruijie# show ipv6 mld snooping gda
Abbr: M - mrouter
      D - dynamic
      S - static
VLAN  Address                Listener ports
----  -
1      FF88::1234             GigabitEthernet 0/7(S)
```

## Configuring Port Fast-leave

Port Fast-leave means that when receiving from a port the MLD leave message sent from a host for leaving certain IPv6 multicast group, a switch will directly delete the port from the list of outgoing ports in the corresponding forwarding-table. If there is only one receiver connecting underneath the port on the switch, you may enable Port Fast-leave to save band width and resource.

To configure the port fast-leave of MLD Snooping, run the following commands:

Command	Function
---------	----------

Ruijie(config)# <b>ipv6 mld snooping fast-leave enable</b>	Enable the fast-leave function for the layer 2 multicast device, by default, this function is disabled.
--	---

Use the **no ipv6 mld snooping fast-leave enable** command to disable the port fast-leave function.

The following example shows how to enable the port fast-leave function:

```
Ruijie# configure terminal
Ruijie(config)# ipv6 mld snooping fast-leave enable
```

## Configuring the Response Suppression for MLD Snooping Membership

### Report Message

When receiving MLD membership report message from one IPv6 multicast listener, layer 2 equipment will forward the message to directly connected layer 3 equipment. Thus, when there exist in layer 2 equipment a number of listeners that belong to one IPv6 multicast group, directly connected layer 3 equipment will receive the same MLD membership report message sent by these listeners.

After enabling MLD membership report message suppression function, layer 2 equipment will only forward to layer 3 equipment the first MLD membership report message of one IPv6 multicast group it receives within one query interval, instead of keeping on forwarding to layer 3 equipment other MLD membership report message from the same multicast group. In this way, message quantity will be reduced in the network.

Run the following command to enable the response suppression for the layer 2 multicast device:

Command	Function
Ruijie(config)# <b>ipv6 mld snooping suppression enable</b>	Enable the response suppression for the layer 2 multicast device, by default, this function is disabled.

Use the **no ipv6 mld snooping suppression enable** command to disable the suppression function.

The following example shows how to enable the suppression function:

```
Ruijie# configure terminal
Ruijie(config)# ipv6 mld snooping suppression enable
```

## Configuring MLD Profiles

MLD Profiles are actually a number of group filters to provide support for following functions of "multicast address range for SVGL mode application", "multicast data area to be filtered by router port", "MLD Filtering range", etc.

To configure the MLD profile, run the following command:

Command	Function
Ruijie(config)# <b>ipv6 mld profile</b> <i>profile-number</i>	Enter the MLD Profile mode and assign for identification a number from 1 to 1024. By default, no profile is configured.
Ruijie (config-profile)# <b>permit</b>   <b>deny</b>	(Optional) Permit or deny the range of the multicast address, deny by default. It indicates that the range of multicast address and other multicast address will be permitted or denied. By default, all groups are denied.
Ruijie(config-profile)# <b>range</b> <i>low-address high_address</i>	Add the multicast address range, which can be both a single IPv6 group address(low IPv6 group address) and a group address zone(high IPv6 group address). Meanwhile, multiple ranges may be configured.
Ruijie(config)# <b>end</b>	Return to the privilege mode.

Use the **no ipv6 mld profile** *profile\_number* command to delete an MLD profile. Use the **no range** *low-address high\_address* command to delete the profile range.

The following example shows how to configure the profile:

```
Ruijie(config)# ipv6 mld profile 1
Ruijie(config-profile)# permit
Ruijie(config-profile)# range ff77::1 ff77::100
Ruijie(config-profile)# range ff88::123
Ruijie(config-profile)# end
Ruijie# show ipv6 mld profile 1
MLD Profile 1
permit
range ff77::1 ff77::100
range ff88::123
```

According to this configuration, the rule for this MLD profile is to permit the multicast addresses from ff77::1 to ff77::100 as well as ff88::123, while other multicast addresses are all denied.

## Configuring the Multicast Address Range for SVGL Mode Application

A profile shall be associated with the SVGL with the MLD Snooping working mode(SVGL mode or IVGL-SVGL mode) configured, to specify which ranges of group addresses may use SVGL mode, i.e., the listener ports of the multicast forwarding-table may transmit across VLAN. However, the listener ports of the multicast forwarding-tables within other multicast address ranges must belong to the same VLAN. By default, no profile associated is considered that no multicast group can apply the SVGL mode.

Command	Function
Ruijie(config)# <b>ipv6 mld profile 1</b>	Enter the MLD Profile mode and assign for identification a number from 1 to 1024. By default, no profile is configured.
Ruijie(config)# <b>ipv6 mld snooping ivgl-svgl</b>	Configure the IVGL-SVGL mode
Ruijie(config)# <b>ipv6 mld snooping svgl profile 1</b>	Associate the profile 1with the SVGL mode.
Ruijie(config)# <b>end</b>	Return to the privilege mode.

The following example shows how to configure the multicast address range for SVGL Mode application

```
Ruijie# configure terminal
Ruijie(config)# ipv6 mld snooping ivgl-svgl
Ruijie(config)# ipv6 mld snooping svgl profile 1
Ruijie(config)# end
Ruijie# show ipv6 mld snooping
MLD-snooping mode      :IVGL
SVGL VLAN-ID           : 1
SVGL profile number     : 1
Source check port       :Disable
Query Max Response Time : 10 (Seconds)
```

## Configuring MLD Filtering

Under certain circumstances, you may need to control certain port so that it can only transmit multicast data flow within a number of specific ranges and what max groups are allowed to join under the port. MLD Filtering can meet this demand.

You may apply certain MLD Profile under a port. When the port receives MLD Report message, layer 2 multicast equipment will find out whether the multicast address for this port to join is permitted by MLD Profile. If so, joining is permitted before later processing.

You may also configure the max group number that are permitted to join one port. When the max group number is exceeded, layer 2 multicast equipment will no longer receive and process

MLD report message.

To configure the MLD Filtering, run the following commands:

Command	Function
Ruijie(config)# <b>interface</b> <i>interface-id</i>	Enter the interface configuration mode.
Ruijie(config-if)# <b>ipv6 mld snooping filter</b> <i>profile-number</i>	(Optional) Apply the profile to this port. <i>profile-number</i> : the valid range is 1-1024. By default, no profile is associated with a port.
Ruijie(config-if)# <b>ipv6 mld snooping max-groups</b> <i>number</i>	(Optional) Permit a max number of groups to join this port dynamically. <i>number</i> : the valid range is 0-1024 By default, the value is 1024.

The following example shows how to configure the MLD Filtering:

```
Ruijie# configure terminal
Ruijie(config)# interface fastEthernet 0/1
Ruijie(config-if)# ipv6 mld snooping filter 1
Ruijie(config-if)# ipv6 mld snooping max-groups 1000
Ruijie (config-if)#end

Ruijie #show ipv6 mld snooping interface fastEthernet 0/1
```

Interface	Filter profile number	max-group
-----	-----	-----
FastEthernet 0/1	1	1000

## Viewing Current Mode of MLD Snooping

To view the current working mode and global configuration of MLD Snooping, run the following command:

Command	Function
Ruijie# <b>show ipv6 mld snooping</b>	View the current working mode and global configuration of MLD Snooping

The following example shows the MLD Snooping configurations:

```
Ruijie# show ipv6 mld snooping
MLD-snooping mode      : IVGL
SVGL VLAN-ID           : 1
SVGL profile number     : 0
Source check port       : Disabled
Query max Response time : 10(Seconds)
```



## Viewing and Clearing MLD Snooping Statistics

To view and clear the MLD Snooping statistics, run the following commands:

Command	Function
Ruijie# <b>show ipv6 mld snooping statistics [VLAN VLAN-ID]</b>	View the MLD Snooping statistics.
Ruijie# <b>clear ipv6 mld snooping statistics</b>	Clear the MLD Snooping statistics.

The following example shows the MLD Snooping statistics:

```
Ruijie# show ipv6 mld snooping statistics
GROUP      Interface      Last report      Last leave      Last
              time          time            reporter
-----
FF88::1 VL1:Gi4/2  0d:0h:0m:7s     ----          2003::1111
              Report pkts: 1          Leave pkts: 0
```

## Viewing Router port Information

To view and clear the MLD Snooping router port information, run the following command:

Command	Function
Ruijie# <b>show ipv6 mld snooping mrouter</b>	View the MLD Snooping router port information.

The following example shows the MLD Snooping router port information:

```
Ruijie# show ipv6 mld snooping mrouter
VLAN      Interface      State      MLD profile number
-----
1 GigabitEthernet 0/7  static      1
1 GigabitEthernet 0/12 dynamic      0
```

## Viewing the Forwarding-table

To view the forwarding rule of each port in a multicast group, i.e., to view GDA (Group Destination Address) table, run the following command:

Command	Function
Ruijie# <b>show ipv6 mld snooping gda-table</b>	View the forwarding rule of each port in a multicast group.

The following example shows each multicast group information in the GDA table and the

information of all listener ports of a multicast group:

```
Ruijie# show ipv6 mld snooping gda-table
Abbr: M - mrouter
      D - dynamic
      S - static
VLAN  Address                Listener ports
-----
1      FF88::1                GigabitEthernet 0/7(S)
```

## Clearing Dynamic Forwarding-table Information

To clear GDA(Group Destination Address) information from dynamic forwarding-table, run the following command:

Command	Function
Ruijie# <b>clear ipv6 mld snooping gda-table</b>	Clear the group information learned in a dynamic way from forwarding-table.

The following example clears the dynamic forwarding-table information:

```
Ruijie# clear IPv6 MLD Snooping GDA-table
```

## Viewing MLD Profile

To view MLD Snooping Profile information, run the following command:

Command	Function
Ruijie# <b>show ipv6 mld profile <i>profile-number</i></b>	View the MLD Snooping Profile information.

The following example shows the MLD Snooping Profile information:

```
Ruijie# show ipv6 mld profile 1
MLD Profile 1
  permit
  range FF77::1 FF77::100
  range FF88::123
```

## Multicast Forwarding Control Configuration

### Configuring Multicast Non-Stop Forwarding

Command	Function
Ruijie( config )# <b>msf nsf convergence-time</b> <i>time</i>	Configure the maximum time of waiting for multicast protocol convergence, in the range of 0 to 3600 seconds. The default value is 70 seconds.
Ruijie( config )# <b>msf nsf leak</b> <i>time</i>	Configure the leak time of multicast packets, in the range of 0 to 3600 seconds. The default value is 80 seconds.

In normal running state, SSP will synchronize the hardware forwarding table to the slave management board. After management switching, the original slave management board multicast control plane is loaded with configuration commands and the multicast protocols such as IGMP Snooping converge again. Multicast Non-Stop Forwarding function ensures non-stop forwarding of multicast data stream during multicast protocol re-convergence.

After the configured protocol convergence time is exceeded, all multicast forwarding tables which are not updated during protocol convergence time will be deleted.

After the slave management board becomes the master management board, re-converging multicast protocols requires the triggering of multicast data stream. After management board switching, SSP still needs to send the multicast data stream to the CPU with rate limit even though the hardware forwarding table exists. The time of waiting for multicast protocol convergence can be controlled by configuring the leak time.

### Monitoring and Maintenance

Command	Function
Ruijie# <b>debug msf api</b>	Displays process of calling the API interface provided by IPv4 multiple-layer multicast forwarding.
Ruijie# <b>debug msf6 api</b>	Displays process of calling the API interface provided by IPv6 multiple-layer multicast forwarding.
Ruijie# <b>debug msf event</b>	Displays process of multiple-layer multicast forwarding event.

Ruijie# <b>debug msf6 event</b>	Displays process of forwarding events on Layer 3 of IPv6 multicast.
Ruijie# <b>debug msf forwarding</b>	Displays the IPv4 multiple-layer multicast packets forwarding process.
Ruijie# <b>debug msf6 forwarding</b>	Displays the IPv6 multiple-layer multicast packets forwarding process.
Ruijie# <b>debug msf mfc</b>	Displays the IPv4 multiple-layer multicast forwarding table operation.
Ruijie# <b>debug msf6 mfc</b>	Displays the IPv6 multiple-layer multicast forwarding table operation.
Ruijie# <b>debug msf ssp</b>	Displays process of IPv4 multiple-layer multicast forwarding bottom hardware.
Ruijie# <b>debug msf6 ssp</b>	Displays process of IPv6 multiple-layer multicast forwarding bottom hardware.
Ruijie# <b>show msf msc</b>	Displays the IPv4 multiple-layer multicast forwarding information.
Ruijie# <b>show msf6 msc</b>	Displays the IPv6 multiple-layer multicast forwarding information.
Ruijie# <b>show msf nsf</b>	Displays the IPv4 multicast non-stop forwarding information.

1. AAA Configuration
2. RADIUS Configuration
3. TACACS+ Configuration
4. 802.1X Configuration
5. SSH Configuration
6. Port-based Flow Control Configuration
7. CPU Protection Configuration
8. DoS Protection Configuration
9. DHCP Snooping Configuration
10. DAI Configuration
11. IP Source Guard Configuration
12. ND Snooping Configuration
13. DHCPv6 Snooping Configuration
14. Gateway Anti-arp-spoofing Configuration
15. NFPP Configuration

## AAA Configuration

The access control is used to control which people can access the network server and which services can be accessed by the users on the network. The authentication, authorization and accounting (AAA) is a key security mechanism for access control.

### Basic AAA Principles

Authentication, Authorization and Accounting (shortened as AAA) provide a consistence framework for configuring the authentication, authorization and accounting functions, which are supported by Ruijie products.

The AAA provides the following services in a modular manner:

- **Authentication:** It verifies whether a user can access, where the Radius protocol or Local can be used. The authentication is the method to identify a user before his/her access to the network and network services. The AAA is configured by the definition of a naming list for authentication method and application of it on every interface. The method list defines the authentication type and execution order. Before a defined authentication is executed, the method list must be applied on a specific interface. The default method list is exceptional. If no other method list is defined, the default method list will automatically apply on all interfaces. The defined method list overwrites the default method list. All authentication methods other than the local, line password and allowing authentication must be defined with AAA.
- **Authorization:** This means authorizing the user with services. The AAA authorization is implemented through the definition of series attributes that describe the operations on the user by the authorization. These attributes can be stored on the network device or the RADIUS security server remotely. All authorization methods must be defined with AAA. When the AAA authorization is enabled, it is automatically applied on all interfaces of the network device.
- **Accounting:** This means recording the user's usage of network resources. When the AAA accounting is enabled, the network access server starts to send the user's network resource usages to the Radius security server through statistics records. Every accounting record is composed of attribute pairs and stored in the security server. These records can be read for analysis by special software to implement the accounting, statistics and tracing for the user's network resource usage. All accounting methods must be defined with AAA. When the AAA accounting is enabled, it is automatically applied on all interfaces of the network device.

**Note**

The AAA of some products only provides the authentication function. For all problems with product specifications, contact the market or technical support personnel.

Although the AAA is the primary access control method, our product also provides simple control accesses out of the range of AAA, such as the local username authentication, line password authentication and more. The difference lies in the degree of their network protection, and the AAA provides the security protection of a higher level.

The AAA has the following advantages:

- Powerful flexibility and controllability

- Expandability
- Standardized authentication
- Multiple backup systems

## Basic AAA Principles

The AAA can configure dynamically authentication, authorization and accounting for a single user (line) or server. It defines the authentication, authorization and accounting by means of creating method lists and then applies them on specific services or interfaces.

## Method List

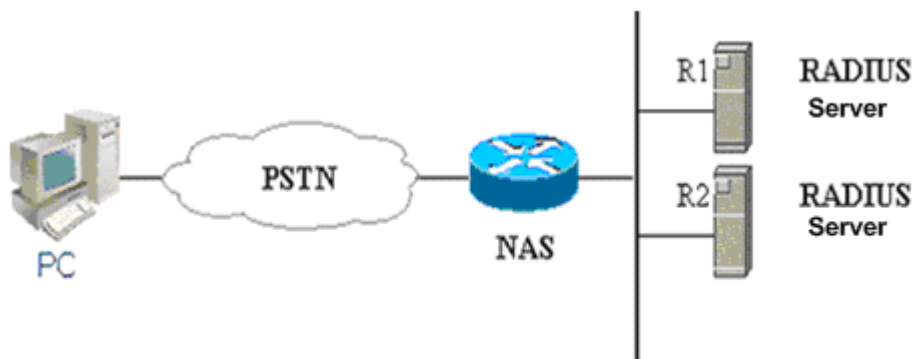
Since the authentication for users can be implemented in a variety of ways, you need to use the method list to define the sequence of using different method to perform authentication for the users. The method list can define one or more security protocols for authentication, so that there are backup systems available for the authentication in case of the failure of the first method. Our product works with the first method in the method list for user authentication, and then selects the next method in the method list in case of no reply from that method. This process goes on till an authentication method listed successfully allows communication or all methods listed are used up. If all methods listed are used up but the communication is not allowed, it declares failure of authentication.



### Caution

Only when there is no reply from a method, our product will attempt the next method. During the authentication, if the user access is refused by a method, the authentication process ends and no other methods will be attempted.

### A typical AAA network configuration



The figure above illustrates a typical AAA network configuration, including two security servers: R1 and R2 are both RADIUS servers, and one NAS (Network Access Server) acting as the RADIUS server. Supposed the system administrator has defined a method list, R1 is used first to capture the identity information, then R2, and finally the local username database on the NAS. If a remote PC user attempts to access the network via dialup, the NAS first queries the authentication information from R1. If the user passes the authentication on R1, R1 sends a SUCCESS reply to the NAS, and thus the user's access to the network is allowed. If R1 returns FAIL reply, the user's access is refused and the disconnected. If R1 has no reply, the NAS regards it as ERROR and queries authentication information from R2. This process continues for the remaining methods till the user passes the authentication, is refused or the session is terminated. If ERROR is returned for all methods, the authentication fails and the user is disconnected.

**Caution**

The REJECT response is not the same as the TIMEOUT response. REJECT means the user fails to comply with the standard in the available authentication database and does not pass the authentication, thus the access request will be refused. TIMEOUT means there is no reply from the security server to the authentication. When an ERROR is detected, the AAA selects the next authentication method in the method list to continue the authentication process.

**Note**

In this chapter, take RADIUS for example of the configuration of the related authentication, authorization and accounting of the AAA security server. For the TACACS+, refer to *TACACS+ Configuration*.

## Basic AAA Configuration Steps

First you shall decide to choose which security solution, evaluate the potential security risks in the specific network and select the proper measures to prevent unauthorized accesses. For the security risk evaluation and the possible security solutions, see Chapter 2, Security Overview. We recommend the use of AAA as much as possible to guarantee the network security.

### Overview of AAA Configuration Steps

The AAA configuration may become simple when the basic operation process of AAA is understood. On the network devices, the AAA is configured through the following steps:

1. Enable AAA by using the global configuration command **aaa new-model**.
2. Configure the security protocol parameters if you decide to use the security server, such as RADIUS.
3. Define the authentication method list by using the **aaa authentication** command.
4. Apply the method list on specific interface or line, if necessary.

**Caution**

When the specific method list is applied, if no named method list is clearly specified, the default authentication method list will apply.  
As a result, if you do not want to use the default authentication method list, you shall specify a specific method list.

For complete descriptions of the commands mentioned in this chapter, see the related chapters in the *Security Configuration Command Reference*.

### Enabling AAA

It is required to enable AAA first to be able to use the AAA security features.

To enable AAA, execute the following command in the global configuration mode:

Command	Function
Ruijie(config)# <b>aaa new-model</b>	Enable AAA

### Disabling AAA

To disable AAA, execute the following command in the global configuration mode:



Command	Function
Ruijie(config)# <b>no aaa new-model</b>	Disable AAA

## Sequential Configuration Steps

After the AAA is enabled, it is time to configure the other parts related with the selected security solutions. Following table lists the possible configuration tasks and their description chapters.

Methods of AAA access control security solution

Configuration Task	Step	Chapter
Configuring Local Login Authentication	3	Configuring Authentication
Defining AAA Authentication Method List	3	Configuring Authentication
Applying Method List on Specific Interface or Line	4	Configuring Authentication
Configuring Radius Security Protocol Parameters	2	Configuring Radius
Enabling Radius Authorization	5	Configuring Authorization

If you are using AAA for authentication, see *Configuring Authentication*.

## Configuring Authentication

The authentication allows the user's identity verification before the user of network resources. In most cases, the authentication is implemented with the AAA security features. We recommend the use of AAA as much as possible.

### Defining AAA Authentication Method List

To configure the AAA authentication, the first step is to define a named list of the authentication method, and then the applications use the defined list for authentication. The method list defines the authentication type and execution order. The defined authentication methods must be applied on specific interfaces before they can be executed. The default method list is exceptional. When not configured, all applications will use the default method list.

The method list is just a list to define the authentication method to be queried in turn to verify the user identity. The method list can define one or more security protocols for authentication, so that there are backup systems available for the authentication in case of the failure of the first method. Our product works with the first method in the method list for user authentication, and then selects the next method in the method list in case of no reply from that method. This process goes on till an authentication method listed successfully allows communication or all methods listed are used up. If all methods listed are used up but the communication is not allowed, it declares failure of authentication.



#### Caution

Only when there is no reply from a method, our product will attempt the next method. During the authentication, if the user access is refused by a method, the authentication process ends and no other methods will be attempted.

## Example of Method List

In a typical AAA network configuration, there are two servers: R1 and R2 are both RADIUS servers. Suppose the network administrator has chosen a security solution, and the NAS authentication uses an authentication method to authenticate the Telnet connection: First, R1 is used for the user authentication. In case of no reply, R2 will be used. In case there is no reply from both R1 and R2, the local database of the access server will perform the authentication. To configure the above authentication list, run the following commands:

Command	Function
<b>configure terminal</b>	Enter the global configuration mode.
<b>aaa authentication login default group radius local</b>	Configure a default authentication method list, where "default" is the name of the method list. The protocols included in this method list are listed behind the name in the order by which they will be queried. The default method list is applied on all applications.

If the system administrator hopes to apply this method list on a specific Login connection, he/she must create a named method list and then apply it on the specific connection. The example below shows how to apply the authentication method list on line 2 only.

Command	Function
<b>configure terminal</b>	Enter the global configuration mode.
<b>aaa new-model</b>	Turn on the AAA switch.
<b>aaa authentication login test group radius local</b>	Define a method list named "test" in the global configuration mode.
<b>line vty 2</b>	Enter VTY line 2 configuration mode.
<b>login authentication test</b>	In the line configuration mode, apply the method list named "test" on the line.

If a remote PC user attempts to Telnet the network access server(NAS), the NAS first queries the authentication information from R1. If the user passes the authentication on R1, R1 sends a ACCEPT reply to the NAS, and thus the user's access to the network is allowed. If R1 returns the REJECT reply, the user's access is refused and then disconnected. If R1 does not respond, NAS considers TIMEOUT and queries the authentication information to R2. This process continues for the remaining methods till the user passes the authentication, is refused or the session is terminated. If all servers (R1 and R2) returns TIMEOUT, the authentication will be performed by the NAS local database.



### Caution

The REJECT response is not the same as the TIMEOUT response. REJECT means the user fails to comply with the standard in the available authentication database and does not pass the authentication, thus the access request will be refused. TIMEOUT means there is no reply from the security server to the authentication. When an TIMEOUT is detected, the AAA selects the next authentication method in the method list to continue the authentication process.

## Authentication Type

Ruijie products support the following authentication types:

- Login Authentication -- the authentication of the user terminal logging in the NAS CLI.
- Enable Authentication -- the authentication of improving the CLI authority after the user terminal logs in the NAS CLI.
- PPP Authentication -- the authentication of PPP dial user.
- DOT1X(IEEE802.1x) Authentication -- the authentication of the IEEE802.1x access user.

## General Steps in Configuring AAA Authentication

The following tasks are common for the configuration of AAA authentication.

- Enable AAA by using the global configuration command **aaa new-model**.
- Configure the security protocol parameters if you decide to use the security server, such as RADIUS. See Configuring Radius for details.
- Define the authentication method list by using the **aaa authentication** command.
- Applying method list on a specific interface or line, if possible.



### Caution

TACACS+ is not supported by the DOT1X authentication.

## Configuring the AAA Login Authentication

This section deals with how to configure the AAA Login authentication methods supported by our product:



### Caution

Only after the AAA is enabled through the command **aaa new-model** in the global configuration mode, the AAA security features are available for your configuration. For the details, see *AAA Overview*.

In many cases, the user needs to Telnet the network access server (NAS). Once such a connection is set up, it is possible to configure NAS remotely. To prevent unauthorized accesses to the network, it is required to perform authentication on the user identity.

The AAA security services make it easy for the network devices to perform line-based authentication. No matter which line authentication method you decide to use, you just need to execute the **aaa authentication login** command to define one or more authentication method list and apply it on the specific line that need the line authentication.

To configure the AAA PPP authentication, execute the following command in the global configuration mode:

Command	Function
<b>configure terminal</b>	Enter the global configuration mode.
<b>aaa new-model</b>	Enable AAA.
<b>aaa authentication login {default  list-name} method1 [method2...]</b>	Define an accounting method list, or repeat this command to define more.
<b>line vty line-num</b>	Enter the line that needs to apply the AAA authentication.
<b>login authentication {default list-name}</b>	Apply the method list on the line.

The keyword "list-name" is used to name the created authentication method list, which can be any string. The keyword "method" means the actual algorithm for authentication. Only when the current method returns ERROR (no reply), the next authentication method will be attempted. If the current method returns FAIL, no authentication method will be used any more. To make the authentication return successfully, even if no specified methods reply, it is possible to specific "none" as the last authentication method.

In the example below, it is possible to pass the identity authentication even if the Radius server returns TIMEOUT. **aaa authentication login default group radius none**



### Caution

Since the keyword "**none**" enables any dialup user can pass the authentication even if the security server has no reply, it is only used as the backup authentication method. We suggest not using the "**none**" identity authentication in general cases. In special case when all possible dialup users are trustful, and no delay due to system fault is allowed for the user's work, it is possible to use "**none**" as the last identity authentication method in case the security server has no reply. And we recommend adding the local authentication method before the "**none**" authentication method.

Keyword	Description
<b>local</b>	Use the local username database for authentication
<b>none</b>	Do not perform authentication
<b>group radius</b>	Use Radius for authentication

The table above lists the AAA login authentication methods supported by our product.

## Using the local database for Login authentication

To configure the login authentication with local database, it is required to configure the local database first. Our product supports authentication based on the local database. To establish the username authentication, run the following commands in the global configuration mode:

Command	Function
<b>configure terminal</b>	Enter the global configuration mode.
<b>username</b> <i>name</i> [ <b>password</b> <i>password</i> ] or <b>username</b> <i>name</i> [ <b>access-class</b> <i>number</i> ]	Establish the username authentication using the password, or the access list.
<b>username</b> <i>name</i> [ <b>privilege</b> <i>level</i> ]	(Optional) Set the privilege level for the user.
<b>username</b> <i>name</i> [ <b>autocommand</b> <i>command</i> ]	(Optional) Set the command auto-executed after the user login.
<b>end</b>	Return to the privileged EXEC mode.
<b>show running-config</b>	Confirm the configuration.

To define the local login authentication method list and apply it, run the following commands:

Command	Function
<b>configure terminal</b>	Enter the global configuration mode.
<b>aaa new-model</b>	Turn on the AAA switch.

Command	Function
<b>aaa authentication login</b> {default   <i>list-name</i> } <b>local</b>	Define the local method list.
<b>end</b>	Return to the privileged EXEC mode.
<b>show aaa method-list</b>	Confirm the configured method list.
<b>configure terminal</b>	Enter the global configuration mode.
<b>line vty</b> <i>line-num</i>	Enter the line configuration mode
<b>login authentication</b> {default   <i>list-name</i> }	Apply the method list.
<b>end</b>	Return to the privileged EXEC mode.
<b>show running-config</b>	Confirm the configuration.

## Using Radius for Login authentication

To configure the use of RADIUS authentication server for login authentication, it is required to first configure the RADIUS server. Our product supports the authentication based on the RADIUS server. To configure the RADIUS server, run the following commands in the global configuration mode:

Command	Function
<b>configure terminal</b>	Enter the global configuration mode.
<b>aaa new-model</b>	Turn on the AAA switch.
<b>radius-server host</b> <i>ip-address</i> [ <b>auth-port</b> <i>port</i> ] [ <b>acct-port</b> <i>port</i> ]	Configure the RADIUS server
<b>end</b>	Return to the privileged EXEC mode.
<b>show radius server</b>	Show the RADIUS server.

After the RADIUS server is configured, make sure of successful communication with the RADIUS server before configuring the RADIUS for authentication. For details of the RADIUS server configurations, see *Configuring RADIUS*.

Now it is possible to configure the RADIUS server based method list. Run the following commands:

Command	Function
<b>configure terminal</b>	Enter the global configuration mode.
<b>aaa new-model</b>	Turn on the AAA switch.
<b>aaa authentication login</b> {default   <i>list-name</i> } <b>group radius</b>	Define the local method list.
<b>end</b>	Return to the privileged EXEC mode.
<b>show aaa method-list</b>	Confirm the configured method list.
<b>configure terminal</b>	Enter the global configuration mode.
<b>line vty</b> <i>line-num</i>	Enter the line configuration mode
<b>login authentication</b> {default   <i>list-name</i> }	Apply the method list.
<b>end</b>	Return to the privileged EXEC mode.
<b>show running-config</b>	Confirm the configuration.

## Configuring the AAA Enable Authentication

This section deals with how to configure the AAA Enable authentication methods supported by our product:

In many cases, the user needs to Telnet the network access server (NAS). After passing the authentication, the user enters the Command Line Interface (CLI) and is assigned an initial command execution privilege (0-15 level). You can execute different commands in different levels and use the **show privilege** command to display the current level. For the details, see *using the CLI*.

After logging in the CLI, you can use the enable command to improve the privilege level if you fail to execute some commands due to low initial privilege level. To prevent the unauthorized access to the network, the identity authentication, named Enable authentication, is necessary when improving the privilege level.

To configure the AAA Enable authentication, execute the following command in the global configuration mode:

Command	Function
<b>configure terminal</b>	Enter the global configuration mode.
<b>aaa new-model</b>	Enable AAA.
<b>aaa authentication enable default</b> <i>method1 [method2...]</i>	Define an enable authentication method list, for example RADIUS.
<b>line vty</b> <i>line-num</i>	Enter the line that needs to apply the AAA authentication.
<b>login</b> <b>authentication</b> <b>{default list-name}</b>	Apply the method list on the line.

It can only define one enable authentication method list globally, so it is no need to define the name of the method list. The keyword "method" means the actual algorithm for authentication. Only when the current method returns ERROR(no reply), the next authentication method will be attempted. If the current method returns FAIL, no authentication method will be used any more. To make the authentication return successfully, even if no specified methods reply, it is possible to specify **none** as the last authentication method.

Once configured, the enable authentication method takes effect. When executing **enable** command in the privileged EXEC mode, it prompts to authenticate if you want to switchover a higher privilege level. It is no need to authenticate if the privilege level to be set is lower than or equal to the current one.



### Caution

The current username will be recorded if the Login authentication (except for **none** method) is done when entering the CLI. At this time, if the Enable authentication processes, it will not prompt to input the username and you can use the same username of Login authentication. Note that the password input must be consistent.

The username information will not be recorded if there is no Login authentication when entering the CLI, or the **none** method is used. At this time, if the Enable authentication processes, you shall input the username again. This username will not be recorded, so you shall input it every time when the Enable authentication processes.

Some authentication methods can bind the security level. Then in the process of authentication, except for the returned response according to the security protocol, it is necessary to verify the binded security level. If the service protocol can bind the security level, the level shall be verified while authenticating. If the binded level is more than or equal to the level to be configured, the enable authentication and level switchover succeed. But if the binded level is less than the level to be configured, the enable authentication fails, prompting the error message and keeping the current level. If the service protocol fails to bind the security level, you can configure the level without verification of the binded level.



### Caution

Now only RADIUS and Local authentication support to bind the security level. To this end, only the security levels of these two methods are checked.

## Using the local username database for Enable authentication

When processing the enable authentication with local database, you can configure the user privilege level while configuring the local user. By default, the privilege level is 1. To configure the enable authentication with local database, it is required to configure the local database first and configure the privilege level. To establish the username authentication, run the following commands in the global configuration mode:

Command	Function
<b>configure terminal</b>	Enter the global configuration mode.
<b>username</b> <i>name</i> [ <b>password</b> <i>password</i> ]	Establish the local username and set the password.
<b>username</b> <i>name</i> [ <b>privilege level</b> ]	Set the user privilege level. (Optional)
<b>end</b>	Return to the privileged EXEC mode.
<b>show running-config</b>	Confirm the configuration.

To define the local Enable authentication method list, run the following commands:

Command	Function
<b>configure terminal</b>	Enter the global configuration mode.
<b>aaa new-model</b>	Turn on the AAA switch.
<b>aaa authentication enable default local</b>	Define the local method list.
<b>end</b>	Return to the privileged EXEC mode.
<b>show aaa method-list</b>	Confirm the configured method list.
<b>configure terminal</b>	Enter the global configuration mode.
<b>show running-config</b>	Confirm the configuration.

## Using Radius for Enable authentication

The standard RADIUS server can pass the privilege level binded with the Service-Type attribute (the standard attribute number is 6), can specify the privilege with 1 or 15 level. The extended RADIUS server (for example, SAM) can configure the privilege level of the administrator (the private attribute number is 42), can specify 0-15 privilege level. For the details of the RADIUS server, see *Specifying the RADIUS Private Attribute Type* in *Configuring RADIUS*.

To configure the use of RADIUS authentication server for enable authentication, it is required to first configure the RADIUS server, then the RADIUS server-based enable authentication method list. Run the following commands in the global configuration mode:

Command	Function
<b>configure terminal</b>	Enter the global configuration mode.
<b>aaa new-model</b>	Turn on the AAA switch.
<b>aaa authentication enable default group radius</b>	Define RADIUS authentication method.
<b>end</b>	Return to the privileged EXEC mode.
<b>show aaa method-list</b>	Confirm the configured method list.
<b>show running-config</b>	Confirm the configuration.

## Configuring the AAA Authentication for PPP User

PPP is a link-layer protocol of carrying the network-layer datagram in the point-to-point link. In many circumstances, the user accesses to the NAS(Network Access Server) by asynchronous or ISDN dial. Once the connection has been set up, the PPP negotiation will be enabled. To prevent the unauthorized access to the network, the identity authentication is required for the dailed user in the process of PPP negotiation.

This section deals with how to configure the AAA Enable authentication methods supported by Ruijie product. To configure the AAA Enable authentication, execute the following command in the global configuration mode:

Command	Function
<b>configure terminal</b>	Enter the global configuration mode.
<b>aaa new-model</b>	Enable AAA.
<b>aaa authentication ppp {default   list-name} method1 [method2...]</b>	Define a PPP authentication method list. RADIUS, TACACS+ remote authentication and using the local database are the supported authentication methods.
<b>interface interface-type interface-number</b>	Enter the asynchronous or ISDN interface that needs to apply the AAA authentication.
<b>ppp authentication {chap   pap} {default   list-name}</b>	Apply the method list on the asynchronous or ISDN interface.

For the detailed configuration method for the PPP, see the related chapter in *Configuring PPP, MP*.

## Configuring the AAA Authentication for 802.1x User

IEEE802.1x is a standard of Port-Based Network Access Control, providing the point-to-point secure access for the LAN, and a means of the authentication of the user connecting to the LAN device.

This section deals with how to configure the 802.1x authentication methods supported by Ruijie product. To configure the AAA Enable authentication, execute the following command in the global configuration mode:



Command	Function
<b>configure terminal</b>	Enter the global configuration mode.
<b>aaa new-model</b>	Enable AAA.
<b>aaa authentication dot1x {default   list-name} method1 [method2...]</b>	Define an IEEE802.1x authentication method list. RADIUS remote authentication and using the local database are the supported authentication methods.
<b>dot1x authentication list-name</b>	Apply the method list to 802.1x.

For the detailed configuration method for the IEEE802.1x, see the related chapter in *Configuring 802.1x*.

## Example of Authentication Configuration

The example below illustrates show to configure the network device to use “Radius + local” for authentication.

```
Ruijie(config)# aaa new-model
Ruijie(config)# username Ruijie password starnet
Ruijie(config)# radius-server host 192.168.217.64
Ruijie(config)# aaa authentication login test group radius local
Ruijie(config)# line vty 0
Ruijie(config-line)# login authentication test
Ruijie(config-line)# end
Ruijie# show running-config
!
aaa new-model
!
!
aaa authentication login test group radius local
username Ruijie password 0 starnet
!
radius-server host 192.168.217.64
!
line con 0
line vty 0
login authentication test
line vty 1 4
!
!
```

In the example above, the access server uses the Radius server (IP 192.168.217.64) to perform authentication for the login users. If the Radius server has no reply, the local database will be used for the identity authentication.

## Example of Terminal Service Application Configuration

In the environment of the terminal service application, the terminal first connects to the asynchronous console, then offers the service accessing the network network server. However, if AAA is enabled, the Login authentication is necessary in all lines. To access the server, the terminal must pass the Login authentication and it influences the terminal service. You can separate two lines by configuration that makes the line using the terminal service directly connecting the server without the Login authentication, and ensures the device security by the Login authentication of the line connecting the

device. That is to say, you can configure a login authentication list specific for the terminal service but the authentication method as **none**. Then apply the configured list to the line with terminal service enabled, while other lines connecting the local device is unchanged. Thereof the terminal can skip the local login authentication.

The example below illustrates the configuration steps:

```
Ruijie(config)# aaa new-model
Ruijie(config)# username Ruijie password starnet
Ruijie(config)# radius-server host 192.168.217.64
Ruijie(config)# radius-server key test
Ruijie(config)# aaa authentication login test group radius local
Ruijie(config)# aaa authentication login terms none
Ruijie(config)# line tty 1 4
Ruijie(config-line)# login authentication terms
Ruijie(config-line)# exit
Ruijie(config)# line tty 5 16
Ruijie(config-line)# login authentication test
Ruijie(config-line)# exit
Ruijie(config)# line vty 0 4
Ruijie(config-line)# login authentication test
Ruijie(config-line)# end
Ruijie(config)# show running-config
!
aaa new-model
!
!
aaa authentication login test group radius local
aaa authentication login terms none
username Ruijie password 0 starnet
!
radius-server host 192.168.217.64
radius-server key 7 093b100133
!
line con 0
line aux 0
line tty 1 4
login authentication terms
line tty 5 16
login authentication test
line vty 0 4
login authentication test
!
!
```

In the example above, the access server uses the Radius server (IP 192.168.217.64) to perform authentication for the login users. If the Radius server has no reply, the local database will be used for the identity authentication. Login authentication is unnecessary for tty 1-4 is the used line of the terminal service, while using other tty and vty lines needs the login authentication.

## Configuring Authorization

The AAA authorization enables the administrator to control the user's use of the services or the rights. After the AAA authorization service is enabled, the network device configures the user sessions by using

the user configuration file stored locally or in the server. After the authorization is completed, the user can only use the services allowed in the profile or has the allowed rights.

## Authorization Types

Our product supports the following AAA authorization methods:

- Exec authorization method – the user terminal logs in the NAS CLI and is granted the privilege level (0-15 level).
- Command authorization method – after the user terminal logs in the NAS CLI, the specific commands are authorized.
- Network authorization method – grant the available service to the user session in the network.



### Note

Only TACACS+ supports the command authorization method. For the detailed information, please refer to *TACACS+ Configuration*.

## Preparations for Authorization

The following tasks must be completed before the AAA authorization is configured:

- Enable the AAA server. For the details, see *AAA Overview*.
- (Optional) Configure the AAA authentication. The authorization is done after the user passes the authentication. But sole authorization can also be done without authentication. For details of the AAA authentication, see *Configuring Authentication*.
- (Optional) Configure security protocol parameters. If the security protocol is required for authorization, it is required to configure the security protocol parameters. The network authorization only supports RADIUS; the Exec authorization supports RADIUS and TACACS+. For details of the RADIUS, see *Configuring RADIUS*. For details of the TACACS+, see *Configuring TACACS+*.
- (Optional) If the local authorization is required, it is required to use the **username** command to define the user rights.

## Configuring Authorization List

To enable AAA authorization, execute the following command in the global configuration mode:

Command	Function
<b>configure terminal</b>	Enter the global configuration mode.
<b>aaa new-model</b>	Turn on the AAA switch.
<b>aaa authorization exec network{default   list-name} method1 [method2 ...]</b>	Define the AAA Exec authorization method.
<b>aaa authorization network network{default   list-name} method1 [method2 ...]</b>	Define the AAA Command authorization method.

## Configuring AAA Exec Authorization

The Exec authorization grants the privilege level of command execution for the user terminal logs in the network access server (NAS). You can use the **show privilege** command to display the specific level after the user logs in the NAS CLI successfully (by telnet, for example).

No matter which Exec authorization method you decide to use, you just need to execute the **aaa authorization exec** command to define one or more authorization method list and apply it to the specific line that need the Exec authorization.

To configure the AAA Exec authorization, run the following commands in the global configuration mode:

Command	Function
<b>configure terminal</b>	Enter the global configuration mode.
<b>aaa new-model</b>	Turn on the AAA switch.
<b>aaa authorization exec network</b> {default   <i>list-name</i> } <i>method1</i> [ <i>method2</i> ...]	Define the AAA Exec authorization method. If you need to define multiple methods, execute this command repeatedly.
<b>line vty</b> <i>line-num</i>	Enter the line to which the AAA Exec authorization method is applied.
<b>authorization exec</b> {default   <i>list-name</i> }	Apply the method to the line.

The keyword "list-name" is used to name the created authorization method list, which can be any string. The keyword "method" means the actual algorithm for authorization. Only when the current method returns ERROR (no reply), the next authorization method will be attempted. If the current method returns FAIL, no authorization method will be used any more. To make the authorization return successfully, even if no specified methods reply, it is possible to specific "none" as the last authorization method. In the example below, it is possible to pass the Exec authorization even if the Radius server returns TIMEOUT:

**aaa authorization exec default group radius none**

Keyword	Description
<b>local</b>	Use the local username database for Exec authorization.
<b>none</b>	Do not perform Exec authorization.
<b>group radius</b>	Use Radius for Exec authorization.
<b>group tacacs+</b>	Use Tacacs+ for Exec authorization.

The table above lists the AAA Exec authorization methods supported by our product.



### Caution

The exec authorization is always used together with the login authentication, and they can be applied to the same line at the same time. But note that it is possible to have different results of the authentication and the authorization towards the same user because they can use different methods and servers. If the exec authorization fails, even though the login authentication has passed, the user can not access the CLI.

## Using the local username database for exec authorization

To configure the Exec authorization with local database, it is required to configure the local database first. You can configure the user privilege level while configuring the local user. By default, the privilege level is 1. Run the following commands in the global configuration mode:

Command	Function
<b>configure terminal</b>	Enter the global configuration mode.
<b>username</b> <i>name</i> [ <b>password</b> <i>password</i> ]	Establish the local username and set the password.
<b>username</b> <i>name</i> [ <b>privilege</b> <i>level</i> ]	Set the user privilege level. (Optional)
<b>end</b>	Return to the privileged EXEC mode.
<b>show running-config</b>	Confirm the configuration.

To define the local Exec authorization method list, run the following commands:

Command	Function
<b>configure terminal</b>	Enter the global configuration mode.
<b>aaa new-model</b>	Turn on the AAA switch.
<b>aaa authorization exec</b> { <b>default</b>   <i>list-name</i> } <b>local</b>	Define the local method list.
<b>end</b>	Return to the privileged EXEC mode.
<b>show aaa method-list</b>	Confirm the configured method list.
<b>configure terminal</b>	Enter the global configuration mode.
<b>line vty</b> <i>line-num</i>	Enter the line configuration mode.
<b>authorization exec</b> { <b>default</b>   <i>list-name</i> }	Apply the method list.
<b>end</b>	Return to the privileged EXEC mode.
<b>show running-config</b>	Confirm the configuration.

### Using Radius for exec authorization

To configure the use of RADIUS server for Exec authorization, it is required to first configure the RADIUS server. For the details of the RADIUS server configuration, see *Configuring RADIUS*.

After configuring the RADIUS server, the RADIUS server-based method list can be configured. Run the following commands in the global configuration mode:

Command	Function
<b>configure terminal</b>	Enter the global configuration mode.
<b>aaa new-model</b>	Turn on the AAA switch.
<b>aaa authentication enable</b> { <b>default</b>   <i>list-name</i> } <b>group radius</b>	Define RADIUS authentication method.
<b>end</b>	Return to the privileged EXEC mode.
<b>show aaa method-list</b>	Confirm the configured method list.
<b>configure terminal</b>	Enter the global configuration mode.
<b>line vty</b> <i>line-num</i>	Enter the line configuration mode.
<b>authorization exec</b> { <b>default</b>   <i>list-name</i> }	Apply the method list.
<b>end</b>	Return to the privileged EXEC mode.
<b>show running-config</b>	Confirm the configuration.

## Example of Configuring Exec Authorization

The example below illustrates how to configure exec authorization. The local login authentication and the “Radius+local” exec authorization are used when the user on the vty line 0-4 logs in. The access server uses the Radius server with IP address 192.168.217.64 and shared keyword *test*. The local username and password are *Ruijie*, and the privilege level is 6.

```
Ruijie# configure terminal
Ruijie(config)# aaa new-model
Ruijie(config)# radius-server host 192.168.217.64
Ruijie(config)# radius-server key test
Ruijie(config)# username Ruijie password Ruijie
Ruijie(config)# username Ruijie privilege 6
Ruijie(config)# aaa authentication login mlist1 local
Ruijie(config)# aaa authentication exec mlist2 group radius local
Ruijie(config)# line vty 0 4
Ruijie(config-line)# login authentication mlist1
Ruijie(config-line)# authorization exec mlist2
Ruijie(config-line)# end
Ruijie(config)# show running-config
!
aaa new-model
!
aaa authorization exec mlist2 group radius local
aaa authentication login mlist1 local
!
username Ruijie password Ruijie
username Ruijie privilege 6
!
Radius-server host 192.168.217.64
radius-server key 7 093b100133
!
line con 0
line vty 0 4
authorization exec mlist2
login authentication mlist1
!
end
```

## Configuring AAA Network Authorization

Our product support the network authorization over the network connection including PPP, SLIP. The network authorization makes the network connection obtain the service like traffic, bandwidth, timeout, ect. The network authorization only support the RADIUS. The authorization information assigned from the server are encapsulated in the RADIUS attribute. For different network connection application, it is possible that these authorization information are different.

**Caution**

Now the configuration does not support the 802.1X AAA authorization, while the 802.1X is implemented by using other commands. For the details of the 802.1X authorization, see *Configuring 802.1X*.

---

To configure the AAA network authorization, run the following commands in the global configuration mode:

Command	Function
<b>configure terminal</b>	Enter the global configuration mode.
<b>aaa new-model</b>	Turn on the AAA switch.
<b>aaa authorization network</b> {default   <i>list-name</i> } <i>method1</i> [ <i>method2</i> ...]	Define the AAA network authorization method. If you need to define multiple methods, execute this command repeatedly.

The keyword "list-name" is used to name the created authorization method list, which can be any string. The keyword "method" means the actual algorithm for authorization. Only when the current method returns ERROR (no reply), the next authorization method will be attempted. If the current method returns FAIL, no authorization method will be used any more. To make the authorization return successfully, even if no specified methods reply, it is possible to specify "none" as the last authorization method.

### Using Radius for network authorization

To configure the use of RADIUS server for network authorization, it is required to first configure the RADIUS server. For the details of the RADIUS server configuration, see *Configuring RADIUS*.

After configuring the RADIUS server, the RADIUS server-based method list can be configured. Run the following commands in the global configuration mode:

Command	Function
<b>configure terminal</b>	Enter the global configuration mode.
<b>aaa new-model</b>	Turn on the AAA switch.
<b>aaa authentication network</b> {default   <i>list-name</i> } <b>group radius</b>	Define RADIUS authentication method.

### Example of Configuring Network Authorization

The example below illustrates how to configure network authorization.

```
Ruijie# configure terminal
Ruijie(config)# aaa new-model
Ruijie(config)# radius-server host 192.168.217.64
Ruijie(config)# radius-server key test
Ruijie(config)# aaa authorization network test group radius local
Ruijie(config-line)# end
Ruijie(config)# show running-config
!
aaa new-model
!
aaa authorization network test group radius none
!
radius-server host 192.168.217.64
radius-server key 7 093b100133
!
```

## Configuring Accounting

The AAA accounting function enables you to trace the services and network resources used by the user. After the accounting function is enabled, the network access server or router sends the user's network

accesses to the Radius security server by means of attribute pair. You may use some analysis software to analyze these data to implement the billing, audition and tracing function for the user's activities.

## Accounting Types

Our product currently supports the following accounting types:

- Exec Accounting -- record the accounting information of entering to and exiting from the CLI of the user terminal logged in the NAS CLI.
- Command Accounting – record the specific command execution information after the user terminal logs in the NAS CLI.
- Network Accounting – records the related information on the user session in the network.



### Note

Only TACACS+ supports the command accounting function. For the detailed information, please refer to *TACACS+ Configuration*.

## Preparations for Accounting

The following tasks must be completed before the AAA accounting is configured:

- Enable the AAA server. For the details, see *AAA Overview*.
- Define the security protocol parameters. It is required to configure the security protocol parameters for accounting. The network accounting only supports RADIUS; the Exec accounting supports RADIUS and TACACS+; the Command accounting supports TACACS+ only. For details of the RADIUS, see *Configuring RADIUS*. For details of the TACACS+, see *Configuring TACACS+*.
- (Optional) Configure the AAA authentication. The accounting is done after the user passes the authentication(for example, Exec accounting). In some circumstances, the accounting can also be done without authentication. For details of the AAA authentication, see *Configuring Authentication*.

## Configuring AAA Exec Accounting

The exec accounting records the information of entering to and exiting from the CLI of the user terminal logged in the NAS. When the user terminal logs in and enters to the NAS CLI, it sends the accounting start information to the security server. When the user terminal exits from the CLI, it sends the accounting stop information to the server.



### Caution

Only after the user terminal logged in the NAS has passed the login authentication, the exec accounting starts. If no login authentication or **none** authentication method has been configured, no exec accounting processes. For the same user terminal, if it sends no accounting start information to the security server when logging in, no accounting stop information will be sent when logging out.

To configure the AAA Exec accounting, run the following commands in the global configuration mode:

Command	Function
<b>configure terminal</b>	Enter the global configuration mode.
<b>aaa new-model</b>	Turn on the AAA switch.



Command	Function
<b>aaa accounting exec network</b> {default   <i>list-name</i> } <b>start-stop</b> <i>method1</i> [ <i>method2</i> ]...	Define the AAA Exec accounting method list. If you need to define multiple method lists, execute this command repeatedly.
<b>line vty</b> <i>line-num</i>	Enter the line to which the AAA Exec accounting is applied.
<b>accounting exec</b> {default   <i>list-name</i> }	Apply the method list to the line.

The keyword "list-name" is used to name the created accounting method list, which can be any string. The keyword "method" means the actual algorithm for accounting. Only when the current method returns ERROR (no reply), the next accounting method will be attempted. If the current method returns FAIL, no accounting method will be used any more. To make the accounting return successfully, even if no specified methods reply, it is possible to specific "none" as the last accounting method.

**Note**

The keyword "start-stop" is used for the network access server to send the accounting information at the start and end of the network service to the security server.

### Using the Radius for exec accounting

To configure the use of RADIUS server for Exec accounting, it is required to first configure the RADIUS server. For the details of the RADIUS server configuration, see *Configuring RADIUS*.

After configuring the RADIUS server, the RADIUS server-based method list can be configured. Run the following commands in the global configuration mode:

Command	Function
<b>configure terminal</b>	Enter the global configuration mode.
<b>aaa new-model</b>	Turn on the AAA switch.
<b>aaa accounting exec</b> {default   <i>list-name</i> } <b>start-stop group radius</b>	Define RADIUS accounting method.
<b>end</b>	Return to the privileged EXEC mode.
<b>show aaa method-list</b>	Confirm the configured method list.
<b>configure terminal</b>	Enter the global configuration mode.
<b>line vty</b> <i>line-num</i>	Enter the line configuration mode.
<b>accounting exec</b> {default   <i>list-name</i> }	Apply the method list.
<b>end</b>	Return to the privileged EXEC mode.
<b>show running-config</b>	Confirm the configuration.

### Example of Configuring Exec Accounting

The example below illustrates how to configure exec accounting. The local login authentication and the Radius exec authorization are used when the user on the vty line 0-4 loggs in. The access server uses the Radius server with IP address 192.168.217.64 and shared keyword *test*. The local username and password are *Ruijie*

```
Ruijie# configure terminal
Ruijie(config)# aaa new-model
Ruijie(config)# radius-server host 192.168.217.64
```

```

Ruijie(config)# radius-server key test
Ruijie(config)# username Ruijie password Ruijie
Ruijie(config)# aaa authentication login auth local
Ruijie(config)# aaa accounting exec acct start-stop group radius
Ruijie(config)# line vty 0 4
Ruijie(config-line)# login authentication auth
Ruijie(config-line)# accounting exec acct
Ruijie(config-line)# end
Ruijie(config)# show running-config
!
aaa new-model
!
aaa accounting exec acct start-stop group radius
aaa authentication login auth local
!
username Ruijie password Ruijie
!
radius-server host 192.168.217.64
radius-server key 7 093b100133
!
line con 0
line vty 0 4
accounting exec acct
login authentication auth
!
end

```

## Configuring AAA Network Accounting

The network accounting provides the accounting information about user session, including the packet number, bytes, IP address and username. Now the network accounting only support RADIUS.



### Note

The format of Radius accounting information varies with the Radius security server. The contents of the account records may also vary with our product version.

To configure the AAA network accounting, run the following commands in the global configuration mode:

Command	Function
<b>configure terminal</b>	Enter the global configuration mode.
<b>aaa new-model</b>	Turn on the AAA switch.
<b>aaa accounting network{default   list-name} start-stop method1 [method2]...</b>	Define the AAA network accounting method list. If you need to define multiple method lists, execute this command repeatedly.

The keyword "list-name" is used to name the created accounting method list, which can be any string. The keyword "method" means the actual algorithm for accounting. Only when the current method returns ERROR (no reply), the next accounting method will be attempted. If the current method returns FAIL, no accounting method will be used any more. To make the accounting return successfully, even if no specified methods reply, it is possible to specific "none" as the last accounting method.

## Using Radius for network accounting

To configure the use of RADIUS server for network accounting, it is required to first configure the RADIUS server. For the details of the RADIUS server configuration, see *Configuring RADIUS*.

After configuring the RADIUS server, the RADIUS server-based method list can be configured. Run the following commands in the global configuration mode:

Command	Function
<b>configure terminal</b>	Enter the global configuration mode.
<b>aaa new-model</b>	Turn on the AAA switch.
<b>aaa accounting network {default   list-name} start-stop group radius</b>	Define RADIUS accounting method.

## Example of Configuring Network Accounting

The example below illustrates how to configure network authorization using RADIUS.

```
Ruijie# configure terminal
Ruijie(config)# aaa new-model
Ruijie(config)# radius-server host 192.168.217.64
Ruijie(config)# radius-server key test
Ruijie(config)# aaa accounting network acct start-stop group radius
Ruijie(config-line)# end
Ruijie(config)# show running-config
!
aaa new-model
!
aaa accounting network acct start-stop group radius
!
radius-server host 192.168.217.64
radius-server key 7 093b100133
!
```

## Monitoring AAA user

To view the information of the current login users, run the following commands in the privileged user mode:

Command	Function
<b>show aaa user { id   all }</b>	View the information of the current AAA user.

## Configuring Failed Authentication Lockout of Login User

To prevent login user from decoding password, use command to limit the attempt times. If you has attempted more than the limited times, you will not login during the lockout.

In the global configuration mode, use the following command to configure login parameters:

Command	Function
<b>configure terminal</b>	Enter the global configuration mode.
<b>aaa new-model</b>	Turn on the AAA switch.

Command	Function
<b>aaa local authentication attempts</b> <i>&lt;1-2147483647&gt;</i>	Configure attempt times of login user.
<b>aaa local authentication lockout-time</b> <i>&lt;1-2147483647&gt;</i>	Configure lockout-time(hour) when the user has attempted more than the limited times.
<b>show aaa user lockout</b>	Display current lockout user list.
<b>clear aaa local user lockout</b> {all   <b>user-name</b> <i>&lt;word&gt;</i> }	Clear lockout user list.
<b>end</b>	Exit to privileged EXEC mode.

**Note**

By default, login attempt times is 3 and the lockout time is restricted to be 15 hours.

## Configuring Domain-name-based AAA Service

The domain-name-based AAA service configurations include:

- Overview
- Domain-name-based AAA service configuration tasks
- Domain-name-based AAA service configuration note
- Domain-name-based AAA service configuration example

**Caution**

The domain-name-based AAA service is applied to the IEEE802.1x authentication service. For the detailed IEEE802.1x protocol configurations, please refer to the chapter of *802.1x Configuration*.

### Overview

In the multi-domain environment, one NAS(Network Access Server) can provide the AAA service for the users in different domains. Due to the different user attributes(such as the username, password, service type, privilege, ect) in each domain, it needs to tell them apart by setting the domain method and set the attribute collection for each domain, including the AAA service method list.

Ruijie product supports the following types of username:

**Note**

1. userid@domain-name
2. domain-name\userid
3. userid.domain-name
4. userid

For the type4 username, i.e., userid, without the domain-name, its domain-name is default.

The followings are the basic principles for the domain-name-based AAA service:

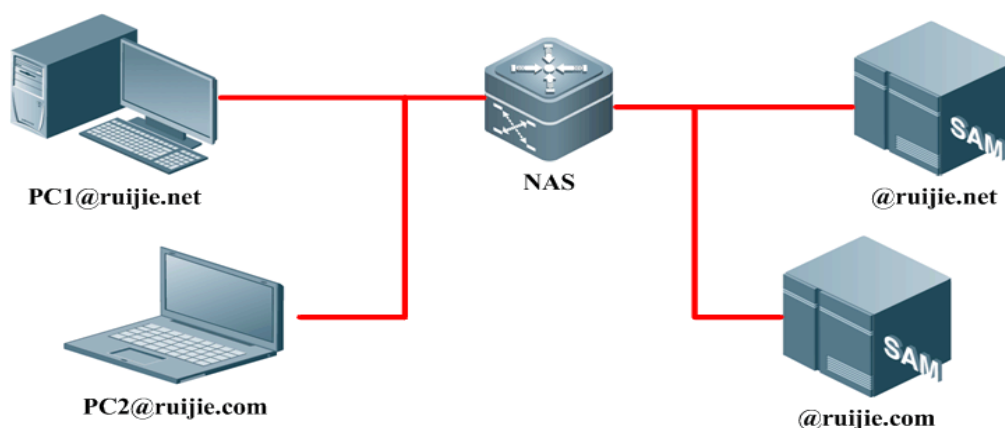
- Resolving the domain-name carried by the user

- Searching for the user domain according to the domain-name
- Searching for the AAA service method list-name according to the domain configurations
- Searching the corresponding method list according to the method list-name in the system
- Providing the AAA service using the method list

**Note**

One of the abovementioned steps fails, the AAA service cannot be used.

The following is the typical topology in the multi-domain environment:



**Figure-2 Typical topology for the multi-domain network**

## Domain-name-based AAA Service Configuration Tasks

**Note**

The system supports up to 32 domains.

### Enabling AAA

Command	Function
<b>configure terminal</b>	Enter the global configuration mode.
<b>aaa new-model</b>	Turn on the AAA switch.

For the detailed command descriptions, please refer to the chapter of *Enabling AAA*.

### Defining the AAA Service Method list

Command	Function
<b>configure terminal</b>	Enter the global configuration mode.
<b>aaa authentication dot1x {default   list-name} method1 [method2...]</b>	Define the IEEE802.1x authentication method list.
<b>aaa accounting network {default   list-name} start-stop method1 [method2...]</b>	Define the Network accounting method list.

Command	Function
<b>aaa authorization network</b> {default   list-name} method1 [method2...]	Define the Network authorization method list.

For the detailed command descriptions, please refer to the chapter of *Configuring authentication*, *Configuring accounting* and *Configuring authorization*..

### Enabling the Domain-name-based AAA Service Switch

Command	Function
<b>configure terminal</b>	Enter the global configuration mode.
<b>aaa domain enable</b>	Enable the domain-name-based AAA service switch.

### Creating the Domain

You shall follow the following rules when searching for the domain-name matched the username:

1. Support to use the single character, such as “.”, “\”, “@” to tell the username and the domain-name apart.
2. The single “@” character is followed by the character string “domain-name”. With multiple “@” characters in the username, use the character string following the last “@” character as the domain-name. For example, if the username is a@b@c@d, use the a@b@c as the username and use the d as the domain-name.
3. The single “\” character follows the character string “domain-name”. With multiple “\” characters in the username, use the character string followed by the first “\” character as the domain-name. For example, if the username is a\b\c\d, use the b\c\d as the username and use the a as the domain-name.
4. The single “.” character is followed by the character string “domain-name”. With multiple “.” characters in the username, according to the pre-settings, use the character string following the last “.” character as the domain-name. For example, if the username is a.b.c.d, use the a.b.c as the username and use the d as the domain-name.
5. If all characters of “.”, “\” and “@” exist in the username, when matching the domain-name, use the rules in sequence of the “@”, “\” and “.” characters.

Command	Function
<b>configure terminal</b>	Enter the global configuration mode.
<b>aaa domain</b> domain-name	Create the domain and enter the domain configuration mode.



#### Note

The domain-name-based AAA service supports the domain name in the length of up to 64 characters, which is not case-sensitive.

### Configuring the Domain Attribute Collection

Use the following commands to select the AAA service method list in the domain configuration mode:

Command	Function
<b>authentication dot1x</b> {default   <i>list-name</i> }	In the domain configuration mode, select the authentication method list.
<b>accounting network</b> {default   <i>list-name</i> }	In the domain configuration mode, select the accounting method list.
<b>authorization network</b> {default   <i>list-name</i> }	In the domain configuration mode, select the authorization method list.

Use this command to configure the domain state:

Command	Function
<b>state</b> {block   active}	In the domain configuration mode, set the domain state.

Use this command to check whether the username carries with the domain-name information:

Command	Function
<b>username-format</b> {without-domain   with-domain}	In the domain configuration mode, check whether the username carries with the domain-name information when the NAS is interacting with the server.

Use this command to set the maximum user number supported in the domain:

Command	Function
<b>access-limit</b> <i>num</i>	In the domain configuration mode, set the maximum user limit in the domain. By default, no user limit has been configured (only valid for the 802.1x user).



#### Note

1. To select the AAA service method list in the domain configuration mode, the AAA service method list is defined before entering the domain configuration mode. Or the configurations are inexistent when selecting the AAA method list-name.
2. With the domain-name-based AAA service enabled, if there is no domain information carried by the username, use the default domain; if there is no configurations for the user domain in the system, the user is determined to be illegal and provides no AAA service.
3. In the domain configuration mode, without the method list configured, use the default method list in the system.

## Showing the domain configuration

Use the following commands to show the domain-name-based AAA service information.

Command	Function
<b>show aaa domain</b> [ <i>domain-name</i> ]	Show the current domain-name-based AAA service information

## Domain-name-based AAA Service Configuration Notes

The followings are the domain-name-based AAA service configuration notes:

1. With the domain-name-based AAA service enabled, use the method list in the domain. Without the service enabled, use the method list selected according to the access protocol(such as 802.1x, ect) for the AAA service. For example, without the service enabled, use the **dot1x authentication** *authen-list-name*, **dot1x accounting** *acct-list-name* *authen-list-name* and **dot1x accounting** *acct-list-name* *acct-list-name* command to provide the AAA service for the authentication and accounting method list name.
2. With the domain-name-based AAA service enabled, by default, there is no default domain, and you shall manually set the default domain-name as "default". After the configuration, user that not carries with the domain information provides the AAA service using the default domain. Without the default domain configured, the user that not carries with the domain information fails to use the AAA service.
3. If the domain information is carried by the auth-user but the domain is not configured on the device, it fails to provide the AAA service for the user.
4. The AAA service method list selected by the domain must be consistent with the one defined by the AAA service. Or it fails to provide the AAA service for the users in the domain.
5. The domain name carried by the user shall be accurately matched with the one configured on the device. For example, the domain.com and the domain.com.cn have been configured on the device, and the request message carried by the user is aaa@domain.com, the device determines that the user belongs to the domain.com but not the domain.com.cn.

## Domain-name-based AAA Service Configuration Example

The following is an example of configuring the domain-name-based AAA service:

```
Ruijie(config)# aaa new-model

Ruijie(config)# radius-server host 192.168.197.154

Ruijie(config)# radius-server key test

Ruijie(config)# aaa authentication dot1x default group radius

Ruijie(config)# aaa domain domain.com

Ruijie(config-aaa-domain)# authentication dot1x default

Ruijie(config-aaa-domain)# username-format without-domain
```

After the configuration, with the user a1 in the radius server, use the 802.1x client to login the server for authentication by keying in the username a1@domain.com and the correct password. The following shows the related domain-name information:

```
Ruijie#show aaa domain domain.com

=====Domain domain.com=====

State: Active

Username format: Without-domain
```



```
Access limit: No limit
```

```
802.1X Access statistic: 0
```

```
Selected method list:
```

```
authentication dot1x default
```

## Typical AAA Configuration Example

### Typical AAA Application

#### Network Topology

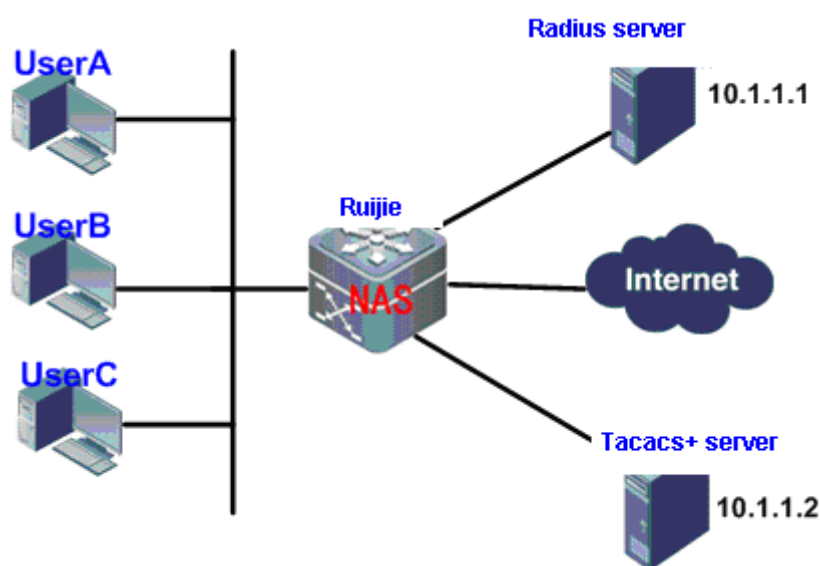


Figure 3 Typical AAA Application Topology

#### Network Requirements

For better security management for the NAS device in the Figure-3, the followings are the network requirements:

1. The administrators shall have the individual username and password for the convenience of the account management.
2. The user authentication methods are divided into local authentication and collection authentication. The method of combining the collection-authentication with the local-authentication shall be adopted, with the collection-authentication mainly-used and the local-authentication as backup. In the process of the collection-authentication, the Radius server authentication shall be passed first, if there is no reply, it will switch to the local authentication.
3. Different users can be configured to access to the specified network device during the authentication.
4. User management priority: divide the network management users into the super users and ordinary users, wherein the super users own the priority of reading and writing while the ordinary users own the reading priority only.

5. The user authentication information, the authorization information and the network information are recorded in the server for the display and audit later(This example uses the TACACS+ for the accounting. )

## Configuration Key-points

From the analysis of the part of “*Network Requirements*”, deploying the AAA function can address the above requirements, which is to dynamically configure the ID authentication, authorization and accounting type for the user(line) or the server. Define the ID authentication, authorization and accounting type by creating the method list, and apply the method list to the specified service or interface. For the details, see the following “*Configuration Steps*”.

## Configuration Steps

### #Enable AAA:

Enable the AAA function on the device

```
Ruijie#configure terminal
Ruijie(config)#aaa new-model
```

### # Configure the security server:

The network security server takes the responsibility for the authentication, the authorization and the accounting. The user information are stored in the server and the software of the server can record, calculate and analyze the various information via the syslogs.

Configure the Radius server information (the shared key for the communication between the device and the Radius server is ruijie)

```
Ruijie(config)#radius-server host 10.1.1.1
Ruijie(config)#radius-server key ruijie
```

Configure Tacacs+ server information (the shared key for the communication between the device and the Tacacs+ server is redgiant)

```
Ruijie(config)#tacacs-server host 10.1.1.2
Ruijie(config)#tacacs-server key redgiant
```

### # Configure the local user:

Configure the password encryption (the key information for the local password and the security server are saved and shown in the simply-encrypted format)

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

Configure the local user database (Configure the username and the password, and set the user privilege level)

```
Ruijie(config)#username bank privilege 10 password yinhang
Ruijie(config)#username super privilege 15 password star
Ruijie(config)#username normal privilege 2 password normal
Ruijie(config)#username test privilege 1 password test
```

### Configure the local enable password for the local enable authentication

```
Ruijie(config)#enable secret w
```

Configure the line login password (with the AAA function enabled, the login password of the terminal line takes no effect. So the line login password configuration is to prevent the login failure with the AAA function disabled)

```
Ruijie(config)#line vty 0 15
Ruijie(config-line)#password w
```

Configure the line user privilege level (with the Exec authorization disabled, or no Exec authorization method list is applied in the line and no default Exec authorization method list, the configure line user privilege level should be used)

```
Ruijie(config)#line vty 0 15
Ruijie(config-line)#privilege level 10
```

## # Configure the authentication

### 1. Login authentication

The Login authentication is used to control the user access. There are two methods to define the authentication method list: 1) Radius; 2) Local.

Configure login authentication method list and apply it to the corresponding line

```
Ruijie(config)# aaa authentication login hello group radius local
Ruijie(config)# line vty 0 15
Ruijie(config-line)# login authentication hello
```

To prevent the user from using the exhaust algorithm to crack the password during the Login authentication, AAA is used to limit the user Login attempts. When the authentication attempts reached the configured limit, the user would fail to log in for the lockout time (by default, the login authentication attempt is 3 times and the lockout time is 15 hours.)

Configure the authentication attempt 2 times and the authentication lockout-time 10 hours

```
Ruijie(config)#aaa local authentication attempts 2
Ruijie(config)#aaa local authentication lockout-time 10
```

### 2. Enable authentication

The Enable authentication is used to switch the user privilege level. An authentication process is needed before the user switches the privilege level to the superuser using the **enable** command. There are two methods to define the authentication method list: 1) Radius; 2) Local. The Enable authentication can only set the default method list, which will be auto-applied after the configuration.

Configure the enable authentication method list

```
Ruijie(config)#aaa authentication enable default group radius local
```

## # Configure the authorization

### 1. Exec authorization

The Exec authorization is used to control the user command privilege level. For example, level 15 is the superuser, level 14 is the configuration user, level 2 is the ordinary user. The remote Exec authorization takes precedence over the local one.

Configure the exec authorization method list and apply it to the line

```
Ruijie(config)#aaa authorization exec shouquan group tacacs+ local
Ruijie(config)#line vty 0 15
Ruijie(config-line)#authorization exec shouquan
```

Configure the exec authorization for the console (by default, the exec authorization is not for the console)

```
Ruijie(config)#aaa authorization console
```

## 2. Command authorization

The Command authorization is used to offer the execution privilege of the key commands only to the administrators. The Command authorization authorizes the level of the command but not of the current user. The Radius protocol is not supported.

Configure the Command authorization method list and apply it to the line.

```
Ruijie(config)#aaa authorization commands 2 abc group tacacs+ local
Ruijie(config)#line vty 0 15
Ruijie(config-line)#authorization commands 2 abc
```

## # Configure the accounting

### 1. Exec accounting

The Exec accounting is used to send the messages of the user login and logout to the server for the displaying, statistics and the auditing.

Configure the exec accounting method list and apply it to the line

```
Ruijie(config)#aaa accounting exec default start-stop group tacacs+
```

### 2. Command accounting

The Command accounting is used to send the commands of a specific level executed by the user to the server for the displaying, statistics and the auditing.

Configure the command accounting method list and apply it to all lines

```
Ruijie(config)#aaa accounting commands 2 default start-stop group tacacs+
```

## Configuration verification

Step 1: Use the **show running-config** command to show the current configurations:

```
Ruijie#show running-config
.....
!
aaa new-model
aaa local authentication attempts 2
```

```
aaa local authentication logout-time 10
aaa authorization exec shouquan group tacacs+ local
aaa authorization commands 2 abc group tacacs+
aaa accounting exec default start-stop group tacacs+
aaa accounting commands 2 default start-stop group tacacs+
aaa authentication login hello group radius local
aaa authentication enable default group radius local
!
username bank password 7 09361c1c2f041c4d
username bank privilege 10
username super password 7 093c011335
username super privilege 15
username normal password 7 09211a002a041e
username normal privilege 2
username test password 7 093b100133
service password-encryption
!
tacacs-server key 7 072c062b121b260b06
tacacs-server host 10.1.1.2
radius-server host 10.1.1.1
radius-server key 7 072c16261f1b22
enable secret 5 $1$2MjW$xr1t0s1Euvt76xs2
!
line con 0
line vty 0 4
    authorization exec shouquan
    authorization commands 2 abc
    privilege level 10
    login authentication hello
    password 7 0938
line vty 5 15
    authorization exec shouquan
    authorization commands 2 abc
    privilege level 10
    login authentication hello
    password 7 005d
!
end
```

**Step 2:** In the actual application, use the **show aaa user { *id* | all }** command to show the current AAA user information.

## AAA Multi-domain Authentication Application

### Network Topology

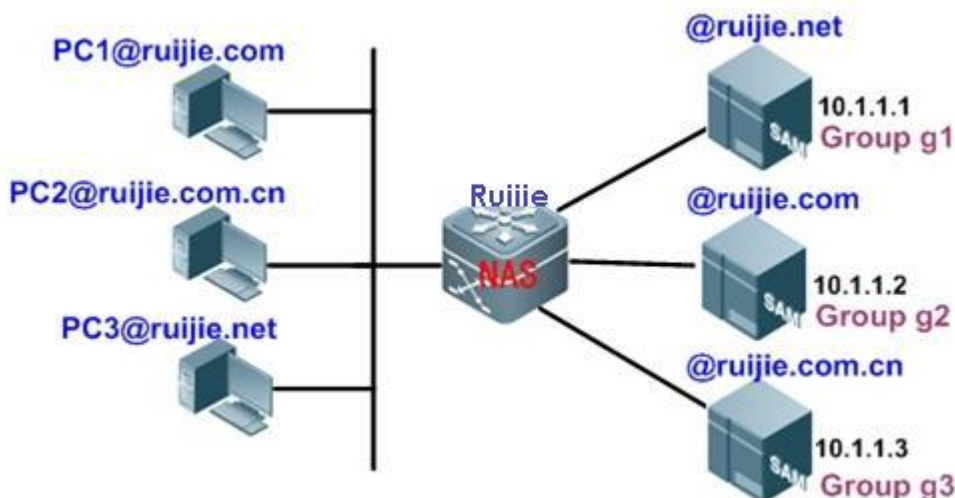


Figure-4 AAA multi-domain authentication application topology

### Network Requirements

Configure the NAS device to enable the domain-name-based AAA service, including the authentication, authorization and the accounting:

- Use the 802.1x client for the login authentication with the username PC1@ruijie.com or PC2@ruijie.com.cn or PC3@ruijie.net and the password.
- User network management: classify the users into the superusers and the ordinary users, wherein the superusers are able to read and write while the ordinary users are able to read only.
- The user authentication, authorization and network action messages are saved in the authentication server for the displaying and the auditing.

### Configuration Key-points

Configure the domain-name-based AAA service to address the above network requirements.

This example takes the 802.1x client for example, therefore the network device must support 802.1x client access, otherwise, this example cannot be applied.

### Configuration Steps

#### #Enable AAA:

Enable the AAA function on the device

```
Ruijie#configure terminal
Ruijie(config)#aaa new-model
```

#### # Configure the security server:

The network security server takes the responsibility for the authentication, the authorization and the accounting. The user information are stored in the server and the

software of the server can record, calculate and analyze the various information via the syslogs.

Configure the Radius server information (the shared key for the communication between the device and the Radius server is ruijie)

```
Ruijie(config)#aaa group server radius g1
Ruijie(config-gs-radius)#server 10.1.1.1
Ruijie(config-gs-radius)#exit
Ruijie(config)#aaa group server radius g2
Ruijie(config-gs-radius)#server 10.1.1.2
Ruijie(config-gs-radius)#exit
Ruijie(config)#aaa group server radius g3
Ruijie(config-gs-radius)#server 10.1.1.3
Ruijie(config-gs-radius)#exit
Ruijie(config)#radius-server key ruijie
```

### # Configure the local user:

Configure the password encryption (the key information for the local password and the security server are saved and shown in the simply-encrypted format)

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

Configure the local user database (Configure the username and the password, and set the user privilege level)

```
Ruijie(config)#username bank privilege 10 password yinhang
Ruijie(config)#username super privilege 15 password star
Ruijie(config)#username normal privilege 2 password normal
Ruijie(config)#username test privilege 1 password test
```

Configure the local enable password for the local enable authentication

```
Ruijie(config)#enable secret w
```

### # Define the AAA service method list

Configure dot1x authentication

```
Ruijie(config)#aaa authentication dot1x renzheng group radius local
```

Configure network authorization

```
Ruijie(config)#aaa authorization network shouquan group radius
```

! Configure network accounting

```
Ruijie(config)#aaa accounting network jizhang start-stop group radius
```

### # Enable the domain-based AAA service switch

```
Ruijie(config)#aaa domain enable
```

## # Create the domain and configure the domain attribute collection

### Create the domain

```
Ruijie(config)#aaa domain ruijie.com
```

### Associate the AAA service method list

```
Ruijie(config-aaa-domain)#authentication dot1x renzheng
```

```
Ruijie(config-aaa-domain)#authorization network shouquan
```

```
Ruijie(config-aaa-domain)#accounting network jizhang
```

### Configure the domain state

```
Ruijie(config-aaa-domain)#state active
```

### Configure the username without the domain

```
Ruijie(config-aaa-domain)#username-format without-domain
```

```
Ruijie(config)#aaa authentication dot1x renzheng group g2
```

```
Ruijie(config)#aaa authorization network shouquan group g2
```

```
!
```

```
Ruijie(config)#aaa accounting network jizhang start-stop group g2
```

```
!
```

The configurations of the ruijie.com.cn and the ruijie.net are similar.

## Configuration verification

Step 1: Use the **show running-config** command to show the current configurations ( take the domain name ruijie.com for example):

```
Ruijie#show running-config
```

```
.....
```

```
!
```

```
aaa new-model
```

```
aaa domain enable
```

```
!
```

```
aaa domain ruijie.com
```

```
authentication dot1x renzheng
```

```
accounting network jizhang
```

```
authorization network shouquan
```



```
username-format without-domain

!

!

aaa group server radius g1

server 10.1.1.1

!

aaa group server radius g2

server 10.1.1.2

!

aaa group server radius g3

server 10.1.1.3

!

!

aaa accounting network jizhang start-stop group g2

aaa authorization network shouquan group g2

aaa authentication dot1x renzheng group g2

!

no service password-encryption

!

radius-server key ruijie
```

## Step 2: Show the domain-based AAA service domain information:

```
Ruijie#show aaa domain

=====Domain ruijie.com=====

State: Active

Username format: Without-domain

Access limit: No limit

802.1X Access statistic: 0

Selected method list:
```

authentication dot1x renzheng

authorization network shouquan

accounting network jizhang

# RADIUS Configuration

## Radius Overview

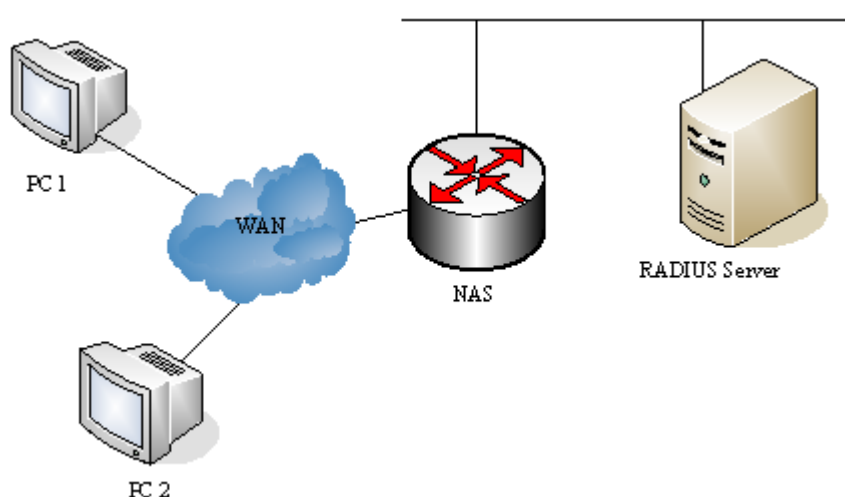
The Remote Authentication Dial-In User Service (Radius) is a distributed client/server system that works with the AAA to perform authentication for the users who are attempting to make connection and prevent unauthorized access. In the implementation of our product, the RADIUS client runs on the router or the network access server (NAS) to send the authentication requests to the central RADIUS server. The central center includes all information of user authentication and network services.

Since the RADIUS is a completely-open protocol, it has become a component and been installed in such systems as UNIX and WINDOWS 2000, so it is the security server most widely used for the time being.

The running process of the RADIUS is as follows:

- Prompt the user to enter username and password.
- The username and the encrypted password are sent to the RADIUS server via the network.
- The RADIUS returns one of the following responses:
- The user authentication passes.
- The user authentication fails and it prompts to reenter the username and password.
- The RADIUS server sends the challenge request to gather more authentication information from the user.
- The user authorization information is included in the ACCEPT response.

Here is a typical RADIUS topology:



**Typical RADIUS network configuration**

## RADIUS Configuration Tasks

To configure Radius on the network device, perform the following tasks first:

- Enable AAA. For the details, see *AAA Overview*.
- Define the RADIUS authentication method list by using the **aaa authentication** command. For details about how to use "aaa authentication" to define the authentication method list, see *Configuring Authentication*.
- Apply the defined authentication list on the specific line; otherwise the default authentication list will be used for authentication. For more details, see *Configuring Authentication*.

After the configuration is completed, you may start to configure the RADIUS. The configuration of the RADIUS consists of the following parts:

- Configuring Radius Protocol Parameters
- Specify the RADIUS authentication.

### Configuring Radius Protocol Parameters

Before configuring the Radius on the network device, the network communication shall operate perfectly on the Radius server. To configure RADIUS protocol parameters, run the following commands:

Command	Function
<b>configure terminal</b>	Enter the global configuration mode.
<b>radius-server host</b> <i>ip-address</i> [ <b>auth-port</b> <i>port</i> ] [ <b>acct-port</b> <i>port</i> ]	Configure the IP address or hostname of the remote Radius security server and specify the authentication port and accounting port.
<b>radius-server key</b> <i>string</i>	Configure the sharing password for the communication between the device and Radius server
<b>radius-server retransmit</b> <i>retries</i>	Specify the times of sending requests before the router confirms Radius invalid (3 by default)
<b>radius-server timeout</b> <i>seconds</i>	Specify the waiting time before the router resend request (2 s by default)
<b>radius-server deadtime</b> <i>minutes</i>	Specify the waiting time before the server is considered dead in case of no response to the request sent by the device (5 minutes by default).



#### Caution

To configure the RADIUS, it is necessary to configure the RADIUS Key. The sharing password on the network device and the sharing password on the Radius server must be the same.

### Specifying the Radius Authentication

This means defining the authentication method list for the Radius after the Radius server is specified and the Radius authentication sharing password is defined. Since the RADIUS authentication is done via

AAA, it is required to execute the **aaa authentication** command to define the authentication method list and specify the authentication method as RADIUS. For more details, see AAA Configurations.

## Specifying the Radius Standard Attribute Type

This chapter introduces configuration of Radius standard attribute type. Now the RADIUS Calling-Station-ID attribute(the attribute type is 31) is supported.

## Configuring Calling-Station-ID Format

RADIUS Calling-Station-ID attribute is used to identify the NAS when the NAS is sending the request packets to the RADIUS server. The contents of the RADIUS Calling-Station-ID are character strings, which can be in multiple formats. The MAC address for the NAS is usually used as the content of the Calling-Station-ID to solely identify the NAS. The table below lists the formats of the MAC address:

Format	Description
<b>ietf</b>	The standard format specified by the IETF RFC3580. - is used as the separator, for example: 00-D0-F8-33-22-AC.
<b>normal</b>	Normal format representing the MAC address. . is used as the separator. For example: 00d0.f833.22ac.
<b>unformatted</b>	No format and separator. By default, unformatted is used. For example: 00d0f83322ac.

To configure the RADIUS Calling-Station-ID MAC-based attribute format, run the following commands:

Command	Function
<b>configure terminal</b>	Enter the global configuration mode.
<b>radius-server attribute 31 mac format {ietf   normal   unformatted}</b>	Configure the RADIUS Calling-Station-ID MAC-based attribute format. The default format is <b>unformatted</b> .

## Specify Radius Private Attribute Type

The contents in this section enable configuring freely the type of private attributes. The default configurations are as follows:

Default configurations of our product private attribute recognition:

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

ID	Function	Type
10	file-count	10
11	file-name-0	11
12	file-name-1	12
13	file-name-2	13
14	file-name-3	14
15	file-name-4	15
16	max up-rate	16
17	version to server	17
18	flux-max-high32	18
19	flux-max-low32	19
20	proxy-avoid	20
21	dailup-avoid	21
22	ip privilege	22
23	login privilege	42
24	limit to user number	50

Extended manufacturer ID default configuration:

ID	Function	TYPE
1	max down-rate	76
2	qos	77
3	user ip	3
4	vlan id	4
5	version to client	5
6	net ip	6
7	user name	7
8	password	8
9	file-directory	9
10	file-count	10
11	file-name-0	11
12	file-name-1	12
13	file-name-2	13
14	file-name-3	14
15	file-name-4	15
16	max up-rate	75
17	version to server	17
18	flux-max-high32	18
19	flux-max-low32	19
20	proxy-avoid	20
21	dailup-avoid	21
22	ip privilege	22
23	login privilege	42
24	limit to user number	50



Two functions cannot be configured with the same type number.

### Note

Here is an example on how to configure the private type for network device:

```
Ruijie# show radius vendor-specific
id      vendor-specific      type-value
----  -
1      max down-rate          76
2      qos                     77
3      user ip                 3
4      vlan id                 4
5      version to client       5
6      net ip                  6
7      user name               7
8      password                8
9      file-diractory          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 privilage             22
23     login privilage          42
24     limit to user number 50

Ruijie# configure
Ruijie(config)# radius attribute 24 vendor-type 67
Ruijie(config)# show radius vendor-specific
id      vendor-specific      type-value
----  -
1      max down-rate          76
2      qos                     77
3      user ip                 3
4      vlan id                 4
5      version to client       5
6      net ip                  6
7      user name               7
8      password                8
9      file-diractory          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
Ruijie(config)#
Ruijie(config)#
```

## Configuring the Reachability Detection for RADIUS server

The device maintains the reachability state of each RADIUS server configured: reachable or unreachable. The device won't send the authentication, authorization and accounting requests of the access user to an unreachable RADIUS server, unless all RADIUS servers in the RADIUS server group are all unreachable.

The device can carry out active detection of the specified RADIUS server, and this feature is disabled by default. If you enable active detection of the specified RADIUS server, the device will periodically send detection requests (authentication requests or accounting requests) to the RADIUS server. The corresponding interval will be:

- RADIUS server in reachable state: the default interval for active detection is 60 minutes.
- RADIUS server in unreachable state: fixed to 1 minute.



To enable active detection of the specified RADIUS server, the following conditions must be met:

1. Testing user name for this RADIUS server has been configured on the device.
2. At least one tested port of this RADIUS server (authentication port or accounting port) has been configured on the device.

For a RADIUS server in reachable state, the device will considered this RADIUS server unreachable if the following two conditions are met:

1. The time configured by "**radius-server dead-criteria time seconds**" is exceeded after correct response is last received from this RADIUS server.
2. After correct response is last received from this RADIUS server, the number of tries to send requests to this RADIUS server when no correct response is received has exceeded the number set by "**radius-server dead-criteria tries number**".



#### Note

For a RADIUS server in unreachable state, the device will considered this RADIUS server reachable if any of the following conditions is met:

1. Correct response is received from this RADIUS server.
2. The duration that this RADIUS server remains unreachable exceeds the time set by "**radius-server deadtime**", and active detection of this RADIUS server is not enabled.
3. The authentication port or accounting port of this RADIUS server is updated on the device.

RADIUS server reachability detection allows the user to configure the dead-criteria conditions for a RADIUS server and active detection.

To configure RADIUS dead-server detection, execute the following commands in global configuration mode:

Command	Function
Ruijie# <b>configure terminal</b>	Enter the global configuration mode.
Ruijie(config)# <b>radius-server dead-criteria time seconds tries number</b>	Globally configure the dead-criteria conditions for a RADIUS server to be marked as dead. The default value of "seconds" is 60, and the default value of "number" is 10.
Ruijie(config)# <b>radius-server deadtime minutes</b>	Configure the duration for the device to stop sending request packets to the RADIUS server in unreachable state (default: 0 minute).

Command	Function
Ruijie(config)# <b>radius-server host</b> <i>ip-address</i> [ <b>auth-port</b> <i>port</i> ] [ <b>acct-port</b> <i>port</i> ] [ <b>test username</b> <i>name</i> [ <b>idle-time</b> <i>time</i> ] [ <b>ignore-auth-port</b> ] [ <b>ignore-acct-port</b> ]	Configure the IP address of remote RADIUS server, specify the authentication port and accounting port, and specify relevant parameters of active detection (testing user name, interval for active detection of RADIUS server in reachable state, and whether the authentication port or the accounting port shall be neglected).

**Caution**

The dedicated testing user name shall be used. This user name must not be used by other valid access users, so as not to affect the authentication, authorization or accounting of other valid users.

## Monitoring RADIUS

To monitor the RADIUS, execute the following commands in the privileged user mode:

Command	Function
<b>debug radius event</b>	Turn on the Radius debug switch to view the Radius debug information

## Radius Configuration Example

In a typical Radius network configuration diagram, the RADIUS server performs authentication for the visiting users, enables the accounting function for the visiting users and records the network usage of the users.

**Note**

The RADIUS server can be a component that comes with the Windows 2000/2003 server (IAS) or the UNIX system, or the special server software of some manufacturers.

Here is an example on how to configure the Radius for network device:

```
Ruijie# configure terminal
Ruijie(config)# aaa new-model
Ruijie(config)# radius-server host 192.168.12.219
auth-port 1645 acct-port 1646
Ruijie(config)# radius-server key aaa
Ruijie(config)# aaa authentication login test group radius
Ruijie(config)# end
Ruijie# show radius server
Server IP:      192.168.12.219
Accounting Port: 1646
Authen Port:    1645
Server State:   Ready
Ruijie#configure terminal
Ruijie(config)#line vty 0
Ruijie(config-line)#login authentication test
Ruijie(config-line)#end
```

```
Ruijie#show running-config
!
aaa new-model
!
!
aaa authentication login test group radius
!
username Ruijie password 0 starnet
!
radius-server host 192.168.12.219 auth-port 1645 acct-port 1646
!
line con 0
line vty 0
login authentication test
line vty 1 4
!
```

## Radius IPv6 Configuration Example

In the typical RADIUS network configuration diagram, RADIUS server authenticates the access users, enables accounting of access users and records the network service usage by users.



### Note

RADIUS server shall be running Windows 2008 Server or other dedicated IPv6 server software recognized by the manufacturer.

The following example shows how to configure RADIUS on the network device:

```
Ruijie# configure terminal
Ruijie(config)# aaa new-model
Ruijie(config)# radius-server host 3000::100 auth-port 1645 acct-port 1646
Ruijie(config)# radius-server key aaa
Ruijie(config)# aaa authentication login test group radius
Ruijie(config)# end
Ruijie# show radius server
Server IP:          3000::100
Accounting Port:    1646
Authen Port:        1645
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 15, timeouts 1
        Author: request 0, timeouts 0
        Account: request 0, timeouts 0
```

```
Ruijie# configure terminal
Ruijie(config)# line vty 0
Ruijie(config-line)# login authentication test
Ruijie(config-line)# end
Ruijie# show running-config
!
aaa new-model
!
!
aaa authentication login test group radius
!
!
!
radius-server host 3000::100 auth-port 1645 acct-port 1646
radius-server key aaa
!
line con 0
line vty 0
login authentication test
line vty 1 4
!
```

## TACACS+ Configuration

### TACACS+ Overview

TACACS+ is a security protocol with more powerful function on the basis of TACACS (RFC 1492 Terminal Access Controller Access Control System). It implements AAA function of multi-users by Client-Server mode and TACACS server communication. It needs to configure the related contents of TACACS+ server before using TACACS+ server.

TACACS+ supports user authentication, authorization and accounting analysis. That is, we can use one server to authenticate, another one to authorize and the third one to account at the same time. Each server has its own user data information, being antagonistic to authenticate, authorize and account.

The table below shows TACACS+ packet format:

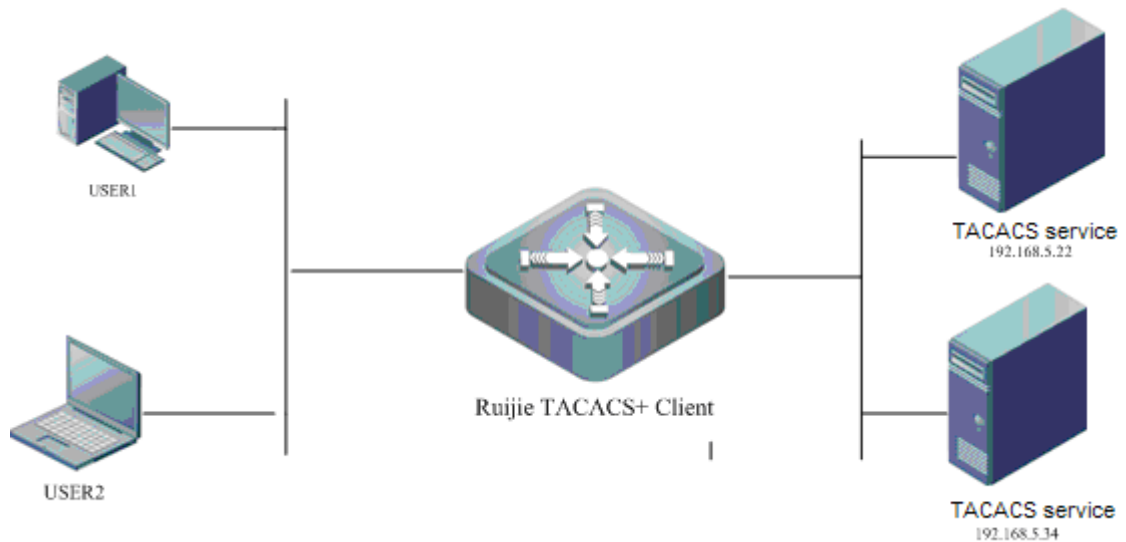
4	8	16	24	32 bit
Major	Minor	Packet type	Sequence no.	Flags
Session ID				
Length				

**Figure 1**

- Major Version — Major TACACS+ Version number;
- Minor Version — Minor TACACS+ Version number;
- Packet Type — the value may include:  
TAC\_PLUS\_AUTHEN: = 0x01 (Authentication);  
TAC\_PLUS\_AUTHOR:= 0x02 (Authorization);  
TAC\_PLUS\_ACCT:= 0x03 (Accounting).
- Sequence Number — packet sequence number in current session. The first TACACS+ packet sequence number in the session must be 1 and every packet sequence number followed is added by 1 gradually. Therefore, the client only sends the packet with odd sequence number, while TACACS+ Daemon only sends the packet with even sequence number.
- Flags — this field includes flag with various bitmap format. The Flag value indicates whether the packet is encrypted or not.
- Session ID — ID in the TACACS+ session.
- Length —body length of TACACS+ packet (excluding head). All the packets are transmitted in the network in the encrypted form.

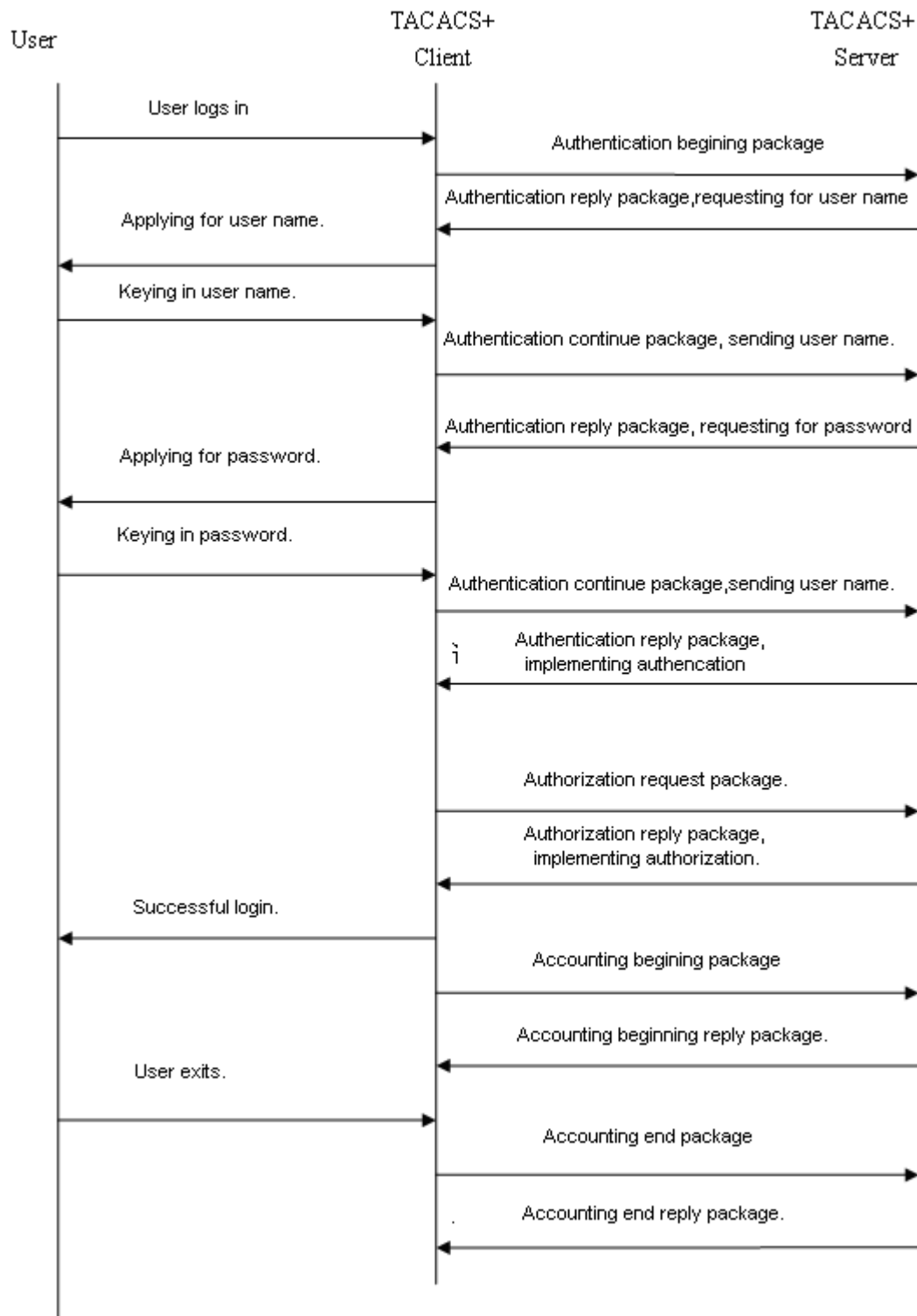
## TACACS+ Application

The typical application of TACACS+ is the login management control of terminal users. TACACS+ client sends user name and password to TACACS+ server for authentication. After authentication and authorization, you can login to the switch for operation, which is shown as figure 2:



**Figure 2**

Figure 3 describes the interaction of the packets running in TACACS+ by login AAA:

**Figure 3**

The whole process of basic information interaction is divided into three parts:

**1. Authentication process includes:**

- a) User requests for logging in to the switch;
- b) After receiving the request, TACACS+ Client sends the authentication beginning message to TACACS+ server;
- c) TACACS+ server sends the authentication reply message, requesting for the user name;

- d) TACACS+ Client asks user for user name.
- e) The user keys in the login user name;
- f) After receiving the user name, TACACS+ Client sends the authentication continue message including user name to TACACS+ server;
- g) TACACS+ server sends authentication reply message, requesting for login password;
- h) TACACS+ Client receives the login password;
- i) The user keys in the login password;
- j) After receiving the login password, TACACS+ Client sends authentication continue message including login password to TACACS+ server;
- k) TACACS+ server sends authentication reply message, indicating that user has been authenticated.

## 2. Authorization process includes:

- a) TACACS+ Client sends authorization request message to TACACS+ server.
- b) TACACS+ server sends authorization reply message, indicating that user has been authenticated;
- c) TACACS+ Client receives successful authorization reply message, outputting the configuration interface of switch to the user.

## 3. Accounting process includes:

- a) TACACS+ Client sends the accounting beginning message to TACACS+ server;
- b) TACACS+ server sends accounting beginning reply message, indicating that it has received the accounting beginning message;
- c) The user exits;
- d) TACACS+ Client sends the accounting end message to TACACS+ server;
- e) TACACS+ server sends accounting end reply message, indicating that it has received the accounting end message.

## TACACS+ Configuration Task

The following tasks must be executed before configuring TACACS+ on the network device:

- Use **aaa new-mode** to enable AAA. AAA must be enabled before using TACACS+; for the information how to enable **aaa new-mode**, please refer to AAA Overview.
- Use **tacacs-server host** to configure one or multiple tacacs+ servers.
- Use **tacacs-server key** to specify server and NAS shared key.
- Use **tacacs-server timeout** to specify timeout time waiting for the server reply;
- Use **tacacs-server directed-request** to enable the function of supporting the user to specify authentication server.



- If you need to authenticate, use **aaa authentication** to define using TACACS+ identity authentication method list. For the detailed information, please refer to authentication configuration.
- If you need to authorize, use **aaa authorization** to define using TACACS+ authorization method list. For the detailed information, please refer to authorization configuration.
- If you need to account, use **aaa accounting** to define using TACACS+ accounting method list. For the detailed information, please refer to accounting configuration.
- You shall use the defined authentication list in the specified line, or you use the list by default.

## Configuring TACACS+ Protocol Parameter

You need to ensure that the network communication of TACACS+ server runs well before configuring TACACS+ on the network device. Use the following commands to configure TACACS+ protocol parameters:

Command	Function
<b>configure terminal</b>	Enter the global configuration mode.
<b>aaa group server tacacs+ <i>group-name</i></b>	Configure TACACS+ group server, dividing different TACACS+ server into different groups.
<b>server <i>ip-address</i></b>	Configure the server addresses in TACACS+ group server.
<b>tacacs-server host <i>ip-address</i> [<i>port integer</i>] [<i>timeout integer</i>] <b>key</b> [0   7] <i>string</i></b>	Configure IP address of remote TACACS+ security server; configures different parameters on this server by different parameter combination: <ul style="list-style-type: none"> <li>● <b><i>ip-address</i></b> :configures server address;</li> <li>● <b><i>port integer</i></b> [optional] :determines the port used by the server; By default , the port number is 49 with the range from 1 to 65535.</li> <li>● <b><i>timeout integer</i></b> [optional] :configures server timeout time; By default, the timeout time is 5s with the range from 1 to 1000s.</li> <li>● <b><i>key string</i></b> [optional]:configures the key shared with the server of corresponding ip.</li> </ul>
<b>tacacs-server key [0   7] <i>string</i></b>	Configure the shared key used to communicate between the device and TACACS+ server. If the corresponding host does not set key by itself, you should set it globally.
<b>tacacs-server timeout <i>seconds</i></b>	Specify the waiting time before the device resends request. By default, it is 5s. if the specified host does not set the specified timeout time, you should set the time globally.

<b>tacacs-server directed-request</b> <b>[restricted] [no-truncate]</b>	Configure the function of supporting the user specified authentication server. The default configuration is enabled.
<b>ip tacacs source-interface</b> <i>interface</i>	Specify to send tacacs+ request to the source IP used by the server. By default, it does not specify.

**Caution**

You must configure TACACS+ Key before configuring TACACS+. The shared passwords on the network device and TACACS+ server must be consistent.

## Using TACACS+ to Authenticate, Authorize and Account

In the typical TACACS+ network configuration figure, TACACS+ server authenticates, authorizes and accounts the access users. The following shows the examples of how to configure TACACS+ to authenticate, authorize and account by login authentication, authorization and accounting.

### Using TACACS+ by Login Authentication

- Enables aaa first:

```
Ruijie# configure terminal
Ruijie(config)# aaa new-model
```

- Then configures tacacs+ server information:

```
Ruijie(config)# tacacs-server host 192.168.12.219
Ruijie(config)# tacacs-server key aaa
```

- Configures authentication method of using tacacs+:

```
Ruijie(config)# aaa authentication login test group tacacs+
```

- Applies the authentication method on the interface:

```
Ruijie(config)# line vty 0 4
Ruijie (config-line)# login authentication test
```

Through the above configuration, you implement to configure login tacacs+ authentication. The configuration is shown as follows;

```
Ruijie#show running-config
!
aaa new-model
!
aaa authentication login test group tacacs+
!
tacacs-server host 192.168.12.219
tacacs-server key aaa
!
```

```
line con 0
line vty 0 4
login authentication test
!
```

## Using TACACS+ by Enable Authentication

1. Enables aaa first:

```
Ruijie# configure terminal
Ruijie(config)# aaa new-model
```

2. Then configures tacacs+ server information:

```
Ruijie(config)# tacacs-server host 192.168.12.219
Ruijie(config)# tacacs-server host 192.168.12.218
Ruijie(config)# tacacs-server host 192.168.12.217
Ruijie(config)# tacacs-server key aaa
```

Configures tacacs+ server group using a part of the servers in the server list:

```
Ruijie(config)# aaa group server tacacs+ tacgroup1
Ruijie(config-gs-tacacs)# server 192.168.12.219
Ruijie(config-gs-tacacs)# server 192.168.12.218
```

3. Configures authentication method of using tacgroup1:

```
Ruijie(config)# aaa authentication enable default group tacgroup1
```

Through the above configuration, you implement to configure enable authentication of some tacacs+ servers. The configuration is shown as follows;

```
Ruijie#show running-config
!
aaa new-model
!
!
aaa group server tacacs+ tacgroup1
server 192.168.12.219
server 192.168.12.218
!
aaa authentication enable default group tacgroup1
!
!
tacacs-server host 192.168.12.219
tacacs-server host 192.168.12.218
tacacs-server host 192.168.12.217
tacacs-server key aaa
!
line con 0
line vty 0 4
!
```

## Using TACACS+ by Login Authorization

1. Enables aaa first:

```
Ruijie# configure terminal
```

```
Ruijie(config)# aaa new-model
```

2. Then configures tacacs+ server information:

```
Ruijie(config)# tacacs-server host 192.168.12.219
```

```
Ruijie(config)# tacacs-server key aaa
```

3. Configures the authorization method of using tacacs+:

```
Ruijie(config)# aaa authorization exec test group tacacs+
```

4. Applies the authorization on the interface:

```
Ruijie(config)# line vty 0 4
```

```
Ruijie (config-line)# authorization exec test
```

Through the above configuration, you implement to configure to use tacacs+ by login authorization. The configuration is shown as follows:

```
Ruijie#show running-config
```

```
!  
aaa new-model  
!  
!  
aaa authorization exec test group tacacs+  
!  
tacacs-server host 192.168.12.219  
tacacs-server key aaa  
!  
line con 0  
line vty 0 4  
authorization exec test  
!
```

## Using TACACS+ by Level 15 Command Audit

- Enables aaa first:

```
Ruijie# configure terminal
```

```
Ruijie(config)# aaa new-model
```

- Then configures tacacs+ server information:

```
Ruijie(config)# tacacs-server host 192.168.12.219
```

```
Ruijie(config)# tacacs-server key aaa
```

- Configures command audit method of using tacacs+:

```
Ruijie(config)# aaa accounting commands 15 test start-stop group tacacs+
```

- Applies the authorization on the interface:

```
Ruijie(config)# line vty 0 4
```

```
Ruijie (config-line)# accounting commands 15 test
```

Through the above configuration, you implement to configure enable authentication of some tacacs+ servers. The configuration is shown as follows;

```
Ruijie# show running-config
```

```
!  
aaa new-model  
!  
!  
aaa accounting commands 15 default group tacacs+  
!  
!  
tacacs-server host 192.168.12.219  
tacacs-server key aaa  
!  
line con 0  
line vty 0 4  
accounting commands 15 test  
!
```

## 802.1x Configuration

This chapter describes the contents related to the AAA service configurations. The 802.1x is used to control the authentication over network access of users, and provide authorization and accounting functions for users.

This chapter includes:

- Overview
- Configuring 802.1x
- Viewing the Configuration and Current Statistics of the 802.1x
- Other Precautions for Configuring 802.1x

**Note**

For details about usage and descriptions of the CLI commands used in this section, please refer to *Configuring 802.1X command*.

### Overview

In an IEEE 802 LAN, users can access the network device without authorization and authorization as long as they are connected to the network device. Therefore, an unauthorized user can access the network unobstructed by connecting the LAN. As the wide application of LAN technology, particularly the appearance of the operating network, it is necessary to address the safety authentication needs of the network. It has become the focus of concerns in the industry that how to provide user with the authentication on the legality of network or device access on the basis of simple and cheap Ethernet technologies. The IEEE 802.1x protocol is developed under such a context.

As a Port-Based Network Access Control standard, **the IEEE802.1x** provides LAN access point-to-point security access. Specially designed by the IEEE Standardization Commission to tackle the safety defects of Ethernet, this standard can provide a means to authenticate the devices and users connected to the LAN by utilizing the advantages of IEEE 802 LAN.

The IEEE 802.1x defines a mode based on Client-Server to restrict unauthorized users from accessing the network. Before a client can access the network, it must first pass the authentication of the authentication server.

Before the client passes the authentication, only the EAPOL (Extensible Authentication Protocol over LAN) packets can be transmitted over the network. After successful authentication, normal data streams can be transmitted over the network.

By using 802.1x, our switches provide Authentication, Authorization, and Accounting (AAA).

- **Authentication:** It is used to determine whether a user has the access, restricting illegal users.
- **Authorization:** It authorizes the services available to users, controlling the rights of valid users.

- Accounting: It records users' use of network resources, providing the supporting data for charging.

The 802.1x is described in the following aspects as below:

- Device Roles
- Authentication Initiation and Packet Interaction During Authentication
- States of Authorized Users and Unauthorized Users
- Topologies of Typical Applications

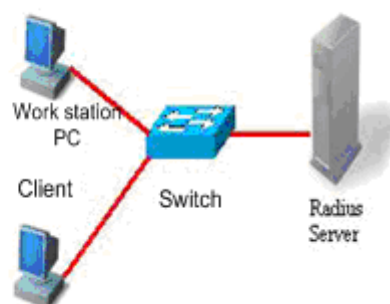
## Device Roles

In the IEEE802.1x standard, there are three roles: **supplicant**, **authenticator**, and **authentication server**. In practice, they are the Client, network access server (NAS) and Radius-Server.

Roles played in the IEEE802.1x protocol



Roles played in the real application



- Supplicant:

The **supplicant** is a role played by the end user, usually a PC. It requests for the access to network services and acknowledges the request packets from the authenticator. The supplicant must run the IEEE 802.1x client. Currently, the most popular one is the IEEE802.1x client carried by Windows XP. In addition, we have also launched the STAR Supplicant software compliant of this standard.

- Authenticator:

The **authenticator** is usually an access device like the switch. The responsibility of the device is to control the connection status between client and the network according to the current authentication status of that client. Between the client and server, this device plays the role of a mediator, which requests the client for username, verifies the authentication information from the server, and forwards it to the client. Therefore, the switch acts as both the IEEE802.1x authenticator and the RADIUS Client, so it is referred to as the network access server (NAS). It encapsulates the acknowledgement received from the client into the RADIUS format packets and forwards them to the RADIUS Server, while resolving the information received from the RADIUS Server and forwards the information to the client.

The device acting as the authenticator has two types of ports: controlled Port and uncontrolled Port. The users connected to a controlled port can only access network resources after passing the authentication, while those connected to a uncontrolled port can directly access network resources without authentication. We can control users by simply connecting them to an controlled port. On the other hand, the uncontrolled port is used to connect the authentication server, for ensuring normal communication between the server and switch.

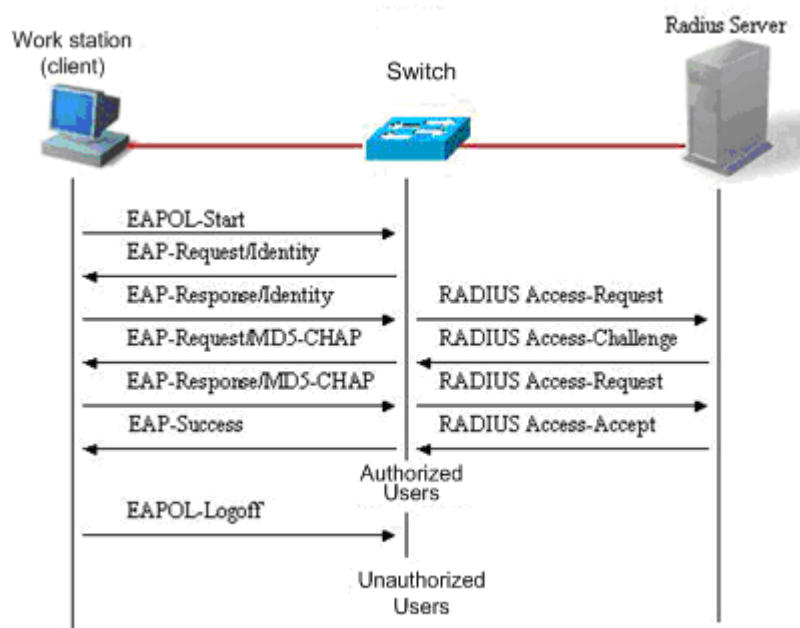
### ■ Authentication server:

The **authentication server** is usually an **RADIUS** server, which works with the authenticator to provide users with authentication services. The authentication server saves the user name and password and related authorization information. One server can provide authentication services for multiple authenticators, thus allowing centralized management of users. The authentication server also manages the accounting data from the authenticator. Our 802.1x device is fully compatible with the standard Radius Server, for example, the Radius Server carried on Microsoft Win2000 Server and the Free Radius Server on Linux.

## Authentication Initiation and Packet Interaction During Authentication

The supplicant and the authenticator exchange information by EAPOL protocol, while the authenticator and authentication server exchange information by RADIUS protocol, completing the authentication process with such a conversion. The EAPOL protocol is encapsulated on the MAC layer, with the type number of 0x888E. In addition, the standard has required for an MAC address (01-80-C2-00-00-03) for the protocol for packet exchange during the initial authentication process.

The following diagram shows a typical authentication process, during which the three role devices exchange packets with one another.



This is a typical authentication process initiated by users (in some special cases, the switch can actively initiate authentication request, whose process is the same as that shown in the diagram, except that it does not contain the step where the user actively initiates the request).

## States of Authorized Users and Unauthorized Users

The 802.1x determines whether the users on the port are allowed to access the network according to the authentication status of the port. Since we expand the 802.1X based on users, we determine whether a user is allowed to access network resources according to the authentication status of that user under a port. All users under an uncontrolled port can use network resources, while those under a controlled port can access network resources only if they are authorized. When a user just initiates an authentication request, its status is unauthorized, in which case it cannot access the network. When the authentication is passed, its status changes to be authorized, in which case it can use the network resources.



If the workstation does not support 802.1x while the machine is connected with the controlled port, when the equipment requests the username of the user, the workstation will not respond to the request due to no support. This means that the user is still unauthorized and cannot access the network resources.

On the contrary, if the client supports 802.1x, while the connected switch does not: The EAPOL-START frames from the user are not responded, and the user deems it connected port as an uncontrolled port and directly uses network resources, when the user fails to receive any response after it sends the specified number of EAPOL-START frames.

On a 802.1x-enabled device, all ports are uncontrolled ports by default. We can set a port as a controlled port, to impose authentication over all the users under that port.

When a user has passed authentication (the switch has received success packets from the RADIUS Server), the user is authorized and therefore can freely use network resources. If the user fails in the authentication and remains in the unauthenticated status, it is possible to initiate authentication once again. If the communication between the switch and the RADIUS server is faulty, the user is still unauthorized and therefore still cannot use the network.

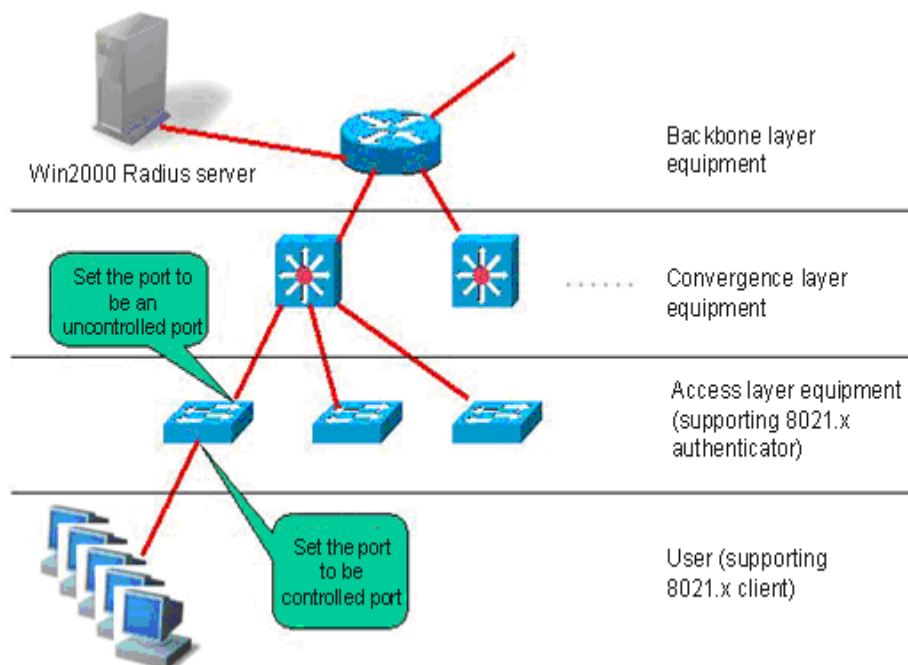
When the user sends the EAPOL-LOGOFF packets, its status changes from authorized to unauthorized. When a port of the switch changes to the LINK-DOWN status, all the users on the port change to the unauthorized status.

When the device restarts, all users on the device turn into the unauthorized status.

To force a user to pass the authentication, you can add a static MAC address.

## Topologies of Typical Applications

A. The 802.1x-enabled device is used as the access layer device



This solution is described as below:

### ■ Requirements of this solution:

1. The user supports 802.1x. That is, it is installed with the 802.1x client (Windows XP carried, Star-suppliant or other IEEE802.1x compliant client software).

2. The access layer device supports IEEE 802.1x.
3. One or multiple RADIUS compliant servers are available as the authentication server.

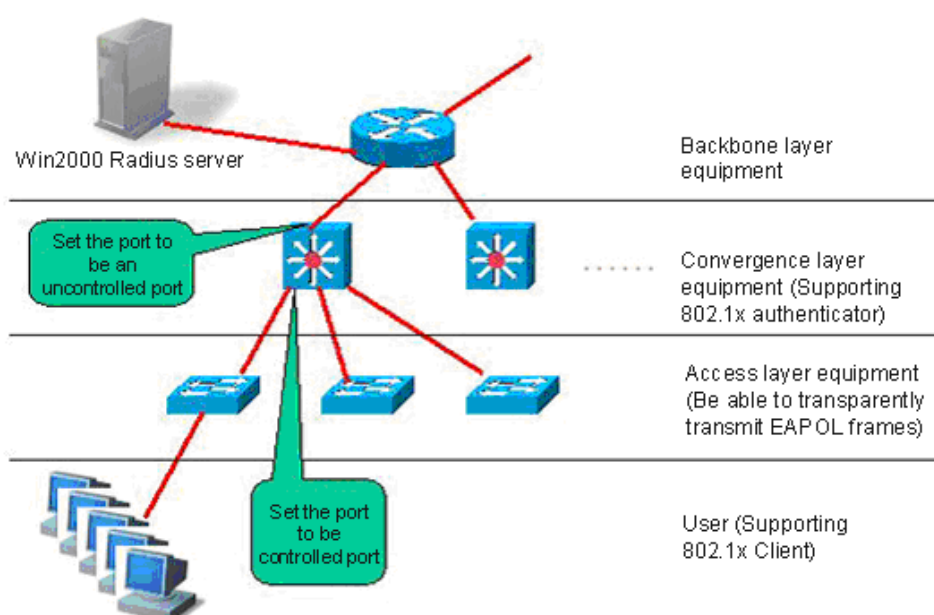
■ Key points for configuration of this solution:

1. The ports connected to the Radius Server and the uplink ports are configured as **uncontrolled ports**, so that the switch can normally communicate with the server and the authorized users can access network resources through the uplink interface.
2. The ports connected to the user must be set as **controlled ports** to control the accessed users, and the users cannot access network resources unless they first pass the authentication.

■ Characteristics of this solution:

1. Each 802.1x-enabled switch is responsible for a small number of clients, thus offering higher speed. The devices are mutually independent, and the restart operation of the device does not affect the users connected with other devices.
2. User management is performed on the Radius Server in a centralized manner. The administrator does not have to know which switch a user is connected to, making management much easier.
3. The administrator can manage the device on the access layer through the network.

B. The 802.1x-enabled device is used as the convergence layer device



This solution is described as below:

■ Requirements of this solution:

1. The user supports 802.1x. That is, it is installed with the 802.1x client (Windows XP carried, Star-suppliant or other IEEE802.1x compliant client software).
2. The access layer device should be able to transparently transmit IEEE 802.1x frames (EAPOL)
3. The convergence layer device supports 802.1x (playing the role of the authenticator)
4. One or multiple RADIUS compliant servers are available as the authentication server.

■ Key points for configuration of this solution:

1. The ports connected to the Radius Server and the uplink ports are configured as uncontrolled ports, so that the switch can normally communicate with the server and the authorized users can access network resources through the uplink interface.
2. The ports connected to the access layer switches must be set as controlled ports to control the accessed users, and the users cannot access network resources unless they first pass the authentication.

■ Characteristics of this solution:

1. The convergence layer device must be of high quality since the network is large and numerous users are connected, since any of its fault may cause the failures of many users to normally access the network.
2. User management is performed on the Radius Server in a centralized manner. The administrator does not have to know which switch a user is connected to, making management much easier.
3. The access layer device can be the less expensive non-NM switches (as long as they support transparent transmission of EAPOL frames).
4. The administrator cannot manage the device on the access layer through the network.

## Configuring 802.1x

The following sections describe how to configure 802.1x.

- Default Configuration of 802.1x
- Precautions for Configuring 802.1x
- Configuring the communication between the device and Radius server
- Setting the 802.1X Authentication Switch
- Enabling/Disabling the Authentication of a Port
- Enabling Timed Re-authentication
- Enabling/Disabling the Filtering of Non-Ruijie Suppliant
- Changing the QUIET Time

- Setting the Packet Retransmission Interval
- Setting the Maximum Number of Requests
- Setting the Maximum Number of Re-authentications
- Setting the Server-timeout
- Configuring the device to initiate the 802.1x authentication proactively
- Configuring 802.1x Accounting
- Configuring the IP authorization mode
- Releasing Advertisement
- List of Authenticable Hosts under a Port
- Authorization
- Configuring the Authentication Mode
- Configure the backup authentication server.
- Configuring and Managing Online Users
- Implementing User-IP Binding
- Port-based Traffic Charging
- Implementing Automatic Switching and Control of VLAN
- Implementing GUEST VLAN
- Shielding Proxy Server and Dial-up
- Configuring On-line Client Probe
- Configuring the Option Flag for EAPOL Frames to Carry TAG
- Configuring Port-based User Authentication
- Configuring Port-based Single User Authentication
- Configuring Dynamic ACL Assignment
- Configuring Dot1x MAC Bypass Authentication
- Configuring Dot1x MAC Bypass Authentication Timeout
- Configuring Dot1x MAC Bypass Authentication Violation
- Configuring Dot1x Auth-Fail VLAN
- Configuring Dot1x Auth-Fail Max-Attempt

## Default Configuration of 802.1x

The following table lists some defaults of the 802.1x

Item	Default
Authentication	DISABLE
Accounting	DISABLE
Radius Server	
*ServerIp	*No default
*Authentication UDP port	*1812
*Key	*No default
Accounting Server	
*ServerIp	*No default
*Accounting UDP port	*1813

Item	Default
All port types	Uncontrolled port (all ports can perform communication directly without authentication)
Timed re-authentication	Off
Timed reauth_period	3,600 seconds
Interval between two authentication requests	10 seconds
Retransmission interval	3 seconds
Maximum retransmissions	3
Client timeout period	3 seconds, if within which no response is received from the client, the communication is deemed as a failure
Server timeout period	5 seconds, if within which no response is received from the server, the communication is deemed as a failure
Lists of authenticable hosts under a port	No default

### Precautions for Configuring 802.1x

- You can perform the following configuration only to the products that support 802.1x.
- The 802.1x can run on both L2 device and L3 device.
- It is required to configure the IP address of the authentication server before the Radius-server authentication mode can operate normally.
- If the dot1x function is enable on the port and the number of authenticated users is larger than the maximum number of users of port security, port security cannot be enabled.
- With both the port security and dot1x function enabled, if the secure address ages, the users corresponding to the dot1x must be re-authenticated to continue communication.
- The static port secure address is available to the Internet without the authentication. If the authorization is required, the address must meet both the authentication and authorization binding to be available to the Internet.
- When the port security and movable authentication mode based on port are co-used, the learnt address which becomes the secure address cannot be moved.
- When the port security and movable authentication mode based on port are co-used, the authentication address aged by the port security must be re-authenticated to perform the communication.

- After the authentication of movable authentication mode based on the port is passed, the port must be re-authenticated in order to perform communication when the port security is enabled.
- Switching between the port-based mode and user-base mode is not allowed in the condition of IP address and MAC address binding.
- If the 1x function is enabled on only one port of a switch, all the port will send the 1x protocol packets to the CPU.

## Configuring the communication between the device and Radius server

The Radius Server maintains the information of all users: user name, password, authorization information and accounting information. All users are managed on the Radius Server in a centralized manner, without being distributed over various switches, making easier management for the administrator.

In order for the switch to normally communicate with the RADIUS SERVER, you must set the following parameters:

Radius Server end: You must register a Radius Client. At registration, you must supply the Radius Server switch's IP address, authentication UDP port (add the accounting UDP port, if needed), and the agreed key for communication between the switch and Radius Server, and select EAP support for the Client. The procedure for registering one Radius Client on the Radius Server varies with different software settings. Please refer to the appropriate document.

Device end: The following settings are necessary at the device end to ensure the communication between the device and the server: Configure the IP address of the Radius Server, authentication (accounting) UDP port and the agreed password for the communication with the server.

In the privileged EXEC mode, you can set the communication between the switch and the Radius Server via the following steps:

Command	Function
<b>configure terminal</b>	Enter the global configuration mode.
<b>aaa new-model</b>	Turn on the AAA switch.
<b>radius-server host</b> <i>ip-address</i> [ <b>auth-port</b> <i>port</i> ] [ <b>acct-port</b> <i>port</i> ]	Configure the RADIUS server
<b>Radius-server key</b> <i>string</i>	Configure RADIUS Key.
<b>end</b>	Return to the privileged EXEC mode.
<b>write</b>	Save the configuration.
<b>show radius server</b>	Show the RADIUS server.

You can use the **no radius-server host** *ip-address* **auth-port** command to restore the authentication UDP port of the Radius Server to its default. You can use the **no radius-server key** command to delete the authentication key of the Radius Server. The following example sets the Server IP as 192.168.4.12, authentication UDP port as 600, and the key as agreed password:

```
Ruijie# configure terminal
Ruijie(config)# radius-server host 192.168.4.12
Ruijie(config)# radius-server host 192.168.4.12 auth-port 600
Ruijie(config)# radius-server key MsdadShaAdasdj878dajL6g6ga
```

```
Ruijie(config)# end
```

- The officially agreed authentication UDP port is 1812.
- The officially agreed accounting UDP port is 1813.
- No less than 16 characters are recommended for the agreed password between the device and the Radius Server.
- The port of the device to connect the Radius Server shall be configured as uncontrolled port.

## Setting the 802.1X Authentication Switch

When the 802.1x authentication is enabled, the switch will impose authentication over the host connected to the controlled port, and the hosts that fail the authentication are not allowed to access the network.

In the privileged EXEC mode, you can enable the 1x authentication by performing the following steps:

Command	Function
<b>configure terminal</b>	Enter the global configuration mode.
<b>aaa new-model</b>	Turn on the AAA switch.
<b>radius-server host</b> <i>ip-address</i> <b>[auth-port</b> <i>port</i> <b>]</b> <b>[acct-port</b> <i>port</i> <b>]</b>	Configure the RADIUS server
<b>Radius-server key string</b>	Configure RADIUS Key.
<b>aaa authentication dot1x</b> <i>auth</i> <b>group radius</b>	Configure the dot1x authentication method list
<b>dot1x authentication</b> <i>auth</i>	dot1x applies authentication method list
<b>end</b>	Return to the privileged EXEC mode.
<b>write</b>	Save the configuration.
<b>show running-config</b>	Show the configuration.

The following example enables 802.1x authentication:

```
Ruijie# configure terminal
Ruijie(config)# aaa new-model
Ruijie(config)# radius-server host 192.168.217.64
Ruijie(config)# radius-server key starnet
Ruijie(config)# aaa authentication dot1x authen group radius
Ruijie(config)# dot1x authentication authen
Ruijie(config)# end
Ruijie# show running-config
!
aaa new-model
!
aaa authentication dot1x authen group radius
!
username Ruijie password 0 starnet
!
radius-server host 192.168.217.64
```

```

radius-server key 7 072d172e071c2211
!
!
!
dot1x authentication authen
!
interface VLAN 1
 ip address 192.168.217.222 255.255.255.0
 no shutdown
!
!
line con 0
line vty 0 4
!
end

```

To apply the RADIUS authentication method in the 802.1x, configure the IP address of the Radius Server and make sure normal communication between the device and the Radius Server. Without the coordination of the Radius Server, the switch cannot perform authentication. For how to set the communication between the Radius Server and the switch, please see the previous section.

## Enabling/Disabling the Authentication of a Port

If you enable authentication for a port when the 802.1x is enabled, the port becomes a controlled port, and the users under the port must first pass authentication before they can access the network. However, the users under the uncontrolled port can directly access the network.

In the privileged EXEC mode, you can set authentication for a port by performing the following steps:

Command	Function
<b>configure terminal</b>	Enter the global configuration mode.
<b>interface</b> <i>interface</i>	Enter the interface configuration mode and specify the Interface to configure.
<b>dot1x port-control auto</b>	Set the port to be a controlled port (enable interface authentication). You can use the no option of the command to disable the authentication of the interface.
<b>end</b>	Return to the privileged EXEC mode.
<b>write</b>	Save the configuration.
<b>show dot1x port-control</b>	View the authentication configuration of the 802.1x interface.

You can use the **no dot1x port-control** command to disable the authentication of the interface. The following example sets Ethernet interface 1/1 to be a controlled interface:

```

Ruijie# configure terminal
Ruijie(config)# interface f 1/1
Ruijie(config-if)# dot1x port-control auto
Ruijie(config)# end

```

When a port is set as a controlled port, only the EAP packets are allowed to pass; the packets to the CPU are also under control.



**Caution**

If you hope that cpu can not receive non-EAP packet from any controlled port, you can separate management VLAN from user VLAN.

## Enabling Timed Re-authentication

The 802.1x can ask users for re-authentication at periodical intervals, to prevent authorized users from being used by other users. This can also detect disconnection, making more accurate charging. In addition to the re-authentication switch, you can also define the re-authentication interval, which is 3600 seconds by default. In the case of charging based on duration, you should determine the re-authentication interval according to the specific network size, which should be sufficient while as accurate as possible.

In the privileged EXEC mode, you can enable/disable re-authentication and set the re-authentication interval by performing the following steps.

Command	Function
<b>configure terminal</b>	Enter the global configuration mode.
<b>dot1x re-authentication</b>	Enable timed re-authentication.
<b>dot1x timeout re-authperiod</b> <i>seconds</i>	Set the re-authentication interval.
<b>end</b>	Return to the privileged EXEC mode.
<b>write</b>	Save the configuration.
<b>show dot1x</b>	Show the dot1x configurations.

You can use the **no dot1x re-authentication** command to disable timed re-authentication, and use the **no dot1x timeout re-authperiod** command to restore the re-authentication interval to the default.

The following example enables re-authentication and sets the re-authentication interval as 1000 seconds.

```
Ruijie# configure terminal
Ruijie(config)# dot1x re-authentication
Ruijie(config)# dot1x timeout re-authperiod 1000
Ruijie(config)# end
Ruijie# show dot1x
802.1X Status:          Disabled
Authentication Mode:    EAP-MD5
Authed User Number:     0
Re-authen Enabled:      Enabled
Re-authen Period:       1000 sec
Quiet Timer Period:     10 sec
Tx Timer Period:        3 sec
Supplicant Timeout:     3 sec
Server Timeout:         5 sec
Re-authen Max:          3 times
Maximum Request:        3 times
Filter Non-RG Supp:     Disabled
Client Online Probe:    Disabled
Eapol Tag Enable:       Disabled
Authorization Mode:     Disabled
```

If re-authentication is enabled, please pay attention to the reasonableness of the re-authentication interval, which must be set according to the specific network size.

## Enabling/Disabling the Filtering of Non-Ruijie Supplicant

When the Ruijie supplicant product is used as the 802.1x authentication client, authentication may fail if you use some other 802.1x authentication clients at the same time (for example, Windows XP 802.1x authentication function is enabled).

In this case, you can enable this function to filter the 802.1x packets from non-Ruijie supplicants so that supplicant authentication is not affected by other 802.1x clients. The function is enabled by default.

In the privileged EXEC mode, you can enable/disable the filtering by performing the following steps:

Command	Function
<b>configure terminal</b>	Enter the global configuration mode.
<b>dot1x private-supplicant-only</b>	Enable the filtering function.
<b>End</b>	Return to the privileged EXEC mode.
<b>Write</b>	Save the configuration.
<b>show dot1x</b>	Show the dot1x configurations.

Following example is the configuration to enable the supplicant function provided by us.

```
Ruijie# configure terminal
Ruijie(config)# dot1x private-supplicant-only
Ruijie(config)# end
Ruijie# show dot1x
802.1X Status:          enable
Authentication Mode:    eap-md5
Total User Number:      0(exclude dynamic user)
Authed User Number:     0(exclude dynamic user)
Dynamic User Number:    0
Re-authen Enabled:      enable
Re-authen Period:       2 sec
Quiet Timer Period:     10 sec
Tx Timer Period:        3 sec
Supplicant Timeout:     3 sec
Server Timeout:         5 sec
Re-authen Max:          3 times
Maximum Request:        3 times
Private supplicant only: enable
Client Online Probe:    disable
Eapol Tag Enable:       disable
Authorization Mode:      disable
```

Use the **no dot1x private-supplicant-only** command to disable this function.

## Changing the QUIET Time

When the user authentication fails, the switch does not allow that user to re-authenticate until a specified period, which is referred to as Quiet Period. This value functions to protect the device from malicious attacks. The default interval for Quiet Period is 5 seconds.

A shorter Quiet Period may speed up re-authentication for the users.

In the privileged EXEC mode, you can set the Quiet Period by performing the following steps:

Command	Function
<b>configure terminal</b>	Enter the global configuration mode.
<b>dot1x timeout quiet-period seconds</b>	Set the Quiet Period.
<b>end</b>	Return to the privileged EXEC mode.
<b>write</b>	Save the configuration.
<b>show dot1x</b>	Show the dot1x configurations.

You can use the **no dot1x timeout quiet-period command** to restore the Quiet Period to its default. In the example below the QuietPeriod value is set as 500 seconds:

```
Ruijie# configure terminal
Ruijie (config)# dot1x timeout quiet-period 500
Ruijie (config)# end
```

## Setting the Packet Retransmission Interval

After the device sends the EAP-request/identity, it resends that message if no response is received from the user within a certain period. By default, this value is 3 seconds. You should modify this value to suit the specific network size.

In the privileged EXEC mode, you can set the packet retransmission interval by performing the following steps:

Command	Function
<b>configure terminal</b>	Enter the global configuration mode.
<b>dot1x timeout tx-period seconds</b>	Setting the Packet Retransmission Interval
<b>end</b>	Return to the privileged EXEC mode.
<b>write</b>	Save the configuration.
<b>show dot1x</b>	Show the dot1x configurations.

You can use the **no dot1x timeout tx-period** to restore the packet re-transmission interval to its default. The following example sets the packet retransmission interval as 100 seconds:

```
Ruijie# configure terminal
Ruijie (config)# dot1x timeout tx-period 100
Ruijie (config)# end
```

## Setting the Maximum Number of Requests

If the switch does not receive response within the ServerTimeout after it sends an authentication request to the RadiusServer, it will retransmit the packets. The maximum number of requests are the maximum

retransmission requests of the device, and the authentication fails if this number is exceeded. By default, this value is 3. You should modify this value to suit the specific network size.

In the privileged EXEC mode, you can set the maximum number of retransmissions by performing the following steps:

Command	Function
<b>configure terminal</b>	Enter the global configuration mode.
<b>dot1x max-req</b> <i>count</i>	Set the maximum number of packet re-transmissions.
<b>end</b>	Return to the privileged EXEC mode.
<b>write</b>	Save the configuration.
<b>show dot1x</b>	Show the dot1x configurations.

```
Ruijie#show dot1x
```

You can use the **no dot1x max-req** command to restore the maximum number of packet re-transmissions to its default. The following example sets the maximum number of packet retransmissions to 5:

```
Ruijie# configure terminal
Ruijie(config)# dot1x max-req 5
Ruijie(config)# end
```

## Setting the Maximum Number of Re-authentications

When the user authentication fails, the device attempts to perform authentication for the user once again. When the number of attempts exceeds the maximum number of authentications, the switch believes that this user is already disconnected, and ends the authentication process accordingly. By default, the number is 3. However, you can modify this value.

In the privileged EXEC mode, you can set the maximum number of re-authentications by performing the following steps:

Command	Function
<b>configure terminal</b>	Enter the global configuration mode.
<b>dot1x reauth-max</b> <i>count</i>	Setting the Maximum Number of Re-authentications
<b>end</b>	Return to the privileged EXEC mode.
<b>write</b>	Save the configuration.
<b>show dot1x</b>	Show the dot1x configurations.

You can use the **no dot1x reauth-max** command to restore the maximum number of re-authentications to its default. The following example sets the maximum number of re-authentications to 3:

```
Ruijie# configure terminal
Ruijie(config)# dot1x reauth-max 3
Ruijie(config)# end
```

## Setting the Server-timeout

This value indicates the maximum response time of the Radius Server. If the switch does not receive the response from the Radius Server within this period, it deems the authentication as a failure.

In the privileged EXEC mode, you can set the Server-timeout and restore it to its default by performing the following steps:

Command	Function
<b>configure terminal</b>	Enter the global configuration mode.
<b>dot1x timeout server-timeout</b> <i>seconds</i>	Set the maximum response time of the Radius Server. You can use the no option of the command to restore it to its default.
<b>end</b>	Return to the privileged EXEC mode.
<b>write</b>	Save the configuration.
<b>show dot1x</b>	Show the dot1x configurations.

### Configuring the device to initiate the 802.1x authentication proactively

The 802.1x is secure access authentication based on port. Users must first undergo authentication before they can access the network. In most cases, authentication is initiated by the user end through EAPOL-START packets. For the information about packet interaction during the authentication process, please see “Authentication Initiation and Packet Interaction During Authentication”.

However, authentication needs to be initiated by the switch in some cases. For example, when the switch is reset and the status of the authentication port changes from linkdown to linkup, the switch needs to automatically initiate authentication to ensure that the authenticated users can continue to use the network. In addition, if you use a 802.1x client that does not actively initiate authentication requests (for example, the Windows XP 802.1x client), the switch should be able to actively initiate authentication. The switch forcedly asks all the users under the authentication port to authenticate by sending the EAP-request/identity multicast packets.

The following section describes how to configure the switch to actively initiate 802.1x authentication and how you should configure appropriately in different application environments.

Turn on/off the switch for the proactive authentication initiation of the device

When this function is disabled, the switch can only initiate an authentication request at resetting or when the status of the authentication port is changed. This ensures that the on-line users can continue to use the network. The switch will not actively initiate an authentication request in any other cases. When this function is enabled, you can configure the times of automatic authentication initiation, authentication request interval, and whether to stop sending requests when the users pass the authentication.

In the privileged EXEC mode, you can enable automatic authentication by performing the following steps:

Command	Function
<b>configure terminal</b>	Enter the global configuration mode.
<b>dot1x auto-req</b>	Enable automatic authentication. It is enabled by default.
<b>end</b>	Return to the privileged EXEC mode.
<b>write</b>	Save the configuration.
<b>show dot1x</b>	Show the dot1x configurations.

The **no** option of the command turns off the function. Only when the function is enabled, the following settings take effect. The user can set the number of proactive authentication requests initiated by the device, which can be determined according to the actual network environment.

In the privileged EXEC mode, you can set the number of automatic authentication requests by performing the following steps:

Command	Function
<b>configure terminal</b>	Enter the global configuration mode.
<b>dot1x auto-req packet-num num</b>	The device proactively initiates num 802.1x authentication request messages. If num is equal to 0, the device will continually send that message. The default is 0 (infinite).
<b>end</b>	Return to the privileged EXEC mode.
<b>write</b>	Save the configuration.
<b>show dot1x auto-req</b>	Show the configuration.

The **no** option of the command restores the value to its default. The following contents introduce how to configure the message sending interval.

In the privileged EXEC mode, you can set the packet sending interval by performing the following steps:

Command	Function
<b>configure terminal</b>	Enter the global configuration mode.
<b>dot1x auto-req req-interval interval</b>	Setting the Packet Sending Interval
<b>end</b>	Return to the privileged EXEC mode.
<b>write</b>	Save the configuration.
<b>show dot1x auto-req</b>	Show the configuration.

The **no** option of the command restores the value to its default. Since sending the authentication request multicast message will cause re-authentication for all users under the authentication interface, the sending interval shall not be too small lest the authentication efficiency is affected.

It is possible to set whether to stop sending the request messages when the user authentication passes. In some applications (only one user under a port, for example), we can stop sending authentication requests to the related port when the device finds the user authentication passes. If the user gets offline, the request is sent continually.

In the privileged EXEC mode, you can set this function by performing the following steps:

Command	Function
<b>configure terminal</b>	Enter the global configuration mode.
<b>dot1x auto-req user-detect</b>	Stop sending the messages when there is some authentication user under the port. This function is enabled by default.
<b>end</b>	Return to the privileged EXEC mode.
<b>write</b>	Save the configuration.

Command	Function
<b>show dot1x auto-req</b>	Show the configuration.

The **no** option of the command disables the function. Before setting this function, take careful considerations on the current network application environment.

The above three commands provide you with flexible application strategies. You can select the appropriate configuration command according to the specific network application environment. To help you configure easily, the following configuration table is provided for your reference:

	Solution 1	Solution 2	Solution 3
User environment	One port for any user	One port for one user	One port for multiple users
Whether the Ruijie supplicant should be used as the authentication client	Yes	No	No
Configuration command recommended	Not necessary to enable the dot1x auto-req function	<b>dot1x auto-req</b>  <b>dot1x auto-req packet-num num</b>  <b>dot1x auto-req req-interval interval</b>  <b>dot1x auto-req user-detect</b>	<b>dot1x auto-req</b>  <b>dot1x auto-req packet-num 0</b>  <b>dot1x auto-req req-interval interval</b>  <b>no dot1x auto-req user-detect</b>

## Configuring 802.1x Accounting

Our 802.1x has implemented the accounting function. Accounting is based on interval. In other words, the 802.1x records the length of the period between the first successful authentication of the user and the user's logoff or when the switch detects user disconnection.

After the first successful user authentication, the switch sends an accounting start request to the server. When the user gets off-line or the switch finds that the user has got off line or when the physical connection of the user is broken, the switch sends an accounting end request to the server. The server

group records this information in the database of the server group. Based on such information, the NMS can provide the basis for accounting.

Our 802.1x stresses the reliability of accounting, and it specially supports the backup accounting server to avoid failures of the accounting server. When a server can no longer provide the accounting service due to various reasons, the switch will automatically forward the accounting information to another backup server. This greatly improves the reliability of accounting.

When a user exits by itself, the accounting duration is accurate. When the connection of the user is broken by accident, the accounting accuracy depends on the re-authentication interval (the switch detects the disconnection of a user by using the re-authentication mechanism).

To enable the accounting function of the device, the following settings are necessary on the device:

1. On the Radius Server, register the switch as a Radius Client, like the authentication operation.
2. Set the IP address of the accounting server.
3. Set the accounting UDP port.
4. Enable the accounting service on the precondition that the 802.1x has been enabled.

In the privileged EXEC mode, you can set the accounting service by performing the following steps:

Command	Function
<b>configure terminal</b>	Enter the global configuration mode.
<b>aaa new-model</b>	Enable the AAA function
<b>aaa group server radius gs</b>	Configure the accounting server group.
<b>server 192.168.4.12 acct-port 11</b>	Add a server to the server group.
<b>exit</b>	Return to the global configuration mode.
<b>aaa accounting network acct start-stop group gs</b>	Configure the accounting method list.
<b>dot1x accounting acct</b>	Apply the accounting method list for the 802.1X.
<b>end</b>	Return to the privileged EXEC mode.
<b>write</b>	Save the configuration.
<b>show running-config</b>	Show the configuration.

The **no aaa accounting network** command deletes the accounting method list. The **no dot1x accounting** command restores the default dot1x accounting method. The following example sets the IP address of the accounting server to 192.1.1.1, that of the backup accounting server to 192.1.1.2, and the UDP port of the accounting server to 1200, and enables 802.1x accounting:

```
Ruijie# configure terminal
Ruijie(config)# aaa new-model
Ruijie(config)# aaa group server radius acct-use
Ruijie(config-gs-radius)# server 192.168.4.12 acct-port 1200
Ruijie(config-gs-radius)# server 192.168.4.13 acct-port 1200
Ruijie(config-gs-radius)# exit
Ruijie(config)# aaa accounting network acct-list start-stop group acct-use
```



```
Ruijie(config)# dot1x accounting acct-list
Ruijie(config)# end
Ruijie# write memory
Ruijie# show running-config
```



### Caution

1. The agreed accounting key must be the same as that of the Radius Server and authentication.
2. The accounting function cannot be enabled unless the AAA is enabled.
3. The accounting is impossible unless the 802.1X authentication passes.
4. By default, the accounting function of the 802.1x is disabled.
5. For the database format of accounting, see the related Radius Server documentation.

Also, the account update is supported. After the account update interval is set on the NAS device, the NAS device will send account update packets to the Radius Server at periodical intervals. On the Radius Server, you can define the number of periods before which the account update packet of a user is not received from the NAS device, the NAS or user will be regarded as off-line. Then, the Radius Server can stop the accounting of the user, and delete the user from the on-line user table.

In the privileged EXEC mode, you can set the account update function by performing the following steps:

Command	Function
<b>configure terminal</b>	Enter the global configuration mode.
<b>aaa new-model</b>	Enable the AAA function
<b>aaa accounting update</b>	Set the account update function.
<b>end</b>	Return to the privileged EXEC mode.
<b>write</b>	Save the configuration.
<b>show running-config</b>	Show the configuration.

You can disable the account update service by using the **no aaa accounting update** command.

```
Ruijie# configure terminal
Ruijie(config)# aaa accounting update
Ruijie(config)# end
Ruijie# write memory
Ruijie# show running-config
```

The following chapters introduce the propriety features of Ruijie's network products:

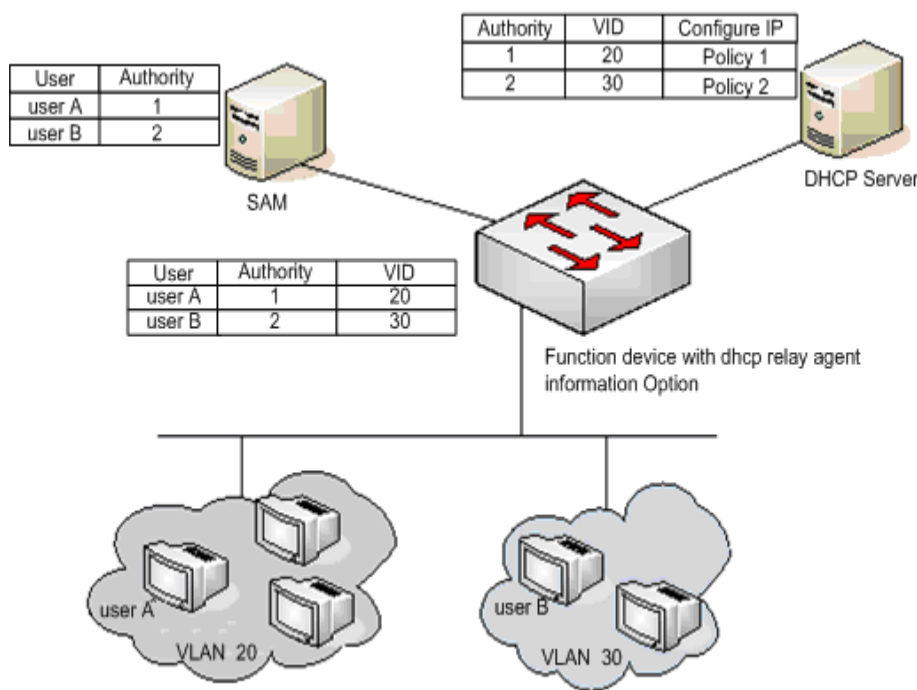
To make it easy for broadband operators and to accommodate use in special environments, our 802.1x has been expanded on the basis of the account (such expansion is completely based on the standard, and has totally compatible with IEEE 802.1x).

## Configuring the IP authorization mode

The 802.1x implemented by Ruijie Network can force the authenticated users to use fixed IP. By configuring the IP authorization mode, the administrator can limit the way the user gets IP address. There are four IP authorization modes: DISABLE, DHCP SERVER, RADIUS SERVER and SUPPLICANT. They are detailed below respectively:

**DISABLE mode (default):** The device has no limitation for the user IP, and the user only needs to pass the authentication to be able to access the network.

**DHCP SERVER mode:** The user IP is obtained via specified DHCP SERVER, and only the IP allocated by the specified DHCP SERVER is considered legal. For the DHCP mode, it is possible to use DHCP relay option82 to implement a more flexible IP allocation policy with the 802.1X. Here is a typical diagram for the plan:



The user initiates IP requests via the DHCP Client. The network device with dhcp relay option82 converges the user authority on the SAM server to construct the option82 field and encapsulate it in the DHCP request message. That option82 field consists of "vid + permission". The DHCP Server chooses different allocation policies by using the option82 field.

In this mode, it is required to configure the DHCP Relay and the related option82. If the DHCP relay function is enabled and the option82 policy is selected, see the DHCP Relay Configuration Guide and Command References for the configurations.

**RADIUS SERVER mode:** The user IP is specified by the RADIUS SERVER. The user can only use the IP specified by the RADIUS SERVER to be able to access the network.

**SUPPLICANT mode:** The IP bound to the user is the IP of the PC during the SUPPLICANT's authentication. After the authentication, the user can only use that IP to be able to access the network.

The application models in the four modes are as follows:

- **DISABLE mode:** Suitable for the environment with no limits for the users. The user can access the network once he/she passes the authentication.
- **DHCP SERVER mode:** The user PC gets the IP address via DHCP. The administrator configures the DHCP RELAY of the device to limit the DHCP SERVER that the users can access. In this way, only the IPs allocated by the specified DHCP SERVER are legal.
- **RADIUS SERVER mode:** The user PC uses fixed IP. The RADIUS SERVER is configured with <user-IP> mapping relations that are notified to the device via the

Framed-IP-Address attributes of the device. The user has to use that IP to be able to access the network.

- **SUPPLICANT mode:** The user PC uses fixed IP. The SUPPLICANT notifies the information to the device. The user has to use the IP at authentication to be able to access the network.



### Caution

When the user switches modes, it will cause all authenticated users to get offline. So, it is recommended to configure the authentication mode before the use.

In the privileged EXEC mode, configure the IP authorization mode as follows:

Command	Function
<b>configure terminal</b>	Enter the global configuration mode.
<b>aaa new-model</b>	Enable the AAA function
<b>aaa authorization ip-auth-mode {disabled   dhcp-server   radius-server   supplicant }</b>	Configure the IP authorization mode
<b>end</b>	Return to the privileged EXEC mode.
<b>write</b>	Save the configuration.
<b>show running-config</b>	Show the configuration.

The example below configures the IP authorization mode as the RADIUS-SERVER mode:

```
Ruijie# configure terminal
Ruijie(config)# aaa authorization ip-auth-mode radius-server
Ruijie(config)# end
Ruijie# show running-config
!
aaa new-model
!
aaa authorization ip-auth-mode radius-server
!
Ruijie# write memory
```

## Releasing Advertisement

Our 802.1x allows you to configure the Reply-Message field on the Radius Server. When authentication succeeds, the information of the field is shown on our 802.1x client of Star-Supplicant, by which the operators can release some information.

Such information is shown at the first user authorization, but not at re-authentication. This avoids frequently disturbing the user.

The window for showing the advertisement information supports html, which converts the http://XXX.XXX.XX in the message into links capable of direct switching, for easier browsing.

Releasing of the advertising information:

1. The operator configures the Reply Message attribute on the Radius Server end.
2. Only our Star-supplicant client supports such information (free for the users of our switch),

Command	Function
<b>configure terminal</b>	Enter the global configuration mode.
<b>dot1x</b> <b>auth-address-table</b> <b>address</b> <i>mac-addr</i> <b>interface</b> <i>interface</i>	Set the list of the hosts that can be authenticated.
<b>end</b>	Return to the privileged EXEC mode.
<b>write</b>	Save the configuration.
<b>show running-config</b>	Show the configuration.

while other clients cannot see the information, which however does not affect their normal use.

3. No setting is required at the device end.

## List of Authenticable Hosts under a Port

For enhanced security of the 802.1x, we have made expansion without affecting the IEEE 802.1x, allowing the NM to restrict the list of hosts authenticated of a port. If the list of hosts authenticated of a port is empty, any user can be authenticated. If the list is not empty, only the hosts in the list can be authenticated. The hosts that can be authenticated are identified by using the MAC addresses.

The following example adds/deletes the hosts that can be authenticated under a port.



### Caution

If the list of the host is empty, the port allows any host to be authenticated.

## Authorization

To make it easier for operators, our products can provide services of different qualities for different types of services, for example, offering different maximum bandwidths. Such information is all stored on the Radius Server, and the administrator does not need to configure every switch.

Since the Radius has no standard attribute to represent the maximum data rate, we can only transfer the authorization information by the manufacturer customized attribute.

The general format of the definition is as follows:

```

0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-----+-----+-----+-----+-----+-----+-----+-----+
|  Type      | Length      | Vendor-Id      |
+-----+-----+-----+-----+-----+-----+-----+
| Vendor-Id (cont) | Vendor type | Vendor length |
+-----+-----+-----+-----+-----+-----+-----+
| Attribute-Specific... |
+-----+-----+-----+-----+-----+-----+

```

For the maximum data rate, you need to fill in the following values:

0x1A	0x0c	0x00	0x00
0x13	0x11	0x01	0x06
Hex value of the maximum data rate			

The unit of the maximum data rate is kbps.

For users with the maximum data rate of 10M, you need to fill in the following values:

0x1A	0x0c	0x00	0x00
0x13	0x11	0x01	0x06
0x00002710			

For the customized header, follow those provided above. The maximum data rate is 10M, that is, 10000kbps, and makes 0x00002710 in the Hex system. You only need to fill in the corresponding field. This function calls for no settings on the device end, and works as long as the device end supports authorization.

## Configuring the Authentication Mode

In the standard, the 802.1x implements authentication through the EAP-MD5. The 802.1X designed by Ruijie can perform authentication through both the EAP-MD5 (default) mode and the CHAP and PAP mode. The advantage of the CHAP is that it reduces the communication between the switch and the RADIUS SERVER, thus alleviating the pressure on the RADIUS SERVER. Same as the CHAP mode, the communication between the PAP and RADIUS SERVER occurs only once. Although the PAP mode is not recommended for its poor security, it can meet the special needs of the user in some cases. For example, when the security server used only supports the PAP authentication mode, this mode can be selected to fully exploit the existing resources, protecting the existing investment.

In the privileged EXEC mode, you can set the authentication mode of the 802.1x by performing the following steps:

Command	Function
<b>configure terminal</b>	Enter the global configuration mode.
<b>dot1x auth-mode mode</b>	Configure the authentication mode
<b>end</b>	Return to the privileged EXEC mode.
<b>write</b>	Save the configuration.
<b>show dot1x</b>	Show the configuration.

The following example configures the authentication mode to the CHAP mode:

```
Ruijie# configure terminal
```

```

Ruijie(config)# dot1x auth-mode CHAP
Ruijie(config)# end
Ruijie# show dot1x
802.1X Status:      Disabled
Authentication Mode: CHAP
Authed User Number: 0
Re-authen Enabled:  Disabled
Re-authen Period:   3600 sec
Quiet Timer Period:  10 sec
Tx Timer Period:     3 sec
Supplicant Timeout:  3 sec
Server Timeout:      5 sec
Re-authen Max:       3 times
Maximum Request:     3 times
Filter Non-RG Supp:  Disabled
Client Oline Probe:  Disabled
Eapol Tag Enable:    Disabled
Authorization Mode:   Group Server

```

## Configuring the backup authentication server.

Our 802.1x-based authentication system can support the backup server. When the master server is down due to various reasons, the device automatically issues a server submission authentication request to the method list server group.

In the privileged EXEC mode, you can set the backup authentication server by performing the following steps:

Command	Function
<b>configure terminal</b>	Enter the global configuration mode.
<b>aaa new-model</b>	Turn on the AAA switch.
<b>aaa group server radius</b> <i>gs-name</i>	Configure the server group.
<b>server sever</b>	Configure the server.
<b>server server-backup</b>	Configure the backup server.
<b>End</b>	Return to the privileged EXEC mode.
<b>Write</b>	Save the configuration.
<b>show dot1x</b>	Show the configuration.

The following example configures 192.168.4.12 to be the backup server:

```

Ruijie# configure terminal
Ruijie# aaa new-model
Ruijie(config)# aaa group server radius auth-11
Ruijie(config-gs-radius)# server 192.168.4.1
Ruijie(config-gs-radius)# server 192.168.4.12
Ruijie(config-gs-radius)# end
Ruijie#

```

## Configuring and Managing Online Users

Ruijie's devices provide management for authenticated users via SNMP. The administrator can view the information of the authorized users via SNMP, and forcedly log off a user. The user forcedly logged off must pass the authentication again before it can use network resources.

This function calls for no configuration on the device.

## Implementing User-IP Binding

With our clients and by correctly configuring the Radius Server, you can implement unique user-IP binding. A user must undergo authentication by using the IP address allocated by the administrator. Otherwise, authentication will fail.

For this function, you do not need to configure the switch. The user needs to use our client and the administrator needs to configure the Radius Server.

## Port-based Traffic Charging

In addition to the duration-based billing, Ruijie's network devices provide the traffic-based billing function in case each port of the equipment has only one user access.

This function calls for no configuration on the device but need the support of the Radius server.

## Implementing Automatic Switching and Control of VLAN

To implement the auto-switching of the dynamic VLAN, the user VLAN shall be assigned and configured by the remote RADIUS server. The remote RADIUS server encapsulates the VLAN assignment information through the defined RADIUS attributes. After receiving those information and the user authentication, the access device automatically adds the port where the user is to the VLAN assigned by the RADIUS server. It is unnecessary of the manual configurations for the administrator.

You shall use the **show dot1x summary** command to on the access device to view the actual VLAN where the user is. Use the **show dot1x user id** command to view the VLAN assigned by the RADIUS server.

The access device is able to receive the VLAN assigned by the RADIUS server in two ways of the extension RADIUS attributes and the standard RADIUS attributes.

The RADIUS server assigns the VLAN to the access device using the standard-extension attributes. The server encapsulates the extension attributes into the No.26 RADIUS standard attributes. The extension manufacturing ID is in hex 0x00001311. By default, the extension attribute type is 4, you can use the **radius attribute 4 vendor-type type** command to set the extension attribute type number to assign the VLAN. For the configuration command, see *RADIUS Configuration*.

The access device supports the RADIUS server to use the standard RADIUS attributes to assign the VLAN, including the following attribute combinations:

- No.64 Attribute Tunnel-Type
- No.65 Attribute Tunnel-Medium-Type
- No.81 Attribute Tunnel-Private-Group-ID

And for the auto-switching of the dynamic VLAN application, the valid range is:

- Tunnel-Type=VLAN(13)
- Tunnel-Medium-Type=802(6)
- Tunnel-Private-Group-ID=VLAN ID or VLAN Name

For the details, see the RFC2868 and the RFC3580.

The processing steps of receiving the assigned VLAN for the access device are: 1. use the assigned VLAN attribute as the VLAN name and view that whether there is the same VLAN name on the access device; 2. if there is the same VLAN name, the port where the user is swithes to the VLAN automatically; if there is no same VLAN name, then the assigned VLAN attribute will be used as the VLAN ID; 3. if the VLAN ID is valid(within the VLAN ID range of the system supported), the port where the user is auto-switches to this VLAN; if the VLAN ID is 0, no VLAN assignment information exist; 4. except for those conditions mentioned above, the user authentication is faulty.

Only the ACCESS port and the TRUNK port are supported by the access device for the 802.1x authentication. In other port modes, it fails to enable the auto-switching function of the dynamic VLAN. The following describes the conditions of the VLAN auto-switching function on the ACCESS and TRUNK ports:

#### 1. VLAN auto-switching function on the ACCESS port

Without the assigned VLAN configured on the device, if the assigned VLAN is identified as the VLAN ID by the device, the device will create the VLAN with the corresponding VLAN ID and switch the auth-port to the newly- created VLAN; while if the assigned VLAN is identified as the VLAN name by the device, the user authentication will be faulty.

With the assigned VLAN configured on the device, if the assigned VLAN is set as the VLAN not supporting the auto-switching on the ACCESS port, the user authentication will be faulty; while if the assigned VLAN is set as the VLAN supporting the auto-switching on the ACCESS port, the user authentication and the auto-switching implementation of the assigned VLAN will be successful.

The following lists the VLANs not supporting the auto-switching on the ACCESS port:

- Private VLAN
- Remote VLAN
- Super VLAN, including Sub VLAN

#### 2. Native VLAN configuration on the TRUNK port

For the TRUNK port with the authentication enabled, set the assigned VLAN as the Native VLAN for the port to be authenticated.

Without the assigned VLAN configured on the device, if the assigned VLAN is identified as the VLAN ID by the device, the Native VLAN for the port to be authenticated will be set as the assigned VLAN; while if the assigned VLAN is identified as the VLAN name by the device, the user authentication will be faulty.

With the settings of the assigned VLAN configured on the device, if the assigned VLAN is set as the VLAN not supporting the auto-switching on the TRUNK port, the user authentication will be faulty; while if the assigned VLAN is set as the VLAN supporting the



auto-switching on the TRUNK port, the user authentication will be successful and the Native VLAN for the port to be authenticated will be set as the assigned VLAN.

The following lists the VLANs not supporting the auto-switching on the TRUNK port:

- Private VLAN
- Remote VLAN
- Super VLAN, including Sub VLAN

### 3. Native VLAN configuration on the HYBRID port

For the HYBRID port with the MAC VLAN disabled, handling methods for the assigned VLAN are as below:

Without the assigned VLAN configured on the device, if the assigned VLAN is identified as the VLAN ID, the device will automatically create the corresponding VLAN and allows the assigned VLAN to pass current HYBRID port without TAG, and changes the Native VLAN of the port to the assigned VLAN. In such case, the user authentication will be successful. While if the assigned VLAN is identified as the VLAN name and the corresponding VLAN ID cannot be found by the device, the user authentication will be faulty.

With the settings of the assigned VLAN configured on the device, if the assigned VLAN is set as the VLAN not supporting the auto-switching on the HYBRID port, or the designated VLAN has existed in the TAG VLAN list carried by the HYBRID port, the user authentication will be faulty; or else, the assigned VLAN can pass the current HYBRID port without TAG and the Native VLAN of the port is changed to the assigned VLAN. In such case, the user authentication will be successful.

With the MAC VLAN enabled on the HYBRID port, handling methods for the assigned VLAN are as blow:

If the VLAN assigned by the authentication server is not existent in the device (MAC VLAN requires that the corresponding VLAN must be statically configured and existent), or the assigned VLAN has been added to the HYBRID port with TAG carried, or the VLAN type is not supported by MAC VLAN (see the description in MAC-VLAN-SCG.doc), the user authentication will be faulty; or else, the device creates the MAC VLAN entry dynamically according to the authentication server assigned VLAN and user MAC address, the user authentication will be successful.

When the user goes offline, the MAC VLAN entry is deleted dynamically.

The following lists the VLANs not supporting the auto-switching on the HYBRID port:

- Private VLAN
- Remote VLAN
- Super VLAN, including Sub VLAN

**Note**

1. When the MAC VLAN is not enabled on the port, VLAN assignment changes the Native VLAN of this port, but the Native VLAN configured by commands is not changed. The priority of the assigned VLAN is higher than the VLA configured by commands. That is, the Native VLAN that takes effect after the authentication is assigned VLAN, and the Native VLAN configured by commands takes effect after the user goes offline.
2. When the MAC VLAN is enabled on the port and the authentication mode is based on MAC, VLAN assignment is implemented through dynamically generating MAC VLAN entry without changing the Native VLAN of this port.
3. For the HYBRID port with MAC VLAN enabled or disabled, VLAN assignment will fail if the assigned VLAN has been added to the port with TAG carried.
4. If the MAC VLAN is enabled on the port, VLAN assignment will create the MAC VLAN entry with the network mask being all Fs. If the MAC address of 802.1x user is overridden by the statically configured MAC address in the MAC VLAN entry with the network mask being not all Fs, the two MAC addresses must be same; otherwise, the following abnormalities about 802.1x users of VLAN assignment will occur: (The following listed do not cover all abnormalities)
  - 1) 802.1x users can be authenticated successfully, but the legal data packets will be dropped after the authentication, resulting in network access failure.
  - 2) After the user sends EAPOL-LOGOFF message to goes offline, the authentication server still shows that user is online as the 802.1x authentication entry is still in the device.

To enable the dynamic VLAN auto-switching function on an interface, run the following commands:

- 1) enable the AAA function

Command	Function
<b>configure terminal</b>	Enter the global configuration mode.
<b>aaa new-model</b>	Enable the AAA function

For the details, see *AAA Configuration*.

- 2) set the RADIUS server

Command	Function
<b>configure terminal</b>	Enter the global configuration mode.
<b>radius-server host <i>host-ip</i></b>	Configure the RADIUS server.
<b>radius-server key <i>text</i></b>	Configure the RADIUS server shared key.

For the details, see *RADIUS Configuration*.

## 3) enable the method list

Command	Function
<b>configure terminal</b>	Enter the global configuration mode.
<b>aaa authentication dot1x list1 group radius</b>	Configure the authentication method list1.
<b>aaa accounting network list2 start-stop group radius</b>	Configure the accounting method list2.

For the details, see *AAA Configuration*.

## 4) 802.1x method list

Command	Function
<b>configure terminal</b>	Enter the global configuration mode.
<b>dot1x authentication list1</b>	Select the authentication method list1.
<b>dot1x accounting list2</b>	Select the accounting method list2.

## 5) enable the 802.1x authentication on the interface

Command	Function
<b>configure terminal</b>	Enter the global configuration mode.
<b>interface interface_id</b>	Enter the interface configuration mode.
<b>dot1x port-control auto</b>	Enable the 802.1x authentication on the interface.

## 6) enable the VLAN auto-switching on the interface

Command	Function
<b>configure terminal</b>	Enter the global configuration mode.
<b>interface interface_id</b>	Enter the interface configuration mode.
<b>dot1x dynamic-vlan enable</b>	Enable the VLAN auto-switching on the interface.

For the VLAN auto-switching function, the dynamic switching must be enabled on the interface. That is, use the **dot1x dynamic-vlan enable** command in the interface configuration mode. Or the RADIUS attributes of the encapsulated assigned VLAN will be ignored.

**Caution**

In the interface configuration mode, the **dot1x dynamic-vlan enable** command must be configured after the **dot1x port-control auto** command has been configured. With the **dot1x port-control auto** command configured, the VLAN auto-switching function is disabled.

The private vlan does not support the dynamic VLAN switching function. That is, the private vlan cannot be set as the 802.x dynamic vlan.

7) view the dynamic VLAN auto-switching settings

Command	Function
<b>show dot1x user id</b> <i>session_id</i>	View the user information in <i>session-id</i> , including the dynamic VLAN auto-switching information.
<b>show dot1x summary</b>	View the actual VLAN where the user is.

For the related precautions, see the chapter of *Other Precautions of 802.1x Configuration*.

## Implementing GUEST VLAN Function

With the GUEST VLAN function enabled on the port, this port will be added to the guest vlan if any of the following conditions is met:

1. No EAPOL response packet is received within 90 seconds.
2. Failed MAC address authentication in MAC mode.
3. The port will successively send out authentication packets for three times. No EAPOL response packet is received within  $\text{auto-req req-interval} \times 3$ .

Use **show running-config** to view the configuration and **show vlan** to check whether the port jumps to guest vlan or not .

Follow these steps to configure a port whether to be allowed to jump to **GUEST VLAN** or not:

Command	Function
<b>configure terminal</b>	Enter the global configuration mode.
<b>interface</b> <i>interface</i>	Enter the interface configuration mode.
<b>dot1x dynamic-vlan enable</b>	Allow Vlan jump on the interface.
<b>[no] dot1x guest-vlan</b> <i>vid</i>	Configure whether to enable guest vlan, which is disabled by default.
<b>end</b>	Return to the privileged EXEC mode.
<b>write</b>	Save the configuration.
<b>show running-config</b>	Show the configuration.

## Shielding Proxy Server and Dial-up

The two major potential threats to network security are: The user sets its own proxy server and the user makes dial-up to access the network after authentication. Star switches provide the function to shield proxy servers and dial-up connections.



1. **Guest vlan** takes effect unless you configure **dot1x dynamic-vlan enable**.
2. It is better not to configure L2 attributes when configuring **guest vlan**, especially not to set **vlan** on the port manually.
3. After the port is added to **guest vlan**, if there is eapol packet received on this port or the port state is switched from linkup to linkdown, the port will exit **guest vlan**.
4. If you configure **guest vlan** on the port, it will check whether the port is added to **guest vlan** when the port state is switched from linkdown to linkup.

To implement this function needs no settings on the device end and needs only the corresponding attributes configured on the Radius server end. Since the Radius has no standard attributes to indicate the maximum data rate, we can transfer the authorization information only through the manufacturer custom attributes. For the general format defined, see the Authorization section.

The proxy server shielding function defines the Vendor type of 0x20, and the dial-up shielding function defines the Vendor type of 0x21.

The Attribute-Specific field is a 4-byte manufacturer defined attribute, which defines the actions taken against proxy server access and dial-up access. 0x0000 means normal connection, without shielding detection. 0x0001 means shielding detection.

To shield the access via the proxy server, you should fill in the following information:

```

+++++
| 0x1A | 0x0c | 0x00 | 0x00 |
+++++
| 0x13 | 0x11 | 0x20 | 0x06 |
+++++
| 0x0001 |
+++++

```

To shield the access via the dial-up connection, you should fill in the following information:

```

+++++
| 0x1A | 0x0c | 0x00 | 0x00 |
+++++
| 0x13 | 0x11 | 0x21 | 0x06 |
+++++
| 0x0001 |
+++++

```

## Configuring On-line Probe on Client End

To ensure accurate charging, an on-line probe mechanism is needed to detect whether a user is on-line within a short period. The re-authentication mechanism specified in the standard can meet such needs, but it needs the participation of the RADIUS server. Accurate user probe will occupy enormous resources of the switch and RADIUS server. To meet the need to implement accurate charging with few resources occupied, we use a new client on-line probe mechanism. Such mechanism only needs interaction between the switch and client and occupies little network traffic, and it implements minute-level charging accuracy (you can set the charging accuracy).



### Caution

To implement on-line client monitoring, the client software must support this function.

The following two timers affect the performance and accuracy of on-line probe:

- Hello Interval: It is the interval at which the client sends advertisement.
- Alive Interval: Client online interval. If the device has not received the client advertisement during this interval, it actively disconnects the client and notifies the billing server. The interval must be greater than the Hello Interval.

In the privileged EXEC mode, you can configure the on-line probe function of the client by performing the following steps:

Command	Function
<b>configure terminal</b>	Enter the global configuration mode.
<b>Dot1x client-probe enable</b>	Enable the on-line probe function of the client

Command	Function
<b>Dot1x probe-timer interval</b> <i>interval</i>	Configure the Hello Interval
<b>Dot1x probe-timer alive interval</b>	Configure the Alive Interval of the device.
<b>end</b>	Return to the privileged EXEC mode.
<b>write</b>	Save the configuration.
<b>show dot1x</b>	Show the configuration.

## Configuring the Option Flag for EAPOL Frames to Carry TAG

In accordance with IEEE 802.1x, the EAPOL packets cannot be added with vlan TAG. However, based on the possible application requirements, the selection flag is provided. When the flag is turned on, tags can be outputted according to the related output rule of the trunk ports.

The typical application environment is to enable 802.1x authentication on the convergence layer. For more information, see “Topologies of Typical Applications”.

In the privileged EXEC mode, you can configure the flag for EAPOL frames to carry TAG by performing the following steps:

Command	Function
<b>configure terminal</b>	Enter the global configuration mode.
<b>dot1x eapol-tag</b>	Enable the flag for EAPOL frames to carry TAG. By default, the function is disabled.
<b>end</b>	Return to the privileged EXEC mode.
<b>write</b>	Save the configuration.
<b>show dot1x</b>	Show the configuration.

You can disable this function by using the **no dot1x eapol-tag** command.

## Configuring Port-based Authentication

The 802.1x controls users on the basis of their MAC addresses by default. Only the authenticated user can use the network. With port-based authentication, the port is authenticated as long as a user is authenticated on a port. Consequently, all users connecting to this port can access the network.

To configure port-based control mode, execute the following commands in the privileged EXEC mode.

Command	Function
<b>configure terminal</b>	Enter the global configuration mode.
<b>interface</b> <interface-id>	Enter the interface mode
<b>dot1x port-control auto</b>	Enable the function being controlled.
<b>dot1x port-control-mode</b> {mac-based port-based}	Select the controlled mode.
<b>end</b>	Return to the privileged EXEC mode.
<b>write</b>	Save the configuration.
<b>show dot1x port-control</b>	Show the configuration of port 802.1X.

You can run **no dot1x port-control-mode** to restore the settings to the default control mode. Following example shows how to configure the authentication mode of a port.

```
Ruijie(config)#
Ruijie# configure terminal
Ruijie(config)# interface gigabitEthernet 4/5
Ruijie(config-if)# dot1x port-control-mode port-base
```



#### Caution

In the port-based authentication mode, a port can be connected with only one authenticated user.

Port-based authentication mode can enable or disable dynamic users to migrate among multiple authenticated ports. By default, the migration is allowed. To prohibit the migration, run the following commands one by one in the privileged EXEC mode.

Command	Function
<b>configure terminal</b>	Enter the global configuration mode.
<b>dot1x stationarity enable</b>	Disable the migration among ports.
<b>end</b>	Exit to the privileged EXEC mode.
<b>write</b>	Save the configuration.

## Configuring Port-based Single-user Authentication

By default, 802.1x controls on the basis of user MAC. Only the authenticated users can use the network, while other users connected to the same port is not able to use the network. In the port-based control mode, the port is authenticated when there is an authenticated user on the port. All the users connected to the authenticated port are able to use the network normally.

However, in the port-based control mode, the port-based single-user authentication controls only one authenticated user. The port is authenticated when it allows only one authenticated user who is enable to use the network normally. Then, if you find other users on the port, you should clear all the users on the port and reauthenticate.

From the privileged EXEC mode, follow the steps below to configure port-based single-user control mode on the port.

Command	Function
<b>configure terminal</b>	Enter the global configuration mode.
<b>interface &lt;interface-id&gt;</b>	Enter the interface configuration mode.
<b>dot1x port-control auto</b>	Enable control function.
<b>dot1x port-control-mode port-based single-host</b>	Port-based single-user control mode.
<b>end</b>	Return to the privileged EXEC mode.



<b>write</b>	Save the configuration.
<b>show dot1x port-control</b>	Show 802.1x configuration.
<b>show running-config</b>	Show all configurations.

You can run `no dot1x port-control-mode` to restore the settings to the default control mode. Following example shows how to configure the authentication mode of a port.

```
Ruijie(config)#
Ruijie#configure terminal
Ruijie(config)#interface <interface-id>
Ruijie(config-if)#dot1x port-control-mode port-base single-host
```



#### Caution

In the port-based authentication mode, every port only can receive one authentication user.

Single-host is port-based single-user 802.1x access control. Use **show dot1x port-control** to display port-based and use **show running-config** to display dot1x port-control-mode port-based single-host.

Since single-host only supports the single-user form, setting default-user-limit on the port manually does not take effect in single-host mode. If you set default-user-limit on the port after setting single-host, only one user can be permitted to use the network still.

In the port-based authentication mode, you can permit or deny dynamic users to migrate among multiple authentication ports, which is permitted by default. If you want to deny the migration of dynamic users, follow the steps below from the privileged EXEC mode.

Command	Function
<b>configure terminal</b>	Enters the global configuration mode.
<b>dot1x stationarity enable</b>	Prohibits migration between ports.
<b>end</b>	Returns to the privileged EXEC mode.
<b>write</b>	Saves the configuration.

## Configuring Dynamic Acl Assignment

802.1x supports ACL assignment from server and dynamic installation of the assigned ACL. Our product support installing acl by default. They will install acl dynamically on condition that the allowed acl is set on the server and is assigned after the successful user authentication.

To implement dynamic acl assignment, you need to set the port as mac-based authentication mode or port-based single-user authentication mode. The ACL assignment is not supported in the port-based multi-user authentication mode. For the configuration, please refer to the related command configuration manual.

In single-host authentication mode, it supports to renew acl when reauthenticating. That is, acl takes effect when the authenticated user sets acl on the server and reauthenticates.

The mac-based authentication mode does not support ACL update when re-authenticating. That is to say, ACL of the authenticated user can only be assigned once. The new acl is ignored and the original acl remains if the acl changes when re-authenticating.

**Caution**

Supported acl type: extension type which can explain acl function on our switch.

Execute the following command if you need to support dynamic acl assignment on the server which is not authenticated by our company.

```
Ruijie#configure terminal
Ruijie(config)# radius vendor-specific extend
```

## Configuring Dot1x MAC Authentication Bypass

GUEST VLAN provides a method of network accessing without the 802.1x authentication client, but this technology is unable to determine whether the access device is secure or insecure. In some conditions, for the network management and security, although there is no 802.1x authentication client, the administrator still needs to control the validity of the access device. MAB(MAC Authentication Bypass) provides a solution for this application.

With the MAB function enabled on the 802.1x authentication port, the authentication request packets are sent continuously to the port and the client response is expected. If there is no client response within the time of "tx-period\*reauth-max", the MAC address learned on the 802.1x authentication port will be monitored, and the authentication will be initiated by sending the username(the learned MAC address) and keyword to the server. It determines whether the learned MAC address is accessible to the network or not according to the returned authentication result from the server.

To configure the MAB function, run the following commands:

Command	Function
<b>configure terminal</b>	Enter the global configuration mode.
<b>interface</b> <interface-id>	Enter the interface configuration mode.
<b>dot1x mac-auth-bypass</b>	Set the dot1x MAC authentication bypass.
<b>end</b>	Return to the privileged EXEC mode.
<b>Write</b>	Save the configurations.
<b>show running-config</b>	Show all configurations.

Following example shows how to configure the MAB function.

```
Ruijie# configure terminal
Ruijie(config)# interface fa 0/1
Ruijie(config-if)# dot1x port-control auto
Ruijie(config-if)# dot1x mac-auth-bypass
```



- Use the format XXXXXXXXXXXX when setting the username and keyword for the MAC address on the server.
- With the port in the MAB mode, only one MAC address that firstly found by the device can be used for the authentication.
- One port for one MAC address authentication is supported in both the port mode and the MAC mode.
- Anytime when the client responses the 802.1x authentication, the MAB on the port takes no effect unless the link state down/up change occurs or the 802.1x function on the port is re-enabled.
- The client online probe function takes no effect for the MAC authentication in the MAB mode.
- With MAB port configured, an authentication request packet is sent at the interval of tx-period. After sending the packets for reauth-max times, if there is no client response, the port enters to the MAB mode. The port in the MAB mode can learn the MAC address and use the learned MAC address as the username for the authentication.
- MAB supports the PAP, CHAP, EAP-MD5 authentication methods. For how to configure the authentication method, see the chapter in *Authentication Method Configuration*.
- In the MAB mode, after the MAC address authentication failure, if the guest vlan has been configured, the authentication port will enter the guest vlan; if the guest vlan has not been configured, the port stays in the original vlan. The MAB does not support auth-fail VLAN, that is, even though the MAB authentication fails and the auth-fail VLAN has been configured, the port will not enter the auth-fail VLAN.
- If one MAC address has passed the MAB authentication for one port and it appears on other ports, the MAB violation will be set for the latter port.
- MAB cannot be co-used with the security channel.
- The MAB authentication is invalid for the static address and the filtering address.
- The MAB authentication offers the access-auth service for the device without the auth-client software. Those devices generally cannot recognize the 802.1Q TAG labels. To this end, it is recommended that the MAB-auth function shall be set on the ACCESS port. Otherwise, even though it passes the authentication, the communication between the devices fails.
- When the GSN address binding function is enabled on the port, the user authenticated in MAB mode can not access the network.

## Configuring Dot1x MAC Authentication Bypass Timeout

After a MAC address authentication in the MAB mode is online, this MAC address will always be online unless the re-auth fails, the port is Down or it is forcibly offline due to the administration policy.

The user can configure the allowed online time of those authentication MAC address. 0 is the default value, indicating that the MAC address is always online.

To configure the MAB timeout, run the following commands:

Command	Function
<b>configure terminal</b>	Enter the global configuration mode.
<b>interface</b> <interface-id>	Enter the interface configuration mode.
<b>dot1x mac-auth-bypass timeout-activity</b> <value>	Set the MAB timeout time, in seconds. No default value and the valid range is 1-65535.
<b>end</b>	Return to the privileged EXEC mode.
<b>write</b>	Save the configurations.
<b>show running-config</b>	Show all configurations.

Following example shows how to configure the MAB timeout time.

```
Ruijie# configure terminal
Ruijie(config)# interface fa 0/1
Ruijie(config-if)# dot1x mac-auth-bypass timeout-activity 3600
```



- If the online time for the MAC address authentication is also assigned by the server, this online time is independent from the timeout-activity.
- After it times out, with guest vlan configured on the port, the port switches to the guest vlan. However, during the authentication, the response timeout for the server will not cause the MAB port in the guest vlan.

## Configuring Dot1x MAC Authentication Bypass Violation

By default, with one MAC address authenticated in the MAB mode, data of all devices under the port are allowed to be forwarded. However, in some safe applications, if only one MAC address is allowed for the MAB port by the administrator, configure the MAB violation. With the MAB violation configured, once the port enters the MAB mode, the violation occurs if there is more than one 1 Mac address for the port.

To configure the MAB violation on the interface, run the following commands:

Command	Function
<b>configure terminal</b>	Enter the global configuration mode.
<b>interface</b> <interface-id>	Enter the interface configuration mode.
<b>dot1x mac-auth-bypass violation</b>	Set the MAB violation.
<b>end</b>	Return to the privileged EXEC mode.
<b>Write</b>	Save the configurations.
<b>show running-config</b>	Show all configurations.

Following example shows how to configure the MAB violation.

```
Ruijie# configure terminal
Ruijie(config)# interface fa 0/1
Ruijie(config-if)# dot1x mac-auth-bypass violation
```



### Caution

- Use the **errdisable recover** command to restore the MAB violation port.
- The same MAC address for the port in the private vlan appears in the primary and the secondary VLAN simultaneously, so the MAB authentication violation shall not be configured on the port in the private vlan. Or it will lead to the MAB violation judgement error and influence the normal use.

## Configuring Dot1x Auth-Fail VLAN

With the auth-fail vlan configured on the switch, when the user authentication on the port fails, the port enters to the auth-fail vlan pre-configured.

To configure the auth-fail VLAN in the interface configuration mode, run the following commands:

Command	Function
<b>configure terminal</b>	Enter the global configuration mode.
<b>interface</b> <interface-id>	Enter the interface configuration mode.
<b>dot1x auth-fail vlan</b> <vid>	Set the auth-fail VLAN on the interface.
<b>end</b>	Return to the privileged EXEC mode.
<b>Write</b>	Save the configurations.
<b>show running-config</b>	Show all configurations.

Following example shows how to configure the auth-fail VLAN.

```
Ruijie# configure terminal
Ruijie(config)# interface fa 0/1
Ruijie(config-if)# dot1x auth-fail vlan 2
```



- If the configured vlan is inexistent, the vlan will be created dynamically when the port enters the auth-fail vlan, and will be auto-removed when the port exits from the auth-fail vlan.
- If the port is down, it will exit from the auth-fail vlan automatically.
- It allows setting the auth-fail vlan and the guest vlan in the same VLAN.
- In the port mode and in the auth-fail vlan, it only allows the last-auth-fail user for the re-auth, and the auth-requests of other users are dropped. This restriction is not applicable for the MAC mode.
- The auth-fail vlan does not support private vlan. That is, the private vlan cannot be set as the dot1x auth-fail vlan.
- When the GSN address binding function is enabled on the port, the auth-fail user cannot access the network.

## Configuring Dot1x Auth-Fail Max-Attempt

To configure the auth-fail max-attempt times, run the following commands:

Command	Function
<b>configure terminal</b>	Enter the global configuration mode.
<b>dot1x auth-fail max-attempt&lt;value&gt;</b>	Set the auth-fail max-attempt times, the default value is 3 and the valid range is 1-3.
<b>end</b>	Return to the privileged EXEC mode.
<b>Write</b>	Save the configurations.
<b>show running-config</b>	Show all configurations.

Following example shows how to configure the auth-fail max-attempt value.

```
Ruijie# configure terminal
Ruijie(config)# dot1x auth-fail max-attempt 2
```

## Configuring to permit MAC Move

By default, after an 802.1x user passes authentication on a certain port, the MAC address of this user will be bound to this port and is not allowed to present on any other port.

However, under certain circumstances, after user passes authentication, it may need to move to other ports. For example: a separate switch is deployed between 802.1x authentication enabled switch and user PC to connect them. When user directly pulls out the network cable and moves from port 1 to port 2, since port 1 didn't receive the Down event and is unaware that the user is disconnected, the PC connected to port 2 won't be able to pass authentication and access network.

To enable the user to access network after being switched to port 2, configure to allow MAC move in global configuration mode. When user appears on port 2, the user on port 1 will be forced to disconnect

from network, and re-authentication will be initiated on port 1. The user can move between different ports of the same device or even across different devices. The user can also move between controlled ports, or move from a controlled port to an uncontrolled port.

Execute the following steps to allow MAC move:

Command	Function
Ruijie# <b>configure terminal</b>	Enter global configuration mode.
Ruijie(config)# <b>dot1x mac-move permit</b>	Enable MAC move.
Ruijie(config)# <b>end</b>	Return to privileged EXEC mode.
Ruijie# <b>show dot1x</b>	Display 802.1x global configurations.

Configuration example:

```
Ruijie# configure terminal
Ruijie(config)# dot1x mac-move permit
```



#### Caution

1. If there is MAC address spoofing on the network, after enabling MAC move, authenticated users may be preempted by fake users.
2. If the user doesn't move to another port but change IP address on the original port or unplug/replug the network cable, the re-authentication process will be triggered.
3. If user's MAC address is configured as a static MAC address, the user won't be able to move.

## Configuring Inaccessible Authentication Bypass

When all RADIUS servers configured on the switch are inaccessible, the user's authentication request won't receive any reply, and the administrator won't be able to verify user's identity. From the perspective of user, if no other authentication method is configured on the switch, it won't be able to access the network. To ensure that the new authenticated user can access network, Inaccessible Authentication Bypass (IAB) can be configured on the port.

Execute the following steps to enable IAB:

Command	Function
Ruijie# <b>configure terminal</b>	Enter global configuration mode.
Ruijie(config)# <b>interface &lt;interface-id&gt;</b>	Enter interface configuration mode.
Ruijie(config-if)# <b>dot1x critical</b>	Configure Inaccessible Authentication Bypass.
Ruijie(config-if)# <b>end</b>	Return to privileged EXEC mode.
Ruijie# <b>show running-config</b>	Display all configurations.

The following example shows how to configure Inaccessible Authentication Bypass:

```
Ruijie# configure terminal
Ruijie(config)# interface fa 0/1
Ruijie(config-if)# dot1x port-control auto
Ruijie(config-if)# dot1x critical
```

After IAB is enabled on the port and all servers become inaccessible:

1. IAB will take effect only if the globally configured 802.1x authentication method list contains only RADIUS authentication method and all RADIUS servers have failed. If there are other authentication methods in the list (such as local, none, etc), IAB won't take effect.
2. After globally enabling AAA multi-domain authentication, the globally configured authentication method list won't be adopted during 802.1x user authentication. Since IAB will directly allow the user to pass authentication without the need to enter username after the RADIUS servers in 802.1x authentication method list have all failed, AAA multi-domain authentication will fail on this port.
3. IAB-authenticated users won't send accounting request to the accounting server.
4. Normally authenticated users won't be affected and can still access network.
5. With 802.1x IP authorization enabled globally, if there is authenticated user on the port, the other users on this port cannot be authenticated in IAB mode.
6. With GSN address binding function enabled on the port, the user authenticated through the IAB cannot access the network.



#### Note

## Configuring IAB Authentication with Switching VLAN

When 802.1x controlled port enters into IAB state, it won't be able to verify user's identity. You can assign this port to a specific VLAN, and only allow the user to access network resources on this specific VLAN.

Execute the following steps to configure IAB authentication with switching VLAN:

Command	Function
Ruijie# <b>configure terminal</b>	Enter global configuration mode.
Ruijie(config)# <b>interface</b> <interface-id>	Enter interface configuration mode.
Ruijie(config-if)# <b>dot1x critical vlan</b> <vlan-id>	Configure IAB authentication with switching VLAN.
Ruijie(config-if)# <b>end</b>	Return to privileged EXEC mode.
Ruijie# <b>show running-config</b>	Display all configurations.

The following example shows how to configure Inaccessible Authentication Bypass:

```
Ruijie# configure terminal
Ruijie(config)# interface fa 0/1
Ruijie(config-if)# dot1x port-control auto
Ruijie(config-if)# dot1x critical
```



```
Ruijie(config-if)# dot1x critical vlan 100
```



### Note

1. If there are already certain authenticated users on the port before all RADIUS servers fail, new users are authorized to access the network after servers have failed and if no inaccessible VLAN is configured on the port. If IAB authentication with inaccessible VLAN has been configured on the server, new users won't be authorized to access network in order to guarantee that the authenticated users have the priority to use network.
2. If there are already normally authenticated users on the port before all servers have failed, the port will remain the original state and won't jump to the inaccessible VLAN if the servers are failed during user's re-authentication.
3. After all users under the port are disconnected, the port will automatically exit from the inaccessible VLAN.
4. If the inaccessible VLAN configured doesn't exist, the inaccessible VLAN will be created automatically when entered by the port and be removed automatically when exited by the port.
5. The inaccessible VLAN doesn't support private VLAN, remote VLAN and super VLAN (including SUB VLAN).

## Configuring IAB Authentication with Recovery action.

When RADIUS server is failed, some users won't be able to pass the authentication, and the switch will authorize the users to access network. When RADIUS server is recovered, this feature will allow IAB users under the port to reinitialize authentication to verify user's identity.

Execute the following steps to configure IAB authentication recovery action:  
The following example shows how to configure Inaccessible Authentication Bypass:

Command	Function
Ruijie# <b>configure terminal</b>	Enter global configuration mode.
Ruijie(config)# <b>interface</b> <interface-id>	Enter interface configuration mode.
Ruijie(config-if)# <b>dot1x critical recovery action reinitialize</b>	Allow IAB users under the port to reinitialize authentication when the server has recovered.
Ruijie(config-if)# <b>end</b>	Return to privilege mode.
Ruijie# <b>show running-config</b>	Display all configurations.

to  
with  
how

```
Ruijie# configure terminal
Ruijie(config)# interface fa 0/1
Ruijie(config-if)# dot1x port-control auto
```

```
Ruijie(config-if)# dot1x critical
```

```
Ruijie(config-if)# dot1x critical recovery action reinitialize
```

**Note**

After the server has recovered, normally authenticated users under the port can continue to access the network without re-authentication. After the server is failed, IAB-authenticated users will be subject to the authentication interaction initiated by the switch.

## Viewing the Configuration and Current Statistics of the 802.1x

Our 802.1X provides a full range of state machine information, which is very useful for network management and can be used by the administrator to monitor user status in real time and make easy troubleshooting.

- Viewing the Radius Authentication and Accounting Configuration
- Viewing the Number of Current Users
- Viewing the List of the Addresses Authenticable
- Viewing the User Authentication Status Information
- Showing the 1x Client Probe Time Configuration

### Viewing the Radius Authentication and Accounting Configuration

Run the **show radius server** command to check the related configuration of the Radius Sever, and run the **show aaa user** command to view the user-related information.

```
Ruijie# sh radius server
Server IP:      192.168.5.11
Accounting Port: 1813
Authen Port:    1812
Server State:   Ready
```

### Viewing the Number of Current Users

Our 802.1X allows you to view the numbers of two types of users: one is the number of current users, and the other is that of the authorized users. The number of current users refers to the total number of users authenticated (whether successfully or unsuccessfully), while the number of authorized users means the total number of users authorized.

In the privileged EXEC mode, run the **show dot1x** command to check the current number of users and authenticated users, 1x configuration, including the current number of users and authenticated users.

The following example shows the 802.1x configuration:

```
Ruijie# show dot1x
802.1X Status:      Disabled
Authentication Mode: EAP-MD5
Authed User Number: 0
Re-authen Enabled:  Disabled
Re-authen Period:   3600 sec
Quiet Timer Period:  10 sec
```

```

Tx Timer Period:      3 sec
Supplicant Timeout:   3 sec
Server Timeout:       5 sec
Re-authen Max:        3 times
Maximum Request:      3 times
Filter Non-RG Supp:   Disabled
Client Oline Probe:   Disabled
Eapol Tag Enable:     Disabled
Authorization Mode:    Disabled

```

## Viewing the Authenticable Address Table

Our 802.1x has expanded functions that allow you to set the hosts that can be authenticated on a particular port. This function allows the administrator to view the currently available settings.

In the privileged EXEC mode, you can view the list of hosts authenticable by performing the following steps:

Command	Function
<b>configure terminal</b>	Enter the global configuration mode.
<b>dot1x auth-address-table</b> <b>address</b> <i>mac-addr</i> <b>interface</b> <i>interface</i>	Set the list of the hosts that can be authenticated.
<b>end</b>	Return to the privileged EXEC mode.
<b>write</b>	Save the configuration.
<b>show dot1x auth-address-table</b>	Show the list of the hosts that can be authenticated.

Use the **no dot1x auth-address-table address** command to delete the specified authenticable host list. The following example shows the list of the hosts that can be authenticated.

```

Ruijie# show dot1x auth-address-table
interface: g3/1
-----
mac addr: 00D0.F800.0001

```

## Viewing the User Authentication Status Information

The administrator can view the authentication status of the current users of the switch for easier troubleshooting.

In the privileged EXEC mode, you can view the user authentication status information by performing the following steps:

Command	Function
<b>show dot1x summary</b>	Viewing the User Authentication Status Information

The following example shows the user authentication status information.

```

Ruijie# show dot1x summary
ID   MAC           Interface  VLAN  Auth-State  Backend-State  Port-Status
---
1    00d0f8000001  Gi3/1     1     Authenticated  IDLE           Authed

```

## Showing the 1x Client Probe Timer Configuration

In the privileged EXEC mode, you can view the 1x timer setting by performing the following steps:

Command	Function
<b>show dot1x probe-timer</b>	Show the 1X timer setting

The following example shows the 1.1x timer setting:

```
Ruijie# show dot1x probe-timer
Hello Interval: 20 Seconds
Hello Alive: 250 Seconds
Ruijie#
```

## Example of Configuring 802.1X port-based dynamic VLAN assignment

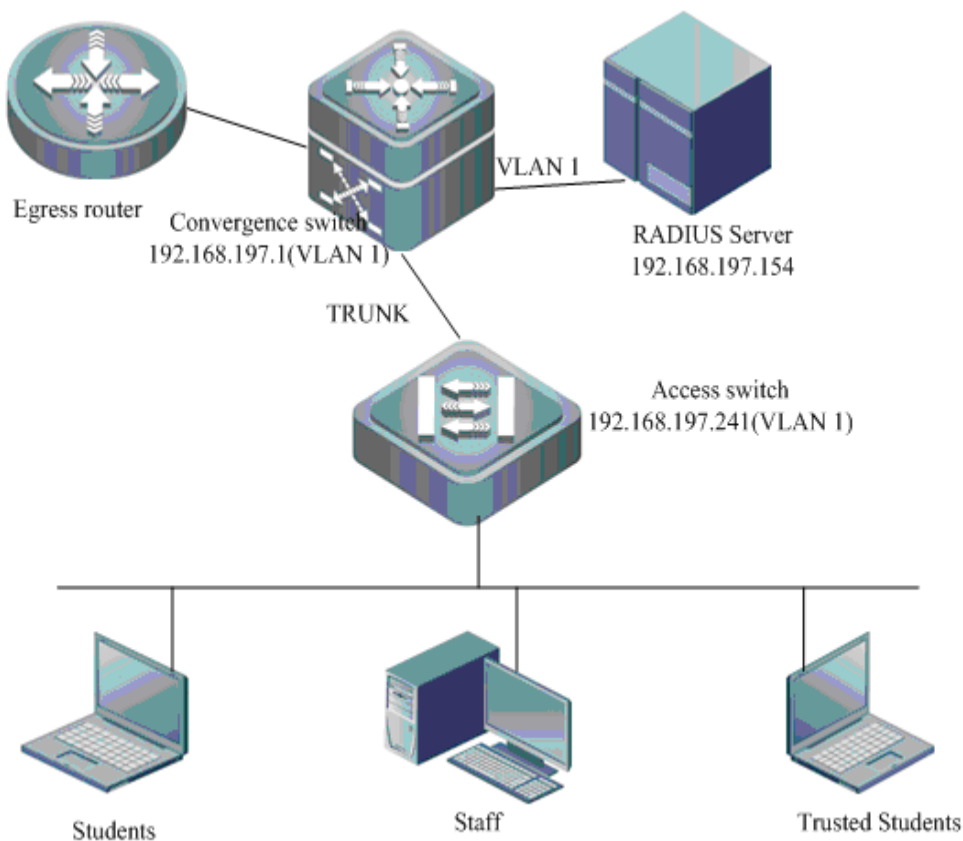
In a school, there are three types of user groups as shown below:

- Students;
- Trusted students (such as student cadres);
- Teaching and administrative staff.

Fundamental requirements are shown below:

- Each member of these three user groups can be connected to any port of the access device and join the corresponding VLAN.
- Complete data isolation shall be achieved between VLANs corresponding to three user groups, namely the members of one group cannot exchange data with members of another group.

Network topology is shown below:



**Figure 11 Typical topology of dynamic VLAN assignment**

Configuration example is shown below

#### 1. Configure RADIUS server

Include a managerial access device of 192.168.197.241, which uses the default authentication and accounting ports of 1812 and 1813 and the shared key of "shared".

Configure the vlan for users of user group "students"

```

Tunnel-Type = "VLAN",
Tunnel-Medium-Type = "IEEE-802",
Tunnel-Private-Group-ID = "students"
Configure the vlan for users of user group "trusted_students"
Tunnel-Type = "VLAN",
Tunnel-Medium-Type = "IEEE-802",
Tunnel-Private-Group-ID = "trusted_students"
Configure the vlan for users of user group "staff"
Tunnel-Type = "VLAN",
Tunnel-Medium-Type = "IEEE-802",
Tunnel-Private-Group-ID = "staff"
  
```

#### 2. Configure access switch

Turn on AAA switch

```

configure terminal
aaa new-model
  
```

Configure RADIUS server

```

configure terminal
radius-server host 192.168.197.154
radius-server key shared
  
```

Configure authentication method list

```
configure terminal
aaa authentication dot1x default group radius
aaa accounting network default start-stop group radius
```

802.1X to select the authentication method list

```
configure terminal
dot1x authentication default
dot1x accounting default
```

Enable 802.1X authentication on the interface

```
configure terminal
interface range fastEthernet 0/1-48
dot1x port-control auto
```

Enable dynamic VLAN assignment on the interface

```
configure terminal
interface interface_id
dot1x dynamic-vlan enable
```

Create VLANs to join after user authentication

```
configure terminal
```

vlan 2

```
name students
```

vlan 3

```
name trusted_students
```

vlan 4

```
name staff
```

Create the management IP for access device

```
configure terminal
interface vlan 1
ip address 192.168.197.241 255.255.255.0
```

By far, user's needs can be met.

## Other Precautions for Configuring 802.1x

### 1. Concurrent use of 1X and ACL

In the non-IP authorization mode, if you enable the 802.1x authentication function of a port and at the same time associate one ACL with a interface, the ACL takes effect on the basis of the MAC address. In other words, only the packets from the source MAC addresses of the authenticated users can pass ACL filtering, and the packets from other source MAC addresses will be discarded. The ACL can only work on the basis of the MAC address.

For example, if the authenticated MAC address is 00d0.f800.0001, then all the packets from the source MAC address of 00d0.f800.0001 can be switched. If the port is associated with an ACL, the ACL will further filter these packets that can be switched, for example, rejecting the ICMP packets from the source MAC address of 00d0.f800.0001.

### 2. The restrictions for the condition that the users on the interface have being authenticated or the users have been authenticated:

- The port mode cannot be modified, such as the command **switchport mode trunk** cannot be used.
- The port Access VLAN can not be modified in the ACCESS mode.

- The port Allowed VLAN and Native VLAN can not be modified in the TRUNK mode.
  - The port can not exit from or be added to the AP port.
3. The restrictions for the condition that the users in the VLAN have being authenticated or the users have been authenticated:
    - ✧ VLAN can not be deleted
    - ✧ VLAN type cannot be modified, such as the command **private-vlan primary** cannot be used.
  4. GVRP cannot be co-used with the dynamic VLAN auto-switching function.
  5. 802.1x function can be co-used with other access control functions, such as the port security, IP+MAC binding, ect. When those access control functions are co-used, the packets can enter the switch on the condition that those packets must address all access controls.
  6. It is not suggested to enable the **dot1x redirect** command after the controlled function is enabled on the AP port. Otherwise, controlled function of this AP port may fail.
  7. After the Native VLAN of the port is changed, effective VLAN-switching functions (such as: GUEST VLAN, FAIL VLAN, VLAN assignment and IAB authentication with switching VLAN) on the Trunk port or Hybrid port will cause the users in other VLANs can access the network without authorization. Therefore, it is suggest the aforementioned VLAN-switching function is enabled on the Access port only.

## Typical 802.1X Configuration Examples

### 802.1X-based AAA Services

#### Network Topology

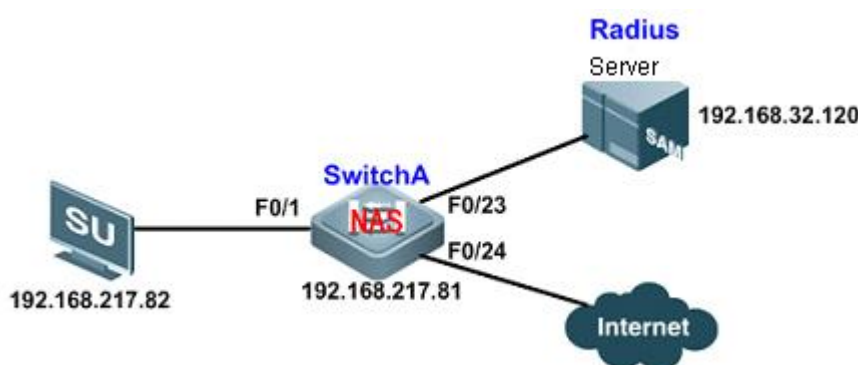


Figure 12 Network topology for the 802.1X-based AAA service

#### Networking Requirements

To ensure the validity of network access, the following requirements must be met:

1. It is required that access users on each port must be subject to 1X authentication in order to control Internet access (unauthenticated users won't be able to access network);
2. Only our client software (supplicant) can be used as the client for 802.1x authentication;
3. Accounting shall be based on online time, and accounting update packets will be periodically sent to Radius Server (real-time accounting packets will be sent to RADIUS server every 15 minutes);
4. After sending the authentication request to RADIUS server, the device will resend the request if no reply is received within 5 seconds, and will try for totally 6 times;
5. Online monitoring of users to prevent authenticated user from being preempted by other users and to detect whether the user is disconnected;
6. To protect server from hostile attacks, the access user can only initialize re-authentication after 500 seconds if it fails in authentication. Meanwhile, after trying for over 5 times, this user will be considered as disconnected and the authentication process will end.

## Configuration Tips

- Turn on AAA switch and configure the communication between device and RADIUS SERVER; configure 802.1X authentication and configure the device port for client access as controlled port (here we take port F0/1 as the example); (corresponding to paragraph 1 of "Application Needs")
- Filter non-Ruijie supplicant (corresponding to paragraph 2 of "Networking requirements")
- Configure 802.1x accounting and accounting update, and configure the interval of accounting update packets (corresponding to paragraph 3 of "Networking requirements")
- Configure the reply timeout timer of Radius Server as 5s, and configure the maximum authentication retries as 6 times (corresponding to paragraph 4 of "Networking requirements")
- Configure periodic re-authentication of device (corresponding to paragraph 5 of "Networking requirements")
- Configure the Quiet Period for failed authentication as 500s (waiting time) and configure the maximum authentication retries as 5 times (corresponding to paragraph 6 of "Networking requirements")

## Configuration Steps

Step 1: Configure relevant attributes of Radius Server



- Login SAM Security Accounting Management System and click "System Management - Device Management" to insert information about NAS device. The required configurations include: "Device IP" - 192.168.217.81, "Device Group" - haha, "Device Type" - switch, "Specific Model" - S21XX and later, "Device Key" - Ruijie, "Read/Write Community" - weilin, "Device Aging Duration" - 3s, as shown below:

设备			
* 设备IP	192.168.217.81	* 设备组	haha
* 设备类型	交换机	* 具体型号	S21XX及以后
* 设备Key	ruijie	* 读写Community	weilin
设备名称	S3760	设备位置	
* 设备超时时间(秒)	3	设备静默时间(秒)	
设备功能	<input type="checkbox"/> 重认证 <input type="checkbox"/> 记账更新 <input type="checkbox"/> 客户端检测 <input type="checkbox"/> Web认证		
地区	(根据设备IP范围划分)	地区	(根据Web认证接入设备IP范围划分)
联动端口		描述	

- Click "User Management - User Management" to insert user information. The required configurations include: "Username" - qq, "Password" - 1234567, "User Group" - ceshi, as shown below:

基本信息			
* 用户名	qq	用户姓名	
* 密码	1234567	* 密码确认	1234567
* 用户组	ceshi	账户	qq
用户模板	自定义模板 模板: ceshi 计费策略: 1元1s		
用户自助权限	所有自助权限	免服务校验	需要校验
自动预销户时间		BACL	
账户余额	0.00		
用户状态	正常	暂停时间	
上次自助暂停时间		下次可自助暂停时间	无限制

## Step 2: Configure access switch "SwitchA"

### ! Turn on AAA switch

```
Ruijie(config)#aaa new-model
```

### ! Configure RADIUS server

```
Ruijie(config)#radius-server host 192.168.32.120
```

### ! Configure RADIUS Key

```
Ruijie(config)#radius-server key ruijie
```

### ! Configure dot1x authentication method list

```
Ruijie(config)#aaa authentication dot1x hello group radius
```

### ! Apply dot1x authentication method list

```
Ruijie(config)#dot1x authentication hello
```

### ! Configure F0/1 as controlled port (enable port-based authentication)

```
Ruijie(config)#interface fastEthernet 0/1
```

```
Ruijie(config-if-FastEthernet 0/1)#dot1x port-control auto
```

```
Ruijie(config-if-FastEthernet 0/1)#exit
```

### ! Filter non-Ruijie supplicant

```
Ruijie(config)#dot1x private-supplicant-only
```

### ! Configure 802.1X accounting method list

```
Ruijie(config)#aaa accounting network jizhang start-stop group radius
```

### ! Apply 802.1X accounting method list

```
Ruijie(config)#dot1x accounting jizhang
```

**! Configure accounting update**

```
Ruijie(config)#aaa accounting update
```

**! Configure the accounting update interval as 15 minutes**

```
Ruijie(config)#aaa accounting update periodic 15
```

**! Configure the reply timeout timer of Radius Server as 5s**

```
Ruijie(config)#dot1x timeout server-timeout 5
```

**! Configure maximum transmission retries as 6 times**

```
Ruijie(config)#dot1x max-req 6
```

**! Enable periodic re-authentication**

```
Ruijie(config)#dot1x re-authentication
```

**! Configure the re-authentication interval as 1000s**

```
Ruijie(config)#dot1x timeout re-authperiod 1000
```

**! Configure the Quiet Period of device as 500s**

```
Ruijie(config)#dot1x timeout quiet-period 500
```

**! Configure the maximum authentication retries of device as 5 times**

```
Ruijie(config)#dot1x reauth-max 5
```

**! Configure the default route of device**

```
Ruijie(config)#ip route 0.0.0.0 0.0.0.0 192.168.217.1
```

**! Configure the IP address of device**

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

```
Ruijie(config-if-VLAN 1)#ip address 192.168.217.81 255.255.255.0
```

Step 3: Use authentication client (such as supplicant) to carry out authentication; type in the correct username and password and select the network adapter, and the authentication will succeed after a few seconds.

**Verify Configurations**

Step 1: Display the authentication state information of current user in order to eliminate faults.

```
Ruijie#show dot1x summary
```

ID	MAC	Interface	VLAN	Auth-State	Backend-State	Port-Status	User-Type
1	00d0.f864.6909	Fa0/1	1	Authenticated	Idle	Authed	static

Step 2: Display detailed information about authenticated user.

```
Ruijie#show dot1x user id 1
```

```
User name: qq
User id: 1
Type: static
Mac address is 00d0.f864.6909
Vlan id is 1
Access from port Fa0/1
Time online: 0days 0h 2m24s
User ip address is 192.168.217.82
Max user number on this port is 6000
Authorization session time is 20736000 seconds
Supplicant is private
Start accounting
Permit proxy user
Permit dial user
IP privilege is 0
user acl-name qq_1_0_0 :
```

Step 3: Display 1X configurations about the existing number of users and the number of authenticated users;

```
Ruijie#show dot1x
```

```
802.1X Status:      enable
Authentication Mode: eap-md5
Total User Number:  1(exclude dynamic user)
Authed User Number: 1(exclude dynamic user)
Dynamic User Number: 0
Re-authen Enabled:  enable
Re-authen Period:   1000 sec
Quiet Timer Period: 500 sec
Tx Timer Period:    3 sec
Supplicant Timeout: 3 sec
Server Timeout:     5 sec
Re-authen Max:      5 times
Maximum Request:    6 times
Private supplicant only: enable
Client Online Probe: disable
Eapol Tag Enable:   disable
Authorization Mode:  disable
```

Step 4: Display Radius authentication and accounting related configurations;

```
Ruijie#show radius server
```

```
Server IP: 192.168.32.120
Accounting Port: 1813
Authen Port: 1812
Server State: ready
```

## Application of 802.1X port-based dynamic VLAN assignment

### Network Topology

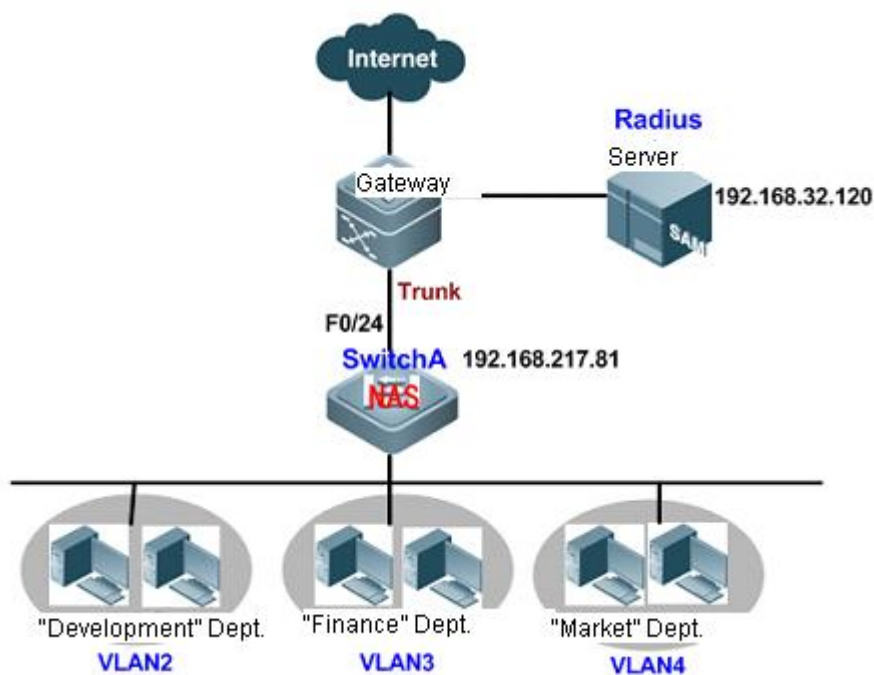


Figure 13 Topology for 802.1X port-based dynamic VLAN assignment

## Networking requirements

A company has three user groups, namely "development" department, "finance" department and "market" department. The following needs must be met:

- Each member of these three user groups can be connected to any port of the access device and join the corresponding VLAN after successful authentication ("development" department to join VLAN2, "finance" department to join VLAN3, and "market" department to join VLAN4).
- Complete data isolation shall be achieved between VLANs corresponding to three user groups, namely the members of one group cannot exchange data with members of another group.

## Configuration Tips

- Turn on AAA switch and configure the communication between device and RADIUS SERVER;
- Configure 802.1X authentication and configure the device port for client access as controlled port;
- Enable dynamic VLAN assignment on the corresponding interface;
- Create VLANs to join after user authentication.

## Configuration Steps

Step 1: Configure relevant attributes of Radius Server (Only key configurations will be described below, and we will not give other unnecessary details):

- Click "User Management - User Group Management" and add the corresponding user group (taking user group "development" as the example):

添加用户组			
* 用户组名	development	* 父用户组名	root
* 默认用户模板	ceshi	描述	development

- Click "User Management - User Management" to insert the basic information about user and corresponding VLAN information (taking user group "development" as the example; the VLAN to which the user belongs is configured as 2):

基本信息			
* 用户名	de	用户姓名	
* 密码	●●●●●●●●	* 密码确认	●●●●●●●●
* 用户组	development	账户	<input type="checkbox"/> 创建并关联同名账户
用户模板	<input type="radio"/> 使用用户组默认模板 <input checked="" type="radio"/> 自定义模板           模板: ceshi		
用户自助权限	所有自助权限	免服务校验	需要校验
自动预销户时间		BACL	请选择
高级选项	<input checked="" type="checkbox"/> 显示高级用户设置选项		

功能信息			
下传IP	<input type="text"/>	用户所属VLAN (0~4094)	<input type="text" value="2"/>
用户访问权限 (0~2147483647)	<input type="text"/>	VPN服务器ACL	<input type="text"/>
所属集团	请选择 ▼		
开户费	<input type="text" value="0"/>		

## Step 2: Configure access switch "SwitchA"

### ! Turn on AAA switch

```
Ruijie(config)#aaa new-model
```

### ! Configure RADIUS server

```
Ruijie(config)#radius-server host 192.168.32.120
```

### ! Configure RADIUS key

```
Ruijie(config)#radius-server key ruijie
```

### ! Configure dot1x authentication method list

```
Ruijie(config)#aaa authentication dot1x hello group radius
```

### ! Apply dot1x authentication method list

```
Ruijie(config)#dot1x authentication hello
```

### ! Configure 802.1X accounting method list

```
Ruijie(config)#aaa accounting network jizhang start-stop group radius
```

### ! Apply 802.1X accounting method list

```
Ruijie(config)#dot1x accounting jizhang
```

### ! Configure the port as controlled port (enable port-based authentication)

```
Ruijie(config)#interface range fastEthernet 0/1-23
```

```
Ruijie(config-if-range)#dot1x port-control auto
```

### ! Enable dynamic VLAN assignment on the corresponding interface

```
Ruijie(config-if-range)# dot1x dynamic-vlan enable
```

### ! Create VLANs to join after user authentication

```
Ruijie(config)#vlan 2
```

```
Ruijie(config-vlan)#name development
```

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

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

```
Ruijie(config-vlan)#name finance
```

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

```
Ruijie(config)#vlan 4
```

```
Ruijie(config-vlan)#name market
```

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

### ! Configure uplink port F0/24 as the trunk port.

```
Ruijie(config)#interface fastEthernet 0/24
```

```
Ruijie(config-if-FastEthernet 0/24)#switchport mode trunk
```

### ! Configure the default route of device

```
Ruijie(config)#ip route 0.0.0.0 0.0.0.0 192.168.217.1
```

### ! Configure the IP address of device

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

```
Ruijie(config-if-VLAN 1)#ip address 192.168.217.81 255.255.255.0
```

Step 3: Use client to complete authentication. After successful authentication, the CLI will display: "%DOT1X-4-TRANS\_AUTHOR: Setting interface FastEthernet 0/1 author-vlan 2 succeeded."

We can see that the user has been assigned to VLAN2.

## Verify Configurations

Step 1: Display the authentication state information of current user to see the true VLAN to which the user belongs.

```
Ruijie#show dot1x summary
```

ID	MAC	Interface	VLAN	Auth-State	Backend-State	Port-Status	User-Type
5	00d0.f864.6909	Fa0/1	2	Authenticated	Idle	Authed	static

Step 2: Display detailed information about authenticated user.

```
Ruijie#show dot1x user id 5
```

User name: st  
 User id: 5  
 Type: static  
 Mac address is 00d0.f864.6909  
 Vlan id is 2  
 Access from port Fa0/1  
 Time online: 0days 0h 4m35s  
 User ip address is 192.168.217.82  
 Max user number on this port is 6000  
 Authorization vlan is 2  
 Authorization session time is 20731685 seconds  
 Supplicant is private  
 Start accounting  
 Permit proxy user  
 Permit dial user  
 IP privilege is 0  
 user acl-name st\_1\_0\_0 :

## Application of 802.1X port-based Guest VLAN and VLAN assignment

### Network Topology

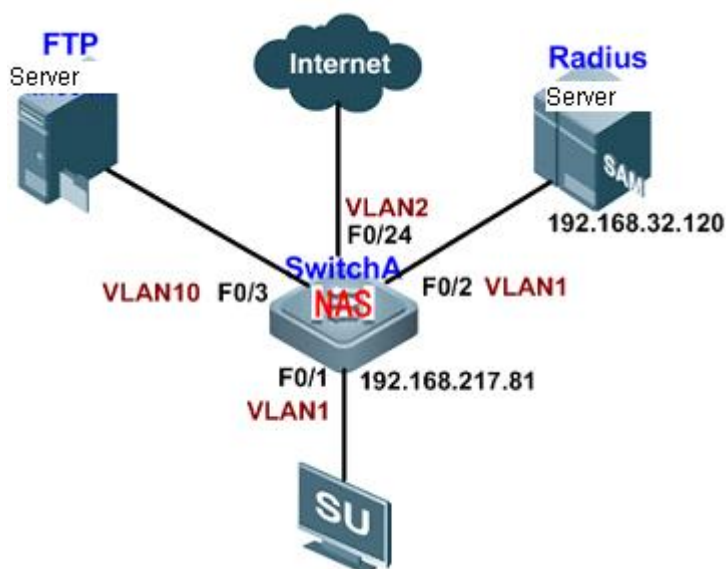


Figure 14 topology for 802.1X port-based Guest VLAN and VLAN assignment

### Networking Requirements

The client accesses network through 802.1x authentication. RADIUS server is the authentication server, and FTP server is the server used by the client for software downloading and pack upgrade while it

belongs to VLAN10. Radius Server is used for authentication, authorization, accounting and dynamic VLAN assignment, and it belongs to VLAN1. The Internet-connecting port F0/24 of switch belongs to VLAN2. The following needs must be met:

- If the switch receives no reply after sending authentication request packets (EAP-Request/Identity) for the configured number of tries, F0/1 will join the Guest VLAN (VLAN10). By this time, both Supplicant and FTP Server belong to VLAN10, and Supplicant can access FTP Server and download 802.1x client.
- After successful authentication, RADIUS server will assign VLAN2. By this time, both Supplicant and F0/24 belong to VLAN2, and Supplicant can access Internet.

## Configuration Tips

- Turn on AAA switch and configure the communication between device and RADIUS SERVER;
- Configure 802.1X authentication and configure the device port for client access as controlled port;
- Enable dynamic VLAN assignment on the corresponding interface;
- Configure whether or not enable guest VLAN on the corresponding interface.

## Configuration Steps

Configure access switch "SwitchA":

! Configure the VLANs to which the port belong:

```
Ruijie(config)#interface fastEthernet 0/3
Ruijie(config-if-FastEthernet 0/3)#switchport access vlan 10
Ruijie(config-if-FastEthernet 0/3)#exit
Ruijie(config)#interface fastEthernet 0/24
Ruijie(config-if-FastEthernet 0/24)#switchport access vlan 2
Ruijie(config-if-FastEthernet 0/24)#exit
```

! Turn on AAA switch

```
Ruijie(config)#aaa new-model
```

! Configure RADIUS server

```
Ruijie(config)#radius-server host 192.168.32.120
```

! Configure RADIUS key

```
Ruijie(config)#radius-server key ruijie
```

! Configure dot1x authentication method list

```
Ruijie(config)#aaa authentication dot1x hello group radius
```

! Apply dot1x authentication method list

```
Ruijie(config)#dot1x authentication hello
```

! Configure 802.1X accounting method list

```
Ruijie(config)#aaa accounting network jizhang start-stop group radius
```

! Apply 802.1X accounting method list

```
Ruijie(config)#dot1x accounting jizhang
```

! Configure the port as controlled port (enable port-based authentication)

```
Ruijie(config)#interface fastEthernet 0/1
Ruijie(config-if-FastEthernet 0/1)#dot1x port-control auto
```

! Enable dynamic VLAN assignment on the corresponding interface

```
Ruijie(config-if-FastEthernet 0/1)# dot1x dynamic-vlan enable
```

### ! Enable GUEST VLAN assignment on the interface

```
Ruijie(config-if-FastEthernet 0/1)#dot1x guest-vlan 10
```

### ! Configure the default route of device

```
Ruijie(config)#ip route 0.0.0.0 0.0.0.0 192.168.217.1
```

### ! Configure the IP address of device

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

```
Ruijie(config-if-VLAN 1)#ip address 192.168.217.81 255.255.255.0
```

## Verify Configurations

Step 1: If no reply is received after sending authentication request packets (EAP-Request/Identity) for the configured number of tries, the user connected to the port will automatically join VLAN10. The CLI will prompt:

```
%DOT1X-5-TRANS_DEFAULT_TO_GUEST: Transformed interface FastEthernet 0/1 from default-vlan 1 to guest-vlan 10 ok.
```

Step 2: The user downloads 802.1x client. After successful authentication, the CLI will prompt:

```
%DOT1X-4-TRANS_AUTHOR: Setting interface FastEthernet 0/1 author-vlan 2 succeeded.
```

#### 1. Display the authentication state information of current user:

```
Ruijie#show dot1x summary
```

ID	MAC	Interface	VLAN	Auth-State	Backend-State	Port-Status	User-Type
8	00d0.f864.6909	Fa0/1	2	Authenticated	Idle	Authed	static

#### Step 2: Display detailed information about authenticated user.

```
Ruijie#show dot1x user id 8
```

```
User name: st
User id: 8
Type: static
Mac address is 00d0.f864.6909
Vlan id is 2
Access from port Fa0/1
Time online: 0days 0h 4m25s
User ip address is 192.168.201.56
Max user number on this port is 6000
Authorization vlan is 2
Authorization session time is 20736000 seconds
Supplicant is private
Start accounting
Permit proxy user
Permit dial user
IP privilege is 0
user acl-name st_1_0_0 :
```



## Application of port-based 1X authentication and IP authorization

### Network Topology

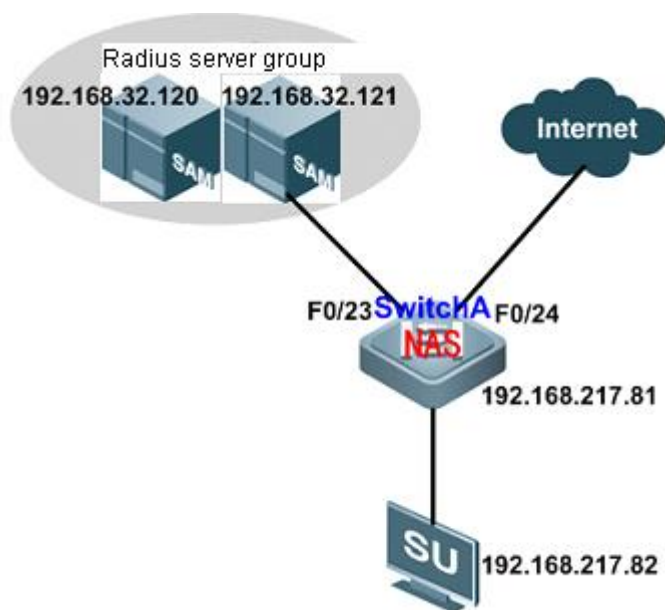


Figure15 topology for port-based 1X authentication and IP authorization

### Networking Requirements

The client accesses network through 802.1x authentication. RADIUS server is the authentication server. The following application needs must be met:

- When the active server fails due to certain reason, the device can automatically submit authentication request to the next server in the method list.
- When a user connected to one port of device passes the authentication, all users connected to this port will be able to access network freely.
- Dynamic user is not allowed to move between multiple authentication ports.
- The IP of an authenticated user must be assigned by the RADIUS Server, namely the authenticated user can only use the IP specified by RADIUS Server to access network.

### Configuration Tips

- Turn on AAA switch and configure the communication between device and RADIUS SERVER;
- Configure 802.1X authentication and configure the device port for client access as controlled port;
- Configure active/standby server group
- Configure the control mode of user authentication under the corresponding port as port-based authentication;

- Configure to prohibit dynamic user from moving between ports;
- Configure IP authorization mode as radius Server mode.

## Configuration Steps

Configure access switch "SwitchA":

! Turn on AAA switch

```
Ruijie(config)#aaa new-model
```

! Configure RADIUS server

```
Ruijie(config)#radius-server host 192.168.32.120
```

```
Ruijie(config)#radius-server host 192.168.32.121
```

! Configure RADIUS key

```
Ruijie(config)#radius-server key ruijie
```

! Configure server group (select active server and standby server)

```
Ruijie(config)#aaa group server radius rj
```

```
Ruijie(config-gs-radius)#server 192.168.32.120
```

```
Ruijie(config-gs-radius)#server 192.168.32.121
```

! Configure dot1x authentication list

```
Ruijie(config)#aaa authentication dot1x hello group radius
```

! Apply dot1x authentication method list

```
Ruijie(config)#dot1x authentication hello
```

! Configure 802.1X accounting method list

```
Ruijie(config)#aaa accounting network jizhang start-stop group radius
```

! Apply 802.1X accounting method list

```
Ruijie(config)#dot1x accounting jizhang
```

! Configure the port as controlled port (enable port-based authentication)

```
Ruijie(config)#interface range fastEthernet 0/1-22
```

```
Ruijie(config-if-range)#dot1x port-control auto
```

! Configure the control mode of user authentication under the corresponding port as port-based authentication

```
Ruijie(config-if-range)# dot1x port-control-mode port-based
```

```
Ruijie(config-if-range)#exit
```

! Configure to prohibit dynamic user from moving between ports;

```
Ruijie(config)#dot1x stationarity enable
```

! Configure IP authorization mode of device as RADIUS Server mode

```
Ruijie(config)#aaa authorization ip-auth-mode radius-server
```

! Configure the default route of device

```
Ruijie(config)#ip route 0.0.0.0 0.0.0.0 192.168.217.1
```

! Configure the IP address of device

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

```
Ruijie(config-if-VLAN 1)#ip address 192.168.217.81 255.255.255.0
```

## Verify Configurations

Step 1: Display the authentication state information of current user:

```
Ruijie#show dot1x summary
```

ID	MAC	Interface	VLAN	Auth-State	Backend-State	Port-Status	User-Type
-----	-----	-----	----	-----	-----	-----	-----
-----							
none	00d0.f864.6909	Fa0/1	1	Authenticated	Idle	Authed	Dynamic

Step 2: Move this user to another authenticated port. It can be found that the user won't be able to access network.

## SSH Terminal Service Configuration

### About SSH

SSH is the shortened form of Secure Shell. The SSH connection functions like a Telnet connection, except that all transmissions based on the connection are encrypted. When the user logs onto the device via a network environment where security cannot be guaranteed, the SSH feature provides safe information guarantee and powerful authentication function to protect the devices from IP address fraud, plain password interception and other kinds of attacks.

Ruijie SSH service supports both the IPv4 and IPv6 protocols.

### Ruijie's SSH Support Algorithms

Support Algorithm	SSH1	SSH2
Signature authentication algorithm	RSA	RSA, DSA
Key exchanging algorithm	RSA public key encryption based key exchanging algorithm	KEX_DH_GEX_SHA1 KEX_DH_GRP1_SHA1 KEX_DH_GRP14_SHA1
Encryption algorithm	DES, 3DES, Blowfish	DES, 3DES, AES-128, AES-192, AES-256
User authentication algorithm	User password based authentication method	User password based authentication method
Message authentication algorithm	Not supported	MD5, SHA1, SHA1-96, MD5-96
Compression algorithm	NONE (uncompressed)	NONE (uncompressed)

### Ruijie's SSH Supports



#### Caution

The products of Ruijie Networks support only the SSH server (compatible with the SSHv1 and SSHv2) but do not support the SSH client.

## SSH Configuration

### Default SSH Configurations

Item	Default Value
SSH service end status	Off
SSH version	Compatible mode (supporting versions 1 and 2)
SSH user authentication timeout period	120s
SSH user re-authentication times	3

### User Authentication Configuration

1. For the consideration of the SSH connection security, the login without authentication is forbidden. Therefore, in the login authentication of the users, the login authentication mode must have password configured (no-authentication login allowed for telnet).
2. The username and password entered every time must have lengths greater than zero. If the current authentication mode does not need the username, the username can be entered randomly but the entry length must be greater than zero.

### Enabling SSH Server

The SSH Server is disabled by default. To enable the SSH Server, run the **enable service ssh-server** command in the global configuration mode while generating SSH key.

Command	Description
<b>configure terminal</b>	Enter the global configuration mode.
<b>enable service ssh-server</b>	Enable SSH Server.
<b>crypto key generate {rsa dsa}</b>	Generate the key



**Caution**

1. To delete the key, use the **crypto key zeroize** command rather than the **[no] crypto key generate** command.
2. The SSH module does not support hot standby. For products supporting management module hot standby, after the management module is switched over, if no SSH key files are in the new mainboard, the **crypto key generate** command must be used to regenerate the key in order to use the SSH.

## Disabling SSH Server

When the SSH Server is enabled, if the public key on the server is deleted, the SSH Server is automatically closed. To delete the public key, run **no enable service ssh-server** in the global configuration mode to disable the SSH Server.

Command	Description
<b>configure terminal</b>	Enter the global configuration mode
<b>no enable service ssh-server</b>	Delete the key to disable SSH Server.

## Configuring the Supported SSH Server Version

By default, the SSHv1 and SSHv2 are compatible. Run the following commands to configure the SSH version.

Command	Description
<b>configure terminal</b>	Enter the configuration mode
<b>ip ssh version {1 2}</b>	Configure the supported SSH version.
<b>no ip ssh version</b>	Restore the SSH default version.

## Configuring SSH User Authentication Timeout

By default, the user authentication timeout period of the SSH SERVER is 120 seconds. Run the following commands to configure the SSH user authentication timeout period.

Command	Description
<b>configure terminal</b>	Enter the configuration mode
<b>ip ssh time-out time</b>	Configure the SSH timeout period (1-120sec)
<b>no ip ssh time-out</b>	Restore the SSH default user authentication timeout period 120 seconds.

## Configuring SSH Re-authentication Times

This command is used to set the authentication attempts for SSH user requesting connections to prevent illegal actions such as malicious guesswork. The authentication attempts are 3 for the SSH Server by default. In other words, it allows the user to enter the username and password for three times to attempt the authentication. Run the following commands to configure the SSH re-authentication times:

Command	Description
<b>configure terminal</b>	Enter the configuration mode
<b>ip ssh authentication-retries retry times</b>	Configure SSH re-authentication times (range 0-5)
<b>no ip ssh authentication-retries</b>	Restore the default SSH re-authentication times as 3.

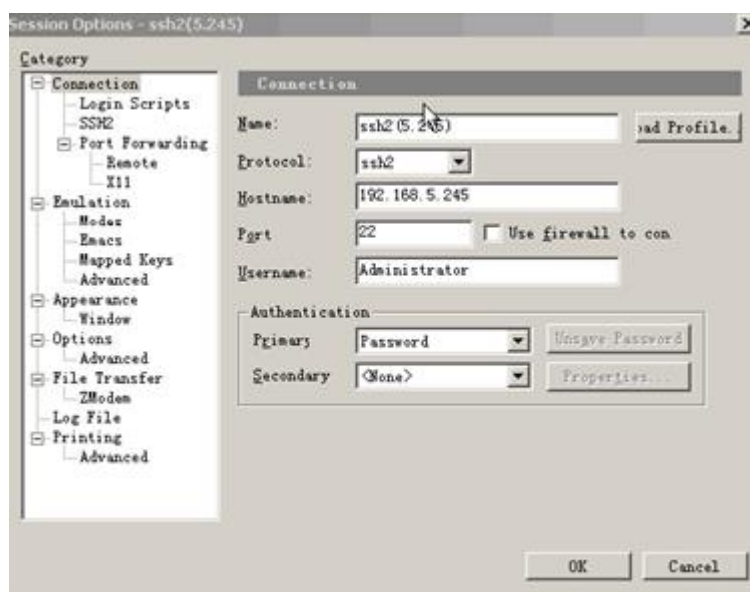
**Note**

For details of the above commands, see *SSH Command Reference Manual*.

## Using SSH for Device Management

You may use the SSH for device management by first enabling the SSH Server function that is disabled by default. Since the Telnet that comes with the Windows does not support SSH, third-party client software has to be used. Currently, the clients with sound forward compatibility include Putty, Linux and SecureCRT. With the client software SecureCRT as an example, the SSH client configuration is described as follows (see the UI below):

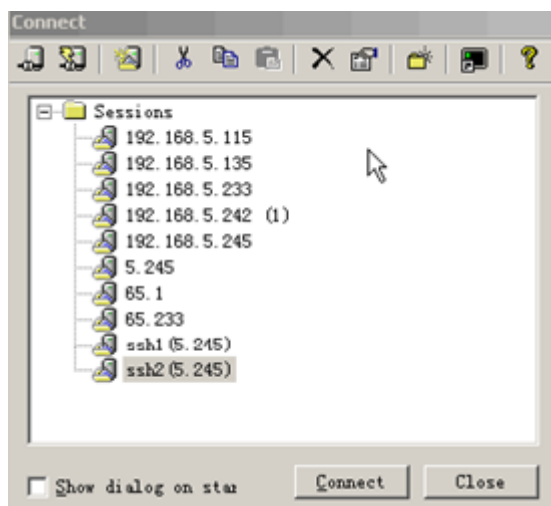
**Figure-1**



As shown in Figure-1, protocol 2 is used for login, so SSH2 is chosen in “Protocol”. “Hostname” indicates the IP address of the host that will log in, 192.168.5.245. Port 22 is the default number of the port for SSH listening. “Username” indicates the username, and does not take effect when the device only requires password. “Authentication” indicates the authentication mode, and the username/password authentication is supported here. The used password is the same as the Telnet password.

Click “OK” to pop up the following dialog:

**Figure-2**



Click “Connect” to log into the host just configured, as shown below:

**Figure-3**



Ask the machine that is logging into the host 192.168.5.245 to see whether the key from the server end is received or not. Select “Accept & Save” or “Accept Once” to enter the password confirmation dialog box, as shown below:

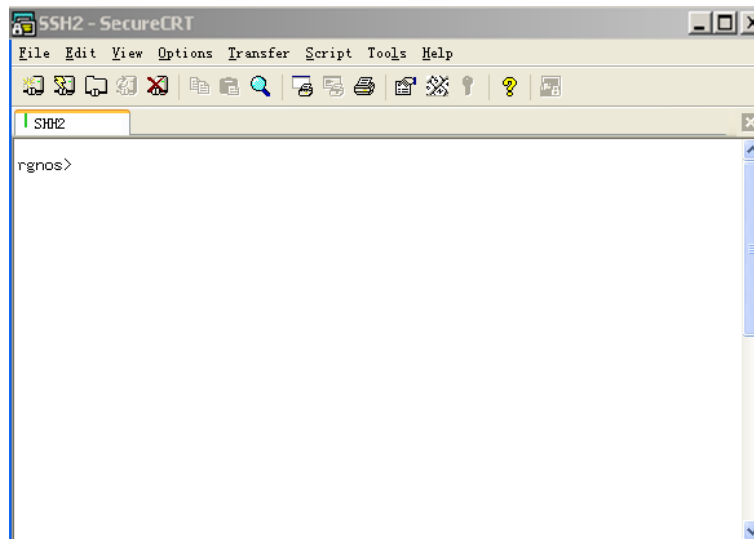
**Figure-4**



Enter the Telnet login password to enter the UI that is the same as the Telnet. See the diagram below:

**Figure-5**

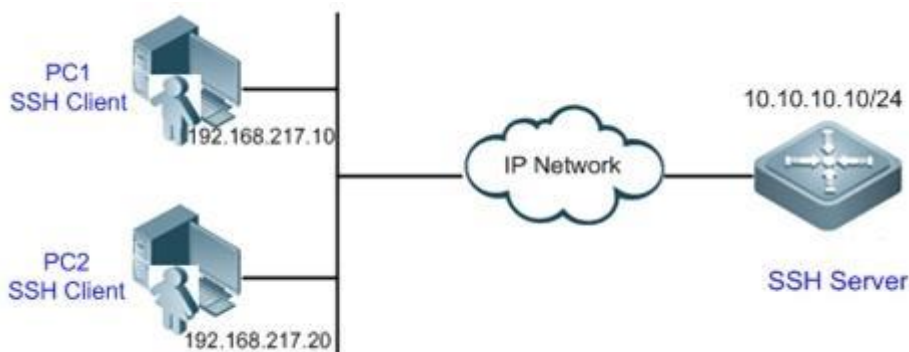




## Typical SSH Configuration Examples

### Example of SSH Local Authentication Configurations

#### Topological Diagram



Networking diagram for SSH local password protection

#### Application Requirements

As shown above, to ensure the security of information exchange, PC1 and PC2 serve as SSH clients which will login the SSH Server through SSH protocol. The specific requirements are shown below:

1. SSH users adopt line password authentication.
2. 0-4 lines are enabled at the same time. The login password for line 0 is "passzero", and the login password for other four lines is "pass". Any user name can be used.

#### Configuration Tips

**SSH Server configuration tips are shown below:**

1. Globally enable SSH Server. By default, SSH Server supports SSH1 and SSH2.

2. Configure key. The SSH server will use this key to decrypt the encrypted password received from SSH client, and compare the decrypted plain text with the password stored on the server before giving the reply about successful or failed authentication. SSH1 uses RSA key, while SSH 2 uses RSA or DSA key.
3. Configure the IP address of the interface Gi 1/1 of SSH server. SSH client will use this address to connect SSH server. The route from SSH client to SSH server shall be reachable.

### Configurations on SSH Client:

There are many SSH client programs, such as Putty, Linux, OpenSSH and etc. Here we will only take the client software of SecureCRT as the example to introduce how to configure SSH Client. The configuration details are given in "Configuration Steps".

## Configuration Steps

### Configure SSH Server

Before configuring relevant SSH features, make sure the route from SSH client to SSH server is reachable. The IP addresses of respective interfaces are shown in the topological diagram, and the steps of IP and route configuration are omitted herein.

#### Step 1: Enable SSH Server

```
Ruijie(config)# enable service ssh-server
```

#### Step 2: Generate RSA key

```
Ruijie(config)#crypto key generate rsa
% You already have RSA keys.
% Do you really want to replace them? [yes/no]:
Choose the size of the key modulus in the range of 360 to 2048 for your
Signature Keys. Choosing a key modulus greater than 512 may take
a few minutes.

How many bits in the modulus [512]:
% Generating 512 bit RSA1 keys ...[ok]
% Generating 512 bit RSA keys ...[ok]
```

#### Step 3: Configure the address of interface Gi 1/1. The client will use this address to connect SSH server.

```
Ruijie(config)#interface gigabitEthernet 1/1
Ruijie(config-if- gigabitEthernet 1/1)#ip address 10.10.10.10 255.255.255.0
Ruijie(config-if- gigabitEthernet 1/1)#exit
```

#### Step 4: Configure login password for lines

##### ! Configure the login password for line 0 as "passzero"

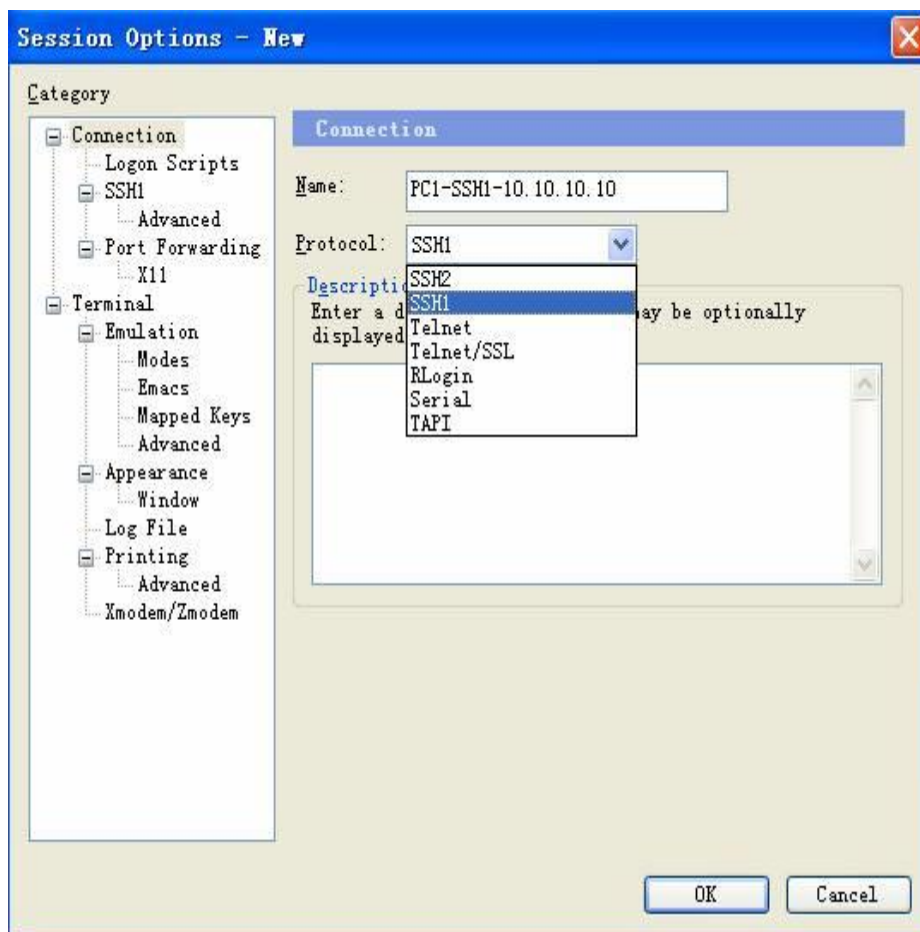
```
Ruijie(config)#line vty 0
Ruijie(config-line)#password passzero
Ruijie(config-line)#privilege level 15
Ruijie(config-line)#exit
```

##### ! Configure the login password for line 1-4 as "pass"

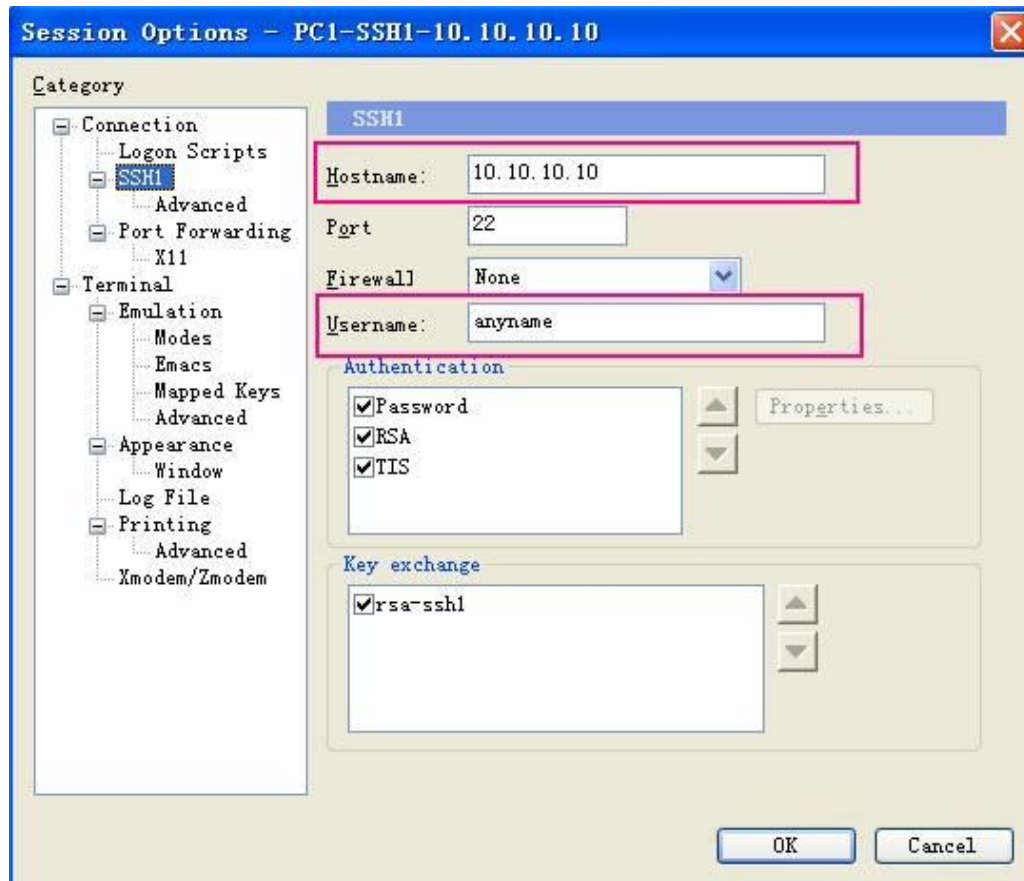
```
Ruijie(config)#line vty 1 4
Ruijie(config-line)#password pass
Ruijie(config-line)#privilege level 15
Ruijie(config-line)#exit
```

## Configure SSH Client (PC1/PC2)

Open SecureCRT connection dialog box, as shown below. Use SSH1 for login authentication. Any session name can be specified (here the session name is configured as PC1-SSH1-10.10.10.10).



Configure SSH attributes. The host name is the IP address of SSH server (10.10.10.10 in this example). Since user name is not required by the currently-used authentication mode, you can type in any user name in the field of "User Name", but this field cannot be left blank (the user name is "anyname" in this example).



## Verifying Configurations

### Verify the configurations of SSH Server

Step 1: Execute "show running-config" command to verify the current configurations:

```
Ruijie#show running-config

Building configuration...

!
enable secret 5 $1$eyy2$xs28FDw4s2q0tx97
enable service ssh-server
!
interface gigabitEthernet 1/1
 ip address 10.10.10.10 255.255.255.0
line vty 0
 privilege level 15
 login
password passzero
line vty 1 4
 privilege level 15
 login
password pass
!
end
```

## Verify the configurations of SSH Client

Step 1: Establish remote connection.

Establish connection and type in the correct password in order to enter the operating interface of SSH Server. The login password for line 0 is "passzero", and the login password for other four lines is "pass".

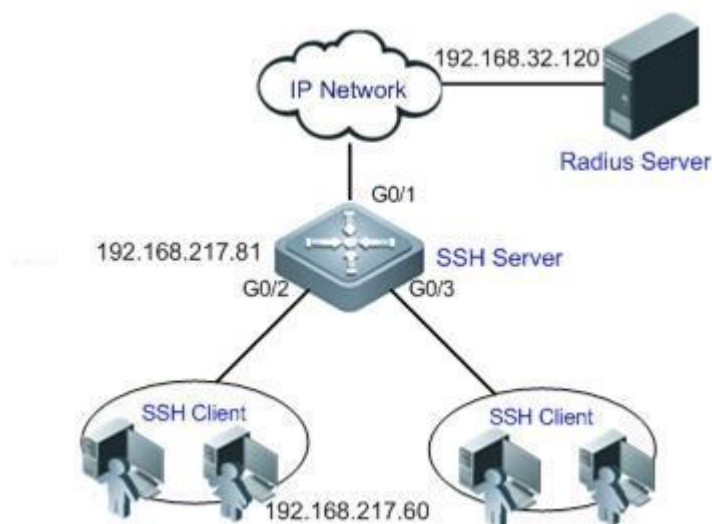
Step 2: Display login user.

```
Ruijie#show users
```

Line	User	Host(s)	Idle	Location
0 con 0		idle	00:03:16	
1 vty 0		idle	00:02:16	192.168.217.10
* 2 vty 1		idle	00:00:00	192.168.217.20

## Example of Configuring AAA Authentication for SSH

### Topological Diagram



Networking diagram for AAA authentication for SSH

### Application Requirements

As shown above, to ensure the security of information exchange, PC serves as SSH clients which will login the SSH Server using SSH protocol.

To better implement security management, SSH client adopts the AAA authentication mode. Meanwhile, for stability consideration, two authentication methods are configured in the AAA authentication method list: Radius server authentication and local authentication. Radius server will always be selected first, and the local authentication method will be selected later if no reply is received from Radius server.

### Configuration Tips

1. The route from SSH client to SSH server and the route from SSH server to Radius client shall be reachable,

2. Complete SSH Server related configurations on the network device. The configuration tips have been described in the previous example, and won't be further introduced herein.
3. Complete AAA authentication related configurations on the network device. AAA defines ID authentication and type by creating the method list, which is then applied to the specific service or interface. Details are given in the section of "Configuration Steps".

## Configuration Steps

The route from SSH client to SSH server and the route from SSH client to Radius server shall be reachable. Route related configurations won't be further introduced. Please refer to the section of route configuration in this manual.

### Configure relevant SSH features on the network device

#### Step 1: Enable SSH Server

```
Ruijie(config)# enable service ssh-server
```

#### Step 2: Generate the key

##### ! Generate RSA key

```
Ruijie(config)#crypto key generate rsa
% You already have RSA keys.
% Do you really want to replace them? [yes/no]:
Choose the size of the key modulus in the range of 360 to 2048 for your
Signature Keys. Choosing a key modulus greater than 512 may take
a few minutes.
How many bits in the modulus [512]:
% Generating 512 bit RSA1 keys ...[ok]
% Generating 512 bit RSA keys ...[ok]
```

##### ! Generate DSA key

```
Ruijie(config)#crypto key generate dsa
Choose the size of the key modulus in the range of 360 to 2048 for your
Signature Keys. Choosing a key modulus greater than 512 may take
a few minutes.

How many bits in the modulus [512]:
% Generating 512 bit DSA keys ...[ok]
```

#### Step 3: Configure the IP address of device. The client will use this address to connect SSH server.

```
Ruijie(config)#interface gigabitEthernet 1/1
Ruijie(config-if-gigabitEthernet 1/1)#ip address 192.168.217.81 255.255.255.0
Ruijie(config-if-gigabitEthernet 1/1)#exit
```

### Configure relevant features of AAA authentication on the network device

#### Step 1: Enable AAA on the device

```
Ruijie#configure terminal
Ruijie(config)#aaa new-model
```

Step 2: Configure information about Radius server (the shared key used by device for communicating with RADIUS server is "aaaradius")

```
Ruijie(config)#radius-server host 192.168.32.120
Ruijie(config)#radius-server key aaaradius
```

### Step 3: Configure AAA authentication method list

! Configure login authentication method list (Radius first, followed by Local), and the name of method list shall be "method".

```
Ruijie(config)#aaa authentication login method group radius local
```

### Step 4: Apply this method list to the line

```
Ruijie(config)#line vty 0 4
Ruijie(config-line)#login authentication method
Ruijie(config-line)#exit
```

### Step 5: Configure local user database

! Configure local user database (configure user name and password, and bind the privilege level)

```
Ruijie(config)#username user1 privilege 1 password 111
Ruijie(config)#username user2 privilege 10 password 222
Ruijie(config)#username user3 privilege 15 password 333
```

! Configure local enable command for local enable authentication

```
Ruijie(config)#enable secret w
```

## Verifying Configurations

Step 1: Execute "show running-config" command to verify the current configurations:

```
Ruijie#show run

aaa new-model
!
aaa authentication login method group radius local
!
username user1 password 111
username user2 password 222
username user2 privilege 10
username user3 password 333
username user3 privilege 15

no service password-encryption
!
radius-server host 192.168.32.120
radius-server key aaaradius
enable secret 5 $1$hbqz$ArCsyqty6yyzpz03
enable service ssh-server
!
interface gigabitEthernet 1/1
no ip proxy-arp
ip address 192.168.217.81 255.255.255.0
!
ip route 0.0.0.0 0.0.0.0 192.168.217.1
!
```

```
line con 0
line vty 0 4
login authentication method
!
end
```

Step 2: Configure Radius Server. This example configures the SAM server.

1. In "System Management-Device Management", type in device IP of "192.168.217.81" and device key of "aaaradius";
2. In "Security Management - Device Management Privilege", configure the privilege level for the login user;
3. In "Security Management - Device Administrator", type in the user name of "user" and password of "pass".

Step 3: Establish remote SSH connection on the PC.

1. SSH client configuration and connection establishment: please refer to the previous example.
2. Type in the correct password: "user" for SSH user name and "pass" for password. The user will login successfully.

Step 4: Display login user.

```
Ruijie#show users
```

Line	User	Host(s)	Idle	Location
0 con 0		idle	00:00:31	
* 1 vty 0	user	idle	00:00:33	192.168.217.60



## Port-based Flow Control Configuration

### Storm Control

#### Overview

Too many broadcast, multicast or unknown unicast packets in the LAN will slow the network speed and increase the possibility of packet transmission timeout significantly. This is called LAN storm. Protocol stack implementation errors or wrong network configuration may lead to such storms.

Storm control can be conducted upon the broadcast, multicast and unknown unicast data streams respectively. When the rate of the broadcast, multicast or unknown unicast packets received by the interface exceeds the specified bandwidth throttling, the device only allows the packets within the bandwidth throttling. The packets that exceed the throttle will be discarded until the data stream becomes normal again. This prevents excessive flooding packets from entering the LAN to form a storm.

#### Configuring Storm Control

In the interface configuration mode, use the following command to configure storm control:

Command	Function
Ruijie(config-if)# <b>storm-control</b> { <b>broadcast</b>   <b>multicast</b>   <b>unicast</b> } [{ <b>level</b> <i>percent</i>   <b>pps</b> <i>packets</i>   <i>rate-bps</i> ]	<b>broadcast</b> : Enable the broadcast storm control function. <b>multicast</b> : Enable the unknown multicast storm control function. <b>unicast</b> : Enable the unknown unicast storm control function. <i>percent</i> : Set according to the bandwidth percentage, for example, 20 means 20% <i>packets</i> : Set according to the pps, which means packets per second <i>Rate-bps</i> : rate allowed

In the interface configuration mode, you can disable the storm control on the appropriate interface by using the **no storm-control broadcast**, **no storm-control multicast**, or **no storm-control unicast** command.

The following example enables the multicast storm control on GigabitEthernet 0/1 and set the allowed rate as 4M.

```
Ruijie# configure terminal
Ruijie(config)# interface GigabitEthernet 0/1
Ruijie(config-if)# storm-control multicast 4096
Ruijie(config-if)# end
```

## Viewing the Enable Status of Storm Control

To view the storm control status of the interface, use the following command:

Command	Function
Ruijie# <b>show storm-control</b> [ <i>interface-id</i> ]	Show storm control information.

The instance below shows the enabled status of the storm control function of interface Gi1/3:

```
Ruijie# show storm-control gigabitEthernet 0/3
Interface Broadcast Control Multicast Control Unicast Control action
GigabitEthernet 0/3 Disabled Disabled Disabled none
```

You can also view the enabling status of the storm control function of all interfaces at a time:

```
Ruijie# show storm-control
Interface Broadcast Control Multicast Control Unicast Control Action
-----
GigabitEthernet 0/1 Disabled Disabled Disabled none
GigabitEthernet 0/2 Disabled Disabled Disabled none
GigabitEthernet 0/3 Disabled Disabled Disabled none
GigabitEthernet 0/4 Disabled Disabled Disabled none
GigabitEthernet 0/5 Disabled Disabled Disabled none
GigabitEthernet 0/6 Disabled Disabled Disabled none
GigabitEthernet 0/7 Disabled Disabled Disabled none
GigabitEthernet 0/8 Disabled Disabled Disabled none
GigabitEthernet 0/9 Disabled Disabled Disabled none
GigabitEthernet 0/10 Disabled Disabled Disabled none
GigabitEthernet 0/11 Disabled Disabled Disabled none
GigabitEthernet 0/12 Disabled Disabled Disabled none
GigabitEthernet 0/13 Disabled Disabled Disabled none
GigabitEthernet 0/14 Disabled Disabled Disabled none
GigabitEthernet 0/15 Disabled Disabled Disabled none
GigabitEthernet 0/16 Disabled Disabled Disabled none
GigabitEthernet 0/17 Disabled Disabled Disabled none
GigabitEthernet 0/18 Disabled Disabled Disabled none
GigabitEthernet 0/19 Disabled Disabled Disabled none
GigabitEthernet 0/20 Disabled Disabled Disabled none
GigabitEthernet 0/21 Disabled Disabled Disabled none
GigabitEthernet 0/22 Disabled Disabled Disabled none
GigabitEthernet 0/23 Disabled Disabled Disabled none
GigabitEthernet 0/24 Disabled Disabled Disabled none
```

## Protected Port

### Overview

In some application environments, some ports are not required to communicate with each other on a device. In such case, frame forwarding is not allowed between the protected ports, no matter the frames are unicast frames, broadcast frames or multicast frames. To achieve this purpose, you can set some ports as protected ports.

Once ports are set as protected ports, they cannot communicate with each other. However, protected ports can still communicate with unprotected ports.

There are two protected port modes: one is to block layer 2 forwarding between protected ports but allow layer 3 routing; the other is to block layer 2 forwarding and layer 3 routing between protected ports. The first mode is by default when both modes are supported.

When you set two protected ports as a SPAN port pair, the frames transmitted or received by the source port of SPAN are sent to the destination port of SPAN according to the SPAN setting. Therefore, it is not recommended to set the destination port of SPAN as the protected port (and you can also save system resources by doing so).

The device supports setting the Aggregated Port as the protected port. Once you do that, all the member ports of the Aggregated Port will be set as the protected port.

## Configuring the Protected Port

Set one port as the protected port:

Command	Function
Ruijie(config-if)# <b>switchport protected</b>	Set this interface as a protected port

You can reset a port as unprotected port with the **no switchport protected** command in the interface configuration mode.

The following example describes how to set the GigabitEthernet 0/3 as the protected port.

```
Ruijie# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Ruijie(config)# interface gigabitEthernet 0/3
Ruijie(config-if)# switchport protected
Ruijie(config-if)# end
```

## Configuring the Route-deny Between Showing Protected Port Configuration

Command	Function
Ruijie(config-if)# <b>show interfaces switchport</b>	Show the configuration of the switching port

You can use the command of **show interfaces switchport** to view the configuration of protected port.

```
Ruijie# show interfaces gigabitEthernet 0/3 switchport
Interface  Switchport  Mode   Access Native Protected  VLAN lists
-----
GigabitEthernet 0/3  enabled   Trunk  1    1    Enabled   ALL
```

## Port Security

### Overview

Port security function allows the packets to enter the switch port by the source MAC address, source MAC+IP address or source IP address. You can control the packets by setting the specific MAC address statically, static IP+MAC binding or IP binding, or dynamically learning limited MAC addresses. The port with port security enabled is named as secure port. Only the packets with the source MAC address in the port security address table, or IP+MAC binding configured, or IP binding configured, or the learned MAC address, can join the switch communication, while other packets are dropped.

To enhance security, you can bind the MAC address with the IP address as the secure address. Of course you can also designate the MAC address without binding the IP address.

You can add the secure addresses on the port in the following ways:

- You can manually configure all the secure addresses of the port by using the commands in the interface configuration mode.
- You can also let this port automatically learn these addresses, which will become the secure address on this port till the total number reaches the maximum value. Note that, however, the automatically-learned secure addresses will not be bound with the IP address. On the same port, if you have configured a secure address bound with the IP address, the port cannot be added with any secure address by automatic learning.
- Manually configure some secure addresses, and let the device to learn the rest.

The port security also supports the Sticky MAC address, which can convert the secure addresses learned dynamically to the statically configured. You can use the **show running-config** command to display the configuration. With the configuration saved, learning these dynamic secure addresses after restarting the system is unnecessary. If this function is not enabled, then the dynamically learned secure MAC addresses should be learned again after the reboot.

When a port is configured as a secure port and the maximum number of its secure addresses is reached, a security violation occurs if the port receives a packet whose source address is not one of the secure addresses on the port. When security violations occur, you can set the following methods to handle:

- **protect:** When the maximum number of secure addresses is reached, the secure port discards the packet of unknown addresses (none of which are among the secure addresses of the port). This is the default method for handling exceptions.
- **restrict:** In the case of violation, a Trap notification is sent
- **shutdown:** In the case of violation, the port is shut down and a Trap notification is sent.

## Configuring Port Security

### Default Configuration of Port Security

The table below shows the default configuration of port security:

Item	Default Configuration
Port security switch	The port security function is disabled for all the ports.
Maximum number of secure addresses	128
Secure address	None
Handling mode for violations	Protect
Secure address binding mode	None
Sticky MAC address learning	Disabled

### Port Security Configuration Guide

The following restrictions apply to port security configuration:

- A secure port is not an Aggregate Port.
- A secure port is not the destination port of SPAN.
- A secure port is and can only be an Access Port.

The 802.1x authentication and port security are mutually exclusive in enabling. The 802.1x authentication and port security can ensure the validity of the network users. You can enable either of them to control port access.

At the same time, the secure addresses of the IP+MAC addresses and IP addresses share with the ACLs the hardware resources of the system. Therefore, when you apply the ACLs on one secure port, the IP+MAC addresses and IP addresses on the port can be configured with less secure addresses.

The secure addresses for the same secure port must have the same format, namely either all or none of them are bound with IP addresses. If a security port includes these two types of security addresses at the same time, the secure address not bound with the IP address will fail (the secure address bound with the IP address has a high priority).

### Configuration of Secure Ports and Violation Handling Modes

In the interface configuration mode, configure secure ports and violation handling modes by using the following commands:

Command	Function
Ruijie(config-if)# <b>switchport port-security</b>	Enable the port security function of this interface.
Ruijie(config-if)# <b>switchport port-security maximum value</b>	Set the maximum number of secure addresses on the interface. The range is between 1 and 1000 and the default value is 128.

Command	Function
Ruijie(config-if)# <b>switchport port-security violation{protect   restrict   shutdown}</b>	<p>Set the violation handling mode:</p> <p><b>protect</b>: Protected port. When the number of secure addresses is full, the security port will discard the packets from unknown address (that is, not any among the secure addresses of the port).</p> <p><b>restrict</b>: In the case of violation, a Trap notification is sent</p> <p><b>shutdown</b>: In the case of violation, the port is shut down and a Trap notification is sent. When a port is closed because of violation, you can recover it from the error status by using the <b>errdisable recovery</b> command in the global configuration mode.</p>
Ruijie(config-if)# <b>switchport port-security mac-address sticky</b>	Enable the Sticky MAC address learning.

In the interface configuration mode, you can disable the port security function of an interface with the command **no switchport port-security**. Use the command **no switchport port-security maximum** to recover to the default maximum value. Use the command **no switchport port-security violation** to set violation handling to the default mode. Use the command **no switchport port-security mac-address sticky** to set the Sticky MAC address learning to the default mode.

The instance below describes how to enable the port security function on interface gigabitethernet 0/3. The maximum number of addresses to be set is 8 and the violation handling mode is set as protect.

```
Ruijie# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Ruijie(config)# interface gigabitethernet 0/3
Ruijie(config-if)# switchport mode access
Ruijie(config-if)# switchport port-security
Ruijie(config-if)# switchport port-security maximum 8
Ruijie(config-if)# switchport port-security violation protect
Ruijie(config-if)# switchport port-security mac-address sticky
Ruijie(config-if)# end
```

**Note**

1. If the DOT1X has been enabled on the interface and the authenticated user number has exceeded the maximum limit, it fails to enable the port security function.
2. With the port security and DOT1X function enabled at the same time, If the secure address ages out, the DOT1X user can continue to communicate after the re-authentication.
3. It needs no authentication to access to the network for the secure address on the static port.
4. If the violation mode is modified on the interface, the new violation mode takes effect only after the security port restores to the non-violation state.

### Configuration of Secure Addresses on the Secure Port

In the global configuration mode, add secure addresses for secure ports by using the following commands:

Command	Function
Ruijie(config)# <b>switchport-security</b> <b>interface</b> <i>interface-id</i> <b>mac-address</b> <i>mac-address</i> <b>vlan</b> [ <i>vlan_id</i> ]	In the global configuration mode, manually configure the secure addresses on the port.

In the interface configuration mode, add secure addresses for secure ports by using the following commands:

Command	Function
Ruijie(config-if)# <b>switchport-security</b> <b>mac-address</b> <i>mac-address</i> <b>vlan</b> [ <i>vlan_id</i> ]	In the interface configuration mode, manually configure the secure addresses on the port.
Ruijie(config-if)# <b>switchport-security</b> <b>mac-address sticky</b> <i>mac-address</i> <b>vlan</b> [ <i>vlan_id</i> ]	In the interface configuration mode, manually configure the Sticky secure addresses on the port.

In the interface configuration mode, you can use the command **no switchport port-security mac-address** *mac-address* to delete the secure address of this interface. Use the command **no switchport port security sticky mac-address** *mac-address* to delete the Sticky secure address of this interface.

The example below describes how to configure a secure address for interface gigabitethernet 0/3: 00d0.f800.073c and bind it with an IP address: 192.168.12.202.

```
Ruijie# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Ruijie(config)# interface gigabitethernet 0/3
Ruijie(config-if)# switchport mode access
Ruijie(config-if)# switchport port-security
```

```
Ruijie(config-if)# switchport port-security mac-address 00d0.f800.073c ip-address
192.168.12.202
Ruijie(config-if)# end
```

The example below describes how to configure a secure address for the Sticky-MAC-learning-enabled interface gigabitethernet 0/3: 00d0.f800.073c.

```
Ruijie# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Ruijie(config)# interface gigabitethernet 0/3
Ruijie(config-if)# switchport mode access
Ruijie(config-if)# switchport port-security
Ruijie(config-if)# switchport port-security mac-address sticky
Ruijie(config-if)# switchport port-security mac-address sticky 00d0.f800.073c vlan 1
Ruijie(config-if)# end
```

## Configuration of Secure Address Binding on the Secure Port

In the global configuration mode, add secure address binding for secure ports by using the following commands:

Command	Function
Ruijie(config)# <b>switchport port-security interface interface-id binding [mac-address vlan vlan_id] [ipv4-address] [ipv6-address]</b>	In the global configuration mode, manually configure the secure addresses binding on the port.

In the interface configuration mode, add secure addresses for secure ports by using the following commands:

Command	Function
Ruijie(config-if)# <b>switchport port-security binding [mac-address vlan vlan_id] [ipv4-address] [ipv6-address]</b>	In the interface configuration mode, manually configure the secure addresses binding on the port.

The example below describes how to configure a secure address for interface gigabitethernet 0/3 and bind it with an IP address: 192.168.12.202.

```
Ruijie# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Ruijie(config)# interface gigabitethernet 0/3
Ruijie(config-if)# switchport mode access
Ruijie(config-if)# switchport port-security
Ruijie(config-if)# switchport port-security binding 192.168.12.202
Ruijie(config-if)# end
```

The example below describes how to configure a secure address for interface gigabitethernet 0/3 and bind it with an source IP+MAC address: 192.168.12.202, : 00d0.f800.073c.

```
Ruijie# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Ruijie(config)# interface gigabitethernet 0/3
```



```
Ruijie(config-if)# switchport mode access
Ruijie(config-if)# switchport port-security
Ruijie(config-if)# switchport port-security binding 00d0.f800.073c vlan 1 192.168.12.202
Ruijie(config-if)# end
```

**Note**

For the packets that correspond to the IP+MAC binding and IP binding, they can be forwarded on the condition that the source MAC address must be the secure address at the same time. For the dynamic secure address, before adding the secure address to the secure address table, any packets that correspond to the secure address binding or IP binding can not be forwarded.

## Configuration of Aging Time for Secure Addresses

You can configure the aging time for all the secure addresses on an interface. To enable this function, you need to set the maximum number of secure addresses. In this way, you can make the device automatically add/remove the secure addresses to/from the interface.

In the interface configuration mode, configure the aging time for secure addresses by using the following command:

Command	Function
<pre>Ruijie(config-if)#<b>switchport</b> <b>port-security aging{static   time</b> <b>time }</b></pre>	<p><b>static:</b> When this keyword is added, the aging time will be applied to both the manually configured secure address and automatically learnt addresses. Otherwise, it is applied only to the automatically learnt addresses.</p> <p><b>time:</b> indicates the aging time for the secure address on this port. Its range is 0-1440 and unit is Minute. If you set it to be 0, the aging function actually is disabled. The aging time is the absolute time, which means that an address will be deleted automatically after the <i>Time</i> specified expires after the address becomes the secure address of the port. The default value of <i>Time</i> is 0.</p>

In the interface configuration mode, use **no switchport port-security aging time** to disable the port security aging. Use the **no switchport port-security aging static** to apply the aging time only to dynamically learned security address.

The example below describes how to configure the port security aging time on interface Gigabitethernet 0/3. The aging time is set to 8 minutes and it is applicable to statically-configured secure addresses:

```
Ruijie# configure terminal
```

```

Enter configuration commands, one per line. End with CNTL/Z.
Ruijie(config)# interface gigabitethernet 0/3
Ruijie(config-if)# switchport port-security aging time 8
Ruijie(config-if)# switchport port-security aging static
Ruijie(config-if)# end

```

**Caution**

The Sticky MAC address is a special MAC address, which is not affected by the aging mechanism. No matter whether the dynamic aging or static aging is configured, the Sticky MAC address will not be aged.

## Viewing Port Security Information

In the privileged EXEC mode, you can view the security information of a port by using the following commands.

Command	Function
Ruijie# <b>show port-security interface</b> [ <i>interface-id</i> ]	View the port security configuration of an interface.
Ruijie# <b>show port-security address</b>	View the secure address information.
Ruijie# <b>show port-security address</b> [ <i>interface-id</i> ]	Show the secure address information on an interface.
Ruijie# <b>show port-security</b>	Show the statistics of all the security ports, including the maximum number of secure addresses, the number of current addresses, and violation handling mode.

The example below shows the port security configuration on interface **gigabitethernet 0/3**:

```

Ruijie# show port-security interface gigabitethernet 0/3
Interface Gi0/3
Port Security: Enabled
Port status : down
Violation mode:Shutdown
Maximum MAC Addresses:8
Total MAC Addresses:0
Configured MAC Addresses:0
Aging time : 8 mins
SecureStatic address aging : Enabled

```

The instance below shows all the secure addresses in the system.

```

Ruijie# show port-security address
Vlan Mac Address IP Address Type Port Remaining Age(mins)
-----
1 00d0.f800.073c 192.168.12.202 Configured Gi0/3 8
1 00d0.f800.3cc9 192.168.12.5 Configured Gi0/1 7

```

You can also only show the secure address on one interface. The instance below shows the secure address on interface **gigabitethernet 0/3**.

```

Ruijie# show port-security address interface gigabitethernet 0/3
Vlan Mac Address IP Address Type Port Remaining Age(mins)
-----

```

```
1 00d0.f800.073c 192.168.12.202 Configured Gi0/3 8
```

The example below shows the statistic information of the secure port.

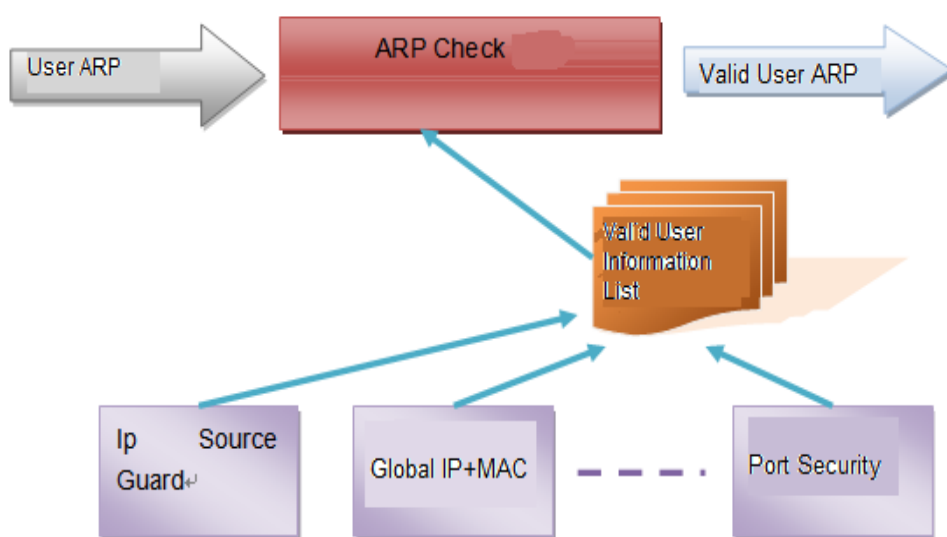
```
Ruijie# show port-security
Secure Port MaxSecureAddr(count) CurrentAddr(count) Security Action
-----
Gi0/1      128                1          Restrict
Gi0/2      128                0          Restrict
Gi0/3       8                1          Protect
```

## ARP-CHECK

### Overview

ARP-Check function filters all ARP packets on the logic interface and drops all illegal ARP packets, avoiding the ARP fraud in the network and improving the network stability.

Ruijie switches support multiple IP security application(such as IP Source Guard, global IP+MAC binding, port security, ect), which effectively filter the user IP packets and avoid the illegal user to use the network resources. The ARP check function generates the corresponding ARP filtering information according to the legal user information (IP or IP+MAC), implementing the illegal ARP packet filtering in the network.



### ARP Check and other security functions

As shown in the above figure, ARP Check function checks whether the Sender IP field or the <Sender IP, Sender MAC> field of all ARP packets on the logic interface matches with the legal user information(IP or IP+MAC), and the ARP packets that not match with the legal user information. The ARP Check function supported security function modules include:

1. Check the IP field only: IP mode for the port security and the ip source guard.

2. Check the IP+MAC field: IP+MAC binding mode for the port security, global IP+MAC binding, 802.1x IP authorization, IP Source Guard, GSN binding function.

There are two modes of ARP-CHECK: enabled, disabled mode. The disabled mode is by default.

- In the enabled mode, ARP Check function is enabled or disabled according to the current security function running state on the switch.

Enabling/disabling the following functions may trigger to enable/disable the ARP Check function:

1. Global IP+MAC binding
2. 802.1X IP authorization
3. IP Source Guard
4. GSN binding

Adding the legal user for the first time or removing the last legal user may trigger to enable/disable the ARP Check function:

1. IP+MAC binding mode for the port security
2. IP-only mode for the port security

ARP check is enabled no matter whether there is security configuration. If there is no legal user on the port, all the arp packets from this port will be discarded.

- In the disabled mode, ARP packet on the port is not checked.



#### Caution

1. Enabling ARP check of port security addresses will decrease the maximum number of the security addresses of binding IP on all the ports by half.

## Configuring ARP-CHECK

Use the following commands to configure ARP-CHECK in the privileged EXEC mode:

Command	Function
Ruijie# <b>configure t</b>	Enter the global configuration mode.
Ruijie(config)# <b>interface</b> <i>interface-id</i>	Enter the interface configuration mode.
Ruijie(config-if)# <b>arp-check</b>	Enable arp check.
Ruijie(config-if)# <b>no arp-check</b>	Disable arp check.
Ruijie(config-if)# <b>arp-check auto</b>	Restore to the default configuration: enabled.

## Showing the ARP Check Entry on the interface

Use the following commands to show the ARP check entry information on the interface:

Command	Function
Ruijie# <b>show interface</b> { <i>interface-type interface-number</i> } <b>arp-check list</b>	Show the ARP check entry information.

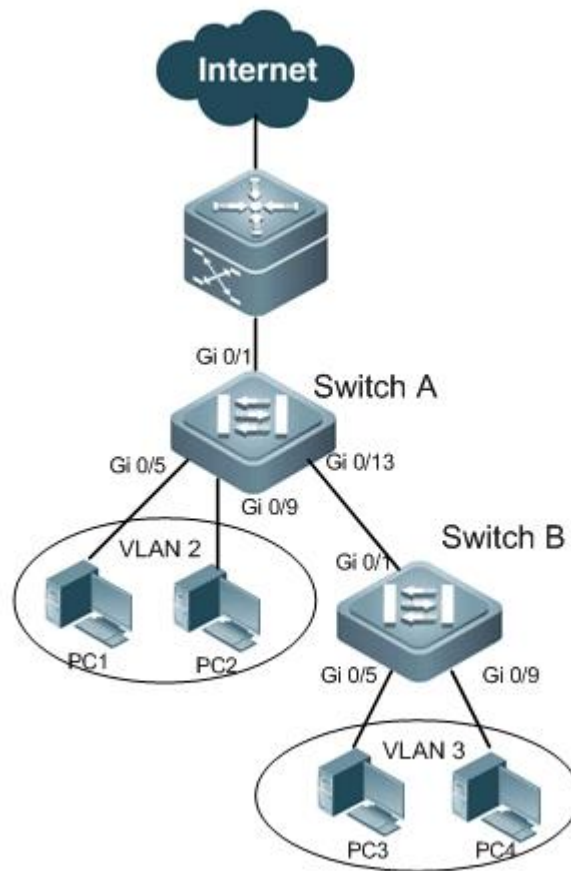
The example below shows the ARP check entry information:

```
Ruijie#show interfaces arp-check list
```

Interface	Sender MAC	Sender IP	Policy Source
Gi 0/1	00D0.F800.0003	192.168.1.3	address-bind
Gi 0/1	00D0.F800.0001	192.168.1.1	port-security
Gi 0/4		192.168.1.3	port-security
Gi 0/5	00D0.F800.0003	192.168.1.3	address-bind
Gi 0/7	00D0.F800.0006	192.168.1.6	AAA ip-auth-mode
Gi 0/8		00D0.F800.0007	192.168.1.7 GSN

## Example of Port-based Flow Control Combination

### Topological Diagram



Network topology

### Application Requirements

The above diagram shows the simplified topology of an typical Intranet. The following requirements must be met:

1. Prevent the devices from being attacked by broadcast, multicast and unknown unicast packets.
2. Allow directly connected users (users directly connected to Switch A) to access Internet with the specified IP/MAC address; packets with source address different from the specified IP/MAC address will be discarded to avoid source IP/MAC spoofing.
3. Access users (users accessing Switch B) are not allowed to carry out layer-2 packet communication, so as to avoid the mutual interference between access users (such as ARP spoofing or DOS attack).

### Configuration Tips

Configuration tips:

1. Enable storm control on the ports of all access devices (Switch A and Switch B).
2. Configure port security feature on the ports (Gi 0/5 and Gi 0/9) of access device (Switch A) to meet the second requirement.
3. Configure port protection on the access device (Switch B) to meet the third requirement.

Note:

After enabling port security and configuring IP/MAC entries, ARP Check will be enabled automatically to check the source address of ARP packets according to the configured IP/MAC address.

## Configuration Steps

### Configure Switch A

Step 1: Create the VLAN to which the switch belongs and configure port attributes.

! Create VLAN 2

```
Ruijie#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Ruijie(config)#vlan 2
Ruijie(config-vlan)#exit
```

! Configure port attributes

```
Ruijie(config)#interface gigabitEthernet 0/5
Ruijie(config-if-GigabitEthernet 0/5)#switchport access vlan 2
Ruijie(config-if-GigabitEthernet 0/5)#exit
Ruijie(config)#interface gigabitEthernet 0/9
Ruijie(config-if-GigabitEthernet 0/9)#switchport access vlan 2
Ruijie(config-if-GigabitEthernet 0/9)#exit
Ruijie(config)#interface gigabitEthernet 0/1
Ruijie(config-if-GigabitEthernet 0/1)#switchport mode trunk
Ruijie(config-if-GigabitEthernet 0/1)#exit
Ruijie(config)#interface gigabitEthernet 0/13
Ruijie(config-if-GigabitEthernet 0/13)#switchport mode trunk
Ruijie(config-if-GigabitEthernet 0/13)#exit
```

Step 2: Enable storm control on all access ports.

```
Ruijie(config)#interface range gigabitEthernet 0/1,0/5,0/9,0/13
Ruijie(config-if-range)#storm-control broadcast
Ruijie(config-if-range)#storm-control multicast
Ruijie(config-if-range)#storm-control unicast
Ruijie(config-if-range)#exit
```

Step 3: Enable port security on the port directly connecting with users and bind the IP address and MAC address

! Bind the access user: IP (1.1.1.1)/MAC (0000.0000.0001)

```
Ruijie(config)#interface gigabitEthernet 0/5
Ruijie(config-if-GigabitEthernet 0/5)#switchport port-security
Ruijie(config-if-GigabitEthernet 0/5)#switchport port-security mac-address 0000.0000.0001
ip-address 1.1.1.1
Ruijie(config-if-GigabitEthernet 0/5)#exit
```

### **! Bind the access user: IP (1.1.1.2)/MAC (0000.0000.0002)**

```
Ruijie(config)#interface gigabitEthernet 0/9
Ruijie(config-if-GigabitEthernet 0/9)#switchport port-security
Ruijie(config-if-GigabitEthernet 0/9)#switchport port-security mac-address 0000.0000.0002
ip-address 1.1.1.2
Ruijie(config-if-GigabitEthernet 0/9)#exit
```

## **Configure Switch B**

**Step 1: Create the VLAN to which the switch belongs and configure port attributes.**

### **! Create VLAN 3**

```
Ruijie#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Ruijie(config)#vlan 3
Ruijie(config-vlan)#exit
Ruijie(config)#interface gigabitEthernet 0/5
Ruijie(config-if-GigabitEthernet 0/5)#switchport access vlan 3
Ruijie(config-if-GigabitEthernet 0/5)#exit
Ruijie(config)#interface gigabitEthernet 0/9
Ruijie(config-if-GigabitEthernet 0/9)#switchport access vlan 3
Ruijie(config-if-GigabitEthernet 0/9)#exit
Ruijie(config)#interface gigabitEthernet 0/1
Ruijie(config-if-GigabitEthernet 0/1)#switchport mode trunk
Ruijie(config-if-GigabitEthernet 0/1)#exit
```

**Step 2: Enable storm control on all access ports.**

```
Ruijie(config)#interface range gigabitEthernet 0/1,0/5,0/9
Ruijie(config-if-range)#storm-control broadcast
Ruijie(config-if-range)#storm-control multicast
Ruijie(config-if-range)#storm-control unicast
Ruijie(config-if-range)#exit
```

**Step 3: Enable port protection on all access ports.**

```
Ruijie(config)#interface gigabitEthernet 0/5
Ruijie(config-if-GigabitEthernet 0/5)#switchport protected
Ruijie(config-if-GigabitEthernet 0/5)#exit
Ruijie(config)#interface gigabitEthernet 0/9
Ruijie(config-if-GigabitEthernet 0/9)#switchport protected
Ruijie(config-if-GigabitEthernet 0/9)#exit
```



## Verification

Step 1: Check the configurations of Switch A. Key points: whether storm control has been enabled on respective ports, whether port security has been enabled on the port directly connecting with users and whether IP+MAC addresses have been bound statically.

```
Ruijie#show running-config
vlan 2
!
interface GigabitEthernet 0/1
  switchport mode trunk
  storm-control broadcast
  storm-control multicast
  storm-control unicast
!
interface GigabitEthernet 0/5
  switchport access vlan 2
  switchport port-security mac-address 0000.0000.0001 ip-address 1.1.1.1
  switchport port-security
  storm-control broadcast
  storm-control multicast
  storm-control unicast
!
interface GigabitEthernet 0/9
  switchport access vlan 2
  switchport port-security mac-address 0000.0000.0002 ip-address 1.1.1.2
  switchport port-security
  storm-control broadcast
  storm-control multicast
  storm-control unicast
!
interface GigabitEthernet 0/13
  switchport mode trunk
  storm-control broadcast
  storm-control multicast
  storm-control unicast
```

Step 2: Check the configurations of Switch B. Key points: whether storm control has been enabled on respective ports, and whether port protection has been enabled on the port directly connecting with users.

```
Ruijie#show running-config
vlan 3
!
interface GigabitEthernet 0/1
  switchport mode trunk
  storm-control broadcast
  storm-control multicast
```

```

storm-control unicast
!
interface GigabitEthernet 0/5
  switchport access vlan 3
  switchport protected
  storm-control broadcast
  storm-control multicast
  storm-control unicast
!
interface GigabitEthernet 0/9
  switchport access vlan 3
  switchport protected
  storm-control broadcast
  storm-control multicast
  storm-control unicast

```

**Step 3: View address bindings on the ports of Switch A and ARP check enabling state.**

```

Ruijie#show port-security all
Vlan Port  Arp-Check  Mac Address  IP Address  Type  remaining Age (mins)
----
2    Gi0/5  Enabled  0000.0000.0001  1.1.1.1    Configured  -
2    Gi0/9  Enabled  0000.0000.0002  1.1.1.2    Configured  -

```

**Step 4: View port security configurations on GigabitEthernet 0/5 of Switch B. Port security configurations on other ports won't be further introduced.**

```

Ruijie#show interfaces gigabitEthernet 0/5 switchport
Interface  Switchport Mode  Access Native Protected VLAN lists
-----
GigabitEthernet0/5 enabled ACCESS 3 1 Enabled ALL

```

## Limiting the Number of Access IPs on the Port

- Overview
- Default configurations to limit the number of access IPs on the port
- Configure the maximum number of access IPs on the port
- Display the number of access IPs on the port

### Overview

Ruijie switches support multiple access control applications (such as: IP Source Guard, port security, global IP+MAC binding and etc). These port access applications implement access control through the source IP address of the user in order to filter IP packets and prevent invalid users from using network resources.

The feature of limiting the number of access IPs on the port is intended to limit the number of access IPs bound by these secure access applications on the port, so as to limit the number of users sharing the port bandwidth of switch.

You can configure the number of IP addresses allowed to access network for each port. If the number of IP addresses bound by respective access applications on the port hasn't reached the configured threshold, the access applications shall be able to further bind and add valid users; if the number of IP addresses has reached the configured threshold, the access applications won't be able to further bind valid users.

If the number of IP addresses under the port has exceeded the configured threshold, the excessive IP addresses won't be allowed to pass through.



1. Limiting the number of access IPs on the port will take effect only if IP+MAC bindings or IP bindings of access control applications have taken effect. If no access application has been configured on the port (or if the port is the excluded port of global IP+MAC bindings), the limiting won't take effect.
2. When a same IP address is bound by IP+MAC binding and IP binding, it will be treated as two user IPs.
3. The access IP limiting only applies to IPv4 packets.
4. Except for the excluded port of global IP+MAC binding, the users added via global IP+MAC binding will be included into the number of IP addresses limited on each port.

## Default Configurations to Limit the Number of Access IPs on the Port

The following table shows the default configurations to limit the number of access IPs on the port

Function	Default Setting
Limiting the number of access IPs on the port	This feature is disabled on all ports. The default value is 0.

## Configuring the Maximum Number of Access IPs on the Port

In privileged EXEC mode, configure the maximum number of access IPs on the port:

Command	Function
Ruijie# configure	Enter configuration mode
Ruijie(config)#interface interface-id	Enter interface mode
Ruijie(config-if)#nac-author-user maximum value	Configure the maximum number of access IPs on the port
Ruijie(config-if)#no nac-author-user maximum	Disable the maximum number of access IPs on the port

## Displaying the Number of Access IPs on the Port

You can view the maximum number of access IPs configured on the port and the number of IP address bindings:

Command	Function
Ruijie#show nac-author-user	Display the maximum number of access IPs on the port and the number of IP address bindings.

As shown below:

```
Ruijie#show nac-author-user
Port      Cur_num  Max_num
-----
Fa0/1      2        50
Fa0/2      0         0
Fa0/3      2       100
Fa0/4      0         0
Fa0/5      0       200
Fa0/6      0         0
Fa0/7      0         0
Fa0/8      0         0
```

## CPU Protection Configuration

### Overview

Various attack packets are broadcasted in the network environment, leading to too high CPU utilization on the switch and abnormal operation of it. For this reason, the switch CPU must be protected, that is, our switches allows you to configure the CPP to control and manage the packets sent to the switch CPU and protect the normal processing capability of the switch.

The implementation model for the CPU Protect is divided into 4 phases: Classifying, Queueing, Scheduling and Shaping. The following explains the 4 phases in detail.

#### ■ Classifying:

Classify every packet sent to the CPU according to the L2, L3 and L4 information of the packet. The table below lists the detailed information:

- 
- L2 switches do not support L3 packets. L3 packets include L3 protocol packets (PIM, OSPF, RIP, and ISIS packets) and packets of udp-helper, error-ttl, error-hop-limit, v4uc-route, and v6uc-route.. As a L2 switch, does not support these packets. IS2700G supports static routing, plus L3 packets including v4uc-route and v6uc-route packets.
- 

#### ■ Queueing:

Send different types of the message to the specified queue. The messages in the different queues have different transmission privilege.

CPU port has 8 privilege queues in total. You can set the queue correspondent with each type of message. Queueing is able to auto-send the type of message to the specified queue.

#### ■ Scheduling:

If the messages in several queues will be transmitted, Scheduling is able to select one of the queues and transmit the messages in this queue.

The Scheduling for the CPU port adopts the SP(Strict Priority) algorithm, with queue7 the highest priority and queue0 the lowest. The queue packets in high priority are always transmitted before the packets in low priority, which allows you to configure the priority values for different queues correspond to the importance of each packet and ensure that the important packets takes the precedence to be transmitted.



#### Note

If rate-limiting packets exist both in high-priority queues and low-priority queues, few packets in low-priority queues are transmitted.

#### ■ Shaping:

Shaping controls the maximum rate of each transmission queue, and the packets transmitted at the rate exceeding the limit will be dropped. You shall configure the maximum rate of each queue according to the actual network condition and configure the maximum rate for the CPU port at the same time.

## Configuring CPU Protect

The following sections describe how to configure CPU Protect.

- CPU Protect Default Configuration
- CPU Protect Configuration Guide
- Configure the Queue for Each Type of Message
- Configure the Max-rate for Each Queue
- Configure the Max-rate for the CPU Port
- Configure the MAC Address Storm Control Rate

### CPU Protect Default Configuration

Different network attacks occur for different types of switches in different network environment. To this end, Ruijie provides different CPU protect default value for different switches.



IS2700G series switches

The packet types and their corresponding queues are listed as follows:

Packet Type	Queue
bpdv	6
arp-request	3
arp-replay	3
tpp	6
802.1x	2
gvrp	5
rldp	5
lacp	5
rerp	5
reup	5
lldp	5
dhcp	2
qinq	2
igmp	2
icmp	4
local-telnet	4
local-snmp	4
local-http	4
local-tftp	4
local-other	4
v4uc-route	0
v6uc-route	0
mld	2
nd	3
erps	5
mpls-data	0
mpls-lspv	4
web-auth	0
cfm	6
other	0

The default maximum rates of all queue are listed as follows:

Queue	Default Rate(pps)
6	3500
5	1500
4	1500
3	1500
2	1500
1	1000
0	1000
CPU port	6000

## CPU Protect Configuration Guide

- ☑ Note that the rate of the CPU port and each queue is pps when configuring IS2700G series switches.
- ☑ The bfd or dldp packet queue sent to the CPU port by IS2700G series switches cannot be modified through the cpp interface.

### Configuring the Queue for Each Type of Message

In the configuration mode, configure the queue of each type of packet by performing the following steps:

Command	Function
<pre>Ruijie(config)# <b>cpu-protect type</b> { <b>bpdu</b>   <b>arp</b>   <b>tpp</b>   <b>dot1x</b>   <b>gvrp</b>   <b>rdlp</b>   <b>dhcp</b>   <b>unknown-ipv6-mc</b>   <b>known-ipv6-mc</b>   <b>unknown-ipv4-mc</b>   <b>known-ipv4-mc</b>   <b>udp-helper</b>   <b>dvmrp</b>   <b>igmp</b>   <b>icmp</b>   <b>ospf</b>   <b>pim</b>   <b>rip</b>   <b>vrrp</b>   <b>error-ttl</b>   <b>error-hop-limit</b>   <b>local-telnet</b>   <b>local-snmp</b>   <b>local-http</b>   <b>local-tftp</b>   <b>local-other</b>   <b>ipv4-uc</b>   <b>ipv6-uc</b>   <b>mld</b>   <b>ns</b>   <b>other</b> } <b>traffic-class</b> <b>traffic-class-num</b></pre>	Set the queue for each type of packets. <i>traffic-class-num</i> : in the range of 0-7.

Use the **no** form of this command to restore the queue of each type of packets.

This example shows the configuration process:

```
Ruijie(config)# cpu-protect type bpdu traffic-class 5
Ruijie(config)# end
Ruijie # show cpu-protect type bpdu traffic-class
%*****packet type      traffic-class*****
                bpdu          5
```



#### Caution

The packet types configured by the **cpu-protect type** command vary by products. For details, refer to Section Classification.

### Configuring the Max-rate for Each Queue

In the configuration mode, configure the max-rate for the queue:

Command	Function
<pre>Ruijie(config)# <b>cpu-protect traffic-class id</b> <b>id_num bandwidth bandwidth_value</b></pre>	Set the max-rate for each queue in kbps. <i>id_num</i> : in the range of 0-7; <i>bandwidth_value</i> : in the range of 32-131072kbps.

Command	Function
Ruijie(config)# <b>cpu-protect traffic-class all bandwidth</b> <i>bandwidth_value</i>	Set the max-rate for all queues in kbps. <i>bandwidth_value</i> : in the range of 32-131072kbps.

Use the **no cpu-protect traffic-class** command to restore the default max-rate value for each queue.

This example shows how to set the max-rate for queue 7 as 312kbps:

```
Ruijie#configure terminal
Ruijie(config)# cpu-protect traffic-class id 7 bandwidth 312
Ruijie(config)#end
Ruijie# show cpu-protect traffic-class id 7
%*****traffic class      bandwidth(kbps)*****
              7              312
```

```
Ruijie# configure terminal
Ruijie(config)# cpu-protect traffic-class id 6 bandwidth 3500
Ruijie(config)#end
Ruijie# show cpu-protect traffic-class id 6
Traffic-class  Bandwidth(pps)  Rate(pps)
-----
6              3500            0
```

## Configuring the Max-rate for the CPU Port

In the configuration mode, configure the queue of each type of packet by performing the following steps:

Command	Function
Ruijie(config)# <b>cpu-protect cpu bandwidth</b> <i>bandwidth_value</i>	Set the max-rate for the CPU port in kbps. <i>bandwidth_value</i> : in the range of 64-1000000kbps.

Use the **no cpu-protect cpu** command to restore the default max-rate value for the CPU port.

This example shows the max-rate for the CPU port as 2000kbps:

```
Ruijie#configure terminal
Ruijie(config)#cpu-protect cpu bandwidth 2000
Ruijie(config)#end
Ruijie#show cpu-protect cpu
%cpu port bandwidth: 2000(kbps)
```

```
Ruijie# configure terminal
Ruijie(config)# cpu-protect cpu bandwidth 6000
Ruijie(config)# end
Ruijie# show cpu-protect cpu
%cpu port bandwidth: 6000(pps)
```



## Configuring Storm Control for MAC Address Learning

In the configuration mode, configure storm control for learning MAC addresses by performing the following steps:

Command	Function
Ruijie(config)# <b>cpu-protect mac-address storm-control enable</b> <i>value</i>	Set the MAC address storm control rate. <i>value</i> : in the range of 200-51200kbps.

This example configures storm control of learning MAC address as 3000(address/second):

```
Ruijie#configure terminal
Ruijie(config)# cpu-protect mac-address storm-control enable 3000
Ruijie(config)#end
Ruijie# show cpu-protect mac-address storm-control
%MAC address storm control state: enable
%MAC address storm control rate: 3000(address/second)
```

## Showing CPU Protect Configuration

- Show the queue for the corresponding type of message
- Show the max-rate for each queue
- Show the max-rate for the CPU port
- Show the MAC address storm control rate

## Showing the Queue for Each Type of Message

In the privileged EXEC mode, use the following command to view the queue for each type of message:

The following example shows how to show the queues for all types of message:

```
Ruijie#show cpu-protect type all
%*****packet type      traffic-class*****
          bpdu           6
          arp            5
          igmp           3
          dot1x          3
          gvrp           3
          dhcp           2
          unicast        4
          multicast      1
          broadcast      0
          error_ttl      0
          co-operate     6
          other          0
```

## Showing the Max-rate for Each Queue

In the privileged EXEC mode, use the following command to view the max-rate for each queue:

Command	Function
Ruijie# <b>show cpu-protect traffic-class</b> <i>id id_num</i>	Show the max-rate for each queue. <i>id_num</i> : in the range of 0-7.
Ruijie# <b>show cpu-protect traffic-class</b> <b>all</b>	Show the max-rate for all queues.

The following example shows the max-rate for all queues:

```
Ruijie(config)# show cpu-protect traffic-class all
%*****traffic class      bandwidth(kbps)*****
      0                1000
      1                1000
      2                1000
      3                1000
      4                1000
      5                1000
      6                1000
      7               100000
```

## Showing the Max-rate for the CPU Port

In the privileged EXEC mode, use the following command to view the max-rate for the CPU port:

Command	Function
Ruijie# <b>show cpu-protect cpu</b>	Show the max-rate for the CPU port.

The following example shows the max-rate for the CPU port:

```
Ruijie# show cpu-protect cpu
%cpu port bandwidth: 100000(kbps)
```

## Showing Storm Control of Learning MAC Addresses

In the privileged EXEC mode, use the following command to show the storm control of learning MAC addresses:

Command	Function
Ruijie# <b>show cpu-protect mac-address</b> <b>storm-control</b>	Show storm control rate of learning MAC address.

The following example shows the MAC address storm control rate:

```
Ruijie# show cpu-protect mac-address storm-control
%MAC address storm control state: enable
%MAC address storm control rate: 2000(address/second)
```

# DoS Protection Configuration

## DoS Protection Configuration

### Overview

The DoS protection function can defend against Land attacks, invalid TCP message attacks and invalid L4 message attacks.

#### ■ Land attack

The attacker sends a SYN packet to the destination host with the source address/port the same as the destination address/port and causes system crash while the attacked host attempts to establish a TCP link with itself (infinite loop).

#### ■ Invalid TCP message attack

The header of TCP message contains several flag fields:

1. SYN: Connection flag. TCP SYN message sets this flag to 1 in order to request a connection.
  2. ACK: Acknowledgment flag. In a TCP connection, except for the first message (TCP SYN), all other messages are set to be the acknowledgement to last message.
  3. FIN: Finish flag. When a host receives a TCP message with FIN flag, it will terminate this TCP connection.
  4. RST: Reset flag. When IP protocol stack receives a TCP message with nonexistent target port, it will reply a message with RST flag.
  5. PSH: notifies the protocol stack to push up TCP data to the upper-layer program as soon as possible.
- Invalid TCP message attack consumes host resources and leads to system crash by setting invalid flag fields. The followings are some frequently found invalid TCP messages:

##### 1. TCP message with both SYN bit and FIN bit

Under normal conditions, SYN flag (connection request flag) and FIN flag (connection termination flag) cannot exist in the same TCP message, and RFC has no related stipulations on how IP protocol stack shall deal with such a deformed message. Therefore, the protocol stack of different operating systems will handle in different ways after receiving such a message. By utilizing this feature, the attacker sends a message with both SYN flag and FIN flag to identify the type of operating system, and initiate further attacks against the target operating system.

##### 2. TCP message with no flag

Under normal conditions, any TCP message will contain at least one of SYN, FIN, ACK, RST and PSH flags. The first TCP message (TCP connection request message) will contain SYN flag, and the following messages will all contain ACK flag. Based on such an assumption, some protocol stack doesn't have the corresponding handling process for TCP message with no flag. Therefore, such a protocol stack may crash upon receipt of such a message. The attacker will utilize this feature to attach the target host.

##### 3. TCP message with FIN flag but no ACK flag

Under normal conditions, except for the first message (SYN message), all other messages will contain the ACK flag, including TCP connection termination message (with FIN flag). However, some attackers

may send a TCP message with FIN flag but no ACK flag to the target host, leading to the crash of target host.

☒ IS27 products do not provide protect against TCP packets with FIN flag and without ACK flag set.

#### ■ Self-consumption attack

In this condition, the attacker sends the message with the same Layer-4 port number as the target host service to the target host, so that the target host sends the TCP request and connection to itself. This attack quickly exhausts the target host resources, even leads the system crash.

☒ IS27 products do not provide protect against self-consumption attack.

## DoS Protection Configuration

### Default DoS Protection Configuration

The default DoS protection configuration is given below:

Function	Default setting
land attack protection	Disabled
Invalid TCP message attack protection	Disabled
Self-consumption message attack protection	Disabled

### Defending against Land attack

To enable Land attack protection function, run the following commands:

Command	Function
Ruijie# <b>configure terminal</b>	Enter global configuration mode
Ruijie(config)# <b>ip deny land</b>	Enable Land attack protection function
Ruijie(config)# <b>end</b>	Return to privileged EXEC mode

### Defending against invalid TCP message attack

To enable invalid TCP message attack protection function, run the following commands:

Command	Function
Ruijie# <b>configure terminal</b>	Enter global configuration mode
Ruijie(config)# <b>ip deny invalid-tcp</b>	Enable invalid TCP message attack protection function
Ruijie(config)# <b>end</b>	Return to privileged EXEC mode

### Defending against self-consumption message attack

To enable self-consumption message attack protection function, run the following commands:

Command	Function
---------	----------

Ruijie# <b>configure terminal</b>	Enter global configuration mode
Ruijie(config)# <b>ip deny invalid-l4port</b>	Enable self-consumption message attack protection function
Ruijie(config)# <b>end</b>	Return to privileged EXEC mode

## Displaying DoS Protection Status

### Displaying Land attack protection status

To display Land attack protection status, run the following commands:

Command	Function
<b>show ip deny land</b>	Display Land attack protection status

The example below shows how to display the Land attack protection status:

```
Ruijie# show ip deny land
DoS Protection Mode      State
-----
protect against land attack      On
```

### Displaying invalid TCP message attack protection status

To display invalid TCP message attack protection status, run the following commands:

Command	Function
<b>show ip deny invalid-tcp</b>	Display invalid TCP message attack protection status

The example below shows how to display the invalid TCP message attack protection status:

```
Ruijie# show ip deny invalid-tcp
DoS Protection Mode      State
-----
protect against invalid tcp attack      On
```

### Displaying self-consumption attack protection status

To display self-consumption attack protection status, run the following commands:

Command	Function
<b>show ip deny invalid-l4port</b>	Display self-consumption attack protection status

The example below shows how to display the self-consumption attack protection status:

```
Ruijie# show ip deny invalid-l4port
DoS Protection Mode      State
-----
protect against invalid l4port attack      On
```

## Ingress Filtering for DoS Attack Protection

### Overview

In recent years, the spread of various DoS (Denial of Service) attack messages over Internet has brought about considerable troubles to Internet users. There are many kinds of DoS attacks, while the basic form of DoS attack utilizes valid service requests to occupy excessive service resources, thus making valid users unable to get service response. The attack messages will mainly disguise the source IP to avoid exposure.

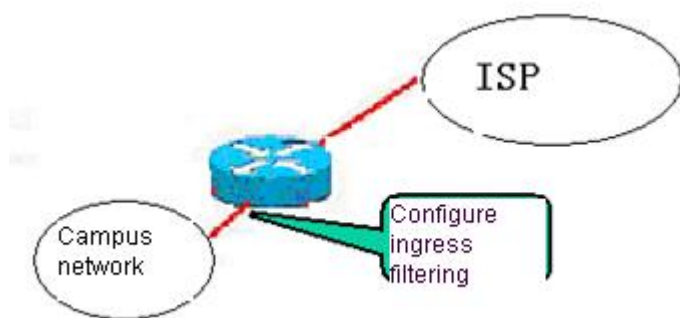
In regard to this, RFC2827 has proposed to set up Ingress Filtering at network access point to prevent messages with disguised source IP from accessing the network. Such an approach puts emphasis upon the early stage of attack and overall prevention of DoS attacks, and thus has satisfactory effects. Such filtering can also help ISP and network administrator to accurately locate the attackers using true and valid source IP addresses.

Ruijie network switch adopts RFC2827-based ingress filtering rules to defend against DoS attacks. The filtering is achieved through the automatic generation of specific ACLs by the switch itself, and will not pile any pressure on network forwarding.

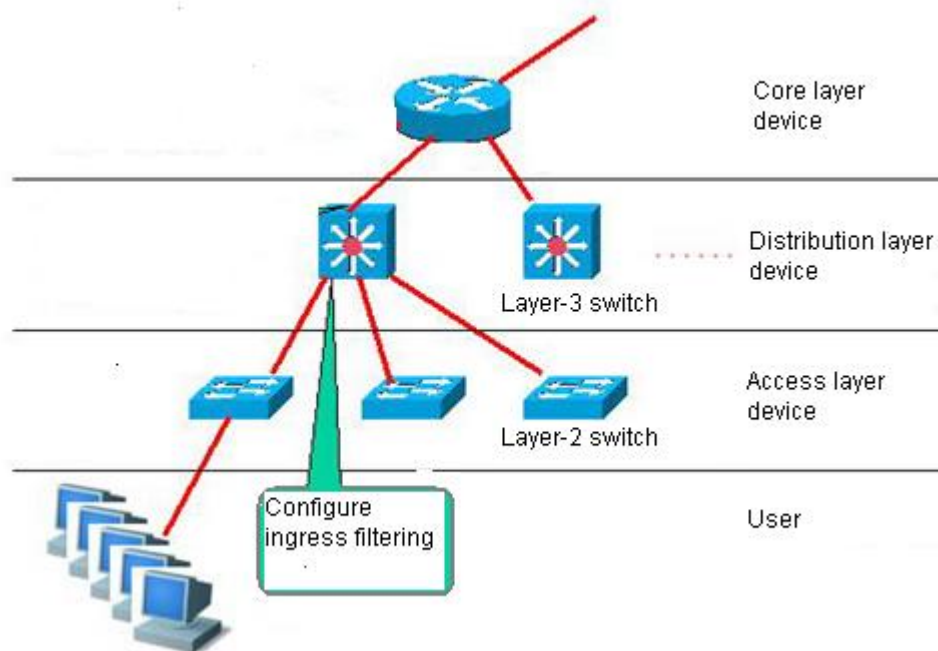
Of course, you can also use the address binding or Dot1x function of Ruijie network switch to achieve filtering effect, or by setting up ACLs.

### Typical applications

A. ISP deploys ingress filtering on the access router to prevent messages with disguised source IP from accessing ISP and Internet:



B. The enterprise network (campus network) deploys ingress filtering on layer-3 switch to prevent messages with disguised source IP from accessing enterprise (campus) network:



## Configuring Ingress Filtering to Defend Against DoS Attack

### Default configuration

The ingress filtering for defending against DoS attacks is disabled on all network interfaces.

### Precautions

Only layer-3 interfaces with network address can support ingress filtering for defending against DoS attacks.

By enabling defeat DoS based ingress filtering on the designated layer-3 interface, the system will automatically establish the corresponding ACL for the network interface to restrict the access of disguised source IP, and apply the ACL to the ingress of layer-3 interface.

For example: The network address on SVI 1 is 192.168.5.1/24. If "ip deny spoofing-source" is configured in the interface configuration mode, the following ACL will be generated automatically and applied to this interface.

```
permit 192.168.5.0 0.0.0.255
```

```
permit host 0.0.0.0 (This ACE permits the access of DHCP requests with source address being 0.0.0.0)
```

```
deny any
```



#### Caution

- This filtering can only be configured on the direct link interface. Apply ingress filtering on convergence-layer interface (uplink port) will prevent Internet messages with various source IP addresses from reaching the downlink hosts at the convergence layer.
- After configuring DoS protection based ingress filtering, the no command must be used to disable DoS protection function in order to modify the address of network interface.

## Set up Ingress Filtering to Defend Against DoS Attack

To set up ingress filtering, run the following commands:

Command	Function
Ruijie# <b>configure terminal</b>	Enter global configuration mode.
Ruijie(config)# <b>interface</b> <i>interface-id</i>	Enter layer-3 interface
Ruijie(config-if)# <b>ip deny spoofing-source</b>	Ingress filtering function to defend against disguised source IP based DoS attacks. Drop all incoming messages without consistent prefix with this network interface. (Note: Only layer-3 interface can be configured with this function)
Ruijie(config-if)# <b>show running interface</b> <i>interface-id</i>	Verify the configuration of ingress filtering.

Use the **no ip deny spoofing-source** command to disable the ingress filtering function (for DoS attack protection) in the interface configuration mode.

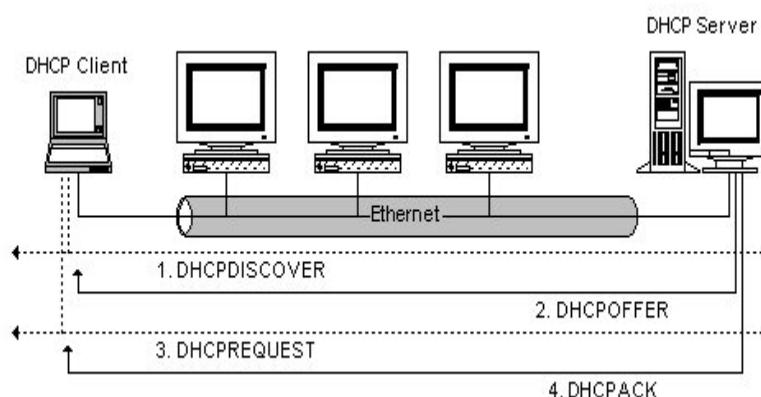


# DHCP Snooping Configuration

## Overview

### Understanding DHCP

The DHCP protocol is widely used to dynamically allocate the recycled network resources, for example, IP address. A typical IP acquisition process using DHCP is shown below:



The DHCP Client sends a DHCP DISCOVER broadcast packet to the DHCP Server. The Client will send the DHCP DISCOVER again if it does not receive a response from the server within a specified time. After the DHCP Server receives the DHCP DISCOVER packet, it allocates resources to the Client, for example, IP address according to the appropriate policy, and sends the DHCP OFFER packet. After receiving the DHCP OFFER packet, the DHCP Client sends a DHCP REQUEST packet to obtain the server lease and notify other servers of receiving the address allocated by the server. After receiving the DHCP REQUEST packet, the server verifies whether the resources are available. If so, it sends a DHCP ACK packet. If not, it sends a DHCP NAK packet. Upon receiving the DHCP ACK packet, the DHCP Client starts to use the resources assigned by the server in condition that the ARP verification resources are available. If it receives the DHCP NAK packet, the DHCP Client will send the DHCP DISCOVER packet again.

### Understanding DHCP Snooping

**DHCP Snooping** monitors users by snooping the packets exchanged between the clients and the server. DHCP Snooping can filter DHCP packets and illegal servers by proper configuration. Some terms and functions used in DHCP Snooping are explained below:

- 1) **DHCP request packets** are sent from DHCP clients to the DHCP server.
- 2) **DHCP response packets** are sent from the DHCP server to DHCP clients.

- 3) **DHCP Snooping TRUST port:** Because the packets for obtaining IP addresses through DHCP are in the form of broadcast, some illegal servers may prevent users from obtaining IP addresses, or even cheat and steal user information. To solve this problem, DHCP Snooping classifies the ports into two types: TRUST port and UNTRUST port. The device forwards only the DHCP reply packets received through the TRUST port while discarding all the DHCP reply packets from the UNTRUST port. In this way, the illegal DHCP Server can be shielded by setting the port connected to the legal DHCP Server as a TRUST port and other ports as UNTRUST ports.
- 4) **DHCP Snooping packet filtering:** To prohibit DHCP packets of an individual user, you need to evaluate all DHCP packets sent from the user device. Then, you can configure the DHCP packet filtering function in the port mode to filter all DHCP packets received by the port.
- 5) **VLAN Based DHCP Snooping:** DHCP Snooping takes effect by VLAN. By default, when DHCP Snooping is enabled, it is enabled for all VLANs on the device. You can perform required configurations to restrict validation on specific VLANs.
- 6) **DHCP Snooping bound database:** Users may randomly set static IP addresses on a network in the DHCP environment. This brings difficulty in maintaining the network, and causes that users fail to use the network properly after legally obtaining the IP address through DHCP. After binding with the database, DHCP Snooping spies on the interactive packets between the client and the server, and forms the user database of DHCP Snooping by using the following items as user record entries:
  - IP addresses obtained by users
  - User MAC addresses
  - VIDs
  - Ports
  - Lease time.Thus, users must legally use IP addresses.
- 7) **DHCP Snooping rate limiting:** DHCP Snooping needs to check all DHCP request packets from all untrusted ends and forward legal DHCP request packets to the network where trusted interfaces reside. To prevent attacks of DHCP request packets from untrusted ends, the rate is limited for transmitting DHCP request packets to the trusted network. DHCP Snooping supports rate limiting for DHCP packets received at a port. When the rate of DHCP packets received at a port exceeds the specified threshold, the threshold-exceeding DHCP packets are discarded. DHCP Snooping limits rate based on the interface configuration. The effect is equal when you configure DHCP Snooping rate limiting by running:
  - Command of DHCP Snooping rate limiting
  - Command of NFPP rate limitingFor products supporting CPP, CPP configuration takes priority over DHCP Snooping rate limiting when the two functions are both configured. In this case, to make DHCP Snooping rate limiting takes effect, ensure that the upper limit of CPP rate limiting is equal to or greater than that of DHCP Snooping rate limiting or NFPP. For details about how to configure CPP, see *Configuring CPU Protection*.  
For details about how to configure NFPP, see the NFPP configuration guide.

DHCP Snooping verifies DHCP packets, accordingly discards illegal DHCP packets, records user information, and generates DHCP Snooping bound database, so that other functions such as the ARP detection function can query the database. The following types of packets are considered as illegal DHCP packets:

- DHCP response packets received by the UNTRUST port, including DHCPACK, DHCPNACK, and DHCPOFFER.
- DHCP request packets with gateway information [giaddr] received by the UNTRUST port.
- Packets whose chaddr value is inconsistent with that in the source MAC address during MAC address verification.
- DHCPRELEASE packets meeting the following conditions:
  - Users in DHCPRELEASE packets exist in the DHCP Snooping bound database;
  - The DHCPRELEASE packet receiving port is inconsistent with the port in the DHCP Snooping bound database.

## Understanding DHCP Snooping Information Option

Some network administrators hope to assign user IP addresses based on user locations during IP address management. That is, they hope to assign user IP addresses based on users' network devices. Thus, when performing DHCP spying, switches can add user device information as DHCP options to DHCP request packets. According to RFC3046, the option ID is 82. Option 82 includes 255 sub-options at most. To define option 82, you need to define one sub-option at least. Currently, devices only support two sub-options:

Circuit ID

Remote ID. If option 82 parsing is configured on the DHCP server, the server can obtain user information from contents uploaded to option 82, thereby assigning user IP addresses more properly.

- Circuit ID:

Default fill contents:

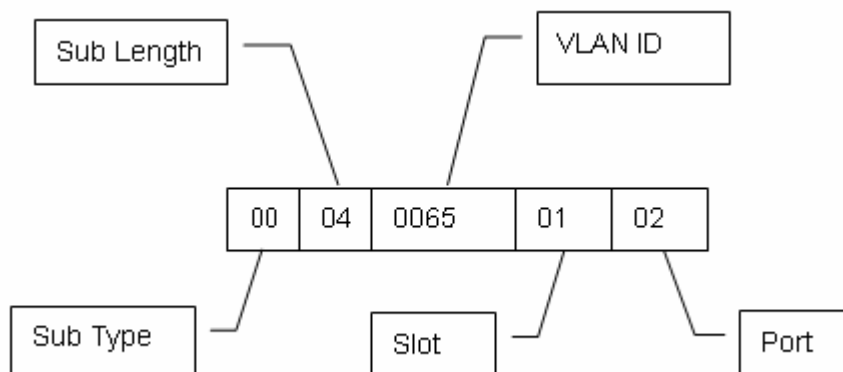
VLAN ID and index of the port that receives request packets from the DHCP client. The port index value consists of the port number and number of the port where the port resides.

Extended fill contents:

Customized character strings.

Circuit ID fill formats can be standard or extended. Either the standard or extended format can be used in one network domain. For the standard fill format, the Circuit ID sub-option can fill contents shown in the following figure.

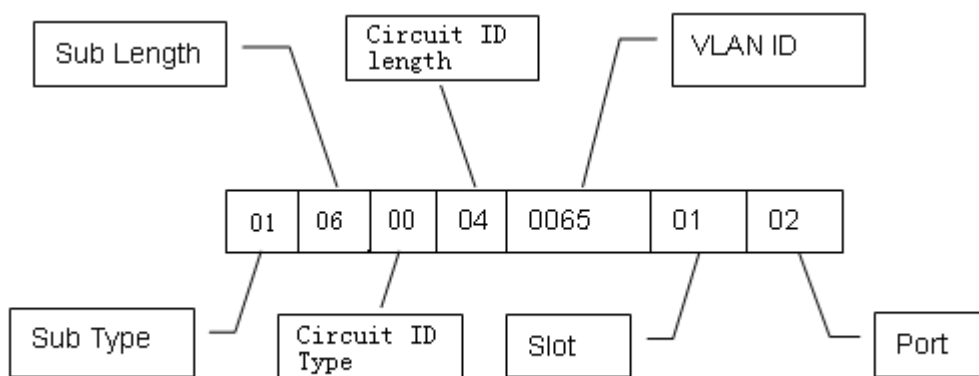
Figure 1-1



To fill customized contents, use the extended fill format. You can fill default or customized contents in the extended fill format. To distinguish fill contents, a byte of content type field and a byte of content length field are added after the sub-option length. For default fill contents, set the content length field to 0. For extended fill contents, set the content length field to 1.

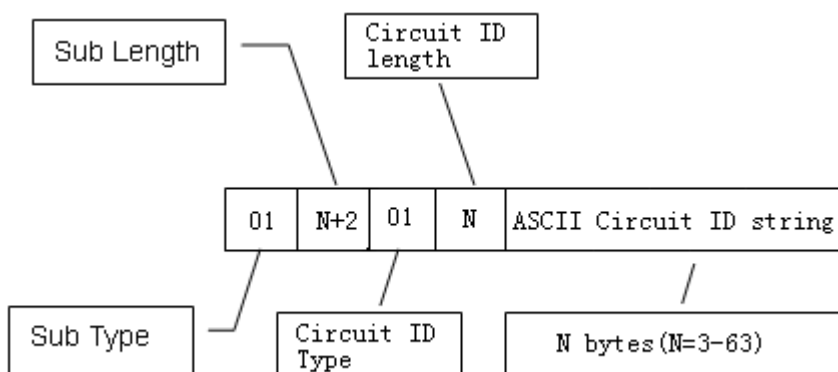
The following figure shows the format of default fill contents.

Figure 1-2



The following figure shows the format of extended fill contents.

Figure 1-3



#### ■ Remote ID:

Default fill contents:

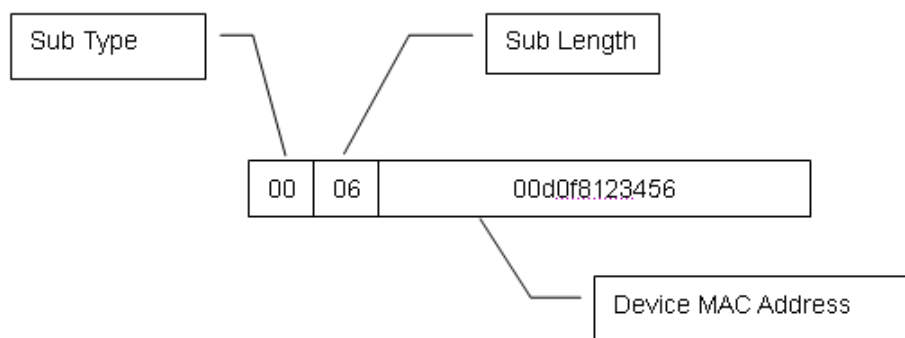
Bridge MAC addresses of DHCP trunk devices that receive request packets from the DHCP client;

Extended fill contents:

Customized character strings.

Remote ID fill formats can be standard or extended. Either the standard or extended format can be used in one network domain. For the standard fill format, the Remote ID sub option can fill contents shown in the following figure.

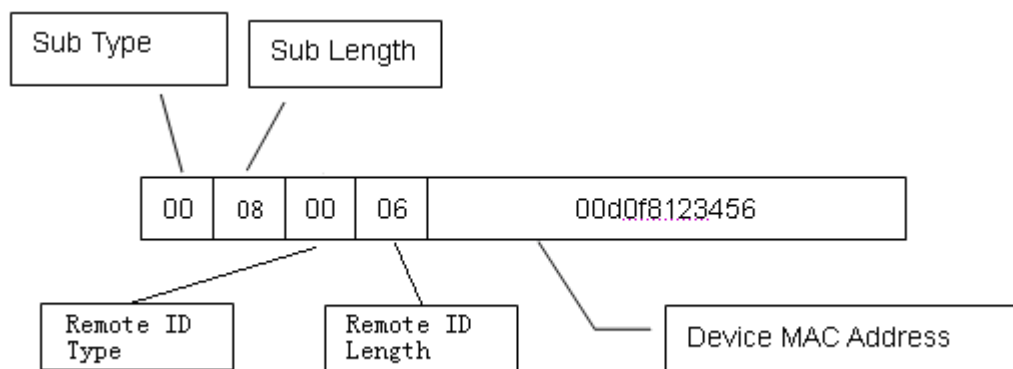
Figure 1-4



To fill customized contents, use the extended fill format. You can fill default or customized contents in the extended fill format. To distinguish fill contents, a byte of content type field and a byte of content length field are added after the sub-option length. For default fill contents, set the content length field to 0. For extended fill contents, set the content length field to 1.

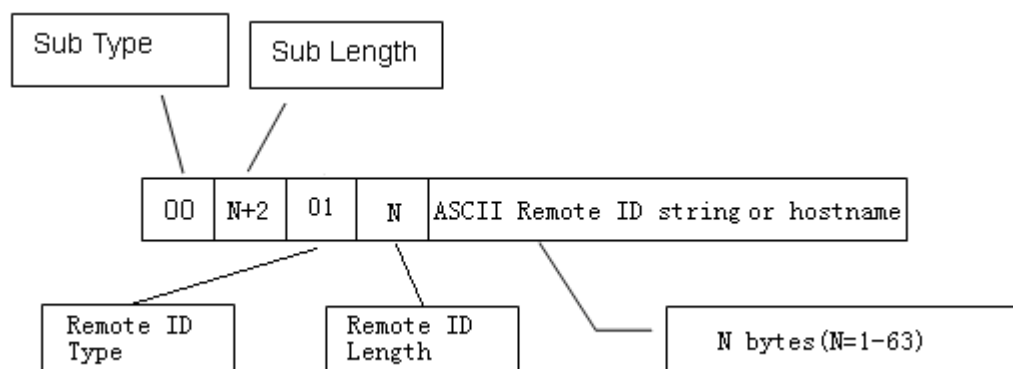
The following figure shows the format of default fill contents.

Figure 1-5



The following figure shows the format of extended fill contents.

Figure 1-6



The port index value consists of the port number and number of the port where the port resides. The port number indicates the sequence number of port in the slot. For an AP port, the port number is the AP number. For example, the port number of Fa0/10 is 10, and the port number of AP 11 is 11. The slot number is the sequence number of the slot among all slots on the device (a stack is considered as a device). The slot number of an AP port is in the last. The slot sequence number starts from 0, and you can view them by running the **show slots** command. The following are two examples. :

Example 1:

```
Ruijie#show slots (only Deve and slot are listed as examples)
```

```
Dev Slot
```

```
--- ---
```

```
1 0 ----->The slot number is 0.
```

```
1 1 ----->The slot number is 1.
```

```
1 2 ----->The slot number is 2.
```

Here, the slot number of the AP port is 3.

Example 2:

```
Ruijie#show slots (only Deve and slot are listed as examples)
```

```
Dev Slot
```

```
--- ---
```

```
1 0 ----->The slot number is 0.
```

```
1 1 ----->The slot number is 1.
```

```
1 2 ----->The slot number is 2.
```

```
2 0 ----->The slot number is 3.
```

```
2 1 ----->The slot number is 4.
```

```
2 2 ----->The slot number is 5.
```

Here, the slot number of the AP port is 6.

## DHCP Snooping Configuration

### Enabling and Disabling DHCP Snooping

The DHCP Snooping function of the device is disabled by default. To enable DHCP Snooping and then monitor DHCP packets, execute the following command.

Command	Function
Ruijie# <b>configure terminal</b>	Enter the global configuration mode.
Ruijie(config)# <b>[no] ip dhcp snooping</b>	Enable or disable DHCP snooping.

The following example demonstrates how to enable the DHCP snooping function of the device:

```
Ruijie# configure terminal
```

```
Ruijie(config)# ip dhcp snooping
```

```
Ruijie(config)# end
```

```
Ruijie# show ip dhcp snooping
```

```
Switch DHCP snooping status : ENABLE
```

```
DHCP snooping Verification of hwaddr status : DISABLE
```

```
DHCP snooping database write-delay time : 0 seconds
```

```
DHCP snooping option 82 status : DISABLE
```

```
DHCP snooping Support bootp bind status : DISABLE
```

Interface	Trusted	Rate limit (pps)
-----	-----	-----
GigabitEthernet 0/1	YES	unlimited

## Relationship Between DHCP Snooping and DAI

Dynamic ARP Inspection (DAI) verifies all ARP packets passing a device. DHCP bound filtering is effective only for IP packets, and cannot filter ARP packets. To enhance security and avoid ARP spoofing, ARP packets need to be verified for DHCP bound users. DHCP Snooping provides database information for ARP detection. On the device where DAI is enabled, assume that ARP packets are received on the port enabled with IP Source Guard address binding. In this case, the DAI module queries the DHCP Snooping bound database, considers the packets are legal, and learns and forwards the packets when their source MAC addresses, source IP addresses, and port information match. Otherwise, these packets are discarded. For more information, see *DAI Configuration Guide*.

## Enabling Filtering the DHCP Request Message on the Port

By default, filtering the DHCP request message is disabled on the port. To enable this function, execute the following command.

Command	Function
Ruijie# <b>configure terminal</b>	Enter the global configuration mode.
Ruijie(config)# <b>interface</b> <i>interface</i>	Enter the interface configuration mode.
Ruijie(config)# <b>[no] ip dhcp snooping suppression</b>	Enable or disable filtering the DHCP request message.

The following example demonstrates how to enable filtering the DHCP request message:

```
Ruijie# configure terminal
Ruijie(config)# interface gigabitEthernet 0/1
Ruijie(config-if)# ip dhcp snooping suppression
```

## Enabling DHCP Snooping in VLAN

By default, DHCP Snooping takes effect for all VLANs. To restrict validation on specific VLANs, remove unwanted VLANs from the validation range of DHCP Snooping.

This command enables DHCP Snooping in the VLAN.

Command	Function
Ruijie# <b>configure terminal</b>	Enter the global configuration mode.
Ruijie(config)# <b>[no] ip dhcp snooping vlan</b> <b>{vlan-rng   {vlan-min [vlan-max]}}</b>	Enable DHCP Snooping in the VLAN.

Here is an example of enabling the DHCP Snooping in VLAN1000:

```
Ruijie# configure terminal
Ruijie(config)# ip dhcp snooping vlan 1000
Ruijie(config)# end
```

When DHCP Snooping is enabled, it is enabled for all VLANs on the device. To restrict validation on specific VLANs, add or remove VLANs from the validation range of DHCP Snooping.

## Configuring DHCP Source MAC Address Check Function

After configuring this command, the device will match the MAC address of the DHCP Request packet from the UNTRUST port against the one in the client field and discard unmatched packet. By default, this function is not enabled.

To configure the source MAC address check function, execute the following command:

Command	Function
Ruijie# <b>configure terminal</b>	Enter the global configuration mode.
Ruijie(config)# <b>[no]ip dhcp snooping verify mac-address</b>	Enable or disable the source MAC address check function.

The following example shows how to enable the DHCP source MAC address check function:

```
Ruijie# configure terminal
Ruijie(config)# ip dhcp snooping verify mac-address
Ruijie(config)# end
Ruijie# show ip dhcp snooping
Switch DHCP snooping status : ENABLE
DHCP snooping Verification of hwaddr status : ENABLE
DHCP snooping database write-delay time : 0 seconds
DHCP snooping option 82 status : DISABLE
DHCP snooping Support bootp bind status : DISABLE
Interface Trusted Rate limit (pps)
-----
GigabitEthernet 0/1 YES unlimited
```

## Configuring Static DHCP Snooping Information Option

Run the following commands to add option 82 to every DHCP request during DHCP spying and forwarding. By default, this function is disabled.

Command	Function
Ruijie# <b>configure terminal</b>	Enter the configuration mode.
Ruijie(config)# <b>[no] ip dhcp snooping information option [standard-format]</b>	Set DHCP Snooping information option. <b>standard-format</b> : The standard fill format is used when this keyword exists. Otherwise, the extended fill format is used.
Ruijie(config)# <b>[no] ip dhcp snooping information option format remote-id [string ASCII-string   hostname]</b>	Configure remote-id in the extended format. <b>string</b> : Fill customized character strings. <b>hostname</b> : Fill host names.
Ruijie(config)# <b>interface interface</b>	Enter the interface configuration mode.
Ruijie(config-if)# <b>[no] ip dhcp snooping vlan vlan-id information option format-type circuit-id string ASCII-string</b>	Configure the customized character string of circuit-id in the extended format.
Ruijie(config-if)# <b>[no] ip dhcp snooping vlan vlan-id information option change-vlan-to vlan vlan-id</b>	Configure the VLAN mapping of circuit-id in the extended format. This command is exclusive of the command in Step 5.

The following configuration enables DHCP snooping information option:



```

Ruijie# configure terminal
Ruijie(config)# ip dhcp snooping information option
Ruijie(config)# end
Ruijie# show ip dhcp snooping
Switch DHCP snooping status : ENABLE
DHCP snooping Verification of hwaddr status : ENABLE
DHCP snooping database write-delay time : 0 seconds
DHCP snooping option 82 status : ENABLE
DHCP snooping Support bootp bind status : DISABLE
Interface Trusted Rate limit (pps)
-----
GigabitEthernet 0/1 YES unlimited

```

**Caution**

After this function is configured, DHCP relay option82 function configured on the device will be ineffective.

## Writing the DHCP Snooping Database to Flash Periodically

By default, this function is disabled. DHCP Snooping provides a command to write the DHCP Snooping database to the flash periodically in order to prevent loss of DHCP user information when the device restarts due to an electricity failure.

Command	Function
Ruijie# <b>configure terminal</b>	Enter the global configuration mode.
Ruijie(config)# <b>[no] ip dhcp snooping database write-delay [time]</b>	Specify the interval at which the switch writes the DHCP database to the flash. <i>time</i> : 600s to 86400s. The default value is 0.

The following example sets the interval at which the switch writes the DHCP database to the flash to 3600s:

```

Ruijie# configure terminal
Ruijie(config)# ip dhcp snooping database write-delay 3600
Ruijie(config)# end
Ruijie# show ip dhcp snooping
Switch DHCP snooping status : ENABLE
DHCP snooping Verification of hwaddr status : ENABLE
DHCP snooping database write-delay time : 3600 seconds
DHCP snooping option 82 status : ENABLE
DHCP snooping Support bootp bind status : DISABLE
Interface Trusted Rate limit (pps)
-----
GigabitEthernet 0/1 YES unlimited

```

**Caution**

You need to set a proper time for writing to the flash since erasing and writing to the flash frequently shortens its life. A shorter time helps to save the device information more effectively. A longer time reduces the times of writing to the flash and increases service life of flash.

## Writing DHCP Snooping Database to Flash Manually

To prevent loss of DHCP user information when the device restarts due to an electricity failure, the administrator can write the DHCP Snooping binding database to the flash manually.

Command	Function
Ruijie# <b>configure terminal</b>	Enter the global configuration mode.
Ruijie(config)# <b>ip dhcp snooping database write-to-flash</b>	Write the DHCP Snooping binding database to the flash manually.

The following example demonstrates how to write the DHCP Snooping binding database to the flash:

```
Ruijie# configure terminal
Ruijie(config)# ip dhcp snooping database write-to-flash
Ruijie(config)# end
```

## Manually Exporting Information in Flash to the DHCP Snooping Database

When enabling DHCP snooping, you need to manually export information in flash to the DHCP Snooping bound database.

Command	Function
Ruijie# <b>renew ip dhcp snooping database</b>	Manually export information in flash to the DHCP Snooping bound database.

Run the following command to manually export information in flash to the DHCP Snooping bound database:

```
Ruijie# renew ip dhcp snooping database
```

## Configuring a Port as a TRUST Port

By default, all the ports are UNTRUST ports. After configuring this command, a port is set as the TRUST port and connected to the legal DHCP server.

Command	Function
Ruijie# <b>configure terminal</b>	Enter the global configuration mode.
Ruijie(config)# <b>interface interface-id</b>	Enter the interface configuration mode.
Ruijie(config-if)# <b>[no] ip dhcp snooping trust</b>	Set the port as a trust port.

The following example shows how to set GigabitEthernet 0/1 as a TRUST port:

```
Ruijie# configure terminal
Ruijie(config)# interface gigabitEthernet 0/1
Ruijie(config-if)# ip dhcp snooping trust
Ruijie(config-if)# end
Ruijie# show ip dhcp snooping
Switch DHCP snooping status : ENABLE
```

```

DHCP snooping  Verification of hwaddr status    :   DISABLE
DHCP snooping database write-delay time        :   3600 seconds
DHCP snooping option 82 status                  :   DISABLE
DHCP snooping Support bootp bind status        :   DISABLE
Interface           Trusted           Rate limit (pps)
-----
GigabitEthernet 0/1   YES             unlimited

```

**Caution**

After DHCP Snooping is enabled, only the DHCP response packets from the server configured with the TRUST port are forwarded.

## Configuring Rate of Receiving DHCP Packet

This command configures rate of receiving DHCP in the corresponding interface:

Command	Function
Ruijie# <b>configure terminal</b>	Enter the global configuration mode.
Ruijie(config)# <b>interface interface-id</b>	Enter the interface configuration mode.
Ruijie(config-if)# <b>[no] ip dhcp snooping limit rate rate-value</b>	Configures rate of receiving DHCP packet on the port.

The following example shows how to set the rate of receiving DHCP packet on GigabitEthernet 0/1 as 100pps:

```

Ruijie# configure terminal
Ruijie(config)# interface gigabitEthernet 0/1
Ruijie(config-if)# ip dhcp snooping limit rate 100
Ruijie(config-if)# end
Ruijie(config-if)#sh run interface gigabitEthernet 0/1
interface GigabitEthernet 0/1
  nfpp dhcp-guard policy per-port 100 200

```

**Caution**

When setting DHCP Snooping rate limiting, check the DHCP rate limit set by CPP. |

If the DHCP rate limit set by CPP is lower, DHCP packets are still discarded within the DHCP Snooping rate limiting range. By default, DHCP rate limiting is disabled.

**Caution**

Assume that:

DHCP Snooping is enabled on a device;

The DHCP server is not deployed on the device;

More than three users apply for IP addresses currently within 1 second.

In this case, you need to adjust the CPP rate limiting of the Trust port based on the network deployment for ensuring that all users can obtain IP addresses normally.

In DHCP application standards, 40 users can send applications currently at most. With this as an example, you need to configure rate-limit-pps of nfpp dhcp-guard policy per-src-mac to 80 pps and attack-threshold-pps to 160 pps for the Trust port.

The output of the **show run interface** command shows that:

From RGOS10.4(2), the rate limiting command of DHCP Snooping is replaced by the rate limiting command of NFPP. To maintain upgrade compatibility, the rate limiting command of DHCP Snooping is still valid, but will be valid in NFPP after configuration. Besides, if the rate limiting command is configured on the AP, the command will take effect on all member ports of the AP because NFPP can be configured based on only physical ports while DHCP Snooping supports AP port configuration. This also means that the configuration of the rate limiting command of DHCP Snooping on an AP without any member port will be lost after upgrade because the AP does not have any member port. However, rate limiting in this case is meaningless. Therefore, this problem does not affect actual network applications.

## Clearing Dynamic User Information from the DHCP Snooping Binding Database

To clear dynamic user information from the DHCP Snooping binding database, execute the following command.

Command	Function
Ruijie# <b>clear ip dhcp snooping binding</b> [vlan <i>vlan-id</i>   <i>mac</i>   <i>ip</i>   <b>interface</b> <i>interface-id</i> ]	Clear information from the current database.

The following example shows how to clear information from the current database manually:

```
Ruijie# clear ip dhcp snooping binding
```

## Showing DHCP Snooping Configuration

### Showing DHCP Snooping

To show DHCP Snooping, execute the following command:

Command	Function
Ruijie# <b>show ip dhcp snooping</b>	Show the configuration of DHCP snooping.

For example:

```
Ruijie# show ip dhcp snooping
Switch DHCP snooping status           :  ENABLE
DHCP snooping Verification of hwaddr status :  ENABLE
DHCP snooping database write-delay time :  3600 seconds
DHCP snooping option 82 status         :  ENABLE
DHCP snooping Support bootp bind status :  ENABLE
Interface          Trusted      Rate limit (pps)
-----
GigabitEthernet 0/1  YES        unlimited
```

### Showing the DHCP Snooping Database

To show the DHCP Snooping database, execute the following command:

Command	Function
---------	----------

Command	Function
Ruijie# <b>show ip dhcp snooping binding</b>	View the user information in the DHCP Snooping binding database.

For example:

```
Ruijie# show ip dhcp snooping binding
Total number of bindings: 1
-----
MacAddress      IpAddress      Lease(sec)  Type           VLAN  Interface
-----
001b.241e.6775  192.168.12.9   7200        dhcp-snooping  1     GigabitEthernet 0/5
```

## Typical Configuration Example of DHCP Snooping

### Topological Diagram

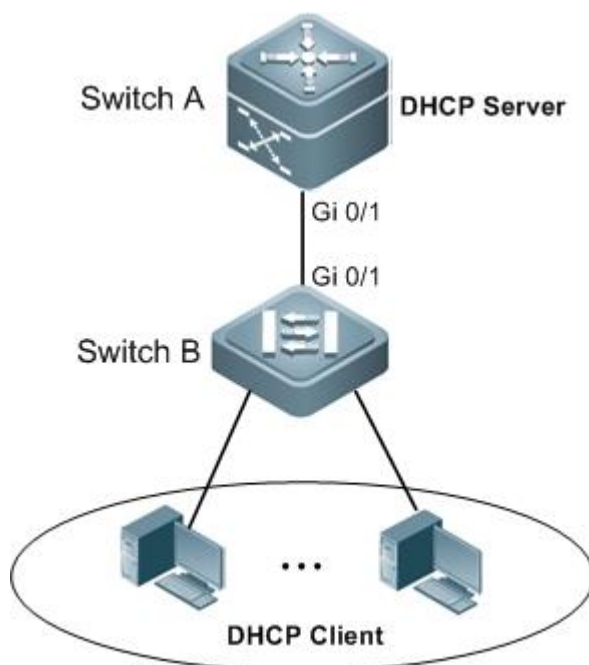


Figure 8

### Application Requirements

The DHCP client obtains the IP address dynamically through the legal DHCP server.  
Prevent other users from setting private DHCP servers.

### Configuration Points

By default, DHCP Snooping takes effect for all VLANs. To disable DHCP Snooping on a specific VLAN, remove it from the validation range of DHCP Snooping.

1. Enable the DHCP Snooping function on the access device (Switch B), and set the uplink port (Gi0/1) as the trusted port.

When DHCP Snooping is enabled, it is enabled for all VLANs on the device. To enable or disable DHCP Snooping on a specific VLAN, add or remove it from the validation range of DHCP Snooping.

## Configuration Steps

- Configure the Switch B

Step 1, enable the DHCP Snooping function.

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

Step2, configure the uplink port as the trusted port.

```
Ruijie(config)#interface gigabitEthernet 0/1
Ruijie(config-if-GigabitEthernet 0/1)#ip dhcp snooping trust
```

## Displaying Verifications

Step 1, check the configuration for the Switch B. Key points: whether the DHCP Snooping function is enabled or not, whether the trusted port configured is the uplink port.

```
Ruijie#show running-config
!
ip dhcp snooping
!
interface GigabitEthernet 0/1
ip dhcp snooping trust
```

Step2, display the DHCP Snooping configuration of the Switch B. Key points: whether the trusted port is correctly.

```
Ruijie#show ip dhcp snooping
Switch DHCP snooping status : ENABLE
DHCP snooping Verification of hwaddr status : DISABLE
DHCP snooping database write-delay time : 0 seconds
DHCP snooping option 82 status : DISABLE
DHCP snooping Support bootp bind status : DISABLE
Interface Trusted Rate limit (pps)
-----
GigabitEthernet 0/1 YES unlimited
```

Step3, display the information about the DHCP Snooping binding database.

```
Ruijie#show ip dhcp snooping binding
Total number of bindings: 1
```

MacAddress	IpAddress	Lease(sec)	Type	VLAN	Interface
0013.2049.9014	172.16.1.2	86207	dhcp-snooping 1		GigabitEthernet 0/11

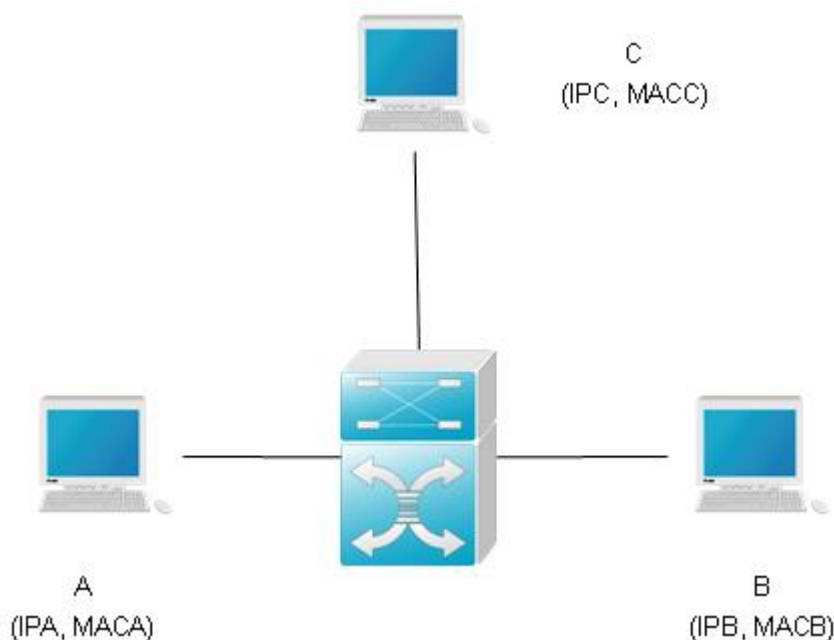
# Dynamic ARP Inspection Configuration

## Overview

DAI, an acronym of Dynamic ARP Inspection, refers to inspect the validity of received ARP packets. Illegal ARP packets will be discarded.

## Understanding ARP Spoofing Attack

ARP itself does not check the validity of incoming ARP packets, a drawback of ARP. In this way, attackers can launch ARP spoofing attacks easily by exploiting the drawback of the protocol. The most typical one is the man in the middle attack, which is described as follows:



As shown in the diagram, devices A, B and C are connected to Ruijie device and located in the same subnet. Their IP and MAC addresses are respectively represented by (IPA, MACA), (IPB, MACB) and (IPC, MACC). When device A needs to communicate with device B in the network layer, device A broadcasts an ARP request in the subnet to query the MAC value of device B. Upon receiving this ARP request packet, device B updates its ARP buffer using IPA and MACA, and sends an ARP response. Upon receiving this response, device A updates its ARP buffer using IPB and MACB.

With this model, device C will cause the corresponding relationship of ARP entries in device A and device B incorrect. The policy is to broadcast ARP response to the network continuously. The IP address in this response is IPA/IPB, and the MAC address is MACC. Then, ARP entries (IPB and MACC) will exist in device A, and ARP entries (IPA and MACC) exist in device B. Communication between device A and device B is changed to communication with device C, which is unknown to devices A and B. Device C acts as an intermediary and it just modifies the received packets appropriately and forwards to another device. This is the well-known man in the middle attack.

## Understanding DAI and ARP Spoofing Attacks

DAI ensures that only legal ARP packets are forwarded by the device. It mainly performs the following operations:

- Intercept all the ARP request and response packets at the untrusted port that corresponds to VLAN with the DAI inspection function enabled.
- Check the validity of the intercepted ARP packets according to the setting of DHCP database before further processing.
- Drop the packets that do not pass the inspection.
- Appropriately process the packets that pass the inspection and send them to the destinations.

According to the DHCP snooping binding database, whether ARP packets is valid or not can be checked . For details, refer to *DHCP Snooping Configuration*.

## Interface Trust Status and Network Security

ARP packets are checked according to the trust status of each port on the device. DAI check is ignored for the packets that are received through trust ports and are considered as legal ARP packets. DAI check will be performed strictly for the ARP packets that are received through untrusted ports.

In a typical network configuration, layer 2 port connected to the network device should be set as a trust port, and layer 2 port connected to the host device should be set as an untrusted port.



### Note

Incorrectly configuring a layer 2 port as an untrusted port may affect normal communication of the network.

For specific configuration commands, refer to *ip arp inspection trust*, *show ip arp inspection interface*.

## Limiting the Rate of ARP Packets

Checking DAI validity will consume a certain CPU resources. Limiting the rate of ARP packets, namely the number of ARP packets received per second, can efficiently prevent the DAI-specific DoS attack. By default, 15 ARP packets are received on an untrusted port per second. This limit does not apply to a trusted port. You can configure rate limit with the **ip arp inspection limit-rate** command on the Layer 2 interface configuration mode.

For details, refer to **ip arp inspection limit-rate** and **show ip arp inspection interface**.

## Configuring DAI

DAI is an ARP-based security filtering technology. A series of filtering policies are configured, so that validity of ARP packets that pass the device is checked more effectively.

To use the functions of DAI, selectively perform the following tasks:

- Enabling DAI Packet Check Function for Specified VLAN (required)
- Set Trust Status of Port (required)
- Set the Maximum Rate of Receiving ARP Packets on the Port(Optional)



## ■ Related Configuration of DHCP Snooping Database (optional)

### Enabling DAI Packet Check Function for Specified VLAN

By default, the DAI packet check function is disabled for all VLANs.

If no DAI packet check function has enabled VLAN vid, DAI-related security check will be skipped for the ARP packets with vlan-id = vid (ARP packet rate restriction is not skipped).

Use the **show ip arp inspection vlan** command to check whether the DAI packet check function has been enabled for all VLANs.

To configure the DAI packet check function for VLAN, execute the following commands in the interface configuration mode:

Command	Function
Ruijie(config)# <b>ip arp inspection vlan</b> <i>vlan-id</i>	Turn on the DAI packet check function switch for VLAN <i>vlan-id</i>
Ruijie(config)# <b>no ip arp inspection vlan</b> [ <i>vlan-id</i> ]	Turn off the DAI packet check function switch for VLAN <i>vlan-id</i> Disable the DAI packet check function for all VLANs if <i>vlan-id</i> is ignored

### Setting the Trust Status of Port

This function is used in the layer 2 interface configuration mode, and this layer 2 interface is a member port of SVI.

All the layer 2 ports are untrusted by default.

If the port is trusted, ARP packets will not be check further. Otherwise, the validity of the current ARP packet will be checked using information in the DHCP snooping database.



#### Note

Upward associated ports are generally set as trusted, while downward associated ports are generally set as untrusted. Because upward associated devices do not initiate to apply for IP addresses, no information about upward associated devices is recorded in the DHCP snooping database.

To set the trust status of a port, execute the following commands in the interface configuration mode:

Command	Function
Ruijie(config-if)# <b>ip arp inspection trust</b>	Set the port as a trust port.
Ruijie(config-if)# <b>no ip arp inspection trust</b>	Set the port as an untrusted port.

### Setting the Maximum Rate of Receiving the ARP Packets on the Port

This function is used in the L2 interface configuration mode, and the L2 interface is a member port of the SVI.

By default, each untrusted switching port receives 15 ARP packets per second, and there is no limitation for the trusted switching port.

If the number of ARP packets received on the interface within 1 second exceeds the limit, the packets received consequently will be discarded.

Use the **show ip arp inspection interface** command to view the rate limit of each L2 interface.

To set the maximum rate of receiving the ARP packets on the port, execute the following commands in the interface configuration mode:

Command	Function
Ruijie(config-if)# <b>ip arp inspection limit-rate</b> { <1-2048>   none }	Set the maximum rate of receiving the ARP packets on the port, in pps. <b>none</b> : no limitation
Ruijie(config-if)# <b>no ip arp inspection trust</b>	Restore to the default value.



#### Note

Ruijie's basic network protection functions include the ARP-GUARD sub-function. Rate limiting based on the source IP address or source MAC address is enabled for this function because the rate of sending ARP packets is much higher than that of a PC. For example, when a gateway is downward associated with thousands of even more than 10000 PCs, the ARP packets sent by the gateway tends to be discarded by ARP-GUARD. To resolve this problem, increase the upper limit rate of ARP-GUARD, so that ARP packets can pass normally.



#### Caution

## Related Configuration of DHCP Snooping Database

Refer to *DHCP Snooping Configuration*.

If DHCP Snooping database is not configured, all the ARP packets pass inspection.

## Showing DAI Configuration

### Showing Whether DAI Function Is Enabled for VLAN

To show the enabling status of VLAN, execute the following command in the global configuration mode:

Command	Function
Ruijie(config)# <b>show ip arp inspection vlan</b>	Show the enabling status of each VLAN

### Showing DAI Configuration Status of Each Layer 2 Interface

To show the DAI configuration status of each layer 2 interface, execute the following command in the global configuration mode:

Command	Function
Ruijie(config)# <b>show ip arp inspection interface</b>	Show the DAI configuration of each layer 2 interface (including trust status and rate restriction)

For the products supporting NFPP, rate limit is done by NFPP, not DAI. Consequently, this command shows only the trust status of an interface.

## Precautions of Configuring the Rate of ARP Packets



### Caution

In the single-device environment, when the CPU is busy, the rate of sending ARP packets is limited to appropriately 150PPS~380PPS, even if the rate oversizely exceeds the rate limitation. The deviation of the rate value may occur in different environment.

In the stack environment, when the CPU of the backup device is busy, the rate of sending ARP packets on the port is appropriately a dozoon PPS with the rate limit configured.

## Typical DAI Configuration Example

### Topological Diagram

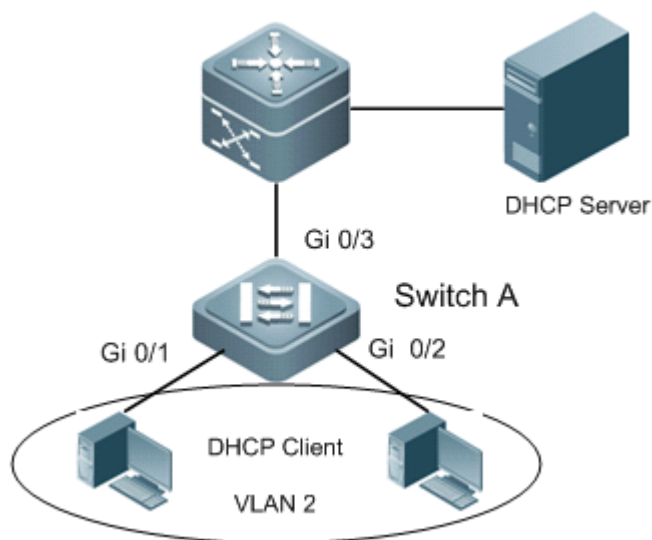


Figure2 DHCP deployment environment

### Application Requirements

As shown above, the IP address of user PC is automatic allocated by the DHCP server. To ensure that users can access network normally, the following requirements must be met:

1. User PC can only acquire IP address from the specified DHCP server, and no additional DHCP server is allowed.
2. Only the IP address allocated by the valid DHCP server can access network, and IP address cannot be configured at will.

## Configuration Tips

- **Configuration tips**

1. On the access switch (SwitchA), enable DHCP Snooping and configure the uplink port (GigabitEthernet 0/3) connecting valid DHCP server as the trusted port to meet the first requirement.
2. On the access switch (SwitchA), further enable DAI to meet the second requirement.

- **Note**

If the convergence switch or core switch is connected with other PCs and there may be a private DHCP server, DHCP Snooping shall also be enabled.

## Configuration Steps

- **Configure Switch A**

Step 1: Configure the VLAN to which the PC-connecting port belongs.

```
Ruijie#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Ruijie(config)#interface range gigabitEthernet 0/1-2
Ruijie(config-if-range)#switchport access vlan 2
```

Step 2: Enable DHCP Snooping.

```
Ruijie(config-if-range)#exit
Ruijie(config)#ip dhcp snooping
```

Step 3: Enable DAI on the corresponding VLAN.

```
Ruijie(config)#ip arp inspection vlan 2
```

Step 4: Configure the uplink port as the trusted port of DHCP Snooping

```
Ruijie(config)#interface gigabitEthernet 0/3
Ruijie(config-if-GigabitEthernet 0/3)#ip dhcp snooping trust
```

Step 5: Configure the uplink port as the trusted port of DAI.

```
Ruijie(config-if-GigabitEthernet 0/3)#ip arp inspection trust
```

## Verifications

Step 1: Verify whether the configurations are correct. Key points: whether DHCP Snooping/DAI has been enabled, and whether the trusted port is correct.

```
Ruijie#show running-config
ip dhcp snooping
```

```

!
ip arp inspection vlan 2
!
interface GigabitEthernet 0/1
 switchport access vlan 2
!
interface GigabitEthernet 0/2
 switchport access vlan 2
!
interface GigabitEthernet 0/3
ip dhcp snooping trust
ip arp inspection trust

```

**Step 2: View DHCP SNOOPING enabling state and the corresponding trusted port. Key point: whether the uplink port has been configured as the trusted port.**

```

Ruijie#show ip dhcp snooping
Switch DHCP snooping status          :  ENABLE
DHCP snooping Verification of hwaddr status  :  DISABLE
DHCP snooping database write-delay time      :  0 seconds
DHCP snooping option 82 status           :  DISABLE
DHCP snooping Support bootp bind status      :  DISABLE
Interface          Trusted      Rate limit (pps)
-----
GigabitEthernet 0/3      YES      unlimited

```

**Step 3: View DAI state. Key point: VLAN enabling state and whether the uplink port has been configured as the trusted port.**

```

Ruijie#show ip arp inspection vlan
Vlan    Configuration
----    -
2        Enable

Ruijie#show ip arp inspection interface
Interface      Trust State
-----
GigabitEthernet 0/1    Untrusted
GigabitEthernet 0/2    Untrusted
GigabitEthernet 0/3    Trusted

```

To view the database binding information generated by DHCP Snooping, execute "**show ip dhcp snooping binding**" command.

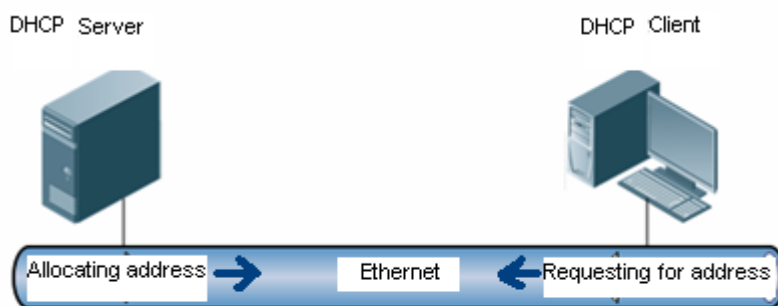
# IP Source Guard Configuration

## Brief Introduction of IP Source Guard

### Understanding DHCP

In the typical DHCP-enabled network, the DHCP server is responsible for managing and allocating addresses for hosts. The hosts apply for legal network addresses from the DHCP server. DHCP is helpful for administrators to manage network addresses and avoid address conflict.

Figure 1 Normal DHCP Address Allocation



However, the server/client mode can not guarantee the efficiency and security of network address management. The traditional DHCP mode is required to have higher security characters because of the illegal packets or even attack packets from the clients (as shown in Figure 3) and various feigned servers (as shown in Figure 2) in the network.

DHCP Snooping solves the problem. The security problem of traditional DHCP mode can be solved by enabling DHCP Snooping on the device connecting the DHCP server with the DHCP clients. DHCP Snooping divides the network into two parts: untrusted network that shields all the DHCP Server response packets in the network and checks the security of the request from the client; trusted network that forwards the request received from legal client to the server in that trusted network which allocates and manages addresses.

Figure 2 Network with feigned DHCP server

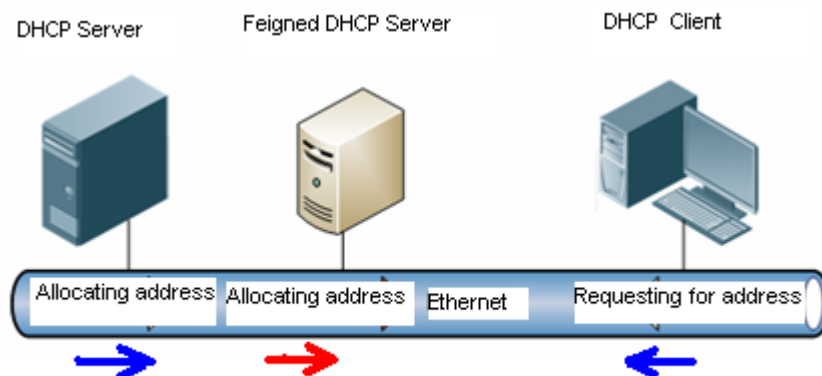


Figure 3 Network with feigned DHCP client attack

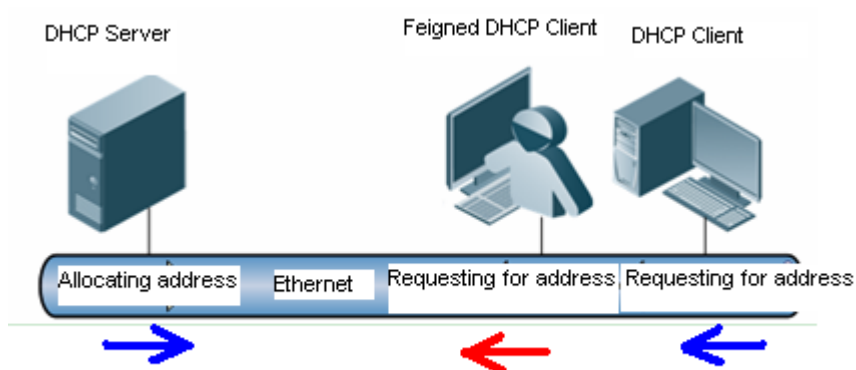
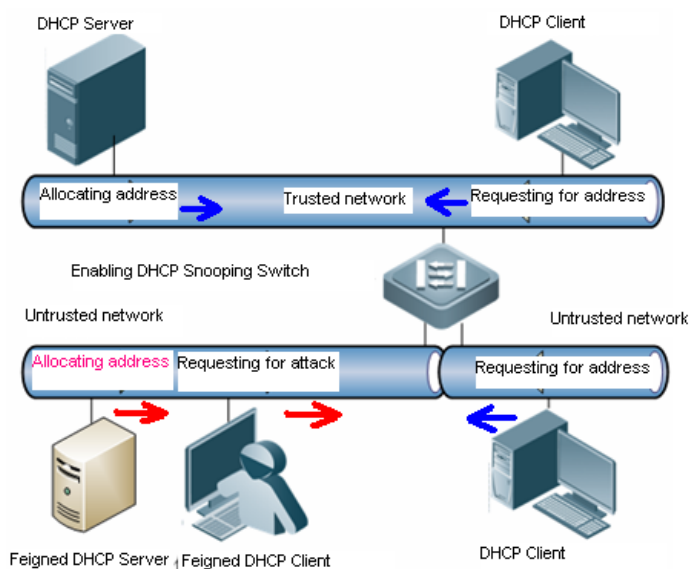


Figure 4 Network protected by DHCP Snooping



By filtering DHCP packets, DHCP Snooping shields feigned servers and block the attacks from the clients. However, it cannot control the users assign IP addresses privately. Those users easily lead to conflict of network addresses and be harm to the management of network addresses. To prevent the clients from assigning addresses privately in the DHCP network, enable IP Source Guard on the device connecting the DHCP server to the DHCP clients. DHCP Snooping-based IP Source Guard

ensures that DHCP clients access network resources properly and block the users who assign addresses privately to access.

## Understanding IP Source Guard

IP Source Guard maintains a hardware-based IP packet filtering database to filter packets, guaranteeing that only the users matching the database can access network resources.

The hardware-based IP packet filtering database is the key for IP Source Guard to enable efficient security control in DHCP applications. This database is on the basis of DHCP Snooping database. After IP Source Guard is enabled, the DHCP Snooping database is synchronized with the hardware-based IP packet filtering database. In this way, IP Source Guard can strictly filter IP packets from clients on the device with DHCP Snooping enabled.

By default, once IP Source Guard is enabled on a port, all the IP packets traveling through the port (except for DHCP packets) will be checked on the port. Only the users attaining IP addresses through DHCP and the configured static binding users can access the network.

IP Source Guard supports source MAC- and source IP-based filtering or source IP-based filtering. In the former case, IP Source Guard will check the source MAC and source IP addresses of all packets and only allow those packets matching the hardware-based IP packet filtering database to pass through. In the latter case, IP Source Guard checks the source IP addresses of IP packets.

## Other Precautions of Configuring IP Source Guard

IP Source Guard is based on DHCP Snooping, namely port-based IP Source Guard takes effect only on the untrusted port under the control of DHCP Snooping, not on the trusted port or the interfaces in the VLAN not controlled by DHCP Snooping.

## IP Source Guard Configuration

### Configuring IP Source Guard on the Interface

By default, IP Source Guard is disabled on the interface and all the users connecting to the interface can use the network. After enabling IP Source Guard on the interface, it will filter the IP packets of the users connecting to the interface according to the hardware-based IP packet filtering database.

Command	Description
Ruijie(config)# <b>interface</b> <i>interface-id</i>	Enter the interface configuration mode.
Ruijie(config)# <b>[no] ip verify source</b> <b>[port-security]</b>	Enable IP Source Guard on the interface. Use port-security to set MAC-based filtering.

The following example shows how to enable IP Source Guard on interface1:

```
Ruijie(config)# interface FastEthernet 0/1
Ruijie(config-if)# ip verify source
Ruijie(config-if)# end
```



**Caution**

The application of IP Source Guard is combined with DHCP Snooping. That is to say, port-based IP Source Guard only takes effect on untrusted port under the control of DHCP Snooping.

## Configuring Static IP Source Address Binding User

Under certain circumstances, users under certain ports may expect to statically use certain IP addresses. This feature can be realized by adding static user information into the IP source binding database.

Command	Description
Ruijie# <b>configure terminal</b>	Enter configuration mode
Ruijie(config)# <b>[no] ip source binding mac-address vlan vlan_id ip-address [ interface interface-id   ip-mac   ip-only ]</b>	Add static IP source binding user into the database. If the interface is not specified, the binding entry will apply to all binding interfaces on the VLAN. interface: bind to interface; ip-mac: global IP+MAC binding; ip-only: global IP binding.

The following example shows how to bind a static user to port 9 of the device:

```
Ruijie# configure terminal
Ruijie(config)# ip source binding 00d0.f801.0101 vlan 1 192.168.4.243 interface FastEthernet
0/9
```

## Showing IP Source Guard Configuration

### Showing IP Source Guard Filtering Entry

Use this command to show IP Source Guard filtering entry.

Command	Description
Ruijie# <b>show ip verify source [interface interface]</b>	Show IP Source Guard filtering entry.

For example:

```
Ruijie # show ip verify source
```

Interface	Filter-type	Filter-mode	Ip-address	Mac-address	VLAN
FastEthernet 0/3	ip	active	3.3.3.3		1
FastEthernet 0/3	ip	active	deny-all		
FastEthernet 0/4	ip+mac	active	4.4.4.4	0000.0000.0001	1
FastEthernet 0/4	ip+mac	active	deny-all		

## Showing Hardware-based IP Packet Filtering Database

Use this command to show the related information of hardware-based IP packet filtering database.

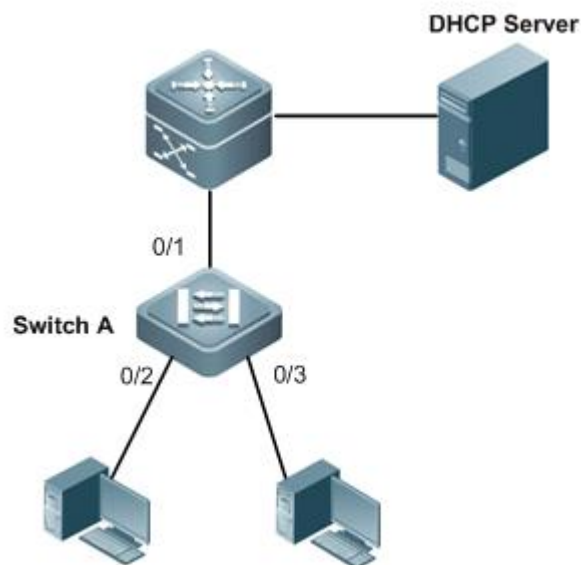
Command	Description
Ruijie# <b>show ip source binding</b> [ <i>ip-address</i> ] [ <i>mac-address</i> ] [ <i>dhcp-snooping</i> ] [ <i>static</i> ] [ <i>vlan vlan-id</i> ] [ <i>interface interface-id</i> ]	Show the hardware-based IP packet filtering database.

For example:

```
Ruijie# show ip source binding
MacAddress      IpAddress      Lease(sec)  Type           VLAN  Interface
-----
0000.0000.0001  1.0.0.1        infinite    static         1     FastEthernet2/1
Total number of bindings: 1
FastEthernet 0/1
Total number of bindings: 1
```

## Example of IP Source Guard Configuration

### Topological Diagram



DHCP deployment environment

### Application Requirements

The user can only use the IP address dynamically allocated by a valid DHCP server or statically allocated by the administrator to access network. IP packets with source IP different from the IP addresses contained in the hardware filtering list of switch will be blocked to ensure network security.

## Configuration Tips

Configure IP Source Guard and DHCP Snooping on the access device (Switch A) to meet the requirements:

1. Configure the uplink port (GigabitEthernet 0/1) as trusted port to avoid DHCP server spoofing.
2. Enable IP Source Guard on PC-connecting ports (GigabitEthernet 0/2 and GigabitEthernet 0/3).
3. The user with IP address assigned by the administrator can be configured through IP Source Guard static binding (IP address: 192.168.216.4; MAC address: 0000.0000.0001).

## Configuration Steps

### Configure Switch A

Step 1: Enable DHCP Snooping.

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

Step 2: Configure the uplink port as the trusted port of DHCP Snooping.

```
Ruijie(config)#interface gigabitEthernet 0/1
Ruijie(config-if-GigabitEthernet 0/1)#ip dhcp snooping trust
Ruijie(config-if-GigabitEthernet 0/1)#exit
```

Step 3: Enable IP Source Guard on the port directly connected with PC

```
Ruijie(config)#interface range gigabitEthernet 0/2-3
Ruijie(config-if-range)#ip verify source port-security
Ruijie(config-if-range)#exit
```

Step 4: Configure static binding user

```
Ruijie(config)#ip source binding 0000.0000.0001 vlan 1 192.168.216.4 interface gigabitEthernet 0/2
```

## Verification

Step 1: Check the configurations of Switch A. Key points: whether DHCP Snooping has been enabled, whether the uplink port has been configured as the trusted port, whether IP Source Guard has been enabled on the user-connecting port, and whether the static binding entries are correct.

```
Ruijie#show running-config
ip dhcp snooping
!
ip source binding 0000.0000.0001 vlan 1 192.168.216.1 interface GigabitEthernet 0/2
!
interface GigabitEthernet 0/1
ip dhcp snooping trust
!
interface GigabitEthernet 0/2
```

```

ip verify source port-security
!
interface GigabitEthernet 0/3
ip verify source port-security

```

### Step 2: Display DHCP Snooping user binding database

```
Ruijie#show ip dhcp snooping binding
```

Total number of bindings: 2

MacAddress	IpAddress	Lease(sec)	Type	VLAN	Interface
0013.2049.9014	192.168.216.4	86233	dhcp-snooping	1	GigabitEthernet 0/3
00e0.4c70.b7e2	192.168.216.3	86228	dhcp-snooping	1	GigabitEthernet 0/2

### Step 3: Display the IP hardware filtering list jointly generated through DHCP Snooping user binding database and static bindings:

```
Ruijie#show ip source binding
```

MacAddress	IpAddress	Lease(sec)	Type	VLAN	Interface
0000.0000.0001	192.168.216.4	infinite	static	1	GigabitEthernet 0/2
0013.2049.9014	192.168.216.4	86176	dhcp-snooping	1	GigabitEthernet 0/3
00e0.4c70.b7e2	192.168.216.3	86171	dhcp-snooping	1	GigabitEthernet 0/2

Total number of bindings: 3

### Step 4: Display the filtering entries of IP Source Guard:

```
Ruijie#show ip verify source
```

Interface	Filter-type	Filter-mode	Ip-address	Mac-address	VLAN
GigabitEthernet 0/2	ip+mac	active	192.168.216.4	0000.0000.0001	1
GigabitEthernet 0/2	ip+mac	active	192.168.216.3	00e0.4c70.b7e2	1
GigabitEthernet 0/2	ip+mac	active	deny-all	deny-all	
GigabitEthernet 0/3	ip+mac	active	192.168.216.4	0013.2049.9014	1
GigabitEthernet 0/3	ip+mac	active			

# ND Snooping Configuration

## Understanding ND Snooping

### Overview

In the IPv6 network, the network nodes use ND (Neighbor Discovery) protocol to discover router and carry out auto-configuration, detect duplicate address, translate link-layer address, detect neighbor accessibility, announce link-layer address change, and redirect route.

Since ND protocol lacks intrinsic security, it is faced with such problems as address resolution attack and routing information attack, and it's very complicated to increase security by deploying extrinsic encryption & authentication system. While the stateless address auto-configuration mechanism realized by ND protocol is bringing about greater convenience to network, IPv6 cannot carry out effective monitoring of network users.

The ND snooping technology well solves the aforementioned problem. It can well prevent IP address embezzlement by snooping ND messages on the network, filtering invalid address resolution messages and routing information messages, snooping IPv6 users on the network, and binding the IPv6 users snooped to the interface.

ND snooping technology also utilizes the feature of IPv6 stateless automatic address configuration and 802.1X authentication technology and port security technology to provide an IPv6 address authentication mechanism for access devices, and is smoothly and transparently compatible with IPv4 security technology, allowing the construction of a secure and reliable IPv6 network.

## ND Attack Protection

When using stateless address auto-configuration, the IPv6 node will use Router Advertisement to configure the IPv6 address of interface, and acquire the prefix of direct-link network segment, gateway IP address, link MTU and etc. The router can also use ND redirect message to modify the next hop information of relevant route in the host routing table. Therefore, the attacker may send invalid RA message and redirect message to modify the routing table of the host being attacked (such as gateway IP address), so as to implement DoS attack and man-in-the-middle attack. Such forms of attacks are called "routing information attack".

When an IPv6 node carries out unicast communication, it will first use ND protocol to perform address resolution in order to acquire the link-layer address of neighboring node, and then send the frame encapsulated with link-layer address. Five types of messages in ND protocol can all carry link-layer address information, and the receiving node will consider such information as trusted. Therefore, the attacker may send fraudulent ND message to modify the corresponding relationship between IP address in the neighbor list of node being attacked and the link-layer address, so as to implement DoS attack and man-in-the-middle attack. Such forms of attacks are called "address resolution attack".

In order to defend against the aforementioned attacks, ND Snooping divides the interfaces of network devices into trust interfaces and untrust interfaces. Trust interfaces will be connected with trust nodes such as Router or server, while untrust interfaces will be connected with untrust nodes such as user PC. The ND messages received by trust interfaces will be forwarded freely, while redirect messages and RA messages received by untrust interfaces will be dropped without exception, well avoiding routing information attack. For RS/NS/NA messages received by the untrust interfaces, the message validity will be checked. Invalid RS/NS/NA messages will be dropped without exception to avoid address resolution attack.

The validity of RS/NS/NA messages will be identified by verifying the matching relationship for four elements (source IP address/target IP address, VID, MAC address, and input interface). The four-element matching relationship of host node is provided by such functions as "IPv6+MAC binding", "DHCPv6 Snooping" and "stateless configuration user snooping" mentioned below. In order to defend against ND address resolution attack, at least one of the aforementioned functions shall be enabled. If the NA message received by the Untrust interfaces carries information which can only be set by router (the R bit is set), such message will also be considered invalid.

The security check of ND messages of all host nodes will be able to defend against gateway address resolution attack. If you only want to defend against gateway address resolution attack, please refer to the section of "Automatic ND Gateway Attack Protection". The protection of ND routing information attack is independent from the aforementioned functions. It may use the command to enable/disable ND address resolution attack protection function, but ND routing information attack protection will always be enabled when ND Snooping is enabled.

## Automatic ND Gateway Attack Protection

Gateway address resolution cheating is the most common type of attack, and will cause considerable impacts. By addressing the problem of gateway address resolution cheating attack, we can solve the vast majority of address resolution attacks on the network. At the same time, implementing only gateway attack protection can effectively save system resources. For convenient use, besides the support to manual configuration of gateway information, ND Snooping also supports automatic acquisition of gateway information.

Gateway is one of the most key nodes of network. ND snooping only support the "ND key-node-only address resolution attack protection". For ND messages received by the untrust interfaces, ND snooping will only verify whether such messages contain fake key nodes, and will not verify whether such messages contain non-key nodes. Fraudulent messages will be dropped without exception, thus greatly alleviating the CPU load of network devices and decreasing device resource expenditure and the reliance on security functions (such as the functions mentioned in "ND attack protection"). The gateway information can be acquired automatically and manually. The gateway information acquired will automatically become the key node information, allowing the ND gateway-only address resolution attack protection.

When the gateway information is acquired automatically, ND Snooping can automatically learn the gateway information by snooping RA messages on the network. If the gateway is changed, ND Snooping can update automatically. The entire process is transparent to the network administrator without specific configuration. If you configure IPv6 network manually, you can manually add gateway information (You can also manually add another key-node "server" information, so as to

defend against address resolution attack on the server. Please refer to the subsequent configuration command.)

## Stateless User Snooping Configuration

Users adopting stateless address auto-configuration are called "stateless configuration user". When using stateless address auto-configuration, the network administrator will be unable to know how many IPv6 users exist on the network and hence unable to deploy the corresponding administration policy.

If there is any attack on the network, the network administrator may be able to acquire the IP address of attacker through certain means. When the network administrator is looking for the physical location of attack source, it can only locate a certain network segment via the IP address, and is unable to locate the specific port and physical terminal of network device. In order to address this problem, you can snoop the stateless configuration user on the network in order to acquire relevant user information. Stateless configuration user snooping can only snoop users through untrust interface.



- 1) ND Snooping doesn't support the snooping of temporary address. In some operating system, the temporary address is enabled by default. For example, in Windows XP, we need to use "netsh interface ipv6 set privacy disabled" command to disable this feature.
- 2) In order to ensure the uniqueness of the address in the segment, the access terminal shall use the MAC address embedded in the network interface card to implement communication instead of modifying the MAC address.

## Stateless User Binding Configuration

When using stateless address auto-configuration, the process of address assignment and use is uncontrollable. IP address may be embezzled. Therefore, IP address and the user terminal is not necessarily connected. If the attacker uses the IP address of host A to implement various attacks, the network administrator will track host A according to the source IP address of attack streams. Host A will be mistaken as the attacker, while the real attacker will seek safety in flight. In order to address IP address embezzlement and DDOS attack in the circumstance of stateless address auto-configuration, ND Snooping allows the binding of stateless configuration user snooped to the hardware interface, and the specific user can only access via the specific interface.

The "address binding mode" for stateless configuration users can be divided into loose mode and strict mode. In loose mode, only the non-link-local address will be bound; in strict mode, both the link-local address and non-link-local address of host will be bound. If there is only one network segment, the strict mode will consume twice the hardware resources consumed by loose mode.

The "address binding information" of stateless configuration user can only support "IPv6 address only" mode and "IPv6+MAC" binding. The former one will check the matching relationship between VID, source IP address and port contained in the message, while the later one will check the matching relationship between VID, source MAC address, source IP address and port contained in the message. The later one can provide higher security than the former one, but its deployment may conflict with certain functions.

## Combined Security Monitoring

In case of IPv6 stateless address auto-configuration, the attacker may falsify extensive users to implement ND interaction, and the monitoring data will become untrusted as the IPv6 users snooped by the network device are all falsified and attacker's IP address may be hidden among them. If the user binding function is enabled, falsified users will consume excessive hardware resources, thus prohibiting other normal IPv6 users from accessing. IPv6 stateless address auto-configuration will allow any terminal to access the network from any node, and the network administrator is unable to bind the physical location of access terminal or implement IPv6 address authorization. In order to solve the aforementioned problems, ND snooping provides the feature of combined security monitoring: you can implement security check of ND messages by integrating Port Security with 802.1X, and may also implement IPv6 address binding or IPv6 address authorization in the circumstance of IPv6 stateless address auto-configuration.

When Port Security is enabled on the interface, only the MAC address learned automatically by Port Security, manually configured MAC address, and MAC address and AP in the manually configured IPv4+MAC binding will be considered trusted. When 802.1X is enabled on the interface, only MAC address and AP from user with 802.1X authentication will be considered trusted. Only those ND messages carrying trusted MAC addresses received by the trusted AP will be considered valid ND messages. The network device only snoops and binds users from valid ND messages.

## ND Snooping and CPP

The security check of ND messages will consume certain CPU resources. In order to prevent the attacker from implementing DoS attack on network device by sending excessive ND messages, the device can use CPP function to implement complete-device flow-limiting and priority control. After ND Snooping is enabled, the control over ND messages by CPP will be enabled automatically. For details about ND message flow-limiting configuration in CPP and the priority relationship between ND messages and other messages, please refer to the section of CPP function configuration.

## ND Snooping and NFPP

Besides applying CPP to implement complete-device control over ND messages, the device can also implement more accurate flow-limiting of ND messages by applying NFPP function, which is only effective for ND messages checked by CPU. Please refer to NFPP configuration section for detailed configuration methods. The ND message flow-limiting can meet the needs for both interface flow-limiting and complete-device flow-limiting.

## ND Snooping and IPv6 Compatibility Mode

In order to control IPv6 messages, some IPv4 security policies provide the configuration option of IPv6 compatibility mode. ND Snooping function can only work under the strict mode of IPv6 compatibility mode. For details about IPv6 compatibility mode, please refer to the section of IPv4+MAC binding.

## Operating Principle

NA



## Protocol Specification

RFC 2464: Transmission of IPv6 Packets over Ethernet Networks

RFC 4861: Neighbor Discovery for IP version 6 (IPv6)

RFC 4862: IPv6 Stateless Address Autoconfiguration

## Default Configurations

Function	Default setting
Enable global ND Snooping	Disabled
Enable VLAN-based ND Snooping	Enabled (This value only makes sense when global ND snooping is enabled. The same below.)
Interface trust mode	Untrust
ND routing information attack protection	Enabled
ND address resolution attack protection	Disabled
Enable global automatic network gateway information acquisition	Disabled
Enable VLAN-based automatic network gateway information acquisition	Disabled
Manual configuration of key nodes	NA
Stateless configuration user snooping	Disabled
Combined security monitoring	Disabled
IPv6 prefix number limit	2/VLAN
Access user number limit	16/interface
Stateless configuration user mobility	Disabled
Stateless configuration user binding	Disabled
Stateless configuration user address binding mode	Loose
Stateless configuration user address binding information	IPv6 address only

## Enable ND Snooping

### Enable global ND Snooping

Command	Function
Ruijie# <b>configure terminal</b>	Enter the global configuration mode.

Ruijie(config)# <b>[no] ipv6 nd snooping</b>	Enable/disable the global IPv6 ND Snooping
--	--

The following example shows how to enable the IPv6 ND Snooping:

For example: enable global IPv6 ND snooping

```
Ruijie# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Ruijie(config)# ipv6 nd snooping
```

## Enable VLAN-based ND Snooping

By default, ND Snooping is enabled on all VLANs. You may use the following command to disable IPv6 ND Snooping on VLAN.

Command	Function
Ruijie# <b>configure terminal</b>	Enter the global configuration mode.
Ruijie(config)# <b>[no] ipv6 nd snooping vlan {vlan-rng   {vlan-min [vlan-max]}}</b>	Enable/disable the VLAN-based IPv6 ND Snooping

For example: disable IPv6 ND snooping on VLAN 100

```
Ruijie# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Ruijie(config)# no ipv6 nd snooping vlan 100
```

For example: disable IPv6 ND snooping on VLAN 4, 5-7 and 15

```
Ruijie# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Ruijie(config)# no ipv6 nd snooping vlan 4,5-7,15
```



### Caution

When enabling user binding, all VLANs must enable ND Snooping.

## Configure ND Attack Protection

### Configure Interface Trust State

By default, the trust state of all interfaces is set to untrust. You may use the following command to set the trust state of a certain interface to trust:

Command	Function
Ruijie# <b>configure terminal</b>	Enter the global configuration mode.
Ruijie(config)# <b>Interface interface_id</b>	Enter the interface configuration mode.

Ruijie(config-if)# <b>ipv6 nd snooping trust</b>	Set the IPv6 ND Snooping trusted interface.
--	---

For example: set interface FastEthernet 0/1 to Trust interface.

```
Ruijie# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Ruijie(config)# interface fastethernet 0/1
Ruijie(config-if)# ipv6 nd snooping trust
```

## Configure ND Address Resolution Attack Protection

Command	Function
Ruijie# <b>configure terminal</b>	Enter the global configuration mode.
Ruijie(config)# <b>[no]ipv6 nd snooping check address-resolution [key-node-only]</b>	Check whether the global ND address resolution is enabled or disabled. The option of "key-node-only" will only check the address resolution of key nodes, and the operating principle is detailed in the section of "Automatic ND Gateway Attack Protection". Without this option will only check general address resolution attacks, and the operating principle is detailed in the section of "ND attack protection".

For example: Enable ND address resolution attack protection.

```
Ruijie# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Ruijie(config)# ipv6 nd snooping check address-resolution
```

For example: Enable ND key-node-only address resolution attack protection.

```
Ruijie# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Ruijie(config)#ipv6 nd snooping check address-resolution key-node-only
```

## Configure Automatic Gateway Information Acquisition

Gateway is one kind of key nodes. If you enable ND key-node-only address resolution attack protection, you may specify the information of trusted gateway to achieve ND gateway address resolution attack protection. To facilitate configuration and provide self-adaptability, you can use the following commands to learn gateway information automatically, which will be used as key-node information to prevent key-node address resolution attacks.

Command	Function
Ruijie# <b>configure terminal</b>	Enter the global configuration mode.

Ruijie(config)# <b>[no]ipv6 nd snooping detect gateway ra</b>	Enable the automatic acquisition of gateway information through RA message snooping.
Ruijie(config)# <b>[no]ipv6 nd snooping detect gateway vlan {vlan-rng}{vlan-min [vlan-max]}</b>	Enable the automatic acquisition of gateway on VLAN

For example: In the circumstance of stateless auto-configuration, enable automatic gateway information acquisition on VLAN 1-64.

```
Ruijie# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Ruijie(config)# ipv6 nd snooping auto-gateway ra
Ruijie(config)# ipv6 nd snooping auto-gateway vlan 1-64
```

## Configure Key Node Information

For the key node of "gateway": During auto-configuration, ND Snooping can allow automatic learning of gateway information. If you use manual mode to assign IPv6 address, you may add gateway information manually. For the key node of "server", you can also add server information manually.

Command	Function
Ruijie# <b>configure terminal</b>	Enter the global configuration mode.
Ruijie(config)# <b>[no] ipv6 nd snooping key-node [link-local vid] ipv6_address/prefix_len</b>	<p>Add the key-node information for ND address resolution attack check. If can specify the IPv6 prefix length to indicate that all IPv6 nodes within a certain address scope are all key nodes. If link-local is inputted, VID must be inputted as well, and the subsequent IPv6 address must be the link-local address.</p> <p>If the key word of link-local is not inputted, the subsequent IPv6 address must be the global unicast address. The prefix length shall be 10-128.</p>

For example: add gateway node information manually.

```
Ruijie# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Ruijie(config)#ipv6 nd snooping key-node 2003::1/128
```

For example: add server node information manually.

```
Ruijie# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Ruijie(config)#ipv6 nd snooping key-node 2003:1001::8/128
```

## Clear Dynamic Key Node

Command	Function
Ruijie# <b>clear ipv6 nd snooping key-node [vlan vid]</b>	In privilege mode, clear the key node information learned dynamically

For example: clear all dynamically learned key node information

```
Ruijie# clear ipv6 nd snooping key-node
```

For example: clear all dynamically learned key node information on VLAN 8.

```
Ruijie# clear ipv6 nd snooping key-node vlan 8
```

## Configure Stateless Configuration User Monitoring

### Enable Stateless Configuration User Monitoring

By default, stateless configuration user monitoring is disabled. You may use the following commands to enable or disable stateless configuration user monitoring.

Command	Function
Ruijie# <b>configure terminal</b>	Enter the global configuration mode.
Ruijie(config)# <b>[no] ipv6 nd snooping monitor stateless-user</b>	Enable or disable the stateless configuration user monitoring

For example: enable global stateless configuration user monitoring.

```
Ruijie# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Ruijie(config)#ipv6 nd snooping monitor stateless-user
```

### Configure Stateless Configuration User Binding

By default, stateless configuration user binding is disabled. You may use the following commands to enable or disable stateless configuration user binding and the binding information.

Command	Function
Ruijie# <b>configure terminal</b>	Enter the global configuration mode.
Ruijie(config)# <b>[no]ipv6 nd snooping stateless-user address-bind [strict] [ip-mac]</b>	Bind the snooped IPv6 stateless address auto-configuration user to the hardware. Strict indicates the binding of both link-local address and non-link-local address. Without this parameter indicates the binding of non-link-local address only. Ip-mac indicates the binding of IP+MAC information, while without this parameter indicates the binding of IP information only.

For example: enable stateless configuration user binding.

```
Ruijie# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Ruijie(config)# ipv6 nd snooping stateless-user address-bind
```

For example: use strict mode to bind stateless configuration user.

```
Ruijie# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Ruijie(config)# ipv6 nd snooping stateless-user address-bind strict
```

For example: bind the IPv6+MAC information of stateless configuration user.

```
Ruijie# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Ruijie(config)# ipv6 nd snooping stateless-user address-bind ip-mac
```

## Configure Combined Security Monitoring

Command	Function
Ruijie# <b>configure terminal</b>	Enter the global configuration mode.
Ruijie(config)# <b>Interface</b> <i>interface_id</i>	Enter the interface configuration mode.
Ruijie(config-if)# <b>[no]ipv6 nd snooping stateless-user combine-security</b>	Configure the binding of stateless configuration user to combined security mode

For example: enable combined security monitoring of interface FastEthernet 0/1

```
Ruijie# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Ruijie(config)# interface fastethernet 0/1
Ruijie(config-if)# ipv6 nd snooping stateless-user combine-security
```

## Stateless Configuration User Mobility Control

By default, the policy of first come first bound can be applied, and no node movement is allowed. In certain cases, you may need IPv6 node movement, and you can use the following commands:

Command	Function
Ruijie# <b>configure terminal</b>	Enter the global configuration mode.
Ruijie(config)# <b>[no] ipv6 nd snooping stateless-user station-move</b>	Control the IPv6 node movement.

For example: enable IPv6 node movement.

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

```
Ruijie(config)#ipv6 nd snooping stateless-user station-move
```

## Access User Number Control

Command	Function
Ruijie# <b>configure terminal</b>	Enter the global configuration mode.
Ruijie(config)# <b>Interface</b> <i>interface_id</i>	Enter the interface configuration mode.
Ruijie(config-if)# <b>[no] ipv6 nd snooping stateless-user limit</b> <i>num</i>	Configure the number of access users allowed by the interface. The default value is 16.

For example: set the access user number of FastEthernet 0/1 to 8.

```
Ruijie# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Ruijie(config)# interface fastethernet 0/1
Ruijie(config-if)# ipv6 nd snooping stateless-user limit 8
```

## VLAN IPv6 Prefix Number Control

A VLAN may have multiple IPv6 prefixes, and each prefix will generate the corresponding IP address for interface. Excessive prefixes will consume too much device resources. You may use the following commands to control the IPv6 prefix number supported by each VLAN.

Command	Function
Ruijie# <b>configure terminal</b>	Enter the global configuration mode.
Ruijie(config)# <b>[no] ipv6 nd snooping stateless-user per-vlan prefix-limit</b> <i>num</i>	Configure the IPv6 prefix number supported by each VLAN (two by default). If the prefix number snooped is larger than the number supported, those with smaller value will be kept.

For example: Allow each VLAN to support 4 IPv6 prefixes.

```
Ruijie# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Ruijie(config)#ipv6 nd snooping stateless-user per-vlan prefix-limit 4
```

## Clear IPv6 Prefix

Command	Function
Ruijie# <b>clear ipv6 nd snooping prefix</b> [ <i>vlan vid</i> ]	In the privilege mode, clear all prefixes or the prefix snooped from certain VLAN.

For example: clear all IPv6 prefixes snooped.

```
Ruijie# clear ipv6 nd snooping prefix
```

For example: clear IPv6 prefixes snooped from VLAN 8.

```
Ruijie# clear ipv6 nd snooping prefix vlan 8
```

## Clear Stateless Configuration User

Command	Function
Ruijie# <b>clear ipv6 nd snooping stateless- user [vlan vid]</b>	In privilege mode, clear stateless configuration user

For example: clear all stateless configuration users.

```
Ruijie# clear ipv6 nd snooping stateless-user
```

For example: clear stateless configuration users on VLAN 8.

```
Ruijie# clear ipv6 nd snooping stateless-user vlan 8
```

## Display ND Snooping

### Display ND Snooping Configurations

Command	Function
Ruijie# <b>show ipv6 nd snooping [interface]</b>	Display the ND snooping configurations. Interface: only display interface information.

For example: display ND Snooping configurations

```
Ruijie# show ipv6 nd snooping
Switch ND snooping: enabled
ND Snooping is disabled on following VLANs:
None
Route information check: enabled
Address resolution check: enabled, key-node-only
Gateway Detection: enabled
Gateway Detection is enabled on following VLANs:
1-64
Stateless-user monitor: enabled
Stateless-user bind: disabled, loose, IP-only
Stateless-user Per-vlan prefix-limit: 2
Interface    Trusted    Combine-security    User-limit
-----
Gi 0/1       Y          -                    -
Gi 0/2       N          Y                    16
```



Gi 0/3	N	Y	16
--------	---	---	----

For example: display ND Snooping interface configurations

```
Ruijie# show ipv6 nd snooping interface
```

Interface	Trusted	Combine-security	User-limit
-----	-----	-----	-----
Gi 0/1	Y	-	-
Gi 0/2	N	Y	16
Gi 0/3	N	Y	16

## Display Key Nodes

Command	Function
Ruijie# <b>show ipv6 nd snooping key-node</b>	Display the information of key nodes

For example: display the information of ND snooping key nodes

```
Ruijie# show ipv6 nd snooping key-node
```

Key-node amount: 2

VLAN	IPv6 address	Type	Lifetime(s)
-----	-----	-----	-----
-	2003::1/128	Manual	INFINITE
1	FE80::218:8BFF:FE84:b738/128	Dynamic	1800

## Display Stateless Configuration User

Command	Function
Ruijie# <b>show ipv6 nd snooping stateless-user</b>	The total number and list of dynamically snooped stateless configuration users.

For example: display the information of stateless users learned.

Ruijie# show ipv6 nd snooping stateless-user

```
Stateless-user amount: 3
```

VLAN	MAC address	Interface	State	IPv6 address
-----	-----	-----	-----	-----
1	0018:8b84.b738	Gi 0/1	Active	FE80::218:8bff:fe84:b738 *
				2004::218:8bff:fe84:b738 *
2	0018:8b84.b739	Gi 0/2	Active	FE80::218:8bff:fe84:b739
				2005::218:8bff:fe84:b739
3	0000.0000.0001	Gi 0/3	Detecting	—

**Caution**

If you enable stateless address configuration user binding, in case of the overflow of hardware resources, IPv6 addresses which cannot be bound to the hardware will be marked with \*.

## Display IPv6 Prefix

Command	Function
Ruijie# <b>show ipv6 nd snooping prefix</b>	Display the VLAN IPv6 prefix configuration and the IPv6 prefix learned.

For example: display information related to IPv6 prefix.

Ruijie# **show ipv6 nd snooping prefix**

```

VLAN      Prefix                               lifetime(s)
----      -
1    1001::/64                               180
1      1002::/64                               180
2      3001::/64                               180
2      3002::/64                               180

```

**Caution**

If the prefix number snooped is larger than the number configured, those with smaller value will be kept.

## Typical ND Snooping Configuration Examples

### Stateless Auto-configuration

#### Networking Requirements

The user uses stateless auto-configuration to assign IPv6 addresses, and now intends to deploy IPv6 ND Snooping to realize the following objectives:

ND routing information attack protection and ND address resolution attack protection.

Monitor IPv6 users in the network and bind IPv6 addresses to avoid IPv6 address embezzlement.

The user also intends to deploy ACL and QOS, and expects ND snooping can reduce the consumption of hardware resources as best as possible and allow the coexistence of multiple security policies.

Since the Port Security and 802.1X IPv4 authentication & authorization system have been deployed, the user expects IPv6 can inherit these security policies, so as to enhance the security and manageability of IPv6 network.

ND Snooping shall allow self-adaptability to the changes in IPv6 network configuration.

## Network Topology

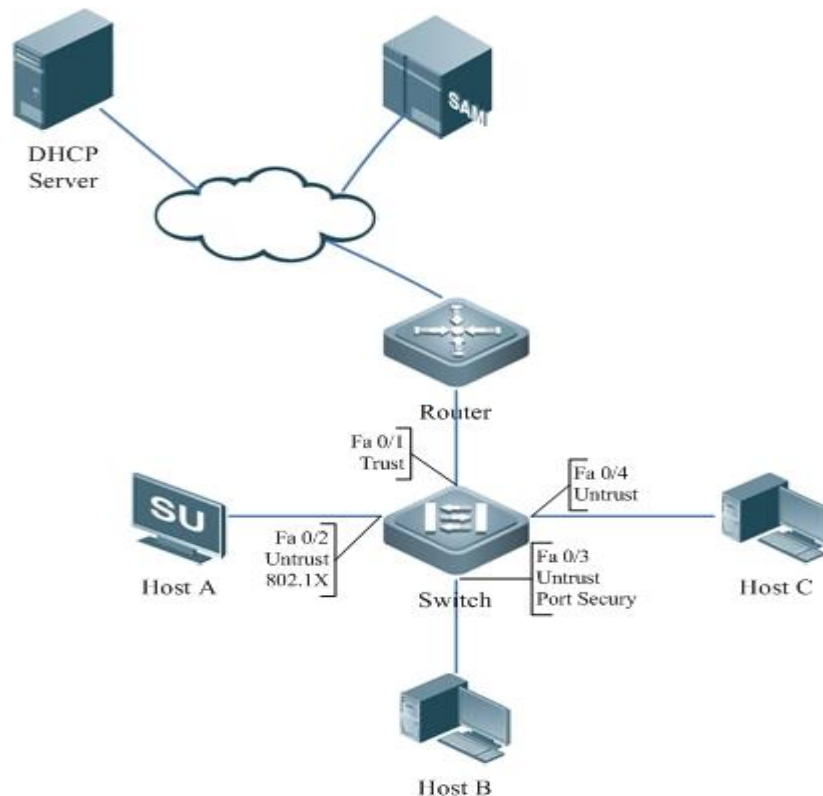
The network adopts stateless address auto-configuration to configure the IPv6 address of interface.

The FA 0/1 interface of Switch is linked to router.

Host A is linked to FA 0/2 interface of Switch (VLAN1, access control with 802.1X).

Host B is linked to FA 0/3 interface of Switch (VLAN2, access control with Port Security).

Host C is linked to FA 0/4 interface of Switch (VLAN3, no access control).



## Configuration Tips

In order to allow lower hardware consumption and the coexistence of other security policies, user binding shall use loose mode, and only IP information can be bound.

Use combined security mode to inherit the existing security policies of IPv4.

## Configuration Steps

### Enable IPv6 ND Snooping

```
Ruijie#configure terminal
```

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

```
Ruijie(config)#ipv6 nd snooping
```

### Configure trust attribute of the interface

```
Ruijie(config)#interface fastethernet 0/1
```

```
Ruijie(config-if)#ipv6 nd snooping trust
```

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

### Enable ND address resolution attack protection

```
Ruijie(config)#ipv6 nd snooping check address-resolution
```

### Enable stateless configuration user monitoring

```
Ruijie(config)#ipv6 nd snooping monitor stateless-user
```

### Enable stateless configuration user binding

```
Ruijie(config)#ipv6 nd snooping stateless-user address-bind
```

### Enable combined security monitoring

```
Ruijie(config)#interface range fastethernet 0/2-3
```

```
Ruijie(config-if)# ipv6 nd snooping stateless-user combine-security
```

## Verification

```
Ruijie# show ipv6 nd snooping
```

```
Switch ND snooping: enabled
```

```
ND Snooping is disabled on following VLANs:
```

```
None
```

```
Route information check: enabled
```

```
Address resolution check: enabled
```

```
Gateway Detection: disabled
```

```
Gateway Detection is enabled on following VLANs:
```

```
None
```

```
Stateless-user monitor: enabled
```

```
Stateless-user bind: enabled, loose, IP-only
```

```
Stateless-user Per-vlan prefix-limit: 2
```

Interface	Trusted	Combine-security	User-limit
-----	-----	-----	-----
Fa 0/1	Y	-	-
Fa 0/2	N	Y	16
Fa 0/3	N	Y	16
Fa 0/4	N	N	16

## Stateful Auto-configuration

### Networking Requirements

The user uses DHCPv6 to assign IPv6 addresses and enables DHCPv6 snooping. Now the user intends to deploy IPv6 ND Snooping to realize ND routing information attack protection and ND address resolution attack protection.

### Network Topology

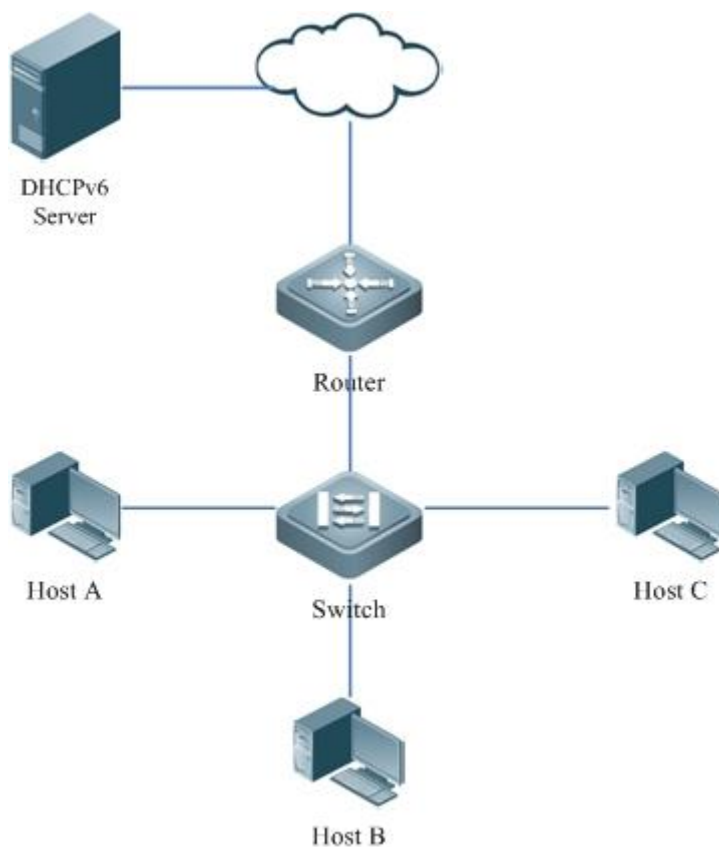
The network adopts DHCPv6 to assign IPv6 addresses, and ND Snooping and DHCPv6 snooping have been enabled on Switch.

The FA 0/1 interface of Switch is linked to router.

Host A is linked to FA 0/2 interface of Switch (VLAN1).

Host B is linked to FA 0/3 interface of Switch (VLAN2).

Host C is linked to FA 0/4 interface of Switch (VLAN3).



### Configuration Tips

NA

### Configuration Steps

Enable IPv6 ND Snooping

```
Ruijie# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Ruijie(config)#ipv6 nd snooping
```

### Configure trust attribute of the interface

```
Ruijie(config)#interface fastethernet 0/1
Ruijie(config-if)#ipv6 nd snooping trust
Ruijie(config-if)#exit
```

### Enable ND address resolution attack protection

```
Ruijie(config)#ipv6 nd snooping check address-resolution
```

## Verification

```
Ruijie# show ipv6 nd snooping
Switch ND snooping: enabled
ND Snooping is disabled on following VLANs:
None
Route information check: enabled
Address resolution check: enabled
Gateway Detection: disabled
Gateway Detection is enabled on following VLANs:
None
Stateless-user monitor: disabled
Stateless-user bind: disabled, loose, IP-only
Stateless-user Per-vlan prefix-limit: 2
```

Interface	Trusted	Combine-security	User-limit
-----	-----	-----	-----
Fa 0/1	Y	-	-
Fa 0/2	N	N	16
Fa 0/3	N	N	16
Fa 0/4	N	N	16

## Manual Configuration

### Networking Requirements

The user uses manual mode to assign IPv6 addresses and now intends to deploy IPv6 ND Snooping to realize ND routing information attack protection and ND address resolution attack protection. No other security policy assistance is needed.

### Network Topology

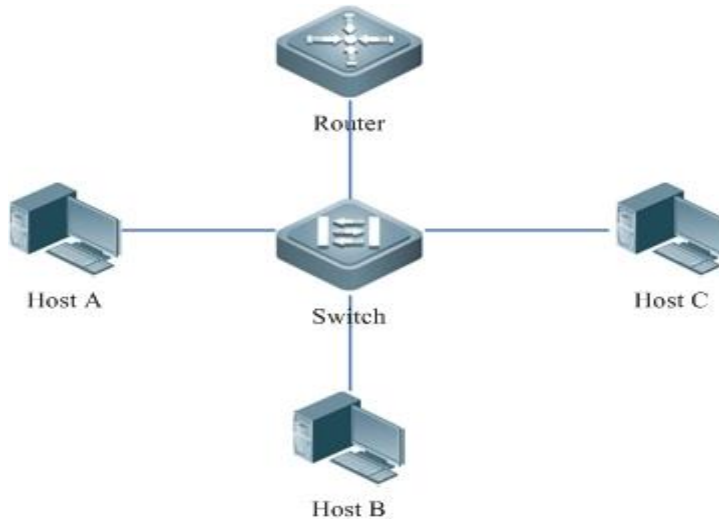
The network adopts manual configuration to configure IPv6 addresses, and ND Snooping has been enabled on Switch.

The FA 0/1 interface of Switch is linked to router.

Host A is linked to FA 0/2 interface of Switch (VLAN1).

Host B is linked to FA 0/3 interface of Switch (VLAN1).

Host C is linked to FA 0/4 interface of Switch (VLAN1).



## Configuration Tips

Since no other security policy assistance is needed to realize ND address resolution attack protection, only gateway address resolution attack protection can be used: enable ND key-node-only address resolution attack protection and manually add gateway information as key node.

## Configuration Steps

### Enable IPv6 ND Snooping

```
Ruijie#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Ruijie(config)#ipv6 nd snooping
```

### Configure trust attribute of the interface

```
Ruijie(config)#interface fastethernet 0/1
Ruijie(config-if)#ipv6 nd snooping trust
Ruijie(config-if)#exit
```

### Enable ND key-node-only address resolution attack protection.

```
Ruijie(config)#ipv6 nd snooping check address-resolution key-node-only
```

### Manually add gateway node information as key node.

```
Ruijie(config)# ipv6 nd snooping key-node 2003::1/128
```

## Verification

```
Ruijie# show ipv6 nd snooping
```

Switch ND snooping: enabled

ND Snooping is disabled on following VLANs:

None

Route information check: enabled

Address resolution check: enabled, key-node-only

Gateway Detection: disabled

Gateway Detection is enabled on following VLANs:

None

Stateless-user monitor: disabled

Stateless-user bind: disabled, loose, IP-only

Stateless-user Per-vlan prefix-limit: 2

Interface	Trusted	Combine-security	User-limit
-----	-----	-----	-----
Fa 0/1	Y	-	-
Fa 0/2	N	N	16
Fa 0/3	N	N	16
Fa 0/4	N	N	16

Ruijie# show ipv6 nd snooping key-node

Key-node amount: 2

VLAN IPv6 address	Status	Lifetime(s)
-----	-----	-----
- 2003::1/128	Manual	INFINITE



# DHCPv6 Snooping Configuration

## Introduction to DHCPv6 Snooping

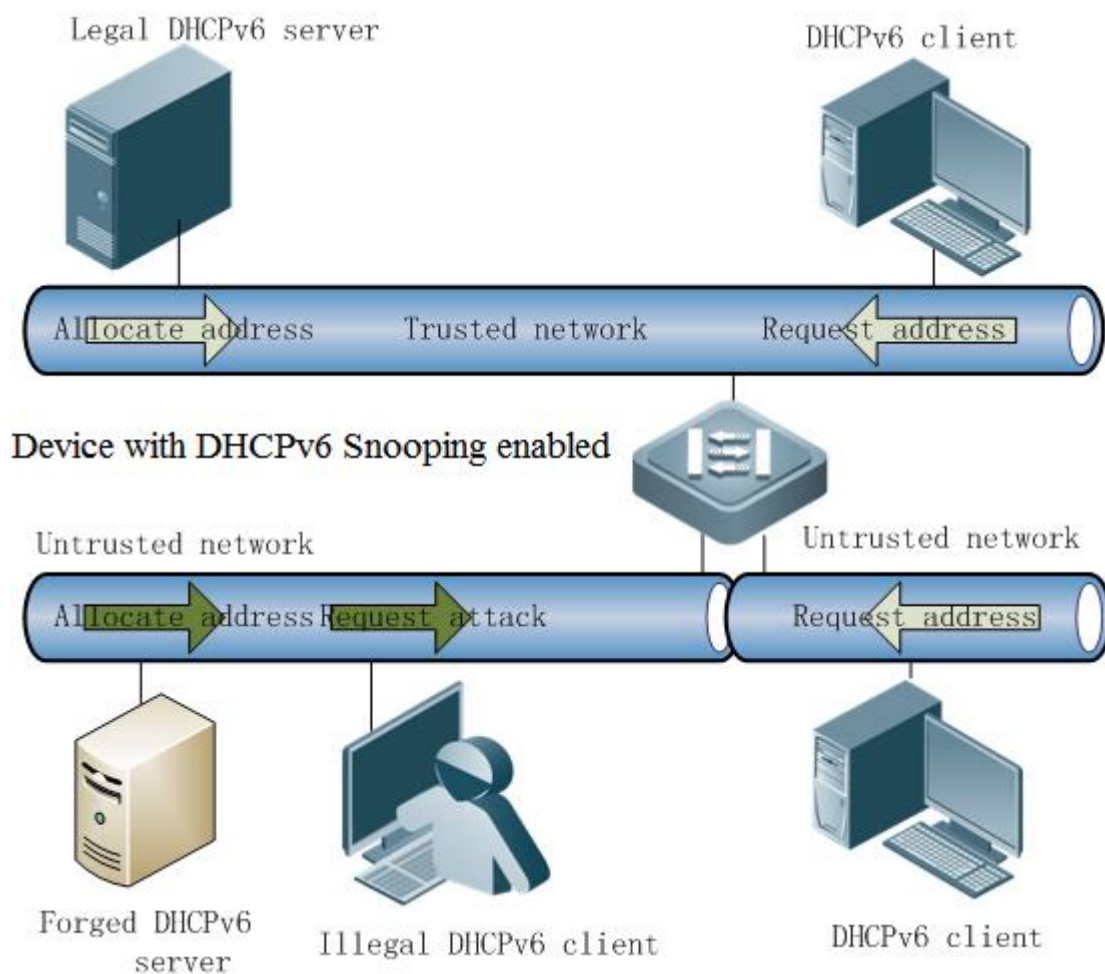
### DHCPv6 Overview

As IPv6 network is growing, IPv6 network-based applications are popularized gradually. As the framework put forward in the initial design stage of IPv6, automatic configuration of nodes is the key point of IPv6 network. Stateless configuration and stateful configuration come into being in the new network framework. With stateless automatic configuration, the newly added nodes in a network can be configured through route advertisement. With statefull automatic configuration, on the other hand, network nodes configure their addresses and other parameters by interacting with the configuration server in the network. As the unique statefull configuration mode at present, DHCPv6 is detailed in RFC3315. Below illustrates a typical DHCPv6 interaction process.

- a) The DHCPv6 client sends a multicast solicitation message with the destination IP address of FF02::1:2 and the destination UDP port of 547 through a local link. All the DHCPv6 server and the DHCPv6 relays along this link will receive this message.
- b) Upon receiving the multicast solicitation message, the DHCPv6 server unicasts an advertisement response message.
- c) After selecting the server, the DHCPv6 client sends a multicast request message with the destination IP address of FF02::1:2 and the destination UDP port of 547 through a local link.
- d) Upon receiving the multicast request message, the DHCPv6 server unicasts a reply message.

### DHCPv6 Snooping Overview

DHCPv6 Snooping snoops the DHCPv6 interaction messages between the DHCPv6 clients and the DHCPv6 server, and filters the response packets from illegal servers under reasonable configuration.



As shown in Figure 2, DHCPv6 Snooping prevents abnormal packet attacks from the forged DHCP server and illegal DHCP clients in a untrusted network.

Furthermore, the snooping packet result is generated and applied. If the DHCPv6 server allocates IPv6 prefix, a user entry is formed based on the information like the allocated IPv6 prefix, user MAC address, port where the user is located in, ID of the VLAN the user belongs to, and lease period, and thus the DHCPv6 Snooping prefix database is generated. If the DHCPv6 server allocates IPv6 address, a user entry is formed based on the information like the allocated IPv6 address, user MAC address, port where the user is located in, ID of the VLAN the user belongs to, and lease period, and thus the DHCPv6 Snooping binding database is generated.

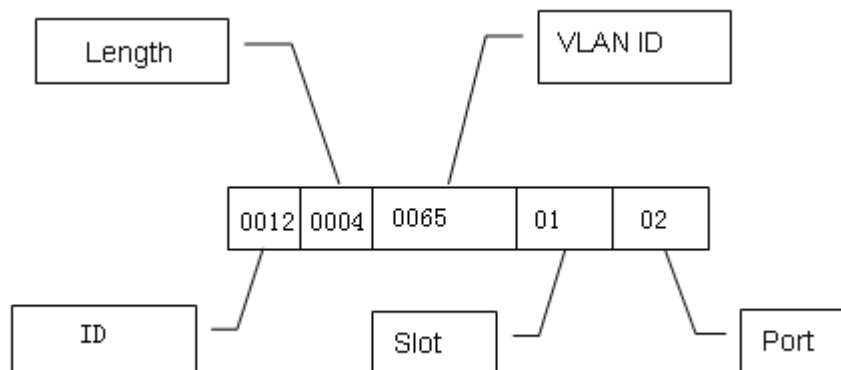
## DHCPv6 Snooping Information Option Overview

While implementing IP management of current users, some network administrators may want to assign IP address according to user's location, namely to assign IP address according to the network device connected by the user, so that the switch can insert certain device information related to user into the DHCP request packets in the format of DHCPv6 option during DHCPv6 snooping. According to RFC3315, the option number used is 18, while according to RFC4649, the option number used shall be 37. By configuring to analyze the option18/37 content on DHCPv6 Server, this server can learn more information about the user according to the contents carried in option18/37, so as to assign IP address to the user in a more accurate manner.

### Option18: Interface ID

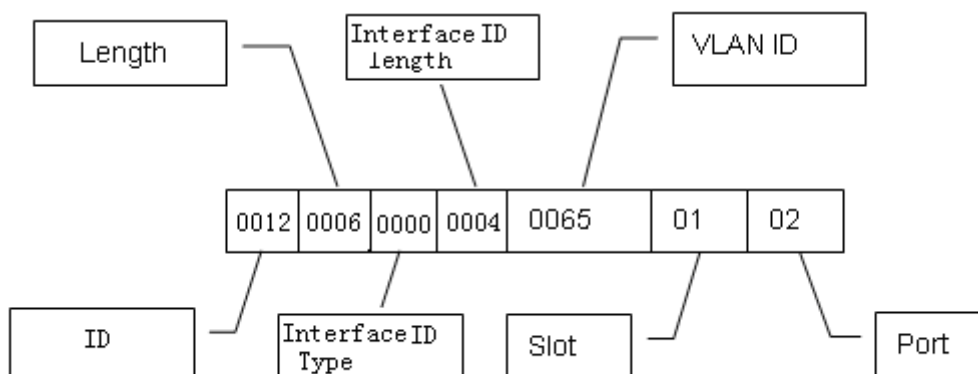
The default insertion contents of Interface ID include the VLAN ID of the port receiving the DHCP client request and the port index (port index is the slot ID and port number). The extended insertion contents include the self-defined string.

The insertion format of Interface ID includes standard format and extended format. Only one format can be used in the same network domain. When standard format is used, the suboption of Interface ID can only include default insertion contents, as shown below:

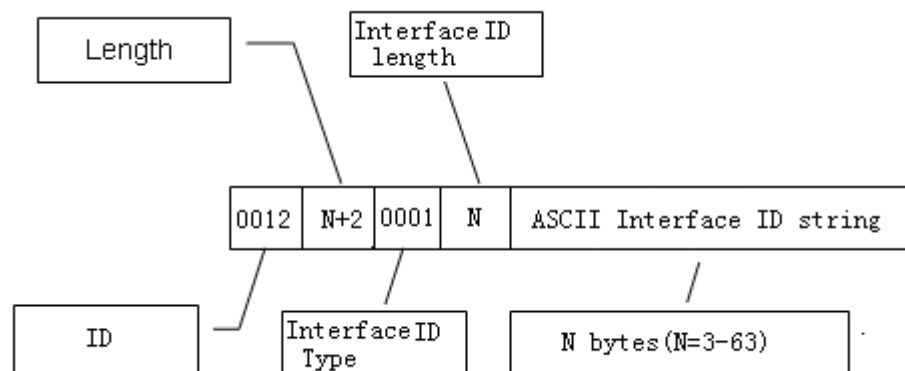


If self-defined insertion contents are needed, the extended format can be used. The inserted contents of extended format can include default insertion contents and extended insertion contents. To distinguish between insertion contents, a one-byte content type field and a one-byte content length field is added after the suboption. In case of default insertion content, the content type will be 0; in case of extended insertion content, the content type will be 1.

The format of default insertion contents is shown below:



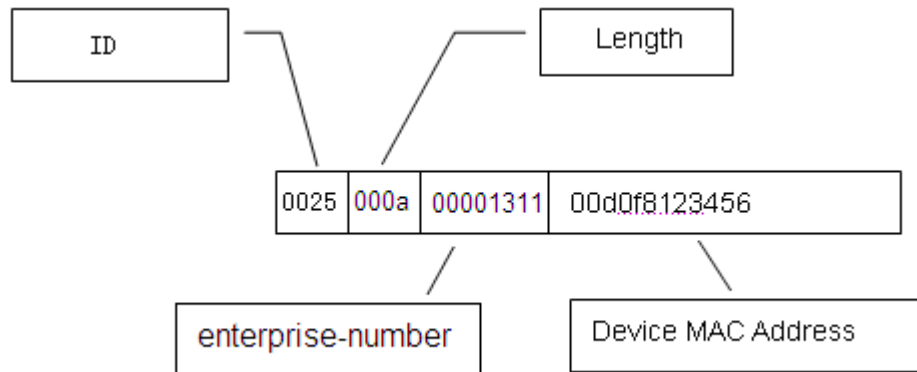
The format of extended insertion contents is shown below:



### Option37: Remote ID

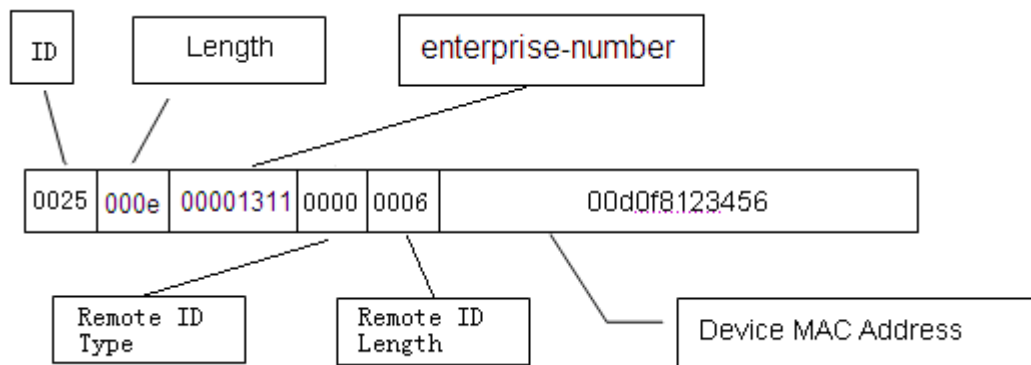
The default insertion contents of Remote ID include the bridge MAC address of DHCP relay receiving the DHCP client request. The extended insertion contents include the self-defined string.

The insertion format of Remote ID includes standard format and extended format. Only one format can be used in the same network domain. When standard format is used, the suboption of Remote ID can only include default insertion contents, as shown below:

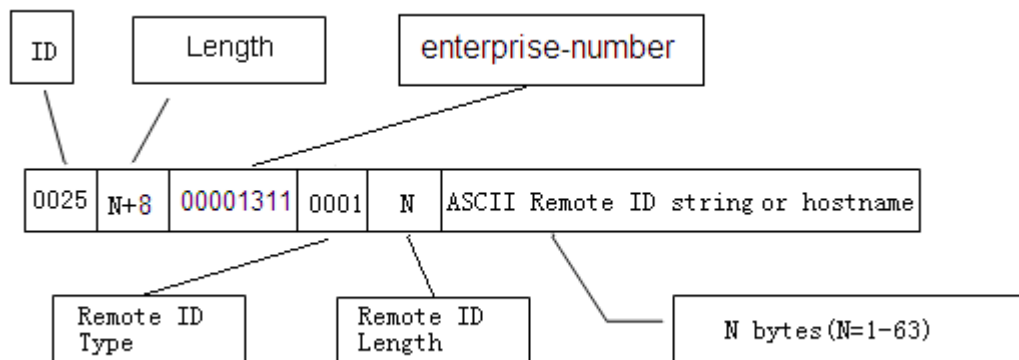


If self-defined insertion contents are needed, the extended format can be used. The inserted contents of extended format can include default insertion contents and extended insertion contents. To distinguish between insertion contents, a one-byte content type field and a one-byte content length field is added after the suboption. In case of default insertion content, the content type will be 0; in case of extended insertion content, the content type will be 1.

The format of default insertion contents is shown below:



The format of extended insertion contents is shown below:



## Basic DHCPv6 Snooping Concepts

### Trusted port

Since the DHCPv6 clients may send request messages in multicast form, the illegal DHCPv6 server in the network will influence the normal DHCPv6 interaction process. To prevent illegal server, ports fall into two types-trusted port and untrusted port. All ports are untrusted ports by default. Devices forward the DHCPv6 server's reply message from trusted ports and discard the DHCPv6 server's reply message from untrusted ports.

Hence, the port connected to the legal DHCPv6 server is set to trusted port and other ports are set to untrusted ports to shield illegal DHCPv6 server.

As specified in RFC3315 and RFC5007 and other protocols, the DHCPv6 reply message falls into the following types-ADVERTISE, REPLY, RECONFIGURE, RELAY-REPLY, LEASEQUERY-REPLY, LEASEQUERY-DATA and LEASEQUERY-DONE, which are filtered on untrusted ports.

### IPv6 source guard

IPv6 source guard is equivalent to adding a hardware ACL entry on a port, which filters all IPv6 packets sent over the port (except for DHCPv6 packet). After a user applies an IPv6 address through DHCPv6 interaction or administrator manually adds a static binding entry, a hardware ACL entry is added on the port that allows the user to do IPv6 communication through this address.



**Caution**

Once IPv6 source guard is enabled, all IPv6 packets will not be forwarded by default. To enable communication through local link address, configure security channel and associate with corresponding ACL. For details, refer to *ACL Configuration Guide*.

### Protocol Standards

Related protocol standards:

- RFC3315 Dynamic Host Configuration Protocol For Ipv6
- RFC5007 DHCPv6 Lease query

## Configure Basic DHCPv6 Snooping Features

Basic DHCPv6 Snooping features include:

- (Optional) Ignore the failure to look up the destination port
- (Optional) Clear the dynamically bound entries when the port is down
- (Optional) Add the bound entry to the hardware filtering table lingeringly

**Note**

For 10.4 version, all products support above configurations.

## Default DHCPv6 Snooping Configuration

Below describes default configurations of DHCPv6 Snooping.

Feature	Default value
Global DHCPv6 Snooping	Disabled
VLAN-based DHCPv6 Snooping	Enabled(once DHCPv6 Snooping is enabled globally, DHCPv6 Snooping is enabled on every VLAN)
Write the bound database to Flash file periodically	Disabled
Manually add statically bound entry	No statically bound entry is available.
Configure the trust attribute of a port	Untrusted
Enable DHCPv6 packet rate limit on the port	Disabled
Filter DHCPv6 request packet on the port	Disabled
Port address binding	Disabled
Ignore the failure to look up the destination port	Disabled
Clear the dynamically bound entry when the port is down	Disabled
Add dynamically bound entry delay to the hardware filtering table	Disabled

## Enable/disable DHCPv6 Snooping Globally

By default, DHCPv6 Snooping is disabled. To enable DHCPv6 Snooping globally, run the following commands in the privileged EXEC mode.

Command	Function
Ruijie# <b>configure terminal</b>	Enter the global configuration mode.
Ruijie(config)# <b>ipv6 dhcp snooping</b>	Enable DHCPv6 Snooping.
Ruijie(config)# <b>show ipv6 dhcp snooping</b>	Show the configuration of DHCPv6 Snooping.

To restore the setting to the default value, run the no ipv6 dhcp snooping command in the global configuration mode.

Configuration example:

```
# Enable DHCPv6 Snooping globally and show its configuration.
```

```

Ruijie# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Ruijie(config)# ipv6 dhcp snooping
Ruijie(config)# show ipv6 dhcp snooping
Switch DHCPv6 snooping status : ENABLE
DHCPv6 snooping vlan: 1-4094
DHCPv6 snooping database write-delay time: 0 seconds
DHCPv6 ignore dest-not-found :DISABLE
DHCPv6 snooping link detection: DISABLE
Interface                Trusted    Filter DHCP
-----
FastEthernet0/10         yes      DISABLE

```

## Enable/disable DHCPv6 Snooping Based on VLAN

Once DHCPv6 Snooping is enabled globally, the DHCPv6 Snooping is enabled on all VLANs. You can disable the DHCPv6 Snooping function form some VLAN as required.

To enable DHCPv6 Snooping for a VLAN, run the following commands in the privileged EXEC mode.

Command	Function
Ruijie# <b>configure terminal</b>	Enter the global configuration mode.
Ruijie(config)# <b>ipv6 dhcp snooping vlan</b> {vlan-list   {vlan-min [vlan-max]}}	Enable DHCPv6 Snooping for the specific VLAN.
Ruijie(config)# <b>show ipv6 dhcp snooping</b>	Show the DHCP Snooping configuration.

To restore the setting to the default value, run the **default ipv6 dhcp snooping vlan** {vlan-list | {vlan-min [vlan-max]}} command in the global configuration mode.

To disable DHCPv6 Snooping for the specific VLAN, run the **no ipv6 dhcp snooping vlan** {vlan-list | {vlan-min [vlan-max]}} command in the global configuration mode.

Configuration example:

# Enable DHCPv6 Snooping on VLANs 1, 3, 4, 5, 7, 9, 10 and 11.

```

Ruijie# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Ruijie(config)# ipv6 dhcp snooping vlan 1,3-5,7,9-11

```



**Caution**

Once a VLAN is created, DHCP Snooping is enabled on this VLAN by default. To disable this function, run the corresponding command on this VLAN manually.

## Write the Bound Database to Flash File Periodically

This function can guarantee the normal communication of the bound user after abnormal reset. By default, this function is disabled.

To write the bound database to Flash file, run the following commands in the privileged EXEC mode.

Command	Function
Ruijie# <b>configure terminal</b>	Enter the global configuration mode.
Ruijie(config)# <b>ipv6 dhcp snooping database write-delay</b> <i>seconds</i>	Write the bound database to Flash at the interval of x seconds.
Ruijie(config)# <b>show ipv6 dhcp snooping</b>	Show DHCPv6 Snooping configuration.

To restore the setting to the default value, run the `no ipv6 dhcp snooping database write-delay` command in the global configuration mode.

Configuration example:

# Write the bound database to Flash file at the interval of 10 minutes (or 600 seconds).

```
Ruijie# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Ruijie(config)# ipv6 dhcp snooping database write-delay 600
```

## Write the Bound Database to Flash File in Real Time

Administrator can manually write the bound database to Flash file before rebooting the device to guarantee the normal operation of the bound user in case of abnormal reboot.

To write the bound database to Flash file, run the following commands in the privileged EXEC mode.

Command	Function
Ruijie# <b>configure terminal</b>	Enter the global configuration mode.
Ruijie(config)# <b>ipv6 dhcp snooping database write-to-flash</b>	Write the bound database to Flash file in real time.
Ruijie(config)# <b>show ipv6 dhcp snooping</b>	Show DHCPv6 Snooping configuration.

Configuration example:

# Write the bound database to Flash file in real time.

```
Ruijie# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Ruijie(config)# ipv6 dhcp snooping database write-to-flash
```

## Manually Import the Information in FLASH into DHCPv6 Snooping Database

While enabling DHCPv6 Snooping, you can manually import the information in flash into the DHCPv6 Snooping database.

Command	Function
---------	----------



Ruijie# renew ipv6 dhcp Snooping database	Manually import the information in flash into DHCPv6 Snooping database
--	---

The following example shows how to manually import the information in flash into DHCPv6 Snooping database:

```
Ruijie# renew ipv6 dhcp Snooping database
```

## Manually Add Statically Bound Entries

For the users using static IPv6 addresses rather than obtaining IPv6 addresses through DHCPv6 interface, administrator can manually add statically bound entries so that users can communicate each other after enabling IPv6 source guard on the port.

To add statically bound entries, run the following commands in the privileged EXEC mode:

Command	Function
Ruijie# <b>configure terminal</b>	Enter the global configuration mode.
Ruijie(config)# <b>ipv6 source binding</b> <i>mac-address vlan vlan-id ipv6-address</i> <b>interface interface-name</b>	Add the statically bound entries so that users can use static IPv6 addresses rather than obtaining IPv6 addresses through DHCPv6 interaction.
Ruijie(config)# <b>end</b>	Exit to the privileged EXEC mode.
Ruijie# <b>show ipv6 source binding</b>	Show all the statically bound entries added by hand and all the dynamically bound entries generated by DHCPv6 Snooping.

To delete the statically bound entries, run the **no ipv6 source binding** *mac-address vlan vlan-id ipv6-address interface interface-name* command in the global configuration mode.

Configuration example:

# Add a statically bound user.

```
Ruijie# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Ruijie(config)# ipv6 source binding 00d0.f866.4777 vlan 10 2001:2002::2003 interface
fastethernet 0/10
Ruijie(config)# end
Ruijie# show ipv6 source binding
Total number of bindings: 1
```

Mac Address	Ipv6 Address	Lease(s)	type	Vlan	Interface
00d0.f866.4777	2001:2002::2003	57	static	10	fa 0/10

## Configure the Trust Attribute of a Port

By default, all ports are untrusted. Once DHCPv6 Snooping enabled, the device forwards the DHCPv6 request message to all trusted ports in a VLAN.

To configure the trust attribute of a port, run the following command in the privileged EXEC mode.

Command	Function
Ruijie# <b>configure terminal</b>	Enter the global configuration mode.
Ruijie(config)# <b>interface</b> <i>interface-name</i>	Enter the interface configuration mode.
Ruijie(config-if)# <b>ipv6 dhcp snooping trust</b>	Configure the port to be trusted.
Ruijie(config-if)# <b>end</b>	Exit to the privileged EXEC mode.
Ruijie# <b>show ipv6 dhcp snooping</b>	Show DHCPv6 Snooping configuration.

To restore the setting to the default value, run the **no ipv6 dhcp snooping trust** command in the interface configuration mode.

Configuration example:

**# Set interface fastethernet 0/10 to be trusted.**

```
Ruijie# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Ruijie(config)# interface fastethernet 0/10
Ruijie(config-if)# ipv6 dhcp snooping trust
Ruijie(config-if)# end
Ruijie# show ipv6 dhcp snooping
Switch DHCPv6 snooping status : ENABLE
DHCPv6 snooping vlan: 1-4094
DHCPv6 snooping database write-delay time: 300 seconds
DHCPv6 ignore dest-not-found :DISABLE
DHCPv6 snooping link detection :DISABLE
Interface           Trusted    Filter DHCP
-----
FastEthernet0/10    yes      DISABLE
```



When DHCPv6 Snooping is enabled globally and enabled on the specific VLAN, the port in the VLAN connecting to the DHCPv6 server should be set to be trusted for normal DHCPv6 interaction for the users in the VLAN.

## Filter DHCPv6 Request Message on the Port

To limit the users under a port not to do DHCPv6 packet interaction, filter DHCPv6 request message on the port.

To filter the DHCPv6 request message on the port, run the following command in the privileged EXEC mode.

Command	Function
Ruijie# <b>configure terminal</b>	Enter the global configuration mode.
Ruijie(config)# <b>interface</b> <i>interface-name</i>	Enter the interface configuration mode.
Ruijie(config-if)# <b>ipv6 dhcp snooping filter-dhcp-pkt</b>	Filter the DHCPv6 request message on the port.
Ruijie(config-if)# <b>end</b>	Exit to the privileged EXEC mode.
Ruijie# <b>show running</b>	Show configuration.

To restore the setting to the default value, run the **no ipv6 dhcp snooping filter-dhcp-pkt** command in the interface configuration mode.

Configuration example:

# Filter the DHCPv6 request message on FastEthernet 0/1.

```
Ruijie# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Ruijie(config)# interface fastEthernet 0/10
Ruijie(config-if)# ipv6 dhcp snooping filter-dhcp-pkt
Ruijie# show ipv6 dhcp snooping
Switch DHCPv6 snooping status : ENABLE
DHCPv6 snooping vlan: 1-4094
DHCPv6 snooping database write-delay time: 0 seconds
DHCPv6 ignore dest-not-found :DISABLE
DHCPv6 snooping link detection :DISABLE
Interface           Trusted    Filter DHCP
-----
FastEthernet0/10    NO        ENABLE
```

## Enable/Disable IPv6 source guard

Once IPv6 source guard is enabled on a port, all the IPv6 packets, except for DHCPv6 packets, on the inbound direction of the port will be filtered. If there is IPv6 address conflict, the ND protocol packets should be allowed to pass through this port. Configuring security channel or enable ND Snooping can realize this end to detect IPv6 address conflict. For details, refer to the configuration sections of related functions. When a user applies IPv6 address through DHCPv6 interaction, DHCPv6 Snooping will add the corresponding user bound information to the hardware filtering table so that his IPv6 packets can be forwarded properly. By default, port-address binding is disabled on the port and all IPv6 packets are forwarded properly.

To enable port-address binding, run the following commands in the privileged EXEC mode mode.

Command	Function
Ruijie# <b>configure terminal</b>	Enter the global configuration mode.

Ruijie(config)# <b>interface</b> <i>interface-name</i>	Enter the interface configuration mode.
Ruijie(config-if)# <b>ipv6 verify source [port-security]</b>	Enable port-address binding. <b>port-security</b> means enabling IPv6-MAC-port binding. Without this option, IPv6-port binding is enabled.
Ruijie(config-if)# <b>end</b>	Exit to the privileged EXEC configuration mode.

To restore the setting to the default value, run the **no ipv6 verify source** command in the interface configuration mode.

Configuration example:

# Enable port-address binding on **interface fastethernet 0/10**.

```
Ruijie# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Ruijie(config)# interface fastethernet 0/10
Ruijie(config-if)# ipv6 verify source port-security
Ruijie(config-if)# end
```

## Ignore the Failure to Look UP the Destination Port

Forwarding the DHCPv6 response message depends on the lookup in the MAC address table. If the port corresponding to the MAC address cannot be found, the DHCPv6 response message will not be forwarded for security.

In some special network environments, learning MAC address may be delayed or lost for some reasons like network congestion, network topology oscillation and too many stacked devices. In this case, the system prompts "DHCPV6\_Snooping-5-DEST\_NOT\_FOUND: Could not find destination port. Destination MAC [mac-address]." For normal DHCPv6 operation in the entire network, the packets that the port corresponding to the MAC address is not found are sent to all the ports of the specific VLAN in broadcast form, or directly forwarded to the source port the DHCP request message recorded in the DHCPv6 Snooping database.

To ignore the failure to look up the destination port, run the following commands in the privileged EXEC mode.

Command	Function
Ruijie# <b>configure terminal</b>	Enter the global configuration mode.
Ruijie(config)# <b>ipv6 dhcp snooping ignore dest-not-found</b>	Ignore the failure to look up the destination port.
Ruijie(config)# <b>end</b>	Exit to the privileged EXEC mode.

To restore the setting to the default value, run the **no ipv6 dhcp snooping ignore dest-not-found** command in the global configuration mode.

Configuration example:

```
Ruijie# configure terminal
```

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

```
Ruijie(config)# ipv6 dhcp snooping ignore dest-not-found
```

```
Ruijie(config)# end
```

## Clear Dynamically Bound Entries when the Port is Linked Down

Once a port is linked down, the users under the port cannot communicate with external users. However, the dynamically bound entries still exist until lease period is expired. Disabling this function is to prevent all entries from losing effectiveness caused by temporary link oscillation. Consequently, this function is disabled by default.

Sometimes, in a stable network, you may need to clear the entries related to the ports who are linked down to reduce the occupation of hardware entries. This function can help you to realize this end. It should be noted that frequent link oscillation should be avoided.

To clear the dynamically bound entries when the port is linked down, run the following commands in the privileged EXEC mode.

Command	Function
Ruijie# <b>configure terminal</b>	Enter the global configuration mode.
Ruijie(config)# <b>ipv6 dhcp snooping link-detection</b>	Clear the dynamically bound entries when the port is linked down.
Ruijie(config)# <b>end</b>	Exit to the privileged EXEC mode.

To restore the setting to the default value, run the **no ipv6 dhcp snooping link-detection** command in the global configuration mode.

Configuration example:

```
Ruijie# configure terminal
```

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

```
Ruijie(config)# ipv6 dhcp snooping link-detection
```

```
Ruijie(config)# end
```

## Add the Dynamically Bound Entries to the Hardware Filtering Table Lingeringly

By default, the dynamically bound entries are added to the hardware filtering table in real time. When the DHCPv6 client detects IPv6 address conflict, it responds with the DHCPv6 decline message, based on which DHCPv6 Snooping deletes the dynamically bound entry. With this function enabled, the dynamically bound entries will be added to the hardware filtering table only when IPv6 address conflict is not detected in the specific period of time. In the environment of fewer IPv6 address conflict, if this function is enabled, the client cannot access the network in the specific delay time after obtaining IPv6 address. Hence, the dynamically bound entries are added to the hardware filtering table by default. In the environment of more IPv6 address conflict, if this function is enabled, the client adds the dynamically bound entries to the hardware filtering table only after detecting no IPv6 address conflict in the specific delay time.

To add the dynamically bound entries to the hardware filtering table lingeringly, run the following commands in the privileged EXEC mode.

Command	Function
Ruijie# <b>configure terminal</b>	Enter the global configuration mode.
Ruijie(config)# <b>ipv6 dhcp snooping binding-delay</b> <i>seconds</i>	Add the dynamically bound entries to the hardware filtering table lingeringly, which is disabled by default.
Ruijie(config)# <b>end</b>	Enter the privileged EXEC mode.

To restore the setting to the default value, run the **no ipv6 dhcp snooping binding-delay** command in the global configuration mode.

Configuration example:

```
Ruijie# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Ruijie(config)# ipv6 dhcp snooping binding-delay 10
Ruijie(config)# end
```

## Configure DHCPv6 Snooping Information Option

Through the aforementioned commands, we can insert option18/37 into every DHCPv6 request while enabling DHCPv6 snooping. This feature is disabled by default.

Command	Function
Ruijie# <b>configure terminal</b>	Enter configuration mode
Ruijie(config)# <b>[no] ipv6 dhcp Snooping Information option [standard-format]</b>	Enable option82; standard-format: This keyword indicates that insertion format is standard format, or else it is extended format.
Ruijie(config)# <b>[no] ipv6 dhcp Snooping information option format remote-id [string ASCII-string   hostname]</b>	Configure remote-id in the extended format. String: the inserted content is the self-defined string; Hostname: the inserted content is host name.
Ruijie(config)# <b>interface</b> <i>interface</i>	Enter interface configuration mode
Ruijie(config-if)# <b>[no] ipv6 dhcp Snooping vlan</b> <i>vlan-id</i> <b>information option format-type interface-id string</b> <i>ASCII-string</i>	Configure the self-defined string of interface-id in extended mode.
Ruijie(config-if)# <b>[no] ipv6 dhcp Snooping vlan</b> <i>vlan-id</i> <b>information option change-vlan-to</b> <i>vlan</i> <i>vlan-id</i>	Configure vlan mapping of interface-id in extended mode; this command conflicts with the command in Step 5.

The following example shows how to enable **DHCPv6 information option**:

```
Ruijie# configure terminal
Ruijie(config)# ipv6 dhcp Snooping information option
Ruijie(config)# end
```

## Show or Clear DHCPv6 Snooping Configurations and States

The following commands show or clear DHCPv6 Snooping configurations and states.

Command	Function
<b>show ipv6 dhcp snooping</b>	Show DHCPv6 Snooping configuration.
<b>show ipv6 dhcp snooping statistics</b>	Show DHCPv6 Snooping statistics.
<b>show ipv6 dhcp snooping binding</b>	Show all dynamically bound entries of DHCPv6 Snooping binding database.
<b>show ipv6 dhcp snooping prefix</b>	Show all entries of the DHCPv6 Snooping prefix database.
<b>show ipv6 source binding</b>	Show all manually added statically bound entries and all dynamically bound entries of the DHCPv6 Snooping binding database.
<b>clear ipv6 dhcp snooping statistics</b>	Clear DHCPv6 Snooping statistics.
<b>clear ipv6 dhcp snooping binding</b>	Clear all dynamically bound entries of DHCPv6 Snooping binding database.
<b>clear ipv6 dhcp snooping prefix</b>	Clear all entries of the DHCPv6 Snooping prefix database.

## Gateway Anti-arp-spoofing Configuration

### Overview

On the switch, ARP packets are broadcasted within this VLAN by default. This makes gateway ARP spoofing possible.

Gateway ARP spoofing means as that when User A sends an ARP packet to request the MAC address of a gateway, User B in the same VLAN will receive this ARP packet. User B may send an ARP response packet and fill in the source IP address of the packet with the IP address of the gateway and in the source MAC address with its own MAC address. Upon receiving this ARP response packet, User A will consider User B's machine as the gateway. Thus, all the packets sent to the gateway within the communication of User A will be sent to User B. Consequently, communication of User A is intercepted and results in ARP spoofing.

Thus, we may configure gateway anti-arp-spoofing on the Layer 2 switches to prevent the gateway anti-ARP-spoofing. After gateway anti-arp-spoofing has been configured, we may check at the port whether the source IP address of an ARP packet is the IP address of the gateway we have configured. If it is, this packet will be discarded to prevent an user to receive a wrong ARP response packet. Thus, only the device connected with the switch can deliver the ARP packets of the gateway. Other PCs cannot send any counterfeit ARP response packet of the gateway.

### Configuring Gateway Anti-arp-spoofing

#### Setting Gateway Anti-arp-spoofing

Set the IP address of gateway anti-arp-spoofing:

Command	Function
Ruijie(config-if)# <b>anti-arp-spoofing ip</b> <i>ip-address</i>	Configure gateway anti-arp-spoofing on this port. <i>ip-address</i> : specify the IP address of the gateway.

In the interface configuration mode, you may use the **no anti-arp-spoofing ip** *ip-address* command to clear the gateway anti-arp-spoofing configuration.



#### Caution

You cannot configure gateway anti-arp-spoofing at an upper link port.



## Viewing Gateway Anti-arp-spoofing Information

View the gateway anti-arp-spoofing of a switch:

Command	Function
Ruijie <b>#show anti-arp-spoofing</b>	Show the gateway anti-arp-spoofing information of all interfaces.

## Typical Anti-arp-spoofing Configuration Example

### Topological Diagram

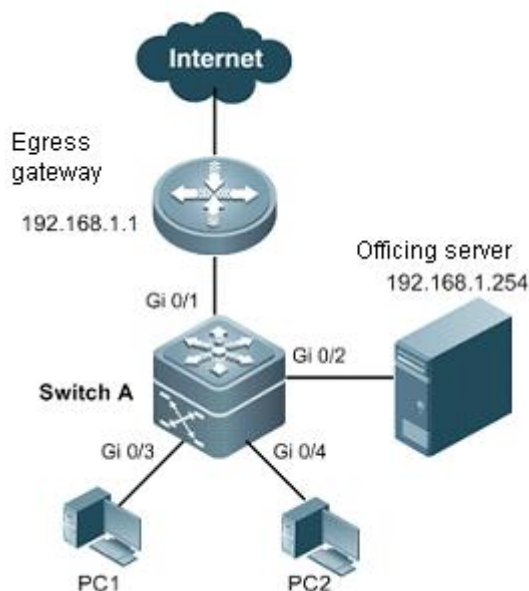


Figure1 Typical topology for anti-ARP-spoofing

### Application needs

The above figure shows the typical network topology of a medium- and small-sized company. PCs access the officing server through access device of Switch A, and are connected to Internet through the gateway device. The ARP spoofing initiated by any illegal user using the gateway IP or server IP will prevent other users from normally accessing Internet and officing server.

Based on the above analysis, the following requirement must be met:

- Block ARP-spoofing packets and guarantee that all users can access Internet normally.

### Configuration Tips

- Configuration tips

- 1) Enable anti-arp-spoofing on the PC-connecting ports (Gi 0/3, Gi 0/4) of access switch (Switch A), with gateway address being the address of Intranet gateway and Intranet server.

- **Notes**

- 1) Anti-arp-spoofing cannot be enabled on the uplink port and the port connecting gateway or server, or else ARP packets with source address being gateway IP or server IP will be blocked.
- 2) If the number of ports is insufficient and a 8-port hub must be attached to the switch, you can still enable anti-arp-spoofing on the access switch. The problem is that the ARP spoofing between computers connected to the same hub cannot be blocked.

## Configuration Steps

- **SwitchA**

### Step 1: Enable anti-arp-spoofing on PC-connecting ports

```
SwitchA# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
SwitchA(config)#interface range gigabitEthernet 0/2-4
SwitchA(config-if-range)# anti-arp-spoofing ip 192.168.1.1
SwitchA(config-if-range)# anti-arp-spoofing ip 192.168.1.254
```

## Verify configurations

Step 1: Verify whether the configurations are correct. Key points: whether anti-arp-spoofing has been enabled, whether the gateway address is correct, and whether anti-arp-spoofing is enabled on the uplink port.

```
SwitchA (config-if)#show running-config
interface GigabitEthernet 0/1
!
interface GigabitEthernet 0/2
anti-arp-spoofing ip 192.168.1.1
anti-arp-spoofing ip 192.168.1.254
!
interface GigabitEthernet 0/3
anti-arp-spoofing ip 192.168.1.1
anti-arp-spoofing ip 192.168.1.254
!
interface GigabitEthernet 0/4
anti-arp-spoofing ip 192.168.1.1
anti-arp-spoofing ip 192.168.1.254
!
```

Step 2: View the anti-arp-spoofing state in order to verify again. Key points are the same as those in Step 1.

```
SwitchA#show anti-arp-spoofing
Anti-arp-spoofing
port          ip
-----
Gi 0/2        192.168.1.1
Gi 0/2        192.168.1.254
Gi 0/3        192.168.1.1
Gi 0/3        192.168.1.254
Gi 0/4        192.168.1.1
Gi 0/4        192.168.1.254
```

Step 3: If possible, configure the IP address of PC1 to the IP address of gateway, and then observe whether the gateway can report IP address conflict and whether PC2 can access Internet normally.

If everything is fine, it means that anti-arp-spoofing has taken effect.

# NFPP Configuration

## NFPP Overview

NFPP is the abbreviation of Network Foundation Protection Policy.

- NFPP Function
- NFPP Principle

### NFPP Function

In the network, some malicious attacks put too much burden on the switch. When the packet traffic bandwidth or the packet percent exceeds the limit, it leads to the CPU over-utilization and abnormal operation of the switch.

DoS attack may lead to the consumption of a large amount of the switch memory, entries and other resources, resulting in the system service failure.

A large amount of the packet traffic uses the CPU bandwidth, resulting in the handling failure of the protocol packet and manage packet by the CPU, influencing the data forwarding, the device management of the administrator and the normal device/network running.

In the NFPP-enabled environment, it prevents the system from being attacked, releasing the CPU load and ensuring the normal and stable operation of various system services and the whole network.

### NFPP Principle

As shown in the Figure-1, the processes of the NFPP datagram processing include hardware filtering, CPU Protect Policy (CPP), packet attack detection/rate-limit, Protocol/Manage/Route flow classification, focus rate-limit and ultimately the application-layer handling.

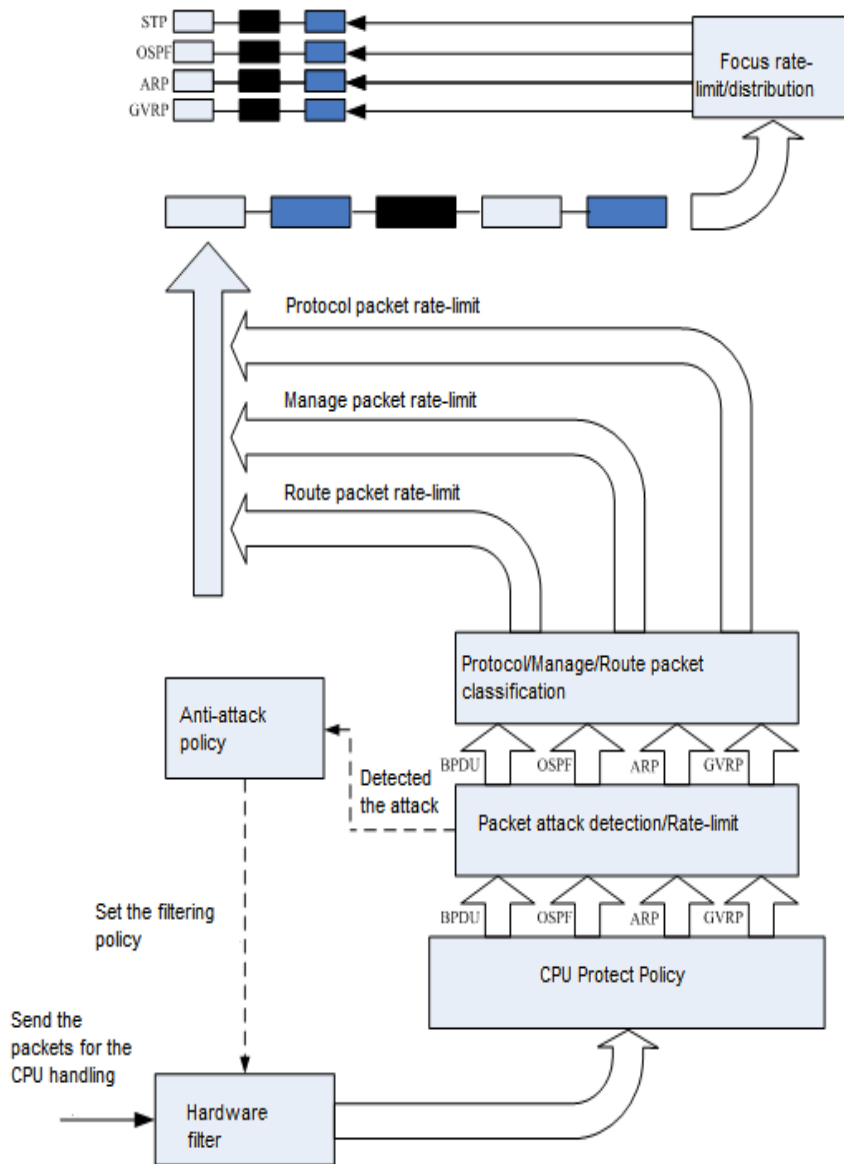
#### 1. CPU Protect Policy(CPP)

The CPP classification and rate-limit configurations not only classify the CPU datagram according to the CPP service classification principle, but also limit the rate of the packet transmission, preventing different packets from competing for the bandwidth and resolving the problem that when a large amount of one packet flow attack occurs, it fails to handle other packets in time. For example, with both the OSPF packet and BPDU packet in the NFPP-enabled device, if the OSPF/BPDU packets consume a large amount of the CPU bandwidth, it will not influence receiving the BPDU/OSPF packets.



#### Caution

In order to make full use of the NFPP function, you can modify the rate-limit value of each packet in CPU Protect Policy according to specified network environment, you can also use the recommended value displayed after executing the **show cpu-protect summary** command.



## 2. Packet attack detection/Rate-limit

NFPP provides the host-based/port-based attack and rate-limit threshold configuration for the administrator to set in the specific network flexibly to control the rate of receiving the packets based on the host/port. With the attack threshold configured, after detecting the attack, the anti-attack policy implements the attack-warning or the isolation action. For the isolation action, the anti-attack policy uses the hardware filter in order to make sure that the attack packets will not be sent to the CPU and ensure the normal device operation.



After detecting an attack, NFPP sends the warning messages to the administrator. However, to avoid the frequent displaying of the warning messages, the warning messages will not be shown again within the continuous 60s after the sending.

Frequently print the syslog consumes the CPU resources, to this end, NFPP writes the syslog on the attack detection to the buffer area and specifies the print rate. No rate-limit is configured for the TRAP message.

### 3. Protocol/Manage/Route flow classification

As shown in the Table-1, the packet types are divided into Manage, Route and Protocol packet. Each packet type owns the independent bandwidth. The bandwidth between the different types cannot be shared and the packet flow exceeding the bandwidth threshold will be discarded. The packet flow classification ensures that the set packet type on the device takes the precedence over other types of packet. The administrator can flexibly allocate the bandwidth of the three types of the packet according to the actual network environment and make sure that the protocol and manage packets takes the precedence of being handled for the purpose of normal protocol running and the administrator management, thereby safeguarding the normal operation of each important function on the device and improving the anti-attack capability.

Table-1

Packet Type	Service Type defined in the CPP
Protocol	tp-guard, dot1x, rldp, rerp, slow-packet, bpdu, isis, dhcps, gvrp, ripng, dvmrp, igmp, mpls, ospf, pim, pimv6, rip, vrrp, ospf3, dhcp-relay-s, dhcp-relay-c, option82, tunnel-bpdu, tunnel-gvrp
Route	unknown-ipmc, unknown-ipmcv6, ttl1, ttl0, udp-helper, ip4-packet-other, ip6-packet-other, non-ip-packet-other, arp
Manage	ip4-packet-local, ip6-packet-local

### 4. Focus rate-limit

After the classification rate-limit, focus on all the flow classification in a queue. If the process rate of one type of the packets is low, the corresponding packets will accumulate in the queue, and consume the queue resources ultimately. The administrator can configure the packet percent. If the length of the queue for one type of the packet is more than the total queue length multiplied by the packet percent, the type of packets will be discarded.

## Configuring NFPP

This section describes how to configure the NFPP.

- Default NFPP configuration.

- Configuring the packet traffic bandwidth.
- Configuring the packet percent.
- Anti-attack Protocols

## Default NFPP Configuration

The default configurations of NFPP are as follows:

Packet Type	Default Bandwidth Traffic	Default Packet Percent
Manage	3000PPS	30
Route	3000PPS	25
Protocol	3000PPS	45

## Configuring the packet traffic bandwidth

This section describes how to configure the packet traffic bandwidth:

Command	Function
Ruijie(config)# <b>cpu-protect sub-interface {manage protocol route} pps pps_vaule</b>	Configure the traffic bandwidth threshold of the corresponding packet, in pps, ranging from 1 to 8192, in integer.

For example:

```
Ruijie(config)# cpu-protect sub-interface manage pps 200
Ruijie(config)# end
```

## Configuring the packet percent

This section describes how to configure the packet percent:

Command	Function
Ruijie(config)# <b>cpu-protect sub-interface {manage protocol route} percent percent_vaule</b>	Configure the packet percent. <i>percent_value</i> : ranging from 1 to 100, in integer.

For example:

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



### Caution

The valid percent value of one packet must be less than 100% minus the percent value of other two types of packets

## Anti-attack Protocols

- ARP-guard
- IP-guard
- ICMP-guard
- DHCP-guard
- DHCPv6-guard
- ND-guard
- NFPP syslog

## ARP-guard

### ARP-guard Overview

The IP address is translated into the MAC address by ARP protocol in the local area network(LAN). ARP protocol plays an important role in the network security. ARP DoS attack sends a large amount of illegal ARP packets to the gateway, preventing the gateway from providing the services. To deal with this attack, on one hand, you can configure the rate-limit of the ARP packet, on the other hand, you can detect and isolate the attack source.

The ARP attack detection could be host-based or port-based. Host-based ARP attack detection could be classified into the following two types again: source IP address/VID/port-based and source MAC address/VID/port-based. For each attack detection, you can configure the rate-limit threshold and warning threshold. The ARP packet will be dropped when the packet rate exceeds the rate-limit threshold. When the ARP packet rate exceeds the warning threshold, it will prompt the warning messages and send the TRAP message. The host-based attack detection can isolate the attack source. Besides, ARP-guard is able to detect the ARP scan. ARP scan is that the source MAC address on link layer is fixed while the source IP address is changing, or the source MAC address and source IP address are fixed while the destination IP address is changing. Ruijie products only support to detect the first ARP scan (the source MAC address on link layer is fixed while the source IP address is changing).

It is worth mentioning that ARP-guard is only for the ARP DoS attack, rather than ARP fraud or dealing with the ARP attack problems in the network.

ARP-guard configuration commands include:

- Enabling arp-guard
- Configuring the isolated time
- Configuring the monitored time
- Configuring the monitored host limit
- Host-based rate-limit and attack detection
- Port-based rate-limit and attack detection
- Clearing the monitored hosts



- Clearing the ARP scanning list
- Showing related arp-guard information

## Enabling ARP-guard

You can enable arp-guard in the nfpp configuration mode or in the interface configuration mode. By default, the arp-guard is enabled.

Command	Function
Ruijie# <b>configure terminal</b>	Enter the global configuration mode.
Ruijie(config)# <b>nfpp</b>	Enter the nfpp configuration mode.
Ruijie(config-nfpp)# <b>arp-guard enable</b>	Enable the arp-guard. By default, arp-guard is enabled.
Ruijie(config-nfpp)# <b>end</b>	Return to the privileged EXEC mode.
Ruijie# <b>configure terminal</b>	Enter the global configuration mode.
Ruijie# <b>interface interface-name</b>	Enter the interface configuration mode.
Ruijie(config-if)# <b>nfpp arp-guard enable</b>	Enable the arp-guard on the interface. By default, arp-guard is not enabled on the interface.
Ruijie(config-if)# <b>end</b>	Return to the privileged EXEC mode.
Ruijie# <b>show nfpp arp-guard summary</b>	Show the configurations.
Ruijie# <b>copy running-config startup-config</b>	Save the configurations.



### Caution

With the arp-guard disabled, the monitored hosts and scan hosts are auto-cleared.

## Configuring the isolated time

For the isolated time of the attacker, it can be configured in the global or interface configuration mode. By default, the isolated time is configured in the global configuration mode.

Command	Function
Ruijie# <b>configure terminal</b>	Enter the global configuration mode.
Ruijie(config)# <b>nfpp</b>	Enter the nfpp configuration mode.

Command	Function
Ruijie(config-nfpp)# <b>arp-guard isolate-period</b> [ <i>seconds</i>   <b>permanent</b> ]	Configure the global isolated time, ranging 0s, 180-86400s(one day). The default value is 0s, representing no isolation. Permanent represents permanent isolation.
Ruijie(config-nfpp)# <b>end</b>	Return to the privileged EXEC mode.
Ruijie# <b>configure terminal</b>	Enter the global configuration mode.
Ruijie(config)# <b>interface</b> <i>interface-name</i>	Enter the interface configuration mode.
Ruijie(config-if)# <b>nfpp arp-guard isolate-period</b> [ <i>seconds</i>   <b>permanent</b> ]	Configure the isolated time on the port, ranging 0s, 180-86400s(one day). By default, the isolated time is configured globally. 0s represents no isolation. Permanent represents permanent isolation.
Ruijie(config-if)# <b>end</b>	Return to the privileged EXEC mode.
Ruijie# <b>show nfpp arp-guard summary</b>	Show the arp-guard parameter settings.
Ruijie# <b>copy running-config startup-config</b>	Save the configurations.

To restore the global isolated time to the default value, use the **no arp-guard isolate-period** command in the nfpp configuration mode. If the isolated time has been configured on a port, you can use the **no arp-guard isolate-period** command to remove the port-based isolated time configuration in the interface configuration mode.

## Configuring the monitored time

If the isolated time is 0 (that is no isolation), the serviceview monitor will be performed to auto-monitor the attacker according to the configured monitored period, providing the attacker information in the system. If the isolated time is but not 0, the arp-guard will perform hardware isolation towards the hosts using the serviceview monitor.

Command	Function
Ruijie# <b>configure terminal</b>	Enter the global configuration mode.
Ruijie(config)# <b>nfpp</b>	Enter the nfpp configuration mode.
Ruijie(config-nfpp)# <b>arp-guard monitor-period</b> <i>seconds</i>	Configure the monitored time, ranging 180-86400s(one day). The default value is 600s.
Ruijie(config-nfpp)# <b>end</b>	Return to the privileged EXEC mode.
Ruijie# <b>show nfpp arp-guard summary</b>	Show the arp-guard parameter settings.

Command	Function
Ruijie# <b>copy running-config startup-config</b>	Save the configurations.

To restore the monitored time to the default value, use the **no arp-guard monitor-period** command in the nfpp configuration mode.



#### Caution

If the isolated time is 0, the serviceview monitor will be performed to monitor the detected attacker, and the timeout time will be the monitored period. In the process of the serviceview monitor, if the isolated time is but not 0, the hardware isolation will be performed to isolate the attacker, and the timeout time will be the isolated period. Only be the monitored period valid when the isolated period is 0.

Modifying the isolated time from non-0 to 0 removes the attackers from the interface rather than performs the serviceview monitor.

## Configuring the monitored host limit

Command	Function
Ruijie# <b>configure terminal</b>	Enter the global configuration mode.
Ruijie(config)# <b>nfpp</b>	Enter the nfpp configuration mode.
Ruijie(config-nfpp)# <b>arp-guard monitored-host-limit seconds</b>	Configure the monitored host limit, ranging 1-4294967295. The default value is 1000.
Ruijie(config-nfpp)# <b>end</b>	Return to the privileged EXEC mode.
Ruijie# <b>show nfpp arp-guard summary</b>	Show the arp-guard parameter settings.
Ruijie# <b>copy running-config startup-config</b>	Save the configurations.

To restore the monitored host limit to the default value, use the **no arp-guard monitored-host-limit** command in the nfpp configuration mode.

If the monitored host number has reached the default 1000, and the administrator sets the monitored host limit smaller than 1000, the existent monitored hosts will not be deleted and it will prompt the message “%ERROR: The value that you configured is smaller than current monitored hosts 1000:please clear a part of monitored hosts.” to notify the administrator of the invalid configuration and removing a part of the monitored hosts.



#### Caution

It prompts the message that “% NFPP\_ARP\_GUARD-4-SESSION\_LIMIT: Attempt to exceed limit of 1000 monitored hosts.” if the monitored host table is full.

## Host-based rate-limit and attack detection

For the host-based attack detection, it can be classified into the following two types: source IP address/VID/port-based and source MAC address/VID/port-based. For each attack detection, you can configure the rate-limit threshold and attack threshold (also called warning threshold). The ARP packet will be dropped when the packet rate exceeds the rate-limit threshold. When the ARP packet rate exceeds the warning threshold, it will prompt the warning messages and send the TRAP message.

ARP-guard supports to detect the ARP scan, which is in 10s, 15s by default. If 15 or more than 15 ARP packets have been received within 10s, and the source MAC address on link layer is fixed while the source IP address is changing, or the source MAC address and source IP address are fixed while the destination IP address is changing, ARP scan is detected and recorded in the syslog and the TRAP messages are sent.

It prompts the following message if the ARP DoS attack was detected:

```
%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)
```

The content in brackets is the attack detection time.

The following example shows the describing information included in the sent TRAP messages:

```
ARP DoS attack from host<IP=N/A,MAC=0000.0000.0004,port=Gi4/1,VLAN=1> was detected.
```

If the isolated time is not set as 0 by the administrator, when the hardware isolation succeeds, it prompts:

```
%NFPP_ARP_GUARD-4-ISOLATED:Host <IP=N/A,MAC=0000.0000.0004,port=Gi4/1,VLAN=1> was isolated. (2009-07-01 13:00:00)
```

The following example shows the describing information included in the sent TRAP messages:

```
Host<IP=N/A,MAC=0000.0000.0004,port=Gi4/1,VLAN=1> was isolated.
```

When it fails to isolate the hardware due to a lack of memory or hardware resources, it prompts:

```
%NFPP_ARP_GUARD-4-ISOLATE_FAILED: Failed to isolate host <IP=N/A,MAC=0000.0000.0004,port=Gi4/1,VLAN=1>. (2009-07-01 13:00:00)
```

The following example shows the describing information included in the sent TRAP messages:

```
Failed to isolate host<IP=N/A,MAC=0000.0000.0004,port=Gi4/1,VLAN=1>.
```

It prompts the following message when the ARP scan was detected:

```
%NFPP_ARP_GUARD-4-SCAN: Host<IP=1.1.1.1,MAC=0000.0000.0004,port=Gi4/1,VLAN=1> was detected. (2009-07-01 13:00:00)
```

The following example shows the describing information included in the sent TRAP messages:

```
ARP scan from host< IP=1.1.1.1,MAC=0000.0000.0004,port=Gi4/1,VLAN=1> was detected.
```

It saves the latest 256 pieces of records in the ARP scan table. When the ARP scan table is full, it prompts:

```
%NFPP_ARP_GUARD-4-SCAN_TABLE_FULL: ARP scan table is full.
```

It prompts the following message to remind the administrator that the configured rate-limit threshold is higher than the attack threshold:

```
ERROR:rate limit is higher than attack threshold 500pps."
```

It prompts the following message to remind the administrator that the configured attack threshold is smaller than the rate-limit threshold:

```
ERROR:attack threshold is smaller than rate limit 300pps."
```



- It sets a policy to the hardware when isolating the attackers. When the hardware resources have been exhausted, it prompts the message to inform the administrator.
- When it fails to allocate the memory to the detected attackers, it prompts the message like %NFPP\_ARP\_GUARD-4-NO\_MEMORY: Failed to alloc memory.to inform the administrator.
- It contains only the latest 256 pieces of the records in the ARP scan table. When the ARP scan table is full, the newest record will overwrite the oldest one.

This section shows the administrator how to configure the host-based rate-limit and attack detection in the nfpp configuration mode and in the interface configuration mode:

Command	Function
Ruijie# <b>configure terminal</b>	Enter the global configuration mode.
Ruijie(config)# <b>nfpp</b>	Enter the nfpp configuration mode.
Ruijie(config-nfpp)# <b>arp-guard rate-limit {per-src-ip   per-src-mac} pps</b>	Configure the arp-guard rate-limit, ranging from 1 to 9999, 4 by default. <b>per-src-ip</b> : detect the hosts based on the source IP address/VID/port; <b>per-src-mac</b> : detect the hosts based on the source MAC address/VID/port.
Ruijie(config-nfpp)# <b>arp-guard attack-threshold {per-src-ip   per-src-mac} pps</b>	Configure the arp-guard attack threshold, ranging from 1 to 9999, 8 by default. When the ARP packet number sent from a host exceeds the attack threshold, the attack is detected and ARP-guard isolates the host, records the message and sends the TRAP packet. <b>per-src-ip</b> : detect the hosts based on the source IP address/VID/port; <b>per-src-mac</b> : detect the hosts based on the source MAC address/VID/port.

Command	Function
Ruijie(config-nfpp)# <b>arp-guard scan-threshold</b> <i>pkt-cnt</i>	Configure the arp-guard scan threshold, in 10s, ranging from 1 to 9999, 15 by default. If 15 or more than 15 ARP packets have been received within 10s, and the source MAC address on link layer is fixed while the source IP address is changing, or the source MAC address and source IP address are fixed while the destination IP address is changing, ARP scan is detected and recorded in the syslog and the TRAP messages are sent.
Ruijie(config-nfpp)# <b>end</b>	Return to the privileged EXEC mode.
Ruijie# <b>configure terminal</b>	Enter the global configuration mode.
Ruijie(config)# <b>interface</b> <i>interface-name</i>	Enter the interface configuration mode.
Ruijie(config-if)#nfpp <b>arp-guard policy</b> { <i>per-src-ip</i>   <i>per-src-mac</i> } <b>rate-limit-pps</b> <i>attack-threshold-pps</i>	Configure the rate-limit and attack threshold on the specified interface. <i>rate-limit-pps</i> : set the rate-limit threshold. The valid range is 1-9999 and by default, it adopts the global rate-limit threshold value. <i>attack-threshold-pps</i> : set the attack threshold. The valid range is 1-9999 and by default, it adopts the global attack threshold value. <b>per-src-ip</b> : to detect the hosts based on the source IP/VID/port; <b>per-src-mac</b> : to detect the hosts based on the source MAC/VID/port on the link layer.
Ruijie(config-if)#nfpp <b>arp-guard scan-threshold</b> <i>pkt-cnt</i>	Configure the arp-guard scan threshold value on each interface, the valid range is 1-9999, in 10s. By default, it adopts the global arp-guard scan threshold value.
Ruijie(config-if)# <b>end</b>	Return to the privileged EXEC mode.
Ruijie# <b>show nfpp arp-guard summary</b>	Show the arp-guard parameter settings.
Ruijie# <b>copy running-config startup-config</b>	Save the configurations.

## Port-based rate-limit and attack detection

You can configure the arp-guard rate limit and attack threshold on the port. The rate limit value must be less than the attack threshold value. When the ARP packet rate on a port exceeds the limit, the ARP

packets are dropped. When the ARP packet rate on a port exceeds the attack threshold limit, the CLI prompts and the TRAP packets are sent.

It prompts the following message when the ARP DoS attack was detected on a port:

```
%NFPP_ARP_GUARD-4-PORT_ATTACKED: ARP DoS attack was detected on port Gi4/1. (2009-07-01 13:00:00)
```

The following is additional information of the sent TRAP packet :

```
ARP DoS attack was detected on port Gi4/1.
```

This section shows the administrator how to configure the port-based rate-limit and attack detection in the nfpp configuration mode and in the interface configuration mode:

Command	Function
Ruijie# <b>configure terminal</b>	Enter the global configuration mode.
Ruijie(config)# <b>nfpp</b>	Enter the nfpp configuration mode.
Ruijie(config-nfpp)# <b>arp-guard rate-limit per-port pps</b>	Configure the arp-guard rate-limit of the ARP packet on the port, ranging from 1 to 9999, 100 by default.
Ruijie(config-nfpp)# <b>arp-guard attack-threshold per-port pps</b>	Configure the arp-guard attack threshold, ranging from 1 to 9999, 200 by default. When the ARP packet number on a port exceeds the attack threshold, the CLI prompts and the TRAP packets are sent.
Ruijie(config-nfpp)# <b>end</b>	Return to the privileged EXEC mode.
Ruijie# <b>configure terminal</b>	Enter the global configuration mode.
Ruijie(config)# <b>interface interface-name</b>	Enter the interface configuration mode.
Ruijie(config-if)# <b>nfpp arp-guard policy per-port rate-limit-pps attack-threshold-pps</b>	Configure the rate-limit and attack threshold on the specified interface.  <i>rate-limit-pps</i> : set the rate-limit threshold. The valid range is 1-9999 and by default, it adopts the global rate-limit threshold value.  <i>attack-threshold-pps</i> : set the attack threshold. The valid range is 1-9999 and by default, it adopts the global attack threshold value.
Ruijie(config-if)# <b>end</b>	Return to the privileged EXEC mode.
Ruijie# <b>show nfpp arp-guard summary</b>	Show the arp-guard parameter settings.
Ruijie# <b>copy running-config startup-config</b>	Save the configurations.



MAC address-based rate limit takes precedence over IP address-based rate limit. IP address-based rate limit takes precedence over port-based rate limit.

It is recommended for the administrator to follow the following principle of configuring the host-based rate-limit and attack threshold, in order to perform the best arp-guard function:

IP address-based rate-limit threshold < IP address-based attack threshold < source MAC address-based rate-limit threshold < source MAC address-based attack threshold.

When configuring the rate limit on the port, you can refer to the user count on this port. For example, if 500 users exist on a port, you can set the rate limit on this port to 500.

## Clearing the monitored hosts

The isolated hosts can be recovered automatically after a period of the time. The administrator can use the following command to clear the isolated hosts manually.

Command	Function
Ruijie# <b>clear nfpp arp-guard hosts</b> [vlan <i>vid</i> ] [interface <i>interface-id</i> ] [ <i>ip-address</i>   <i>mac-address</i> ]	<p><b>clear nfpp arp-guard hosts:</b> Clear all isolated hosts.</p> <p><b>clear nfpp arp-guard hosts vlan <i>vid</i>:</b> Clear all isolated hosts in a VLAN.</p> <p><b>clear nfpp arp-guard hosts [vlan <i>vid</i>] [interface <i>interface-id</i>]:</b> Clear all isolated hosts on a interface in a VLAN.</p> <p><b>clear nfpp arp-guard hosts [vlan <i>vid</i>] [interface <i>interface-id</i>] [<i>ip-address</i>   <i>mac-address</i>]:</b> An isolated host has been cleared. Use the IP address or the MAC address to identify the hosts.</p>

## Clearing the ARP scan table

The administrator can use the following command to clear the ARP scan table manually.

Command	Function
Ruijie# <b>clear nfpp arp-guard scan</b>	Clear the ARP scan table.

## Showing arp-guard

- Showing arp-guard configuration
- Showing monitored host configuration
- Showing arp scan table



## Showing arp-guard configuration

Use this command to show the arp-guard configurations.

Command	Function
Ruijie# <b>show nfpp arp-guard summary</b>	Show the arp-guard configurations.

For example,


```
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
G 0/1	Enable	180	5/-/-	8/-/-	-
G 0/2	Disable	200	4/5/60	8/10/100	20

Maximum count of monitored hosts: 1000

Monitor period:300s

 Note	Field	Description
	Interface	Global refers to the global configuration.
	Status	Enable/disable the arp-guard.
	Rate-limit	In the format of source IP address-based rate-limit threshold / source MAC address-based rate-limit threshold / port-based rate-limit threshold.
	Attack-threshold	In the same format of the Rate-limit.
	-	No configuration.

## Showing monitored host configuration

Command	Function
Ruijie# <b>show nfpp arp-guard hosts statistics</b>	Show the arp-guard hosts statistics, including total host amount, isolated host amount and non-isolated host amount.

Command	Function
<pre>Ruijie#show nfpp arp-guard hosts [vlan vid] [interface interface-id] [ip-address   mac-address]</pre>	<p>Show the isolated hosts information.</p> <p><b>show nfpp arp-guard hosts vlan vid:</b> Show the isolated hosts in a VLAN.</p> <p><b>show nfpp arp-guard hosts [vlan vid] [interface interface-id]:</b> Show the isolated hosts on a interface in a VLAN.</p> <p><b>show nfpp arp-guard hosts [vlan vid] [interface interface-id] [ip-address   mac-address]:</b> Show the isolated hosts. Use the IP address or the MAC address to identify the hosts.</p>

For example,

```
Ruijie#show nfpp arp-guard hosts statistics
```

```
success    fail    total
-----
100        20      120
```

```
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
```

```
Ruijie# show nfpp arp-guard hosts vlan 1 interface G 0/1 1.1.1.1
```

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
Total:1 host
```



#### Note

If the MAC address column shows "-", it means "the host is identified by the source IP address";

If the IP address column shows "-", it means "the host is identified by the source MAC address".

## Showing the ARP scan table

Command	Function
Ruijie# <b>show nfpp arp-guard scan statistics</b>	Show the arp-guard scan statistics.
Ruijie# <b>show nfpp arp-guard scan [vlan vid] [interface interface-id] [ip-address] [mac-address]</b>	<p>Show the arp-guard scan information.</p> <p>show nfpp arp-guard scan vlan <i>vid</i>: Show the arp-guard scan information in a VLAN.</p> <p>show nfpp arp-guard scan [vlan <i>vid</i>] [interface <i>interface-id</i>]: Show the arp-guard scan information on a interface in a VLAN.</p> <p>show nfpp arp-guard scan [vlan <i>vid</i>] [interface <i>interface-id</i>] [<i>ip-address</i>] [<i>mac-address</i>]: Show the arp-guard scan information for a MAC address on a interface in a VLAN.</p>

For example,

```
Ruijie#show nfpp arp-guard scan statistics
ARP scan table has 4 record(s).
```

```
Ruijie# show nfpp arp-guard scan
VLAN    interface  IP address  MAC address  timestamp
----    -
1       Gi0/1      N/A        0000.0000.0001  2008-01-23 16:23:10
2       Gi0/2      1.1.1.1    0000.0000.0002  2008-01-23 16:24:10
3       Gi0/3      N/A        0000.0000.0003  2008-01-23 16:25:10
4       Gi0/4      N/A        0000.0000.0004  2008-01-23 16:26:10
Total:4 record(s)
```

“timestamp” represents the time when the ARP scan was detected. For example, “2008-01-23 16:23:10” represents that the ARP scan was detected at 16:23:10, Jan 23, 2008.

```
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)
```

## IP-guard

### IP-guard Overview

As is known to all, many hacker attacks and the network virus invasions begin with the network scanning. To this end, a large amount of the scanning packets take up the network bandwidth, leading to the abnormal network communication.

Ruijie Layer-3 device provides the IP-guard function to prevent the attacks from the hacker and the virus such as “Blaster”, reducing the CPU burden of the layer-3 devices.

There are two types of the IP packet attack:

- **Scanning the destination IP address change:** not only consumes the network bandwidth and increases the device burden, but also is a prelude of the hacker attack.
- **Sending the IP packets to the inexistent destination IP address at the high-rate:** for the layer-3 device, the packets are directly forwarded by the switching chip without the consumption of the CPU resources if the destination IP address exists. While if the destination IP address is inexistent, the ARP request packets are sent from the CPU to ask for the corresponding MAC address for the destination IP address when the IP packets are sent to the CPU. It consumes the CPU resources if many IP packets are sent to the CPU. The workaround for this attack: one one hand, you may configure the IP packet rate-limit; on the other hand, you may detect and isolate the attack source.

The IP attack detection could be host-based or port-based. Host-based ARP attack detection adopts the combination of source IP address/VID/port-based. For each attack detection, you can configure the rate-limit threshold and warning threshold. The IP packet will be dropped when the packet rate exceeds the rate-limit threshold. When the ARP packet rate exceeds the warning threshold, it will prompt the warning messages and send the TRAP message. The host-based attack detection can isolate the attack source.



#### Caution

It is worth mentioning that the IP-guard is for the attack of the IP packets with the destination IP address not the host IP address. For the IP packet with the destination IP address the host IP address, use the CPP(CPU Protect Policy) to limit the rate.

The IP-guard is supported in the layer-3 switches only.

With the ip-guard enabled on the interface and the non-0 isolated period configured, it isolates the hosts attacked by the IP packets.

IP-guard configuration commands include:

- Enabling ip-guard
- Configuring the isolated time
- Configuring the monitored time
- Configuring the monitored host limit
- Host-based rate-limit and attack detection
- Port-based rate-limit and attack detection
- Configuring trusted host

## ■ Showing related ip-guard information

### Enabling IP-guard

You can enable ip-guard in the nfpp configuration mode or in the interface configuration mode. By default, the ip-guard is enabled.

Command	Function
Ruijie# <b>configure terminal</b>	Enter the global configuration mode.
Ruijie(config)# <b>nfpp</b>	Enter the nfpp configuration mode.
Ruijie(config-nfpp)# <b>ip-guard enable</b>	Enable the ip-guard. By default, ip-guard is enabled.
Ruijie(config-nfpp)# <b>end</b>	Return to the privileged EXEC mode.
Ruijie# <b>configure terminal</b>	Enter the global configuration mode.
Ruijie# <b>interface</b> <i>interface-name</i>	Enter the interface configuration mode.
Ruijie(config-if)# <b>nfpp ip-guard enable</b>	Enable the ip-guard on the interface. By default, ip-guard is not enabled on the interface.
Ruijie(config-if)# <b>end</b>	Return to the privileged EXEC mode.
Ruijie# <b>show nfpp ip-guard summary</b>	Show the configurations.
Ruijie# <b>copy running-config startup-config</b>	Save the configurations.



#### Caution

With the ip-guard disabled, the monitored hosts are auto-cleared.

### Configuring the isolated time

For the isolated time of the attacker, it can be configured in the global or interface configuration mode. By default, the isolated time is configured in the global configuration mode.

Command	Function
Ruijie# <b>configure terminal</b>	Enter the global configuration mode.
Ruijie(config)# <b>nfpp</b>	Enter the nfpp configuration mode.

Command	Function
Ruijie(config-nfpp)# <b>ip-guard isolate-period</b> [ <i>seconds</i>   <b>permanent</b> ]	Configure the global isolated time, ranging 0s, 30-86400s(one day). The default value is 0s, representing no isolation. Permanent represents permanent isolation.
Ruijie(config-nfpp)# <b>end</b>	Return to the privileged EXEC mode.
Ruijie# <b>configure terminal</b>	Enter the global configuration mode.
Ruijie(config)# <b>interface</b> <i>interface-name</i>	Enter the interface configuration mode.
Ruijie(config-if)# <b>nfpp arp-guard isolate-period</b> [ <i>seconds</i>   <b>permanent</b> ]	Configure the isolated time on the port, ranging 0s, 180-86400s(one day). By default, the isolated time is configured globally. 0s represents no isolation. Permanent represents permanent isolation.
Ruijie(config-if)# <b>end</b>	Return to the privileged EXEC mode.
Ruijie# <b>show nfpp ip-guard summary</b>	Show the parameter settings.
Ruijie# <b>copy running-config startup-config</b>	Save the configurations.

To restore the global isolated time to the default value, use the **no ip-guard isolate-period** command in the nfpp configuration mode. If the isolated time has been configured on a port, you can use the **no ip-guard isolate-period** command to remove the port-based isolated time configuration in the interface configuration mode.

## Configuring the monitored time

If the isolated time is 0 (that is no isolation), the serviceview monitor will be performed to auto-monitor the attacker according to the configured monitored period, providing the attacker information in the system. If the isolated time is but not 0, the ip-guard will perform hardware isolation towards the hosts using the serviceview monitor.

Command	Function
Ruijie# <b>configure terminal</b>	Enter the global configuration mode.
Ruijie(config)# <b>nfpp</b>	Enter the nfpp configuration mode.
Ruijie(config-nfpp)# <b>ip-guard monitor-period</b> <i>seconds</i>	Configure the monitored time, ranging 180-86400s(one day). The default value is 600s.
Ruijie(config-nfpp)# <b>end</b>	Return to the privileged EXEC mode.
Ruijie# <b>show nfpp ip-guard summary</b>	Show the parameter settings.
Ruijie# <b>copy running-config startup-config</b>	Save the configurations.

To restore the monitored time to the default value, use the **no ip-guard monitor-period** command in the nfpp configuration mode.



#### Caution

If the isolated time is 0, the serviceview monitor will be performed to monitor the detected attacker, and the timeout time will be the monitored period. In the process of the serviceview monitor, if the isolated time is but not 0, the hardware isolation will be performed to isolate the attacker, and the timeout time will be the isolated period. Only be the monitored period valid when the isolated period is 0.

Modifying the isolated time from non-0 to 0 removes the attackers from the interface rather than performs the serviceview monitor.

## Configuring the monitored host limit

Command	Function
Ruijie# <b>configure terminal</b>	Enter the global configuration mode.
Ruijie(config)# <b>nfpp</b>	Enter the nfpp configuration mode.
Ruijie(config-nfpp)# <b>ip-guard monitored-host-limit</b> <i>seconds</i>	Configure the monitored host limit, ranging 1-4294967295. The default value is 1000.
Ruijie(config-nfpp)# <b>end</b>	Return to the privileged EXEC mode.
Ruijie# <b>show nfpp ip-guard summary</b>	Show the parameter settings.
Ruijie# <b>copy running-config startup-config</b>	Save the configurations.

To restore the monitored host limit to the default value, use the **no ip-guard monitored-host-limit** command in the nfpp configuration mode.

If the monitored host number has reached the default 1000, and the administrator sets the monitored host limit smaller than 1000, the existent monitored hosts will not be deleted and it will prompt the message “%ERROR: The value that you configured is smaller than current monitored hosts 1000:please clear a part of monitored hosts.” to notify the administrator of the invalid configuration and removing a part of the monitored hosts.



#### Caution

It prompts the message that “% NFPP\_IP\_GUARD-4-SESSION\_LIMIT: Attempt to exceed limit of 1000 monitored hosts.” if the monitored host table is full.

## Host-based rate-limit and attack detection

Use the source IP address/VID/port-based method to detect the host-based attack. For each attack detection, you can configure the rate-limit threshold and attack threshold (also called warning threshold).

The IP packet will be dropped when the packet rate exceeds the rate-limit threshold. When the IP packet rate exceeds the warning threshold, it will prompt the warning messages and send the TRAP message. It prompts the following message if the IP DoS attack was detected:

```
%NFPP_IP_GUARD-4-  DOS_DETECTED:Host<IP=1.1.1.1,MAC=  N/A,port=Gi4/1,VLAN=1>  was
detected. (2009-07-01 13:00:00)
```

The following example shows the describing information included in the sent TRAP messages:

```
IP DoS attack from host<IP=1.1.1.1,MAC= N/A,,port=Gi4/1,VLAN=1> was detected.
```

If the isolated time is not set as 0 by the administrator, when the hardware isolation succeeds, it prompts:

```
%NFPP_IP_GUARD-4-ISOLATED:Host <IP=1.1.1.1, MAC= N/A,port=Gi4/1,VLAN=1> was isolated.
(2009-07-01 13:00:00)
```

The following example shows the describing information included in the sent TRAP messages:

Host<IP=1.1.1.1, MAC= N/A,port=Gi4/1,VLAN=1> was isolated.

When it fails to isolate the hardware due to a lack of memory or hardware resources, it prompts:

```
%NFPP_IP_GUARD-4-ISOLATE_FAILED: Failed to isolate host <IP=1.1.1.1, MAC= N/A,port=Gi4/
1,VLAN=1>. (2009-07-01 13:00:00)
```

The following example shows the describing information included in the sent TRAP messages:

Failed to isolate host<IP=1.1.1.1, MAC= N/A,port=Gi4/1,VLAN=1>.

It prompts the following message when the IP scan was detected:

```
%NFPP_IP_GUARD-4-SCAN: Host<IP=1.1.1.1, MAC=  N/A,port=Gi4/1,VLAN=1>  was  detected.
(2009-07-01 13:00:00)
```

The following example shows the describing information included in the sent TRAP messages:

IP scan from host< IP=1.1.1.1, MAC= N/A,port=Gi4/1,VLAN=1> was detected.



#### Caution

- It sets a policy to the hardware when isolating the attackers. When the hardware resources have been exhausted, it prompts the message to inform the administrator.
- When it fails to allocate the memory to the detected attackers, it prompts the message like %NFPP\_IP\_GUARD-4-NO\_MEMORY: Failed to alloc memory.to inform the administrator.

This section shows the administrator how to configure the host-based rate-limit and attack detection in the nfpp configuration mode and in the interface configuration mode:

Command	Function
Ruijie# <b>configure terminal</b>	Enter the global configuration mode.
Ruijie(config)# <b>nfpp</b>	Enter the nfpp configuration mode.



Command	Function
Ruijie(config-nfpp)# <b>ip-guard rate-limit per-src-ip pps</b>	Configure the ip-guard rate-limit, ranging from 1 to 9999, 20 by default. per-src-ip: detect the hosts based on the source IP address/VID/port;
Ruijie(config)# <b>ip-guard attack-threshold per-src-ip pps</b>	Configure the ip-guard attack threshold, ranging from 1 to 9999, 20 by default. When the IP packet number sent from a host exceeds the attack threshold, the attack is detected and IP-guard isolates the host, records the message and sends the TRAP packet. per-src-ip: detect the hosts based on the source IP address/VID/port;
Ruijie(config)# <b>ip-guard scan-threshold pkt-cnt</b>	Configure the ip-guard scan threshold, in 10s, ranging from 1 to 9999, 100 by default.
Ruijie(config-nfpp)# <b>end</b>	Return to the privileged EXEC mode.
Ruijie# <b>configure terminal</b>	Enter the global configuration mode.
Ruijie(config)# <b>interface interface-name</b>	Enter the interface configuration mode.
Ruijie(config-if)# <b>nfpp ip-guard policy per-src-ip rate-limit-pps attack-threshold-pps</b>	Configure the rate-limit and attack threshold on the specified interface. <i>rate-limit-pps</i> : set the rate-limit threshold. The valid range is 1-9999 and by default, it adopts the global rate-limit threshold value. <i>attack-threshold-pps</i> : set the attack threshold. The valid range is 1-9999 and by default, it adopts the global attack threshold value. per-src-ip: to detect the hosts based on the source IP/VID/port;
Ruijie(config-if)# <b>nfpp ip-guard scan-threshold pkt-cnt</b>	Configure the ip-guard scan threshold value on each interface, the valid range is 1-9999, in 10s. By default, it adopts the global arp-guard scan threshold value.
Ruijie(config-nfpp)# <b>end</b>	Return to the privileged EXEC mode.
Ruijie(config-if)# <b>show nfpp ip-guard summary</b>	Show the parameter settings.
Ruijie# <b>copy running-config startup-config</b>	Save the configurations.

## Port-based rate-limit and attack detection

You can configure the ip-guard rate limit and attack threshold on the port. The rate limit value must be less than the attack threshold value. When the IP packet rate on a port exceeds the limit, the IP packets are dropped. When the IP packet rate on a port exceeds the attack threshold limit, the CLI prompts and the TRAP packets are sent.

It prompts the following message when the IP DoS attack was detected on a port:

```
%NFPP_IP_GUARD-4-PORT_ATTACKED: IP DoS attack was detected on port Gi4/1.
(2009-07-01 13:00:00)
```

The following is additional information of the sent TRAP packet :

IP DoS attack was detected on port Gi4/1.

This section shows the administrator how to configure the port-based rate-limit and attack detection in the nfpp configuration mode and in the interface configuration mode:

Command	Function
Ruijie# <b>configure terminal</b>	Enter the global configuration mode.
Ruijie(config)# <b>nfpp</b>	Enter the nfpp configuration mode.
Ruijie(config)# <b>ip-guard rate-limit per-port pps</b>	Configure the ip-guard rate-limit of the IP packet on the port, ranging from 1 to 9999, 100 by default.
Ruijie(config)# <b>ip-guard attack-threshold per-port pps</b>	Configure the ip-guard attack threshold, ranging from 1 to 9999, 200 by default. When the IP packet number on a port exceeds the attack threshold, the CLI prompts and the TRAP packets are sent.
Ruijie(config-nfpp)# <b>end</b>	Return to the privileged EXEC mode.
Ruijie# <b>configure terminal</b>	Enter the global configuration mode.
Ruijie(config)# <b>interface interface-name</b>	Enter the interface configuration mode.
Ruijie(config-if)# <b>nfpp ip-guard policy per-port rate-limit-pps attack-threshold-pps</b>	Configure the rate-limit and attack threshold on the specified interface. <i>rate-limit-pps</i> : set the rate-limit threshold. The valid range is 1-9999 and by default, it adopts the global rate-limit threshold value. <i>attack-threshold-pps</i> : set the attack threshold. The valid range is 1-9999 and by default, it adopts the global attack threshold value.
Ruijie(config-nfpp)# <b>end</b>	Return to the privileged EXEC mode.
Ruijie(config-if)# <b>show nfpp ip-guard summary</b>	Show the parameter settings.
Ruijie# <b>copy running-config startup-config</b>	Save the configurations.



The source IP address-based rate limit takes precedence over port-based rate limit.

## Configuring the trusted hosts

Use the following commands to set the trusted host to make a host free from monitoring. The IP packets are allowed to be sent to the CPU from the trusted host.

Command	Function
Ruijie# <b>configure terminal</b>	Enter the global configuration mode.
Ruijie(config)# <b>nfpp</b>	Enter the nfpp configuration mode.
Ruijie(config-nfpp)# <b>ip-guard trusted-host</b> <i>ip mask</i>	Configure the IP address range for the trusted hosts. Up to 500 pieces of IP addresses can be configured.
Ruijie(config-nfpp)# <b>end</b>	Return to the privileged EXEC mode.
Ruijie(config-if)# <b>show nfpp ip-guard trusted-host</b>	Show the trusted host settings.
Ruijie# <b>copy running-config startup-config</b>	Save the configurations.

In the nfpp configuration mode, use the **no** form of this command to delete a trusted host entry and use the **all** form of this command to delete all trusted hosts.

For example:

The following example shows how to delete all trusted hosts:

```
Ruijie(config-nfpp)# no ip-guard trusted-host all
```

The following example shows how to delete a trusted host entry:

```
Ruijie(config-nfpp)# no ip-guard trusted-host 1.1.1.1 255.255.255.255
```

It prompts that "ERROR: Attempt to exceed limit of 500 trusted hosts." to inform the administrator of the full trusted host table.

If the IP address for the trusted host entry is the same to the one existing in the untrusted host list, the system will auto-delete the entry according to the IP address.

It prompts that "ERROR:Failed to delete trusted host 1.1.1.0 255.255.255.0." to inform the administrator of the failure of trusted host removal.

It prompts that "ERROR:Failed to add trusted host 1.1.1.0 255.255.255.0." to inform the administrator of the failure of adding the trusted host.



It prompts that "ERROR:Failed to add trusted host 1.1.1.0 255.255.255.0." to inform the administrator of the failure of adding the trusted host.

It prompts that "ERROR:Failed to add trusted host 1.1.1.0 255.255.255.0." to inform the administrator of the failure of adding the trusted host.

It prompts that "ERROR:Trusted host 1.1.1.0 255.255.255.0 has already been configured." to inform the administrator of the existence of the trusted host to be added.

It prompts that "ERROR:Trusted host 1.1.1.0 255.255.255.0 is not found." to inform the administrator of the inexistence of the trusted host to be deleted.

It prompts that "ERROR:Trusted host 1.1.1.0 255.255.255.0 is not found." to inform the administrator if it fails to allocate the memory for the trusted host.

## Clearing the monitored hosts

The isolated hosts can be recovered automatically after a period of the time. The administrator can use the following command to clear the isolated hosts manually.

Command	Function
---------	----------

Command	Function
Ruijie# <b>clear nfpp ip-guard hosts [vlan vid] [interface interface-id] [ip-address]</b>	<p><b>clear nfpp ip-guard hosts:</b> Clear all isolated hosts.</p> <p><b>clear nfpp ip-guard hosts vlan vid:</b> Clear all isolated hosts in a VLAN.</p> <p><b>clear nfpp ip-guard hosts [vlan vid] [interface interface-id]:</b> Clear all isolated hosts on a interface in a VLAN.</p> <p><b>clear nfpp ip-guard hosts [vlan vid] [interface interface-id] [ip-address]:</b> An isolated host has been cleared. Use the IP address to identify the hosts.</p>

## Showing ip-guard

- Showing ip-guard configuration
- Showing monitored host configuration
- Showing trusted host configuration

## Showing ip-guard configuration

Use this command to show the ip-guard configurations.

Command	Function
Ruijie# <b>show nfpp ip-guard summary</b>	Show the ip-guard configurations.

For example,

```
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
G 0/1	Enable	180	5/-/-	8/-/-	-
G 0/2	Disable	200	4/-/60	8/-/100	20

Maximum count of monitored hosts: 1000

Monitor period:300s

**Note**

Field	Description
Interface	Global refers to the global configuration.
Status	Enable/disable the arp-guard.
Rate-limit	In the format of source IP address-based rate-limit threshold / source MAC address-based rate-limit threshold / port-based rate-limit threshold.
Attack-threshold	In the same format of the Rate-limit.
-	No configuration.

**Showing monitored host configuration**

Command	Function
Ruijie# <b>show nfpp ip-guard hosts statistics</b>	Show the ip-guard hosts statistics, including total host amount, isolated host amount and non-isolated host amount.
Ruijie# <b>show nfpp ip-guard hosts [vlan vid] [interface interface-id] [ip-address   mac-address]</b>	Show the isolated hosts information. <b>show nfpp ip-guard hosts vlan vid:</b> Show the isolated hosts in a VLAN. <b>show nfpp ip-guard hosts [vlan vid] [interface interface-id]:</b> Show the isolated hosts on a interface in a VLAN. <b>show nfpp ip-guard hosts [vlan vid] [interface interface-id] [ip-address   mac-address]:</b> Show the isolated hosts. Use the IP address or the MAC address to identify the hosts.

For example,

```
Ruijie#show nfpp ip-guard hosts statistics
```

```
success  fail   total
-----  ----  -----
100      20     120
```

```
Ruijie# show nfpp ip-guard hosts
```

If column 1 shows '\*', it means "hardware do not isolate user" .

```
VLAN  interface IP address  MAC address      remain-time(s)
```

```

-----
1      Gi0/1      1.1.1.1      ATTACK      110
2      Gi0/2      1.1.2.1      SCAN        61
Total:2 hosts

```

```
Ruijie# show nfpp ip-guard hosts vlan 1 interface G 0/1 1.1.1.1
```

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      ATTACK      110
Total:1 host

```



#### Note

If the MAC address column shows "-", it means "the host is identified by the source IP address";

If the IP address column shows "-", it means "the host is identified by the source MAC address".

## Showing the trusted host configuration

Command	Function
Ruijie# <b>show nfpp ip-guard trusted-host</b>	Show the trusted hosts.

For example,

```

Ruijie#show nfpp ip-guard trusted-host
IP address      mask
-----
1.1.1.1.0      255.255.255.0
1.1.2.0        255.255.255.0
Total:2 record(s)

```

## ICMP-guard

### ICMP-guard Overview

The ICMP attack detection could be host-based or port-based. Host-based ICMP protocol is used to diagnose the network trouble. Its basic principle is that the host sends an ICMP echo request packet, and the router/switch sends an ICMP echo reply packet upon receiving the ICMP echo request packet. The "ICMP flood" attack is that the attacker sends a large amount of the ICMP echo request packets to the destination device, resulting in the consumption of the CPU resources and the error of the device working. The workaround for the "ICMP flood" attack: on one hand, you may configure the ICMP packet rate-limit; on the other hand, you may detect and isolate the attack source.

ARP attack detection adopts the combination of source IP address/VID/port-based. For each attack detection, you can configure the rate-limit threshold and warning threshold. The ICMP packet will be dropped when the packet rate exceeds the rate-limit threshold. When the ICMP packet rate exceeds the warning threshold, it will prompt the warning messages and send the TRAP message. The host-based attack detection can isolate the attack source.

ICMP-guard configuration commands include:

- Enabling icmp-guard
- Configuring the isolated time
- Configuring the monitored time
- Configuring the monitored host limit
- Host-based rate-limit and attack detection
- Port-based rate-limit and attack detection
- Configuring trusted host
- Clearing monitored host
- Showing related icmp-guard information

## Enabling ICMP-guard

You can enable icmp-guard in the nfpp configuration mode or in the interface configuration mode. By default, the icmp-guard is enabled.

Command	Function
Ruijie# <b>configure terminal</b>	Enter the global configuration mode.
Ruijie(config)# <b>nfpp</b>	Enter the nfpp configuration mode.
Ruijie(config-nfpp)# <b>icmp-guard enable</b>	Enable the icmp-guard. By default, icmp-guard is enabled.
Ruijie(config-nfpp)# <b>end</b>	Return to the privileged EXEC mode.
Ruijie# <b>configure terminal</b>	Enter the global configuration mode.
Ruijie# <b>interface</b> <i>interface-name</i>	Enter the interface configuration mode.
Ruijie(config-if)# <b>nfpp icmp-guard enable</b>	Enable the icmp-guard on the interface. By default, icmp-guard is not enabled on the interface.
Ruijie(config-if)# <b>end</b>	Return to the privileged EXEC mode.
Ruijie# <b>show nfpp icmp-guard summary</b>	Show the configurations.
Ruijie# <b>copy running-config startup-config</b>	Save the configurations.





With the icmp-guard disabled, the monitored hosts are auto-cleared.

## Configuring the isolated time

For the isolated time of the attacker, it can be configured in the global or interface configuration mode. By default, the isolated time is configured in the global configuration mode.

Command	Function
Ruijie# <b>configure terminal</b>	Enter the global configuration mode.
Ruijie(config)# <b>nfpp</b>	Enter the nfpp configuration mode.
Ruijie(config-nfpp)# <b>icmp-guard isolate-period</b> [seconds   permanent]	Configure the global isolated time, ranging 0s, 30-86400s(one day). The default value is 0s, representing no isolation. Permanent represents permanent isolation.
Ruijie(config-nfpp)# <b>end</b>	Return to the privileged EXEC mode.
Ruijie# <b>configure terminal</b>	Enter the global configuration mode.
Ruijie(config)# <b>interface</b> interface-name	Enter the interface configuration mode.
Ruijie(config-if)# <b>nfpp arp-guard isolate-period</b> [seconds   permanent]	Configure the isolated time on the port, ranging 0s, 180-86400s(one day). By default, the isolated time is configured globally. 0s represents no isolation. Permanent represents permanent isolation.
Ruijie(config-if)# <b>end</b>	Return to the privileged EXEC mode.
Ruijie# <b>show nfpp icmp-guard summary</b>	Show the parameter settings.
Ruijie# <b>copy running-config startup-config</b>	Save the configurations.

To restore the global isolated time to the default value, use the **no icmp-guard isolate-period** command in the nfpp configuration mode. If the isolated time has been configured on a port, you can use the **no icmp-guard isolate-period** command to remove the port-based isolated time configuration in the interface configuration mode.

## Configuring the monitored time

Without the global and port-based isolated period configured(including set the interface isolated time 0), the serviceview monitor will be performed to auto-monitor the attacker according to the configured monitored period, providing the attacker information in the system. With the global or port-based isolated

period configured, the ICMP-guard will perform hardware isolation towards the hosts using the serviceview monitor.

Command	Function
Ruijie# <b>configure terminal</b>	Enter the global configuration mode.
Ruijie(config)# <b>nfpp</b>	Enter the nfpp configuration mode.
Ruijie(config-nfpp)# <b>icmp-guard monitor-period</b> <i>seconds</i>	Configure the monitored time, ranging 180-86400s(one day). The default value is 600s.
Ruijie(config-nfpp)# <b>end</b>	Return to the privileged EXEC mode.
Ruijie# <b>show nfpp icmp-guard summary</b>	Show the parameter settings.
Ruijie# <b>copy running-config startup-config</b>	Save the configurations.

To restore the monitored time to the default value, use the **no icmp-guard monitor-period** command in the nfpp configuration mode.



#### Caution

If the isolated time is 0, the serviceview monitor will be performed to monitor the detected attacker, and the timeout time will be the monitored period. In the process of the serviceview monitor, if the isolated time is but not 0, the hardware isolation will be performed to isolate the attacker, and the timeout time will be the isolated period. Only be the monitored period valid when the isolated period is 0.

Modifying the isolated time from non-0 to 0 removes the attackers from the interface rather than performs the serviceview monitor.

## Configuring the monitored host limit

Command	Function
Ruijie# <b>configure terminal</b>	Enter the global configuration mode.
Ruijie(config)# <b>nfpp</b>	Enter the nfpp configuration mode.
Ruijie(config-nfpp)# <b>icmp-guard monitored-host-limit</b> <i>seconds</i>	Configure the monitored host limit, ranging 1-4294967295. The default value is 1000.
Ruijie(config-nfpp)# <b>end</b>	Return to the privileged EXEC mode.
Ruijie# <b>show nfpp icmp-guard summary</b>	Show the parameter settings.
Ruijie# <b>copy running-config startup-config</b>	Save the configurations.

To restore the monitored host limit to the default value, use the **no icmp-guard monitored-host-limit** command in the nfpp configuration mode.

If the monitored host number has reached the default 1000, and the administrator sets the monitored host limit smaller than 1000, the existent monitored hosts will not be deleted and it will prompt the

message “%ERROR: The value that you configured is smaller than current monitored hosts 1000.please clear a part of monitored hosts.” to notify the administrator of the invalid configuration and removing a part of the monitored hosts.

**Caution**

It prompts the message that “% NFPP\_ICMP\_GUARD-4-SESSION\_LIMIT: Attempt to exceed limit of 1000 monitored hosts.” if the monitored host table is full.

## Host-based rate-limit and attack detection

Use the source IP address/VID/port-based method to detect the host-based attack. For each attack detection, you can configure the rate-limit threshold and attack threshold (also called warning threshold). The ICMP packet will be dropped when the packet rate exceeds the rate-limit threshold. When the ICMP packet rate exceeds the warning threshold, it will prompt the warning messages and send the TRAP message.

It prompts the following message if the ICMP DoS attack was detected:

```
%NFPP_ICMP_GUARD-4- DOS_DETECTED:Host<IP=1.1.1.1,MAC= N/A,port=Gi4/1,VLAN=1> was detected. (2009-07-01 13:00:00)
```

The following example shows the describing information included in the sent TRAP messages:

```
ICMP DoS attack from host<IP=1.1.1.1,MAC= N/A,,port=Gi4/1,VLAN=1> was detected.
```

If the isolated time is not set as 0 by the administrator, when the hardware isolation succeeds, it prompts:

```
%NFPP_ICMP_GUARD-4-ISOLATED:Host <IP=1.1.1.1, MAC= N/A,port=Gi4/1,VLAN=1> was isolated. (2009-07-01 13:00:00)
```

The following example shows the describing information included in the sent TRAP messages:

```
Host<IP=1.1.1.1, MAC= N/A,port=Gi4/1,VLAN=1> was isolated.
```

When it fails to isolate the hardware due to a lack of memory or hardware resources, it prompts:

```
%NFPP_ICMP_GUARD-4-ISOLATE_FAILED: Failed to isolate host <IP==1.1.1.1, MAC= N/A,port=Gi4/1,VLAN=1>. (2009-07-01 13:00:00)
```

The following example shows the describing information included in the sent TRAP messages:

```
Failed to isolate host<IP=1.1.1.1, MAC= N/A,port=Gi4/1,VLAN=1>.
```

**Caution**

When it fails to allocate the memory to the detected attackers, it prompts the message like %NFPP\_ICMP\_GUARD-4-NO\_MEMORY: Failed to alloc memory.to inform the administrator.

This section shows the administrator how to configure the host-based rate-limit and attack detection in the nfpp configuration mode and in the interface configuration mode:

Command	Function
Ruijie# <b>configure terminal</b>	Enter the global configuration mode.
Ruijie(config)# <b>nfpp</b>	Enter the nfpp configuration mode.

Command	Function
Ruijie(config-nfpp)# <b>icmp-guard rate-limit per-src-ip pps</b>	Configure the icmp-guard rate-limit, ranging from 1 to 9999, the default value is the half of the port-based global rate-limit. per-src-ip: detect the hosts based on the source IP address/VID/port;
Ruijie(config)# <b>icmp-guard attack-threshold per-src-ip pps</b>	Configure the icmp-guard attack threshold, ranging from 1 to 9999, and the default value is the source IP address-based rate limit. When the ICMP packet number sent from a host exceeds the attack threshold, the attack is detected and ICMP-guard isolates the host, records the message and sends the TRAP packet. per-src-ip: detect the hosts based on the source IP address/VID/port;
Ruijie(config-nfpp)# <b>end</b>	Return to the privileged EXEC mode.
Ruijie# <b>configure terminal</b>	Enter the global configuration mode.
Ruijie(config)# <b>interface interface-name</b>	Enter the interface configuration mode.
Ruijie(config-if)# <b>nfpp icmp-guard policy per-src-ip rate-limit-pps attack-threshold-pps</b>	Configure the rate-limit and attack threshold on the specified interface. <i>rate-limit-pps</i> : set the rate-limit threshold. The valid range is 1-9999 and by default, it adopts the global rate-limit threshold value. <i>attack-threshold-pps</i> : set the attack threshold. The valid range is 1-9999 and by default, it adopts the global attack threshold value. per-src-ip: to detect the hosts based on the source IP/VID/port;
Ruijie(config-nfpp)# <b>end</b>	Return to the privileged EXEC mode.
Ruijie(config-if)# <b>show nfpp icmp-guard summary</b>	Show the parameter settings.
Ruijie# <b>copy running-config startup-config</b>	Save the configurations.

## Port-based rate-limit and attack detection

You can configure the icmp-guard rate limit and attack threshold on the port. The rate limit value must be less than the attack threshold value. When the ICMP packet rate on a port exceeds the limit, the ICMP packets are dropped. When the ICMP packet rate on a port exceeds the attack threshold limit, the CLI prompts and the TRAP packets are sent.

It prompts the following message when the ICMP DoS attack was detected on a port:

```
%NFPP_ICMP_GUARD-4-PORT_ATTACKED: ICMP DoS attack was detected on port Gi4/1.
(2009-07-01 13:00:00)
```

The following is additional information of the sent TRAP packet :

ICMP DoS attack was detected on port Gi4/1.

This section shows the administrator how to configure the port-based rate-limit and attack detection in the nfpp configuration mode and in the interface configuration mode:

Command	Function
Ruijie# <b>configure terminal</b>	Enter the global configuration mode.
Ruijie(config)# <b>nfpp</b>	Enter the nfpp configuration mode.
Ruijie(config)# <b>icmp-guard rate-limit per-port pps</b>	Configure the icmp-guard rate-limit of the ICMP packet on the port, ranging from 1 to 9999. The default values vary with different products: different default values vary with different CMs--- (a) For M8606-CM and M8610-CM, the default value is 400; (b) For M8606-CM II, M8610-CM II and M8614-CM II, the default value is 2000.
Ruijie(config)# <b>icmp-guard attack-threshold per-port pps</b>	Configure the icmp-guard attack threshold, ranging from 1 to 9999. The default value is the port-based rate limit. When the ICMP packet number on a port exceeds the attack threshold, the CLI prompts and the TRAP packets are sent.
Ruijie(config-nfpp)# <b>end</b>	Return to the privileged EXEC mode.
Ruijie# <b>configure terminal</b>	Enter the global configuration mode.
Ruijie(config)# <b>interface interface-name</b>	Enter the interface configuration mode.

Command	Function
Ruijie(config-if)# <b>nfpp</b> <b>icmp-guard policy per-port</b> <i>rate-limit-pps</i> <i>attack-threshold-pps</i>	Configure the rate-limit and attack threshold on the specified interface. <i>rate-limit-pps</i> : set the rate-limit threshold. The valid range is 1-9999 and by default, it adopts the global rate-limit threshold value. <i>attack-threshold-pps</i> : set the attack threshold. The valid range is 1-9999 and by default, it adopts the global attack threshold value.
Ruijie(config-nfpp)# <b>end</b>	Return to the privileged EXEC mode.
Ruijie(config-if)# <b>show nfpp icmp-guard summary</b>	Show the parameter settings.
Ruijie# <b>copy running-config startup-config</b>	Save the configurations.

**Caution**

The source IP address-based rate limit takes precedence over port-based rate limit.

## Configuring the trusted hosts

Use the following commands to set the trusted host to make a host free from monitoring. The ping packets are allowed to be sent to the CPU from the trusted host.

Command	Function
Ruijie# <b>configure terminal</b>	Enter the global configuration mode.
Ruijie(config)# <b>nfpp</b>	Enter the nfpp configuration mode.
Ruijie(config-nfpp)# <b>icmp-guard trusted-host ip mask</b>	Configure the IP address range for the trusted hosts. Up to 500 pieces of IP addresses can be configured.
Ruijie(config-nfpp)# <b>end</b>	Return to the privileged EXEC mode.
Ruijie(config-if)# <b>show nfpp icmp-guard trusted-host</b>	Show the trusted host settings.
Ruijie# <b>copy running-config startup-config</b>	Save the configurations.

In the nfpp configuration mode, use the **no** form of this command to delete a trusted host entry and use the **all** form of this command to delete all trusted hosts.

For example:

The following example shows how to delete all trusted hosts:

```
Ruijie(config-nfpp)# no icmp-guard trusted-host all
```

The following example shows how to delete a trusted host entry:

---

```
Ruijie(config-nfpp)# no icmp-guard trusted-host 1.1.1.1 255.255.255.255
```

---

It prompts that "ERROR: Attempt to exceed limit of 500 trusted hosts." to inform the administrator of the full trusted host table.

If the IP address for the trusted host entry is the same to the one existing in the untrusted host list, the system will auto-delete the entry according to the IP address.

It prompts that "ERROR:Failed to delete trusted host 1.1.1.0 255.255.255.0." to inform the administrator of the failure of trusted host removal.

It prompts that "ERROR:Failed to add trusted host 1.1.1.0 255.255.255.0." to inform the administrator of the failure of adding the trusted host.



### Caution

It prompts that "ERROR:Failed to add trusted host 1.1.1.0 255.255.255.0." to inform the administrator of the failure of adding the trusted host.

It prompts that "ERROR:Failed to add trusted host 1.1.1.0 255.255.255.0." to inform the administrator of the failure of adding the trusted host.

It prompts that "ERROR:Trusted host 1.1.1.0 255.255.255.0 has already been configured." to inform the administrator of the existence of the trusted host to be added.

It prompts that "ERROR:Trusted host 1.1.1.0 255.255.255.0 is not found." to inform the administrator of the inexistence of the trusted host to be deleted.

It prompts that "ERROR:Trusted host 1.1.1.0 255.255.255.0 is not found." to inform the administrator if it fails to allocate the memory for the trusted host.

---

## Clearing the monitored hosts

The isolated hosts can be recovered automatically after a period of the time. The administrator can use the following command to clear the isolated hosts manually.

Command	Function
---------	----------

Command	Function
Ruijie# <b>clear nfpp icmp-guard hosts</b> [vlan <i>vid</i> ] [interface <i>interface-id</i> ] [ <i>ip-address</i> ]	<b>clear nfpp icmp-guard hosts</b> : Clear all isolated hosts. <b>clear nfpp icmp-guard hosts vlan <i>vid</i></b> : Clear all isolated hosts in a VLAN. <b>clear nfpp icmp-guard hosts [vlan <i>vid</i>] [interface <i>interface-id</i>]</b> : Clear all isolated hosts on a interface in a VLAN. <b>clear nfpp icmp-guard hosts [vlan <i>vid</i>] [interface <i>interface-id</i>] [<i>ip-address</i>]</b> : An isolated host has been cleared. Use the IP address to identify the hosts.

## Showing icmp-guard

- Showing icmp-guard configuration
- Showing monitored host configuration
- Showing trusted host configuration

## Showing icmp-guard configuration

Use this command to show the icmp-guard configurations.

Command	Function
Ruijie# <b>show nfpp icmp-guard summary</b>	Show the icmp-guard configurations.

For example,

```
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
G 0/1      Enable  180           5/-/-     8/-/-
G 0/2      Disable 200           4/-/60    8/-/100

Maximum count of monitored hosts: 1000
Monitor period:300s
```



**Note**

Field	Description
Interface	Global refers to the global configuration.
Status	Enable/disable the arp-guard.
Rate-limit	In the format of source IP address-based rate-limit threshold / source MAC address-based rate-limit threshold / port-based rate-limit threshold.
Attack-threshold	In the same format of the Rate-limit.
-	No configuration.

## Showing monitored host configuration

Command	Function
Ruijie# <b>show nfpp icmp-guard hosts statistics</b>	Show the icmp-guard hosts statistics, including total host amount, isolated host amount and non-isolated host amount.
Ruijie# <b>show nfpp icmp-guard hosts</b> [vlan <i>vid</i> ] [interface <i>interface-id</i> ] [ <i>ip-address</i> ]	Show the isolated hosts information. <b>show nfpp icmp-guard hosts vlan <i>vid</i></b> : Show the isolated hosts in a VLAN. <b>show nfpp icmp-guard hosts [vlan <i>vid</i>] [interface <i>interface-id</i>]</b> : Show the isolated hosts on a interface in a VLAN. <b>show nfpp icmp-guard hosts [vlan <i>vid</i>] [interface <i>interface-id</i>] [<i>ip-address</i>]</b> : Show the isolated hosts. Use the IP address to identify the hosts.

For example,

```
Ruijie#show nfpp icmp-guard hosts statistics
```

```
success  fail   total
-----  ----  -----
100      20      120
```

```
Ruijie# show nfpp icmp-guard hosts
```

If column 1 shows '\*', it means "hardware do not isolate user" .

```
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 hosts

```
Ruijie# show nfpp icmp-guard hosts vlan 1 interface G 0/1 1.1.1.1
```

If column 1 shows '\*', it means "hardware do not isolate user".

VLAN	interface	IP address	remain-time(s)
1	Gi0/1	1.1.1.1	80

Total:1 host

## Showing the trusted host configuration

Command	Function
Ruijie# <b>show nfpp icmp-guard trusted-host</b>	Show the trusted hosts.

For example,

```
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)

## DHCP-guard

### DHCP-guard Overview

The DHCP protocol is widely used to dynamically allocate the IP address in the LAN, and plays an important role in the network security. The “DHCP exhaustion” attack occurs in the way of broadcasting the DHCP request packets through faking the MAC address. If there are too many DHCP request packets, the attacker may use up the addresses provided in the DHCP server. To this end, a legal host fails to request for a DHCP IP address and access to the network. The workaround for the “DHCP exhaustion” attack: one one hand, you may configure the DHCP packet rate-limit; on the other hand, you may detect and isolate the attack source.

The DHCP attack detection could be host-based or port-based. Host-based ARP attack detection adopts the combination of source IP address/VID/port-based. For each attack detection, you can configure the rate-limit threshold and warning threshold. The DHCP packet will be dropped when the packet rate exceeds the rate-limit threshold. When the DHCP packet rate exceeds the warning threshold, it will prompt the warning messages and send the TRAP message. The host-based attack detection can isolate the attack source.

DHCP-guard configuration commands include:

- Enabling dhcp-guard
- Configuring the isolated time
- Configuring the monitored time

- Configuring the monitored host limit
- Host-based rate-limit and attack detection
- Port-based rate-limit and attack detection
- Clearing monitored host
- Showing related dhcp-guard information

## Enabling DHCP-guard

You can enable dhcp-guard in the nfpp configuration mode or in the interface configuration mode. By default, the dhcp-guard is enabled.

Command	Function
Ruijie# <b>configure terminal</b>	Enter the global configuration mode.
Ruijie(config)# <b>nfpp</b>	Enter the nfpp configuration mode.
Ruijie(config-nfpp)# <b>dhcp-guard enable</b>	Enable the dhcp-guard. By default, dhcp-guard is enabled.
Ruijie(config-nfpp)# <b>end</b>	Return to the privileged EXEC mode.
Ruijie# <b>configure terminal</b>	Enter the global configuration mode.
Ruijie# <b>interface interface-name</b>	Enter the interface configuration mode.
Ruijie(config-if)# <b>nfpp dhcp-guard enable</b>	Enable the dhcp-guard on the interface. By default, dhcp-guard is not enabled on the interface.
Ruijie(config-if)# <b>end</b>	Return to the privileged EXEC mode.
Ruijie# <b>show nfpp dhcp-guard summary</b>	Show the configurations.
Ruijie# <b>copy running-config startup-config</b>	Save the configurations.



### Caution

With the dhcp-guard disabled, the monitored hosts are auto-cleared.

## Configuring the isolated time

For the isolated time of the attacker, it can be configured in the global or interface configuration mode. By default, the isolated time is configured in the global configuration mode.

Command	Function
Ruijie# <b>configure terminal</b>	Enter the global configuration mode.

Command	Function
Ruijie(config)# <b>nfpp</b>	Enter the nfpp configuration mode.
Ruijie(config-nfpp)# <b>dhcp-guard isolate-period</b> [seconds   permanent]	Configure the global isolated time, ranging 0s, 30-86400s(one day). The default value is 0s, representing no isolation. Permanent represents permanent isolation.
Ruijie(config-nfpp)# <b>end</b>	Return to the privileged EXEC mode.
Ruijie# <b>configure terminal</b>	Enter the global configuration mode.
Ruijie(config)# <b>interface</b> interface-name	Enter the interface configuration mode.
Ruijie(config-if)# <b>nfpp arp-guard isolate-period</b> [seconds   permanent]	Configure the isolated time on the port, ranging 0s, 180-86400s(one day). By default, the isolated time is configured globally. 0s represents no isolation. Permanent represents permanent isolation.
Ruijie(config-if)# <b>end</b>	Return to the privileged EXEC mode.
Ruijie# <b>show nfpp dhcp-guard summary</b>	Show the parameter settings.
Ruijie# <b>copy running-config startup-config</b>	Save the configurations.

To restore the global isolated time to the default value, use the **no dhcp-guard isolate-period** command in the nfpp configuration mode. If the isolated time has been configured on a port, you can use the **no dhcp-guard isolate-period** command to remove the port-based isolated time configuration in the interface configuration mode.

## Configuring the monitored time

If the isolated time is 0 (that is no isolation), the serviceview monitor will be performed to auto-monitor the attacker according to the configured monitored period, providing the attacker information in the system. If the isolated time is but not 0, the DHCP-guard will perform hardware isolation towards the hosts using the serviceview monitor.

Command	Function
Ruijie# <b>configure terminal</b>	Enter the global configuration mode.
Ruijie(config)# <b>nfpp</b>	Enter the nfpp configuration mode.
Ruijie(config-nfpp)# <b>dhcp-guard monitor-period</b> seconds	Configure the monitored time, ranging 180-86400s(one day). The default value is 600s.
Ruijie(config-nfpp)# <b>end</b>	Return to the privileged EXEC mode.
Ruijie# <b>show nfpp dhcp-guard summary</b>	Show the parameter settings.

Command	Function
Ruijie# <b>copy running-config startup-config</b>	Save the configurations.

To restore the monitored time to the default value, use the **no dhcp-guard monitor-period** command in the nfpp configuration mode.



#### Caution

If the isolated time is 0, the serviceview monitor will be performed to monitor the detected attacker, and the timeout time will be the monitored period. In the process of the serviceview monitor, if the isolated time is but not 0, the hardware isolation will be performed to isolate the attacker, and the timeout time will be the isolated period. Only be the monitored period valid when the isolated period is 0.

Modifying the isolated time from non-0 to 0 removes the attackers from the interface rather than performs the serviceview monitor.

## Configuring the monitored host limit

Command	Function
Ruijie# <b>configure terminal</b>	Enter the global configuration mode.
Ruijie(config)# <b>nfpp</b>	Enter the nfpp configuration mode.
Ruijie(config-nfpp)# <b>dhcp-guard monitored-host-limit</b> <i>seconds</i>	Configure the monitored host limit, ranging 1-4294967295. The default value is 1000.
Ruijie(config-nfpp)# <b>end</b>	Return to the privileged EXEC mode.
Ruijie# <b>show nfpp dhcp-guard summary</b>	Show the parameter settings.
Ruijie# <b>copy running-config startup-config</b>	Save the configurations.

To restore the monitored host limit to the default value, use the **no dhcp-guard monitored-host-limit** command in the nfpp configuration mode.

If the monitored host number has reached the default 1000, and the administrator sets the monitored host limit smaller than 1000, the existent monitored hosts will not be deleted and it will prompt the message “%ERROR:: The value that you configured is smaller than current monitored hosts 1000:please clear a part of monitored hosts.” to notify the administrator of the invalid configuration and removing a part of the monitored hosts.



#### Caution

It prompts the message that “%NFPP\_DHCP\_GUARD-4-SESSION\_LIMIT: Attempt to exceed limit of 1000 monitored hosts.” if the monitored host table is full.

## Host-based rate-limit and attack detection

Use the source MAC/VID/port-based method to detect the host-based attack. For each attack detection, you can configure the rate-limit threshold and attack threshold (also called warning threshold). The DHCP packet will be dropped when the packet rate exceeds the rate-limit threshold. When the DHCP packet rate exceeds the warning threshold, it will prompt the warning messages and send the TRAP message.

It prompts the following message if the DHCP DoS attack was detected:

```
%NFPP_DHCP_GUARD-4- DOS_DETECTED:Host<IP=N/A,MAC=0000.0000.0001,port=Gi4/1,VLAN=1> was detected. (2009-07-01 13:00:00)
```

The following example shows the describing information included in the sent TRAP messages:

```
DHCP DoS attack from host<IP= N/A,MAC=0000.0000.0001,port=Gi4/1,VLAN=1> was detected.
```

If the isolated time is not set as 0 by the administrator, when the hardware isolation succeeds, it prompts:

```
%NFPP_DHCP_GUARD-4-ISOLATED:Host <IP= N/A,MAC=0000.0000.0001,port=Gi4/1,VLAN=1> was isolated. (2009-07-01 13:00:00)
```

The following example shows the describing information included in the sent TRAP messages:

```
Host<IP=N/A,MAC=0000.0000.0001,port=Gi4/1,VLAN=1> was isolated.
```

When it fails to isolate the hardware due to a lack of memory or hardware resources, it prompts:

```
%NFPP_DHCP_GUARD-4-ISOLATE_FAILED: Failed to isolate host <IP=N/A,MAC=0000.0000.0001,port=Gi4/1,VLAN=1>. (2009-07-01 13:00:00)
```

The following example shows the describing information included in the sent TRAP messages:

```
Failed to isolate host<IP=N/A,MAC=0000.0000.0001,port=Gi4/1,VLAN=1>.
```



### Caution

When it fails to allocate the memory to the detected attackers, it prompts the message like %NFPP\_DHCP\_GUARD-4-NO\_MEMORY: Failed to alloc memory.to inform the administrator.

This section shows the administrator how to configure the host-based rate-limit and attack detection in the nfpp configuration mode and in the interface configuration mode:

Command	Function
Ruijie# <b>configure terminal</b>	Enter the global configuration mode.
Ruijie(config)# <b>nfpp</b>	Enter the nfpp configuration mode.
Ruijie(config-nfpp)# <b>dhcp-guard rate-limit per-src-mac pps</b>	Configure the dhcp-guard rate-limit, ranging from 1 to 9999, 5 by default. per-src-mac: detect the hosts based on the source MAC address/VID/port;

Command	Function
Ruijie(config)# <b>dhcp-guard</b> <b>attack-threshold</b> <b>per-src-mac</b> <i>pps</i>	Configure the dhcp-guard attack threshold, ranging from 1 to 9999, 10 by default. When the DHCP packet number sent from a host exceeds the attack threshold, the attack is detected and DHCP-guard isolates the host, records the message and sends the TRAP packet.  per-src-mac: detect the hosts based on the source MAC address/VID/port;
Ruijie(config-nfpp)# <b>end</b>	Return to the privileged EXEC mode.
Ruijie# <b>configure terminal</b>	Enter the global configuration mode.
Ruijie(config)# <b>interface</b> <i>interface-name</i>	Enter the interface configuration mode.
Ruijie(config-if)# <b>nfpp</b> <b>dhcp-guard</b> <b>policy</b> <b>per-src-mac</b> <i>rate-limit-pps</i> <i>attack-threshold-pps</i>	Configure the rate-limit and attack threshold on the specified interface. <i>rate-limit-pps</i> : set the rate-limit threshold. The valid range is 1-9999 and by default, it adopts the global rate-limit threshold value. <i>attack-threshold-pps</i> : set the attack threshold. The valid range is 1-9999 and by default, it adopts the global attack threshold value. per-src-mac: to detect the hosts based on the source MAC/VID/port;
Ruijie(config-nfpp)# <b>end</b>	Return to the privileged EXEC mode.
Ruijie(config-if)# <b>show nfpp</b> <b>dhcp-guard summary</b>	Show the parameter settings.
Ruijie# <b>copy running-config</b> <b>startup-config</b>	Save the configurations.

## Port-based rate-limit and attack detection

You can configure the dhcp-guard rate limit and attack threshold on the port. The rate limit value must be less than the attack threshold value. When the DHCP packet rate on a port exceeds the limit, the DHCP packets are dropped. When the DHCP packet rate on a port exceeds the attack threshold limit, the CLI prompts and the TRAP packets are sent.

It prompts the following message when the DHCP DoS attack was detected on a port:

```
%NFPP_DHCP_GUARD-4-PORT_ATTACKED: DHCP DoS attack was detected on port Gi4/1.
(2009-07-01 13:00:00)
```

The following is additional information of the sent TRAP packet :

DHCP DoS attack was detected on port Gi4/1.

This section shows the administrator how to configure the port-based rate-limit and attack detection in the nfpp configuration mode and in the interface configuration mode:

Command	Function
Ruijie# <b>configure terminal</b>	Enter the global configuration mode.
Ruijie(config)# <b>nfpp</b>	Enter the nfpp configuration mode.
Ruijie(config)# <b>dhcp-guard rate-limit per-port pps</b>	Configure the dhcp-guard rate-limit of the DHCP packet on the port, ranging from 1 to 9999, 150 by default.
Ruijie(config)# <b>dhcp-guard attack-threshold per-port pps</b>	Configure the dhcp-guard attack threshold, ranging from 1 to 9999, 300 by default. When the DHCP packet number on a port exceeds the attack threshold, the CLI prompts and the TRAP packets are sent.
Ruijie(config-nfpp)# <b>end</b>	Return to the privileged EXEC mode.
Ruijie# <b>configure terminal</b>	Enter the global configuration mode.
Ruijie(config)# <b>interface interface-name</b>	Enter the interface configuration mode.
Ruijie(config-if)# <b>nfpp dhcp-guard policy per-port rate-limit-pps attack-threshold-pps</b>	Configure the rate-limit and attack threshold on the specified interface. <i>rate-limit-pps</i> : set the rate-limit threshold. The valid range is 1-9999 and by default, it adopts the global rate-limit threshold value. <i>attack-threshold-pps</i> : set the attack threshold. The valid range is 1-9999 and by default, it adopts the global attack threshold value.
Ruijie(config-nfpp)# <b>end</b>	Return to the privileged EXEC mode.
Ruijie(config-if)# <b>show nfpp dhcp-guard summary</b>	Show the parameter settings.
Ruijie# <b>copy running-config startup-config</b>	Save the configurations.



The source MAC address-based rate limit takes precedence over port-based rate limit.

## Clearing the monitored hosts

The isolated hosts can be recovered automatically after a period of the time. The administrator can use the following command to clear the isolated hosts manually.



Command	Function
Ruijie# <b>clear nfpp dhcp-guard hosts [vlan vid] [interface interface-id] [mac-address]</b>	<p><b>clear nfpp dhcp-guard hosts:</b> Clear all isolated hosts.</p> <p><b>clear nfpp dhcp-guard hosts vlan vid:</b> Clear all isolated hosts in a VLAN.</p> <p><b>clear nfpp dhcp-guard hosts [vlan vid] [interface interface-id]:</b> Clear all isolated hosts on a interface in a VLAN.</p> <p><b>clear nfpp dhcp-guard hosts [vlan vid] [interface interface-id] [mac-address]:</b> An isolated host has been cleared. Use the MAC address to identify the hosts.</p>

## Showing dhcp-guard

- Showing dhcp-guard configuration
- Showing monitored host configuration

## Showing dhcp-guard configuration

Use this command to show the dhcp-guard configurations.

Command	Function
Ruijie# <b>show nfpp dhcp-guard summary</b>	Show the dhcp-guard configurations.

For example,

```
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
G 0/1      Enable   180           -/6/-     -/8/-
G 0/2      Disable  200           -/5/30    -/10/50

Maximum count of monitored hosts: 1000
Monitor period:300s
```

Field	Description
Interface	Global refers to the global configuration.
Status	Enable/disable the arp-guard.
Rate-limit	In the format of source IP address-based rate-limit threshold / source MAC address-based rate-limit threshold / port-based rate-limit threshold.
Attack-threshold	In the same format of the Rate-limit.
-	No configuration.



#### Note

## Showing monitored host configuration

Command	Function
Ruijie# <b>show nfpp dhcp-guard hosts statistics</b>	Show the dhcp-guard hosts statistics, including total host amount, isolated host amount and non-isolated host amount.
Ruijie# <b>show nfpp dhcp-guard hosts</b> [vlan vid] [interface interface-id] [mac-address]	Show the isolated hosts information. <b>show nfpp dhcp-guard hosts vlan vid:</b> Show the isolated hosts in a VLAN. <b>show nfpp dhcp-guard hosts [vlan vid] [interface interface-id]:</b> Show the isolated hosts on a interface in a VLAN. <b>show nfpp dhcp-guard hosts [vlan vid] [interface interface-id] [mac-address]:</b> Show the isolated hosts. Use the MAC address to identify the hosts.

For example,

```
Ruijie#show nfpp dhcp-guard hosts statistics
```

```
success  fail   total
-----  ----  -----
100      20      120
```

```
Ruijie# show nfpp dhcp-guard hosts
```

If column 1 shows '\*', it means "hardware do not isolate user" .

```
VLAN  interface  MAC address      remain-time(s)
```

```

-----
*1   Gi0/1   0000.0000.0001 110
2    Gi0/2   0000.0000.2222 61
Total:2 host(s)

```

```

Ruijie# show nfpp dhcp-guard hosts vlan 1 interface g 0/1 0000.0000.0001
If column 1 shows '*', it means "hardware failed to isolate host".
VLAN interface MAC address remain-time(s)
-----
*1   Gi0/1   0000.0000.0001 110
Total:1 host(s)

```

## DHCPv6-guard

### DHCPv6-guard Overview

The DHCPv6 protocol is widely used to dynamically allocate the IPv6 address in the LAN, and plays an important role in the network security. Being similar to the DHCP attack, the DHCPv6 attack occurs in the way of broadcasting the DHCPv6 request packets through faking the MAC address. If there are too many DHCPv6 request packets, the attacker may use up the addresses provided in the DHCPv6 server. To this end, a legal host fails to request for an IPv6 address and access to the network. The workaround for the DHCPv6 attack: on one hand, you may configure the DHCPv6 packet rate-limit; on the other hand, you may detect and isolate the attack source.

The DHCPv6 attack detection could be host-based or port-based. Host-based ARP attack detection adopts the combination of source IP address/VID/port-based. For each attack detection, you can configure the rate-limit threshold and warning threshold. The DHCPv6 packet will be dropped when the packet rate exceeds the rate-limit threshold. When the DHCPv6 packet rate exceeds the warning threshold, it will prompt the warning messages and send the TRAP message. The host-based attack detection can isolate the attack source.

DHCPv6-guard configuration commands include:

- Enabling dhcpv6-guard
- Configuring the isolated time
- Configuring the monitored time
- Configuring the monitored host limit
- Host-based rate-limit and attack detection
- Port-based rate-limit and attack detection
- Clearing monitored host
- Showing related dhcpv6-guard information

## Enabling DHCPv6-guard

You can enable dhcpv6-guard in the nfpp configuration mode or in the interface configuration mode. By default, the dhcpv6-guard is enabled.

Command	Function
Ruijie# configure terminal	Enter the global configuration mode.
Ruijie(config)# <b>nfpp</b>	Enter the nfpp configuration mode.
Ruijie(config-nfpp)# <b>dhcpv6-guard enable</b>	Enable the dhcpv6-guard. By default, dhcpv6-guard is enabled.
Ruijie(config-nfpp)# <b>end</b>	Return to the privileged EXEC mode.
Ruijie# <b>configure terminal</b>	Enter the global configuration mode.
Ruijie# <b>interface</b> <i>interface-name</i>	Enter the interface configuration mode.
Ruijie(config-if)# <b>nfpp</b> <b>dhcpv6-guard enable</b>	Enable the dhcpv6-guard on the interface. By default, dhcpv6-guard is not enabled on the interface.
Ruijie(config-if)# <b>end</b>	Return to the privileged EXEC mode.
Ruijie# <b>show nfpp</b> <b>dhcpv6-guard summary</b>	Show the configurations.
Ruijie# <b>copy running-config</b> <b>startup-config</b>	Save the configurations.



### Caution

With the dhcpv6-guard disabled, the monitored hosts are auto-cleared.

## Configuring the isolated time

For the isolated time of the attacker, it can be configured in the global or interface configuration mode. By default, the isolated time is configured in the global configuration mode.

Command	Function
Ruijie# <b>configure terminal</b>	Enter the global configuration mode.
Ruijie(config)# <b>nfpp</b>	Enter the nfpp configuration mode.
Ruijie(config-nfpp)# <b>dhcpv6-guard isolate-period</b> [ <i>seconds</i>   <b>permanent</b> ]	Configure the global isolated time, ranging 0s, 30-86400s(one day). The default value is 0s, representing no isolation. Permanent represents permanent isolation.

Command	Function
Ruijie(config-nfpp)# <b>end</b>	Return to the privileged EXEC mode.
Ruijie# <b>configure terminal</b>	Enter the global configuration mode.
Ruijie(config)# <b>interface</b> <i>interface-name</i>	Enter the interface configuration mode.
Ruijie(config-if)# <b>nfpp arp-guard</b> <b>isolate-period</b> [ <i>seconds</i>   <b>permanent</b> ]	Configure the isolated time on the port, ranging 0s, 180-86400s(one day). By default, the isolated time is configured globally. 0s represents no isolation. Permanent represents permanent isolation.
Ruijie(config-if)# <b>end</b>	Return to the privileged EXEC mode.
Ruijie# <b>show nfpp</b> <b>dhcpv6-guard summary</b>	Show the parameter settings.
Ruijie# <b>copy running-config</b> <b>startup-config</b>	Save the configurations.

To restore the global isolated time to the default value, use the **no dhcpv6-guard isolate-period** command in the nfpp configuration mode. If the isolated time has been configured on a port, you can use the **no dhcpv6-guard isolate-period** command to remove the port-based isolated time configuration in the interface configuration mode.

## Configuring the monitored time

If the isolated time is 0 (that is no isolation), the serviceview monitor will be performed to auto-monitor the attacker according to the configured monitored period, providing the attacker information in the system. If the isolated time is but not 0, the DHCPv6-guard will perform hardware isolation towards the hosts using the serviceview monitor.

Command	Function
Ruijie# <b>configure terminal</b>	Enter the global configuration mode.
Ruijie(config)# <b>nfpp</b>	Enter the nfpp configuration mode.
Ruijie(config-nfpp)# <b>dhcpv6-guard monitor-period</b> <i>seconds</i>	Configure the monitored time, ranging 180-86400s(one day). The default value is 600s.
Ruijie(config-nfpp)# <b>end</b>	Return to the privileged EXEC mode.
Ruijie# <b>show nfpp</b> <b>dhcpv6-guard summary</b>	Show the parameter settings.
Ruijie# <b>copy running-config</b> <b>startup-config</b>	Save the configurations.

To restore the monitored time to the default value, use the **no dhcpv6-guard monitor-period** command in the nfpp configuration mode.



If the isolated time is 0, the serviceview monitor will be performed to monitor the detected attacker, and the timeout time will be the monitored period. In the process of the serviceview monitor, if the isolated time is but not 0, the hardware isolation will be performed to isolate the attacker, and the timeout time will be the isolated period. Only be the monitored period valid when the isolated period is 0.

Modifying the isolated time from non-0 to 0 removes the attackers from the interface rather than performs the serviceview monitor.

## Configuring the monitored host limit

Command	Function
Ruijie# <b>configure terminal</b>	Enter the global configuration mode.
Ruijie(config)# <b>nfpp</b>	Enter the nfpp configuration mode.
Ruijie(config-nfpp)# <b>dhcpv6-guard monitored-host-limit seconds</b>	Configure the monitored host limit, ranging 1-4294967295. The default value is 1000.
Ruijie(config-nfpp)# <b>end</b>	Return to the privileged EXEC mode.
Ruijie# <b>show nfpp dhcpv6-guard summary</b>	Show the parameter settings.
Ruijie# <b>copy running-config startup-config</b>	Save the configurations.

To restore the monitored host limit to the default value, use the **no dhcpv6-guard monitored-host-limit** command in the nfpp configuration mode.

If the monitored host number has reached the default 1000, and the administrator sets the monitored host limit smaller than 1000, the existent monitored hosts will not be deleted and it will prompt the message “%ERROR: The value that you configured is smaller than current monitored hosts 1000.please clear a part of monitored hosts.” to notify the administrator of the invalid configuration and removing a part of the monitored hosts.



It prompts the message that “%NFPP\_DHCPV6\_GUARD-4-SESSION\_LIMIT: Attempt to exceed limit of 1000 monitored hosts.” if the monitored host table is full.

## Host-based rate-limit and attack detection

Use the source MAC/VID/port-based method to detect the host-based attack. For each attack detection, you can configure the rate-limit threshold and attack threshold (also called warning threshold). The DHCPv6 packet will be dropped when the packet rate exceeds the rate-limit threshold. When the DHCPv6 packet rate exceeds the warning threshold, it will prompt the warning messages and send the TRAP message.

It prompts the following message if the DHCPv6 DoS attack was detected:

```
%NFPP_DHCPV6_GUARD-4- DOS_DETECTED:Host<IP=N/A,MAC=0000.0000.0001,port=Gi4/1,VLAN=1>
was detected. (2009-07-01 13:00:00)
```

The following example shows the describing information included in the sent TRAP messages:

```
DHCPV6 DoS attack from host<IP=N/A,MAC=0000.0000.0001,port=Gi4/1,VLAN=1> was detected.
```

If the isolated time is not set as 0 by the administrator, when the hardware isolation succeeds, it prompts:

```
%NFPP_DHCPV6_GUARD-4-ISOLATED:Host <IP= N/A,MAC=0000.0000.0001,port=Gi4/1,VLAN=1> was
isolated. (2009-07-01 13:00:00)
```

The following example shows the describing information included in the sent TRAP messages:

```
Host<IP=N/A,MAC=0000.0000.0001,port=Gi4/1,VLAN=1> was isolated.
```

When it fails to isolate the hardware due to a lack of memory or hardware resources, it prompts:

```
%NFPP_DHCPV6_GUARD-4-ISOLATE_FAILED: Failed to isolate host <IP=N/A,MAC=0000.0000.0001,
port=Gi4/1,VLAN=1>. (2009-07-01 13:00:00)
```

The following example shows the describing information included in the sent TRAP messages:

```
Failed to isolate host<IP=N/A,MAC=0000.0000.0001,port=Gi4/1,VLAN=1>.
```



#### Caution

When it fails to allocate the memory to the detected attackers, it prompts the message like `%NFPP_DHCPV6_GUARD-4-NO_MEMORY: Failed to alloc memory.` to inform the administrator.

This section shows the administrator how to configure the host-based rate-limit and attack detection in the nfpp configuration mode and in the interface configuration mode:

Command	Function
Ruijie# <b>configure terminal</b>	Enter the global configuration mode.
Ruijie(config)# <b>nfpp</b>	Enter the nfpp configuration mode.
Ruijie(config-nfpp)# <b>dhcpv6-guard rate-limit</b> <b>per-src-mac pps</b>	Configure the dhcpv6-guard rate-limit, ranging from 1 to 9999, 5 by default. <b>per-src-mac</b> : detect the hosts based on the source MAC address/VID/port;

Command	Function
Ruijie(config)# <b>dhcpv6-guard</b> <b>attack-threshold</b> <b>per-src-mac</b> <i>pps</i>	Configure the dhcpv6-guard attack threshold, ranging from 1 to 9999, 10 by default. When the DHCPv6 packet number sent from a host exceeds the attack threshold, the attack is detected and DHCPv6-guard isolates the host, records the message and sends the TRAP packet. <b>per-src-mac</b> : detect the hosts based on the source MAC address/VID/port;
Ruijie(config-nfpp)# <b>end</b>	Return to the privileged EXEC mode.
Ruijie# <b>configure terminal</b>	Enter the global configuration mode.
Ruijie(config)# <b>interface</b> <i>interface-name</i>	Enter the interface configuration mode.
Ruijie(config-if)# <b>nfpp</b> <b>dhcpv6-guard</b> <b>policy</b> <b>per-src-mac</b> <i>rate-limit-pps</i> <i>attack-threshold-pps</i>	Configure the rate-limit and attack threshold on the specified interface. <i>rate-limit-pps</i> : set the rate-limit threshold. The valid range is 1-9999 and by default, it adopts the global rate-limit threshold value. <i>attack-threshold-pps</i> : set the attack threshold. The valid range is 1-9999 and by default, it adopts the global attack threshold value. <b>per-src-mac</b> : to detect the hosts based on the source MAC/VID/port;
Ruijie(config-nfpp)# <b>end</b>	Return to the privileged EXEC mode.
Ruijie(config-if)# <b>show nfpp</b> <b>dhcpv6-guard summary</b>	Show the parameter settings.
Ruijie# <b>copy running-config</b> <b>startup-config</b>	Save the configurations.

## Port-based rate-limit and attack detection

You can configure the dhcpv6-guard rate limit and attack threshold on the port. The rate limit value must be less than the attack threshold value. When the DHCPv6 packet rate on a port exceeds the limit, the DHCPv6 packets are dropped. When the DHCPv6 packet rate on a port exceeds the attack threshold limit, the CLI prompts and the TRAP packets are sent.

It prompts the following message when the DHCPv6 DoS attack was detected on a port:



%NFPP\_DHCPV6\_GUARD-4-PORT\_ATTACKED: DHCPV6 DoS attack was detected on port Gi4/1.  
(2009-07-01 13:00:00)

The following is additional information of the sent TRAP packet :

DHCPV6 DoS attack was detected on port Gi4/1.

This section shows the administrator how to configure the port-based rate-limit and attack detection in the nfpp configuration mode and in the interface configuration mode:

Command	Function
Ruijie# <b>configure terminal</b>	Enter the global configuration mode.
Ruijie(config)# <b>nfpp</b>	Enter the nfpp configuration mode.
Ruijie(config)# <b>dhcpv6-guard rate-limit per-port pps</b>	Configure the dhcpv6-guard rate-limit of the DHCPV6 packet on the port, ranging from 1 to 9999, 150 by default.
Ruijie(config)# <b>dhcpv6-guard attack-threshold per-port pps</b>	Configure the dhcpv6-guard attack threshold, ranging from 1 to 9999, 300 by default. When the DHCPV6 packet number on a port exceeds the attack threshold, the CLI prompts and the TRAP packets are sent.
Ruijie(config-nfpp)# <b>end</b>	Return to the privileged EXEC mode.
Ruijie# <b>configure terminal</b>	Enter the global configuration mode.
Ruijie(config)# <b>interface interface-name</b>	Enter the interface configuration mode.
Ruijie(config-if)# <b>nfpp dhcpv6-guard policy per-port rate-limit-pps attack-threshold-pps</b>	Configure the rate-limit and attack threshold on the specified interface. <i>rate-limit-pps</i> : set the rate-limit threshold. The valid range is 1-9999 and by default, it adopts the global rate-limit threshold value. <i>attack-threshold-pps</i> : set the attack threshold. The valid range is 1-9999 and by default, it adopts the global attack threshold value.
Ruijie(config-nfpp)# <b>end</b>	Return to the privileged EXEC mode.
Ruijie(config-if)# <b>show nfpp dhcpv6-guard summary</b>	Show the parameter settings.
Ruijie# <b>copy running-config startup-config</b>	Save the configurations.



The source MAC address-based rate limit takes precedence over port-based rate limit.

## Clearing the monitored hosts

The isolated hosts can be recovered automatically after a period of the time. The administrator can use the following command to clear the isolated hosts manually.

Command	Function
Ruijie# <b>clear nfpp dhcpv6-guard hosts</b> [vlan <i>vid</i> ] [interface <i>interface-id</i> ] [mac-address]	<b>clear nfpp dhcpv6-guard hosts:</b> Clear all isolated hosts. <b>clear nfpp dhcpv6-guard hosts vlan <i>vid</i>:</b> Clear all isolated hosts in a VLAN. <b>clear nfpp dhcpv6-guard hosts [vlan <i>vid</i>] [interface <i>interface-id</i>]:</b> Clear all isolated hosts on a interface in a VLAN. <b>clear nfpp dhcpv6-guard hosts [vlan <i>vid</i>] [interface <i>interface-id</i>] [mac-address]:</b> An isolated host has been cleared. Use the MAC address to identify the hosts.

## Showing dhcpv6-guard

- Showing dhcpv6-guard configuration
- Showing monitored host configuration

## Showing dhcpv6-guard configuration

Use this command to show the dhcpv6-guard configurations.

Command	Function
Ruijie# <b>show nfpp dhcpv6-guard summary</b>	Show the dhcpv6-guard configurations.

For example,

```
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
G 0/1      Enable   180           -/6/-     -/8/-
G 0/2      Disable  200           -/5/30    -/10/50

Maximum count of monitored hosts: 1000
Monitor period;300s
```

**Note**

Field	Description
Interface	Global refers to the global configuration.
Status	Enable/disable the arp-guard.
Rate-limit	In the format of source IP address-based rate-limit threshold / source MAC address-based rate-limit threshold / port-based rate-limit threshold.
Attack-threshold	In the same format of the Rate-limit.
-	No configuration.

## Showing monitored host configuration

Command	Function
Ruijie# <b>show nfpp dhcpv6-guard hosts statistics</b>	Show the dhcpv6-guard hosts statistics, including total host amount, isolated host amount and non-isolated host amount.
Ruijie# <b>show nfpp dhcpv6-guard hosts [vlan vid] [interface interface-id] [mac-address]</b>	Show the isolated hosts information. <b>show nfpp dhcpv6-guard hosts vlan vid</b> : Show the isolated hosts in a VLAN. <b>show nfpp dhcpv6-guard hosts [vlan vid] [interface interface-id]</b> : Show the isolated hosts on a interface in a VLAN. <b>show nfpp dhcpv6-guard hosts [vlan vid] [interface interface-id] [mac-address]</b> : Show the isolated hosts. Use the MAC address to identify the hosts.

For example,

```
Ruijie#show nfpp dhcpv6-guard hosts statistics
```

```
success  fail   total
-----  ----  -----
100      20      120
```

```
Ruijie# show nfpp dhcpv6-guard hosts
```

If column 1 shows '\*', it means "hardware do not isolate user" .

```
VLAN  interface  MAC address      remain-time(s)
----  -
-----
```

```
*1    Gi0/1    0000.0000.0001  110
2     Gi0/2    0000.0000.2222   61
Total:2 host(s)
```

```
Ruijie# show nfpp dhcpv6-guard hosts vlan 1 interface g 0/1 0000.0000.0001
```

If column 1 shows '\*', it means "hardware failed to isolate host".

```
VLAN interface  MAC address      remain-time(s)
----
*1    Gi0/1     0000.0000.0001  110
Total:1 host(s)
```

## ND-guard

### ND-guard Overview

ND, the abbreviation of "Neighbor Discovery", is responsible for the address resolution, router discovery, prefix discovery and the redirection. ND uses the following 5 types of the ND packets: Neighbor Solicitation, Neighbor Advertisement, Router Solicitation, Router Advertisement and Redirect, which are abbreviated as the NS, NA, RS and RA.

ND Snooping monitors the ND packets in the network, filters the illegal ND packets and associates the monitored IPv6 users with the interface to prevent the IPv6 address from being stolen. ND Snooping shall send the ND packets to the CPU at the configured rate-limit to implement the ND-guard function, for sending the ND packets at the high rate leads to the CPU attack.

ND-guard classifies the ND packets into the following three types: 1) NS-NA: the Neighbor Solicitation and the Neighbor Advertisement, used for the address resolution; 2) RS: the Router Solicitation, used for the gateway discovery by the host; 3) RA and Redirect: the Router Advertisement and Redirect, used to advertise the gateway and prefix, and the better next-hop.

At present, only the port-based ND packet attack detection is implemented. You may configure the rate-limit threshold and the attack threshold for the ND packets.

When the ND packet rate on a port exceeds the limit, the ND packets are dropped. When the ND packet rate on a port exceeds the attack threshold limit, the CLI prompts and the TRAP packets are sent.

ND-guard configuration commands include:

- Enabling ND-guard
- Port-based rate-limit and attack detection
- Showing related dhcpv6-guard information

### Enabling ND-guard

You can enable ND-guard in the nfpp configuration mode or in the interface configuration mode. By default, the ND-guard is enabled.

Command	Function
---------	----------

Command	Function
Ruijie# <b>configure terminal</b>	Enter the global configuration mode.
Ruijie(config)# <b>nfpp</b>	Enter the nfpp configuration mode.
Ruijie(config-nfpp)# <b>nd-guard enable</b>	Enable the nd-guard. By default, nd-guard is enabled.
Ruijie(config-nfpp)# <b>end</b>	Return to the privileged EXEC mode.
Ruijie# <b>configure terminal</b>	Enter the global configuration mode.
Ruijie# <b>interface</b> <i>interface-name</i>	Enter the interface configuration mode.
Ruijie(config-if)# <b>nfpp nd-guard enable</b>	Enable the nd-guard on the interface. By default, nd-guard is not enabled on the interface.
Ruijie(config-if)# <b>end</b>	Return to the privileged EXEC mode.
Ruijie# <b>show nfpp dhcpv6-guard summary</b>	Show the configurations.
Ruijie# <b>copy running-config startup-config</b>	Save the configurations.

**Caution**

With the nd-guard disabled, the monitored hosts are auto-cleared.

## Port-based rate-limit and attack detection

You can configure the ND-guard rate-limit and attack threshold on the port. The rate-limit value must be less than the attack threshold value. When the ND packet rate on a port exceeds the limit, the ND packets are dropped. When the ND packet rate on a port exceeds the attack threshold limit, the CLI prompts and the TRAP packets are sent.

ND Snooping divides the port into the untrusted port and the trusted port, which connect to the host and the gateway respectively. The rate-limit threshold for the trusted port shall be higher than the one for the untrusted port because the traffic for the trusted port is generally higher than the one for the untrusted port. With the ND Snooping enabled, the ND Snooping advertises the ND-guard to set the rate-limit threshold and the attack threshold of the ND packets on the trusted port as 800pps and 900pps respectively.

For the rate-limit threshold configured by the ND Snooping and the one configured by the administrator, the latter configured threshold value overwrites the former configured one.

When the administrator saves the settings, the rate-limit threshold configured by the ND Snooping saved into the configuration file.

It prompts the following message when the **NS-NA DoS attack** was detected on a port:

%NFPP\_ND\_GUARD-4-PORT\_ATTACKED: **NS-NA** DoS attack was detected on port Gi4/1.  
(2009-07-01 13:00:00)

The following is additional information of the sent TRAP packet :

**NS-NA** DoS attack was detected on port Gi4/1.

It prompts the following message when the **RS DoS attack** was detected on a port:

%NFPP\_ND\_GUARD-4-PORT\_ATTACKED: **RS** DoS attack was detected on port Gi4/1.  
(2009-07-01 13:00:00)

The following is additional information of the sent TRAP packet :

**RS** DoS attack was detected on port Gi4/1.

It prompts the following message when the **RA-REDIRECT DoS attack** was detected on a port:

%NFPP\_ND\_GUARD-4-PORT\_ATTACKED: **RA-REDIRECT** DoS attack was detected on port Gi4/1.  
(2009-07-01 13:00:00)

The following is additional information of the sent TRAP packet :

**RA-REDIRECT** DoS attack was detected on port Gi4/1.

This section shows the administrator how to configure the port-based rate-limit and attack detection in the nfpp configuration mode and in the interface configuration mode:

Command	Function
Ruijie# <b>configure terminal</b>	Enter the global configuration mode.
Ruijie(config)# <b>nfpp</b>	Enter the nfpp configuration mode.
Ruijie(config)# <b>nd-guard</b> <b>rate-limit per-port [ns-na   rs  </b> <b>ra-redirect] pps</b>	Configure the rate-limit of the ND packets on the port, ranging from 1 to 9999, 15 by default.
Ruijie(config)# <b>nd-guard</b> <b>attack-threshold per-port</b> <b>[ns-na   rs   ra-redirect] pps</b>	Configure the attack threshold, ranging from 1 to 9999, 30 by default. When the ND packet number on a port exceeds the attack threshold, the CLI prompts and the TRAP packets are sent.
Ruijie(config-nfpp)# <b>end</b>	Return to the privileged EXEC mode.
Ruijie# <b>configure terminal</b>	Enter the global configuration mode.
Ruijie(config)# <b>interface</b> <i>interface-name</i>	Enter the interface configuration mode.
Ruijie(config-if)# <b>nfpp nd-guard</b> <b>policy per-port [ns-na   rs  </b> <b>ra-redirect] rate-limit-pps</b> <i>attack-threshold-pps</i>	Configure the rate-limit and attack threshold on the specified interface. <i>rate-limit-pps</i> : set the rate-limit threshold. The valid range is 1-9999. <i>attack-threshold-pps</i> : set the attack threshold. The valid range is 1-9999.
Ruijie(config-nfpp)# <b>end</b>	Return to the privileged EXEC mode.
Ruijie(config-if)# <b>show nfpp</b> <b>nd-guard summary</b>	Show the parameter settings.

Command	Function
Ruijie# <b>copy running-config startup-config</b>	Save the configurations.

## Showing dhcpv6-guard

- Showing ND-guard configuration

## Showing ND-guard configuration

Use this command to show the ND-guard configurations.

Command	Function
Ruijie# <b>show nfpp nd-guard summary</b>	Show the ND-guard configurations.

For example,

```
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

G 0/1   Enable   15/15/15   30/30/30

G 0/2   Disable   -/5/30   -/10/50



### Note

Field	Description
Interface	Global refers to the global configuration.
Status	Enable/disable the arp-guard.
Rate-limit	In the format of NS-NA rate-limit threshold / RS rate-limit threshold / RA-redirect rate-limit threshold.
Attack-threshold	In the same format of the Rate-limit.
-	No configuration.

## Defined-guard

### Defined-guard Overview

There are a great variety of network protocols, including such routing protocols as OSPF, BGP, RIP and etc. Protocol communication is realized by exchanging packets between different devices, and the exchange packets must be delivered to the CPU in order to be processed by respective protocols. Once a protocol is running on the network device, a "window" is opened to potential attackers. If the attacker sends excessive protocol packets to the network device, the CPU resource of the device will be heavily consumed, and the device may not work properly.

Given the diversity of network protocols and the fact that different protocols may be used under different user environment during sustainable development, Ruijie devices have provided the feature of Defined Guard to allow users to define guard against various attacks, so as meet different attack protection needs.

### Define-guard Policy

The administrator can define a guard policy in NFPP configuration mode. Defined Guard requires that the user must configure packet type, rate-limiting threshold, attack threshold and how to identify such basic information. The type of Defined Guard will only take effect after configuring the basic information. The user-defined packet type may include Ethernet link layer type (etype), source MAC address (smac), destination MAC address (dmac), IPv4/v6 protocol number (protocol), source IPv4/v6 address (sip), destination IPv4/v6 address (dip), source transport layer port (sport) and destination transport layer port (dport).

Defined Guard must configure how to take classified statistics of the data rate of defined type of packets, including source IP/VID/port based data rate statistics, source MAC/VID/port based data rate statistics and port-based data rate statistics, or any combination thereof. You must configure the corresponding rate-limiting threshold and attack threshold for these classes. The class will only take effect after configuring the rate-limiting threshold and attack threshold for such class.

Command	Function
<b>Ruijie#configure terminal</b>	Enter global configuration mode.
<b>Ruijie(config)#nfpp</b>	Enter NFPP configuration mode.
<b>Ruijie(config-nfpp)#define name</b>	Configure the name of defined guard type



<pre> Ruijie(config-nfpp-define)# match [etype type] [ src-mac smac [src-mac-mask smac_mask]] [dst-mac dmac [dst-mac-mask dst_mask]] [ protocol protocol ] [ src-ip sip [src-ip-mask sip-mask]] [ src-ipv6 sipv6 [src-ipv6-masklen sipv6-masklen]] [dst-ip dip [dst-ip-mask dip-mask]] [dst-ipv6 dipv6 [dst-ipv6-masklen dipv6-masklen]][src-port sport] [dst-port dport] </pre>	<p>Configure the packet fields to be matched by the defined guard type.</p> <p>By default, <b>src-mac-mask</b>, <b>dst-mac-mask</b>, <b>src-ip-mask</b> and <b>dst-ip-mask</b> are all 1, and <b>src-ipv6-masklen</b> and <b>dst-ipv6-masklen</b> are all 128.</p> <p><b>Protocol</b> will only take effect when <b>etype</b> is ipv4 or ipv6; <b>src-ip</b> and <b>dst-ip</b> will only take effect when <b>etype</b> is ipv4; <b>src-ipv6</b> and <b>dst-ipv6</b> will only take effect when <b>etype</b> is ipv6; <b>src-port</b> and <b>dst-port</b> will only take effect when <b>protocol</b> is tcp or udp.</p>
<pre> Ruijie(config-nfpp-define)# define-policy {per-src-ip   per-src-mac   per-port} rate-limit-pps attack-threshold-pps </pre>	<p>Configure host-based or port-based rate-limiting threshold and attack threshold.</p> <p><b>per-src-ip</b> means to take statistics of data rate as per source IP/VID/port; <b>per-src-mac</b> means to take statistics of data rate as per source MAC/VID/port. <b>per-port</b> means to take statistics of data rate as per each packet-receiving physical port. You must configure any of <b>per-src-ip</b>, <b>per-src-mac</b> and <b>per-port</b>, or else the policy won't take effect.</p> <p><b>per-src-ip</b> will only take effect when <b>etype</b> is ipv4 or ipv6.</p> <p><i>Rate-limit-pps</i> means the rate-limiting threshold (1-9999). By default, no rate limiting will be implemented. Packets exceeding the rate-limiting threshold will be discarded.</p> <p><i>Attack-threshold-pps</i> means the attack threshold (1-9999).</p> <p>By default, no rate limiting will be implemented.</p> <p>The attack threshold must be greater than or equal to the rate-limiting threshold.</p>
<pre> Ruijie#show nfpp define summary name </pre>	<p>Verify configurations.</p>

Ruijie#**copy running-config startup-config**

Save configurations.

To delete the defined guard type, execute "**no nfpp define name**" in NFPP configuration mode. Deleting defined guard type will delete all related configurations, including global and interface based configurations and all isolated hosts.



**Caution**

The name of defined guard type cannot be repeated. The field and value to be matched cannot be completely same or be same with the guard type of arp, icmp, dhcp, ip, or dhcpv6. When the configured type is repeated, the system will prompt configuration failure.

When the match type and value of defined guard are completely the same with the existing defined guard type, the following prompting message will be displayed: "%ERROR: the match type and value are the same with define name (name of the existing defined guard type)", indicating that the configuration has failed.

When protocol has been configured for the match field but etype is neither IPv4 or IPv6, the following prompting message will be displayed: "%ERROR:protocol is valid only when etype is IPv4 (0x0800) or IPv6 (0x86dd)."

When src-ip and dst-ip have been configured for the match field but etype is not IPv4, the following prompting message will be displayed: "%ERROR:IP address is valid only when etype is IPv4 (0x0800)."

When src-ipv6 and dst-ipv6 have been configured for the match field but etype is not IPv6, the following prompting message will be displayed: "%ERROR:IPv6 address is valid only when etype is IPv6 (0x86dd)."

When src-port and dst-port have been configured for the match field but protocol is not TCP or UDP, the following prompting message will be displayed: "%ERROR:Port is valid only when protocol is TCP (6) or UDP (17)."

## Common Define-guard Policy

The following table shows the guard policies corresponding to certain commonly used network protocols. The corresponding rate-limiting threshold and attack threshold can meet the needs in most application scenarios. The network administrator shall configure effective rate-limiting threshold and attack threshold according to the actual application scenario.

Protocol	match	policy per-src-ip	policy per-src-mac	policy per-port
RIP	etype 0x0800 protocol	rate-limit 100 attatch-thresho ld 150	Not applicable	rate-limit 300 attatch-threshold 500

	17			
	dst-port			
	520			
RIPng	etype	rate-limit 100	Not applicable	rate-limit 300
	0x86dd	attatch-thresho		attatch-threshold
	protocol	ld 150		500
	17			
	dst-port			
	521			
BGP	etype	rate-limit 1000	Not applicable	rate-limit 2000
	0x0800	attatch-thresho		attatch-threshold
	protocol	ld 1200		3000
	6			
	dst-port			
	179			
BPDU	dst-mac	Not applicable	rate-limit 20	rate-limit 100
	0180.c2		attatch-threshol	attatch-threshold
	00.0000		d 40	100
RERP	dst-mac	Not applicable	rate-limit 20	rate-limit 100
	01d0.f80		attatch-threshol	attatch-threshold
	0.0001		d 40	100
REUP	dst-mac	Not applicable	rate-limit 20	rate-limit 100
	01d0.f80		attatch-threshol	attatch-threshold
	0.0007		d 40	100
BGP	etype	Not applicable	Not applicable	Not applicable
	0x0800			
	protocol			
	6			
	dst-port			
	179			
OSPFv	etype	rate-limit 800	Not applicable	rate-limit 2000
2	0x0800	attatch-thresho		attatch-threshold
	protocol	ld 1200		3000
	89			
OSPFv	etype	rate-limit 800	Not applicable	rate-limit 2000
3	0x86dd	attatch-thresho		attatch-threshold
	protocol	ld 1200		3000
	89			
VRRP	etype	rate-limit 64	Not applicable	rate-limit 1024
	0x0800	attatch-thresho		attatch-threshold
	protocol	ld 100		1024
	112			
IPv6	etype	rate-limit 64	Not applicable	rate-limit 1024
VRRP	0x86dd	attatch-thresho		attatch-threshold
	protocol	ld 100		1024

	112			
SNMP	ettype	rate-limit 1000	Not applicable	rate-limit 2000
	0x0800	attatch-thresho		attatch-threshold
	protocol	ld 1200		3000
	17			
	dst-port			
	161			
RSVP	ettype	rate-limit 800	Not applicable	rate-limit 1200
	0x0800	attatch-thresho		attatch-threshold
	protocol	ld 1200		1500
	46			
LDP	ettype	rate-limit 10	Not applicable	rate-limit 100
(UDP	0x0800	attatch-thresho		attatch-threshold
hello)	protocol	ld 15		150
	17			
	dst-port			
	646			



### Caution

Defined guard is intended to furthest include existing protocol types and facilitate new protocol type extension. It allows free combinations of type fields. If improperly configured, it will result in abnormal network. Therefore, the network administrator shall have a good command of network protocols. This table shows the effective configurations for popular protocols, and the administrator can configure accordingly. For other protocols which have been listed in the table, configurations shall be made with caution.

## Configuring Attacker Isolation Period

By default, the attacker isolation period is 0, namely the attacker won't be isolated.

Command	Function
<b>Ruijie#configure terminal</b>	Enter global configuration mode.
<b>Ruijie(config)#nfpp</b>	Enter NFPP configuration mode.
<b>Ruijie(config-nfpp)#define name</b>	Enter defined guard configuration mode
<b>Ruijie(config-nfpp)#isolate- period {seconds   permanent}</b>	Configure attacker isolation period Range: 0 and 30-86400 seconds (i.e., one day); default value is 0 second, meaning no isolation; <b>permanent</b> means permanent isolation.
<b>Ruijie(config-nfpp)#end</b>	Return to privilege mode.
<b>Ruijie#configure terminal</b>	Enter global configuration mode.

<b>Ruijie(config)#interface</b> <i>interface-name</i>	Enter interface configuration mode.
<b>Ruijie(config-if)# nfpp</b> <b>define</b> <i>name</i> <b>isolate-period</b> { <i>seconds</i>   <b>permanent</b> }	Configure attacker isolation period on the port. Range: 0 and 180-86400 seconds (i.e., one day). By default, the local isolation period is not configured, and the global isolation period will be used. The value of 0 means no isolation, and <b>permanent</b> means permanent isolation.
<b>Ruijie(config-if)#end</b>	Return to privileged EXEC mode.
<b>Ruijie#show nfpp define</b> <b>summary</b> <i>name</i>	Verify configurations.
<b>Ruijie#copy running-config</b> <b>startup-config</b>	Save configurations.

To restore global isolation period to the default value, execute "**no isolate-period**" command in NFPP defined guard configuration mode. If one port has been configured with local isolation period and it is now expected to apply the global isolation period, execute "**no nfpp define** *name* (name of defined guard) **isolate-period**" in interface configuration mode to delete the configuration of local isolation period.

## Configuring Attacker Monitoring Period

If the isolation period is 0 (i.e., no isolation), the guard module will automatically monitor the attacker as per the monitoring period configured and provide information about the existing attackers in the system. When the isolation period is configured to a non-zero value, the guard module will automatically isolate the host being monitored.

Command	Function
<b>Ruijie#configure terminal</b>	Enter global configuration mode.
<b>Ruijie(config)#nfpp</b>	Enter NFPP configuration mode.
<b>Ruijie(config-nfpp)#define</b> <i>name</i>	Enter defined guard configuration mode
<b>Ruijie(config-nfpp)#</b> <b>monitor-period</b> <i>seconds</i>	Configure attacker monitoring period. Range: 180-86400 seconds (i.e., one day); default value is 600 seconds.
<b>Ruijie(config-nfpp)#end</b>	Return to privileged EXEC mode.
<b>Ruijie#show nfpp define</b> <b>summary</b> <i>name</i>	Verify configurations.
<b>Ruijie#copy running-config</b> <b>startup-config</b>	Save configurations.

To restore the monitoring period to default value, execute "**no monitor-period**" command in NFPP defined guard configuration mode.

**Caution**

When an attacker is detected and if the isolation period is 0, the attacker will be monitored, and the timeout timer is the monitoring period. During the process of software monitoring, when the isolation period is configured to a non-zero value, the attacker being monitored will be automatically isolated at hardware layer, and the timeout timer is the isolation period. The monitoring period will only make sense when the isolation period is 0.

Changing isolation period from a non-zero value to zero will directly delete the attackers on the relevant port instead of implementing software monitoring.

## Configuring the Maximum Number of Monitored Hosts

Command	Function
<b>Ruijie#configure terminal</b>	Enter global configuration mode.
<b>Ruijie(config)#nfpp</b>	Enter NFPP configuration mode.
<b>Ruijie(config-nfpp)#define <i>name</i></b>	Enter defined guard configuration mode
<b>Ruijie(config-nfpp)#monitored-host-limit <i>number</i></b>	Configure the maximum number of monitored hosts Range: 1-4294967295. By default, the maximum number of monitored hosts is 1000.
<b>Ruijie(config-nfpp)#end</b>	Return to privileged EXEC mode.
<b>Ruijie#show nfpp define summary <i>name</i></b>	Verify configurations.
<b>Ruijie#copy running-config startup-config</b>	Save configurations.

To restore the maximum number of monitored hosts to default value, execute "**no monitored-host-limit**" command in NFPP defined guard configuration mode.

If the maximum number of monitored hosts has reached the default value of 1000 and the administrator configures a value lower than 1000 by this time, the existing hosts being monitored won't be deleted, but the following message will be displayed to remind the administrator to clear a certain part of monitored hosts in order to effect the configuration: "%ERROR: The value that you configured is smaller than current monitored hosts 1000 (number of monitored hosts configured), please clear a part of monitored hosts."

**Caution**

When the table of monitored hosts is full, the following message will be displayed to remind the administrator: "%NFPP\_DEFINE-4-SESSION\_LIMIT: Attempt to exceed limit of name (name of defined guard type)'s 1000 (number of monitored hosts configured) monitored hosts."

## Configuring the Trusted Hosts Exempt from Monitoring

If the administrator expects not to monitor a host (i.e., the host is trusted), the command can be configured. IP packets from trusted hosts are allowed to be sent to the CPU. Trusted hosts can only be added after configuring the match rule.

Command	Function
<b>Ruijie#configure terminal</b>	Enter global configuration mode.
<b>Ruijie(config)#nfpp</b>	Enter NFPP configuration mode.
<b>Ruijie(config-nfpp)#define name</b>	Enter NFPP defined guard configuration mode
<b>Ruijie(config-nfpp-define)#tr usted-host {mac mac_mask   ip mask   IPv6/prefixlen}</b>	Configure trusted hosts exempt from monitoring. You can configure up to 500 entries.
<b>Ruijie(config-nfpp-define)#en d</b>	Return to privileged EXEC mode.
<b>Ruijie# show nfpp define trusted-host name</b>	Display the trusted hosts configured.
<b>Ruijie#copy running-config startup-config</b>	Save configurations.

In NFPP defined guard configuration mode, execute the corresponding "no" command to delete one entry of trusted host. Use "no" form of this command and "all" option to delete all trusted hosts.

To delete all trusted hosts:

```
Ruijie(config-nfpp-define)# no trusted-host all
```

Or to delete one trusted host:

```
Ruijie(config-nfpp)# no trusted-host 1.1.1.1 255.255.255.255
```



When match rule is not configured, the following prompting message will be displayed: "%ERROR: Please configure match rule first."

While adding an IPv4 trusted host but the etype of match rule is not IPv4, the following prompting message will be displayed: "%ERROR: Match type can't support IPv4 trusted host."

While adding an IPv6 trusted host but the etype of match rule is not IPv6, the following prompting message will be displayed: "%ERROR: Match type can't support IPv6 trusted host."

When the table of trusted hosts is full, the following prompting message will be displayed: "%ERROR: Attempt to exceed limit of 500 trusted hosts."

When the table of monitored hosts contains an entry matching a trusted host (with same IP address), the system will automatically delete the corresponding entry of this IP address.

When it is failed to delete a trusted host, the following prompting message will be displayed "%ERROR: Failed to delete trusted host 1.1.1.0 255.255.255.0 (the trusted host configured)."

When it is failed to add a trusted host, the following prompting message will be displayed "%ERROR: Failed to add trusted host 1.1.1.0 255.255.255.0 (the trusted host configured)."

When a trusted host to be added exists already, the following prompting message will be displayed "%ERROR: Trusted host 1.1.1.0 255.255.255.0 (the trusted host configured) has already been configured."

When a trusted host to be deleted doesn't exist, the following prompting message will be displayed "%ERROR: Trusted host 1.1.1.0 255.255.255.0 (the trusted host configured) is not found."

When it is unable to allocate memory for a trusted host, the following message will be displayed "%ERROR: Failed to allocate memory."

---

## Host-based rate-limit and attack detection

The host detection method shall be determined according to the guard policy, including host detection based on source IP/VID/Port (per-src-ip) and host detection based on source MAC/VID/Port (per-src-mac). These two methods can apply or not at the same time. To effect host detection, the user must configure the rate-limiting threshold and attack threshold for such method. Each host has



rate-limiting threshold and attack threshold (also called the alert threshold), and the rate-limiting threshold shall be lower than the attack threshold. When the data rate of defined type of packets from a single host exceeds the rate-limiting threshold, the excessive packets will be discarded. If the data rate of defined type of packets from a single host exceeds the attack threshold, the host will be isolated and logged, and the Trap will be sent as well.

When attack is detected, the following log information will be displayed:

```
%NFPP_DEFINE_GUARD-4- DOS_DETECTED: Host<IP=1.1.1.1,MAC= N/A,port=Gi4/1,VLAN=1>
was detected by name(name of defined guard). (2009-07-01 13:00:00)
```

The Traps sent will include the following descriptive information:

Name (guard name) DoS attack from host<IP=1.1.1.1, MAC= N/A,port=Gi4/1,VLAN=1> was detected.

If the administrator sets the isolation period to a non-zero value, the following log information will be displayed when hardware isolation is successful:

```
%NFPP_DEFINE_GUARD-4-ISOLATED: Host<IP=1.1.1.1, MAC= N/A ,port=Gi4/1,VLAN=1> was
isolated by name (name of defined guard). (2009-07-01 13:00:00)
```

The Traps sent will include the following descriptive information:

Host<IP=1.1.1.1,MAC=N/A,port=Gi4/1,VLAN=1> was isolated by name (name of defined guard).

If hardware isolation is failed (generally due to insufficient memory or insufficient hardware resources), the following log information will be displayed:

```
%NFPP_DEFINE_GUARD-4-ISOLATE_FAILED:Failed to isolate host<IP=1.1.1.1, MAC=
N/A ,port=Gi4/1,VLAN=1> by name (name of defined guard).(2009-07-01 13:00:00)
```

The Traps sent will include the following descriptive information:

Failed to isolate host<IP=1.1.1.1,MAC= N/A,port=Gi4/1,VLAN=1> by name (name of defined guard).

The administrator can configure in NFPP defined guard configuration mode and interface configuration mode:

Command	Function
<b>Ruijie#configure terminal</b>	Enter global configuration mode.
<b>Ruijie(config)#nfpp</b>	Enter NFPP configuration mode.
<b>Ruijie(config-nfpp)#define name</b>	Enter NFPP defined guard configuration mode.

<pre> Ruijie(config-nfpp-define)# define-policy {per-src-ip   per-src-mac} rate-limit-pps attack-threshold-pps </pre>	<p>Configure host-based rate-limiting threshold and attack threshold.</p> <p><b>per-src-ip</b> means to take data rate statistics of the host detected as per source IP/VID/port, while <b>per-src-mac</b> means to take data rate statistics of the host detected as per source MAC/VID/port.</p> <p><i>Rate-limit-pps</i> means the rate-limiting threshold (1-9999). By default, no rate limiting will be implemented. Packets exceeding the rate-limiting threshold will be discarded.</p> <p><i>Attack-threshold-pps</i> means the attack threshold (1-9999). When the packets of defined type exceed the attack threshold, an attack is considered existing and will be logged. The traps will be sent and the user will be isolated as per the isolation period configured.</p> <p>By default, no rate limiting will be implemented.</p> <p>The attack threshold must be greater than or equal to the rate-limiting threshold.</p>
<pre> Ruijie(config-nfpp)#end </pre>	<p>Return to privileged EXEC mode.</p>
<pre> Ruijie#configure terminal </pre>	<p>Enter global configuration mode.</p>
<pre> Ruijie(config)#interface interface-name </pre>	<p>Enter interface configuration mode.</p>

<b>Ruijie(config-if)#nfpp define <i>name</i></b> <b>policy {per-src-ip   per-src-mac}</b> <i>rate-limit-pps attack-threshold-pps</i>	<p>The local rate-limiting threshold and attack threshold configured will only apply to the associated port.</p> <p><b>per-src-ip</b> means to take data rate statistics of the host detected as per source IP/VID/port, while <b>per-src-mac</b> means to take data rate statistics of the host detected as per source MAC/VID/port.</p> <p><i>Rate-limit-pps</i> means the rate-limiting threshold (1-9999). By default, no rate limiting will be implemented. Packets exceeding the rate-limiting threshold will be discarded.</p> <p><i>Attack-threshold-pps</i> means the attack threshold (1-9999). When the packets of defined type exceed the attack threshold, an attack is considered existing and will be logged. The traps will be sent and the user will be isolated as per the isolation period configured.</p> <p>By default, the globally configured rate-limiting threshold and attack threshold will be used.</p> <p>The attack threshold must be greater than or equal to the rate-limiting threshold.</p>
<b>Ruijie(config-if)#end</b>	Return to privileged EXEC mode.
<b>Ruijie#show nfpp define summary <i>name</i></b>	Verify configurations.
<b>Ruijie#copy running-config startup-config</b>	Save configurations.

**Caution**

The priority of source MAC/VID/port based rate limiting is higher than that of source IP/VID/port based rate limiting.

The policy of port-based host detection shall be same with the global policy.

If per-src-ip policy is not configured globally, when configuring per-src-ip policy on the port, the following message will be displayed to remind the administrator that the configuration has failed: "%ERROR: name (name of defined guard) has not per-src-ip policy."

If per-src-mac policy is not configured globally, when configuring per-src-mac policy on the port, the following message will be displayed to remind the administrator that the configuration has failed: "%ERROR: name (name of defined guard) has not per-src-mac policy."

When it is unable to allocate memory for the attacker detected, the following message will be displayed to remind the administrator: "%NFPP\_DEFINE\_GUARD-4-NO\_MEMORY: Failed to allocate memory."

## Port-based rate-limit and attack detection

You can configure port-based rate-limiting threshold and attack threshold for the guard policy, and the rate-limiting threshold shall be lower than the attack threshold. When the data rate of defined type of packets from certain port exceeds the rate-limiting threshold, the excessive packets will be discarded. If the data rate of defined type of packets from certain port exceeds the attack threshold, the port will be logged and the Trap will be sent as well.

When the port is subject to ARP DoS attack, the following alert message will be displayed:

%NFPP\_DEFINE\_GUARD-4-PORT\_ATTACKED: name (name of defined guard) DoS attack was detected on port Gi4/1. (2009-07-01 13:00:00)

The Traps sent will include the following descriptive information:

Name (name of defined guard) DoS attack was detected on port Gi4/1.

The administrator can configure in NFPP defined guard configuration mode and interface configuration mode:

Command	Function
<b>Ruijie#configure terminal</b>	Enter global configuration mode.
<b>Ruijie(config)#nfpp</b>	Enter NFPP configuration mode.
<b>Ruijie(config-nfpp)#define name</b>	Enter NFPP defined guard configuration mode

<b>Ruijie(config-nfpp-define)#</b> <b>define-policy            per-port</b> <i>rate-limit-pps</i> <i>attack-threshold-pps</i>	<p>Configure host-based rate-limiting threshold and attack threshold.</p> <p><b>per-port</b> means to take data rate statistics as per the physical port receiving packets.</p> <p><i>Rate-limit-pps</i> means the rate-limiting threshold (1-9999). By default, no rate limiting will be implemented. Packets exceeding the rate-limiting threshold will be discarded.</p> <p><i>Attack-threshold-pps</i> means the attack threshold (1-9999). When the packets of defined type exceed the attack threshold, an attack is considered existing and will be logged. The traps will be sent and the user will be isolated as per the isolation period configured.</p> <p>By default, the globally configured rate-limiting threshold and attack threshold will be used.</p> <p>The attack threshold must be greater than or equal to the rate-limiting threshold.</p>
<b>Ruijie(config-nfpp)#end</b>	Return to privileged EXEC mode.
<b>Ruijie#configure terminal</b>	Enter global configuration mode.
<b>Ruijie(config)#interface</b> <i>interface-name</i>	Enter interface configuration mode.

<b>Ruijie(config-if)#nfpp define</b> <b>name policy per-port</b> <i>rate-limit-pps</i> <i>attack-threshold-pps</i>	<p>The local rate-limiting threshold and attack threshold configured will only apply to the associated port.</p> <p><b>per-port</b> means to take data rate statistics as per the physical port receiving packets.</p> <p><i>Rate-limit-pps</i> means the rate-limiting threshold (1-9999). By default, no rate limiting will be implemented. Packets exceeding the rate-limiting threshold will be discarded.</p> <p><i>Attack-threshold-pps</i> means the attack threshold (1-9999). When the packets of defined type exceed the attack threshold, an attack is considered existing and will be logged. The traps will be sent.</p> <p>By default, no rate limiting will be implemented.</p> <p>The attack threshold must be greater than or equal to the rate-limiting threshold.</p>
<b>Ruijie(config-if)#end</b>	Return to privileged EXEC mode.
<b>Ruijie#show nfpp define summary</b> <i>name</i>	Verify configurations.
<b>Ruijie#copy running-config startup-config</b>	Save configurations.



### Caution

The priority of host-based rate limiting is higher than that of port-based rate limiting.

If per-port policy is not configured globally, when configuring per-port policy on the port, the following message will be displayed to remind the administrator that the configuration has failed: "%ERROR: name (name of defined guard) has not per-port policy."

## Applying Defined-guard

The administrator can apply defined guard in NFPP configuration mode or interface configuration mode. This feature is disabled by default.

Command	Function
<b>Ruijie#configure terminal</b>	Enter global configuration mode.
<b>Ruijie(config)#nfpp</b>	Enter NFPP configuration mode.

<b>Ruijie(config-nfpp)# define name enable</b>	Globally enable defined guard. By default, defined guard is enabled on all ports.
<b>Ruijie(config-nfpp)#end</b>	Return to privileged EXEC mode.
<b>Ruijie#configure terminal</b>	Enter global configuration mode.
<b>Ruijie(config)#interface interface-name</b>	Enter interface configuration mode.
<b>Ruijie(config-if)#nfpp define name enable</b>	Enable defined guard attack on the port. By default, the local switch is not configured on the port, and the global switch will be adopted.
<b>Ruijie(config-if)#end</b>	Return to privileged EXEC mode.
<b>Ruijie#show nfpp define summary name</b>	Verify configurations.
<b>Ruijie#copy running-config startup-config</b>	Save configurations.

To disable defined guard, execute "no define name enable" command in NFPP configuration mode to globally disable the feature of defined guard, or execute "no define name enable" command in interface configuration mode to disable defined guard configured on the interface (to restore defined guard on interface, enable defined guard globally).



### Caution

When defined guard policy is not fully configured, the defined guard cannot be enabled, and the system will remind the user of the corresponding absent policy configurations.

When the name of defined attack doesn't exist, the following prompting message will be displayed: "%ERROR: The name is not exist."

When match type is not configured for the defined guard, the following prompting message will be displayed: "%ERROR: name (name of defined guard) doesn't match any type."

When the policy is not configured for the defined guard, the following prompting message will be displayed: "%ERROR: name (name of defined guard) doesn't specify any policy."

## Clearing Monitored Hosts

Isolated hosts will be released after certain period. To manually clear this host, the administrator can execute the following commands in the privileged EXEC mode.

Command	Function
<b>Ruijie# clear nfpp define hosts name [vlan vid] [interface interface-id] [ip-address] [mac-address]</b>	The parameters define the specific hosts to be cleared.

## Showing Defined-guard

### Showing defined guard configuration

Execute "**show nfpp define summary**" command to display defined guard configurations:

Command	Function
<b>Ruijie#show nfpp define summary</b> [ <i>name</i> ]	Display defined guard configurations. If "name" is not specified, the configurations of all defined guard policies will be displayed.

An example is shown below:

```
Ruijie# show nfpp define summary tcp

Define tcp summary:

match etype 0x0800 protocol 0x06

Maximum count of monitored hosts: 1000

Monitor period:300s

Format of column Rate-limit and Attack-threshold is per-src-ip/per-src-mac/per-port.

Interface Status Isolate-period Rate-limit Attack-threshold
Global      Enable  300          -/5/150      -/10/300
G 0/1       Enable  180          -/6/-        -/8/-
G 0/2       Disable 200          -/5/30       -/10/50
```

### Showing information about monitored hosts

Command	Function
<b>Ruijie# show nfpp define hosts</b> <i>name</i> [ <b>statistics</b>   <b>[[vlan vid] [interface interface-id] [ip-address] [mac-address]]</b> ]	Display hosts detected to be under attack. If no parameter is specified, all hosts detected to be under attack will be displayed. The parameters define the specific hosts to be displayed.

An example is shown below:

```
Ruijie#show nfpp define hosts tcp statistics

Define tcp:

success    fail    total
-----    ----    -----
100         20         120

Meaning: Totally 120 hosts are isolated, including 100 successful hosts and 20 failed hosts.

Ruijie#show nfpp define hosts tcp

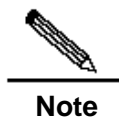
Define tcp:

If column 1 shows '*', it means "hardware do not 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)



### Note

The above fields mean VLAN ID, port, IP address, MAC address and remaining time of isolation.

If "\*" is displayed before the first column of fine line, it means that this host is currently subject to software monitoring or the hardware isolation has failed due to insufficient resources. When etype is IPv6, source IP based host isolation users will be displayed in the form of IPv6 address, and source MAC based host isolation users will be displayed in the form of MAC address.

## Showing trusted hosts exempt from monitoring

Execute "**show nfpp define trusted-host**" to display trusted hosts exempt from monitoring.

Command	Function
Ruijie# <b>show nfpp define trusted-host name</b>	Display trusted hosts exempt from monitoring.

An example is shown below:

```
Ruijie# show nfpp define trusted-host tcp
Define tcp:
IP address      mask
-----
1.1.1.0         255.255.255.0
1.1.2.0         255.255.255.0
Total:2 record(s)
```

## NFPP Syslog

### NFPP Syslog Overview

A NFPP log is generated in the NFPP syslog buffer area after detecting the attack. Use the NFPP log to generate the syslog at the specified rate and delete the NFPP log from the NFPP syslog buffer area.

NFPP syslog configuration commands include:

- Configuring NFPP log-buffer entry number
- Configuring the rate of generating NFPP syslog
- Configuring NFPP log filtering
- Clearing NFPP syslog
- Showing NFPP syslog

### Configuring NFPP log-buffer entry number

The administrator can configure the NFPP log-buffer entry number in the nfpp configuration mode.

Command	Function
Ruijie# <b>configure terminal</b>	Enter the global configuration mode.
Ruijie(config)# <b>nfpp</b>	Enter the nfpp configuration mode.
Ruijie(config-nfpp)# <b>log-buffer entries number</b>	Configure the NFPP log-buffer area size(in the range of 0-1024), 256 by default.
Ruijie(config-nfpp)# <b>end</b>	Return to the privileged EXEC mode.
Ruijie# <b>show nfpp log summary</b>	Show the configurations.

## Configuring the rate of generating NFPP syslog

The administrator can configure the rate of generating the NFPP syslog in the nfpp configuration mode.

Command	Function
Ruijie# <b>configure terminal</b>	Enter the global configuration mode.
Ruijie(config)# <b>nfpp</b>	Enter the nfpp configuration mode.
Ruijie(config-nfpp)# <b>log-buffer logs number_of_message interval length_in_seconds</b>	<p>Set the rate of generating the syslog from the NFPP syslog buffer area.</p> <p><i>number_of_message</i>  <i>/length_in_seconds</i>: The rate of generating the syslog. The correspondent information in the NFPP syslog buffer area will be removed while generating the syslog.</p> <p><i>number_of_message</i>: The valid range is 0-1024, the default value is 1. 0 indicates that all syslogs are recorded in the NFPP syslog buffer area and the syslog is not generated.</p> <p><i>length_in_seconds</i>: The valid range is 0-86400s(one day), the default value is 30s. 0 indicates to generate the syslog immediately.</p> <p>Setting the <i>number_of_message</i> and the <i>length_in_seconds</i> 0 indicates to generate the syslog immediately.</p>
Ruijie(config-nfpp)# <b>end</b>	Return to the privileged EXEC mode.
Ruijie# <b>show nfpp log summary</b>	Show the configurations.

## Configuring NFPP syslog filtering

The administrator can filter the NFPP syslog and record the syslog in the specific VLAN or on the specific interface.

Command	Function
Ruijie# <b>configure terminal</b>	Enter the global configuration mode.
Ruijie(config)# <b>nfpp</b>	Enter the nfpp configuration mode.
Ruijie(config-nfpp)# <b>logging</b> <b>vlan</b> <i>vlan-range</i>	Specify the syslog recorded in the VLAN;
Ruijie(config-nfpp)# <b>logging</b> <b>interface</b> <i>interface-id</i>	Specify the syslog recorded on the port.  By default, all syslogs are recorded.
Ruijie(config-nfpp)# <b>end</b>	Return to the privileged EXEC mode.
Ruijie# <b>show nfpp log summary</b>	Show the configurations.

## Clearing NFPP syslog

Command	Function
Ruijie# <b>clear nfpp log</b>	Clear the NFPP syslog in the log-buffer area.

## Showing NFPP syslog

Command	Function
Ruijie# <b>show nfpp log summary</b>	Show the NFPP syslog configuration.
Ruijie# <b>show nfpp log buffer</b> <b>[statistics]</b>	Show the NFPP syslog in the log-buffer area.  The parameter <b>statistics</b> shows the log number in the log-buffer area.

The following example shows the NFPP syslog 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 shows the NFPP syslog number in the log-buffer area:

```
Ruijie#show nfpp log buffer statistics
There are 6 logs in buffer.
```

The following example shows the NFPP syslog buffer area:

```
Ruijie#show nfpp log buffer

Protocol VLAN  Interface IP address MAC address      Reason      Timestamp
-----
ARP      1      Gi0/1      1.1.1.1      -           DoS          2009-05-30 16:23:10
ARP      1      Gi0/1      1.1.1.1      -           ISOLATED     2009-05-30 16:23:10
ARP      1      Gi0/1      1.1.1.2      -           DoS          2009-05-30 16:23:15
ARP      1      Gi0/1      1.1.1.2      -           ISOLATE_FAILED 2009-05-30 16:23:15
ARP      1      Gi0/1      -            0000.0000.0001 SCAN         2009-05-30 16:30:10
ARP      -      Gi0/2      -            -           PORT_ATTACKED 2009-05-30 16:30:10
```

Field	Description
Protocol	Includes ARP,IP,ICMP,DHCP,DHCPv6,NS-NA,RS,RA-REDIRECT
Reason	Includes DoS,ISOLATED,ISOLATED_FAILED,SCAN,PORT_ATTACKED.



If the syslog buffer area is full, the subsequent syslog will be discarded and an entry with all attributes “-” will be shown in the syslog buffer area. The administrator shall increase the capacity of the syslog buffer area or improve the rate of generating the syslog.

The syslog that generated from the syslog buffer area carries with the event 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)
```



## ACL and QoS Configuration

---

1. Access Control List Configuration
2. QoS Configuration

# Access Control List Configuration

## Overview

---

As part of our security solution, ACL is used to provide a powerful data flow filtering function. At present, our product supports the following access lists:

- IP access control list(Standard/Extended)
- MAC extended access control list
- Expert extended access control list
- IPV6 extended access control list

Depending on the conditions of networks, you can choose different access control lists to control data flows.

## Access Control List Introduction

---

ACL is the shortened form of Access Control Lists, or Access Lists. It is also popularly called firewall, or packet filtering in some documentation. ACL controls the messages on the device interface by defining some rules: Permit or Deny. According to usage ranges, they can be divided into ACLs and QoS ACLs.

By filtering the data streams, you can restrict the communication data types in the network and restrict the users of the network and the device they can use. When data streams pass the switch, ACLs classify and filter them, that is, check the data streams input from the specified interface and determine whether to permit or deny them according to the matching conditions.

To sum up, the security ACL is used to control which dataflow is allowed to pass through the network device. The QoS policy performs priority classification and processing for the dataflow.

ACLs consist of a series of entries, known as Access Control Entry (ACE). Each entry specifies its matching condition and behavior.

Access list rules can be about the source addresses, destination addresses, upper layer protocols, time-ranges or other information of data flows.

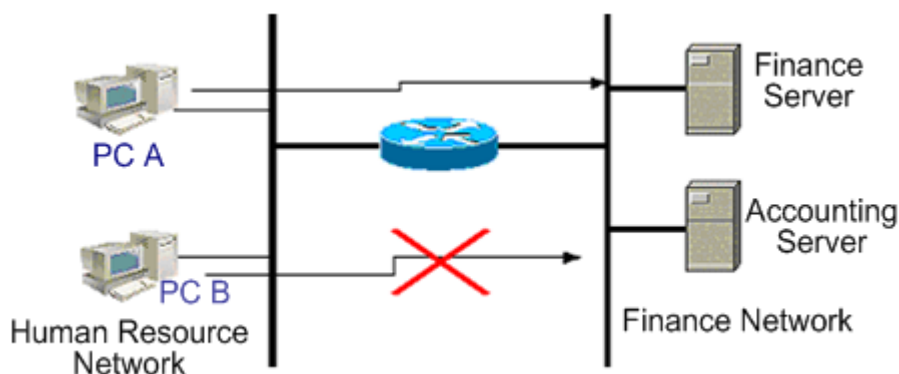
## Why to Configure Access Lists

---

There are many reasons why we need configure access lists. Some of them are as follows:

- Restrict route updating: Control where to send and receive the route updating information.
- Restrict network access: To ensure network security, by defining rules, make users unable to access some services. (When a user only need access the WWW and E-mail services, then other services like TELNET are disabled). Or, allow users to access services only during a given period or only allow some hosts to access networks.

Figure 1 is a case. In the case, only host A is allowed to access Finance Network, while Host B is disallowed to do so. See Figure 1.



**Figure 1 Using Access List to Control Network Access**

## When to Configure Access Lists

Depending on your requirements, you can select the basic access list or dynamic access list. In general, the basic access list can meet the security requirement. However, experienced hackers may use some software spoof source address and cheat the devices so as to gain accesses. Before the user can access the network, the dynamic access list requires the pass of authentication so that the hackers are difficult to invade the network. So, in some sensitive areas the dynamic access list can be used to ensure the network security.



### Note

A inherent problem of all access lists is electric spoofing, the behavior of providing spoof source addresses to deceive switches. Even you use the dynamic list, a spoofing problem occurs. During the valid access period of an authenticated user, a hacker may use a counterfeit user address and accesses the network. There are two methods to resolve the problem. One method is to set free time for a user to access the network as little as possible, making it hard for a hacker to attack the network. Another method is to use the IPSEC encryption protocol to encrypt network data, ensuring that all the data entering switches are encrypted.

Access lists are usually configured in the following locations of network devices:

- Devices between the inside network and outside network (such as the Internet)
- Devices at the borders of two parts in a network
- Devices on the access control port

The execution of the ACL statements must follow the order in the table strictly. Starting from the first statement, once the header of a packet matches a conditional judge statement in the table, the sequential statements are ignored.

## Input/Output ACL, Filtering Domain Template and Rule

When a device interface receives a message, the input ACL checks whether the message matches an ACE of the ACL input on the interface. When a device interface is ready to output a message, the output ACL



checks whether the message matches an ACE of the ACL output on the interface.

When detailed filtering rules are formulated, all or some of the above eight items may be used. As long as the message matches one ACE, the ACL processes the message as the ACE defined (permit or deny). The ACE of an ACL identifies Ethernet messages according to some fields of Ethernet messages. The fields include the following:

**Layer-2 fields:**

- 48-bit source MAC address (all the 48 bits must be declared)
- 48-bit destination MAC address (all the 48 bits must be declared)
- 16-bit layer-2 type field

**Layer 3 fields:**

- Source IP address field (you can specify all the 32 bits of the IP address, or specify a type of streams of the defined subnet)
- Destination IP address field (you can specify all the 32 bits of the IP address, or specify a type of streams of the defined subnet)
- Protocol type fields

**Layer-4 fields:**

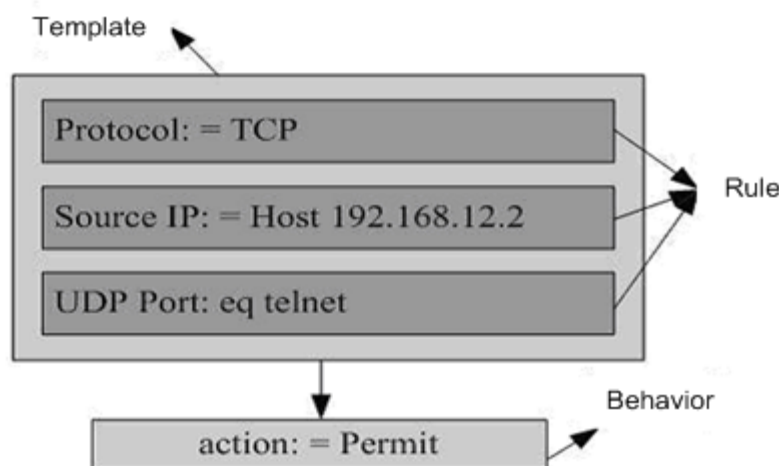
- You can specify one UDP source port, destination port, or both
- You can specify one UDP source port, destination port, or both

The filtering domain consists of the fields in the packets based on which the packets are identified and classified when you create an ACE. A filtering domain template is the definition formed by these fields. For example, when one ACE is generated, you want to identify and classify messages according to the destination IP field of a message. When another ACE is generated, you want to identify and classify messages according to the source IP address field of a message and the source port field of UDP. In this way, these two ACEs use different filtering domain templates.

Rules refer to the values of the ACE mask. For example, one ACE is:

**permit tcp host 192.168.12.2 any eq telnet**

In this ACE, the filtering domain template is a collection of the following fields: Source IP Address Fields, IP Protocol Fields and Destination TCP Port Fields. Corresponding values (rules) are respectively as follows: Source IP Address=host 192.168.12.2; IP Protocol=tcp; TCP Destination Port=telnet.



**Figure 2 Analysis of the ACE: permit tcp host 192.168.12.2 any eq telnet**



**Note**

A filtering domain template can be the collection of L3 fields (Layer 3 Field) and L4 fields (Layer 4 Field) or the collection of multiple L2 fields (Layer 2 Field). However, the filtering domain templates of a standard and extended ACL cannot be the collection of L2 and L3, L2 and 4, L2 and L3, or L4 fields. To use the combination of L2, L3 and L4 fields, it is possible to apply the Expert ACLs.



**Caution**

1. When associating SVI with the ACL at the outbound direction, you should note that:

- Standard IP ACL, extended IP ACL, extended MAC ACL and expert ACL are supported.
- There are some limits on matching the destination IP address and the destination MAC address in an ACL. When you configure to match the destination MAC address in an extended MAC ACL or expert ACL and then apply this ACL to the outbound direction of SVI, the entry will be set, but will not take effect. If you need to match the destination IP address not in the subnet IP range of the associated SVI in the standard IP ACL, extended IP ACL or expert ACL, this ACL will not take effect. For example, VLAN 1's IP address is 192.168.64.1 255.255.255.0. Now you create an ACL with the ACE of **deny udp any 192.168.65.1 0.0.0.255 eq 255** and apply this ACL at the egress of VLAN 1. This ACL will not function for the destination IP address is not in the subnet IP range of VLAN 1. If the ACE is **deny udp any 192.168.64.1 0.0.0.255 eq 255**, this ACL will take effect.

2. When configuring the expert ACL and applying it to the outbound direction of the interface, if some ACEs in the ACL contains the layer-3 matching information (such as IP, L4 port), it leads to the failure of controlling the non-IP packets transmitted on the interface by the ACL permit and deny rules.

- 
3. When applying the ACL, if the ACEs in the ACL (including IP access list and expert extended access list) match with the non-L2 field(such as SIP, DIP), the tagged MPLS packet matching is invalid.
- 

## Configuring IP Access List

---

To configure access lists on a device, you must specify unique names or numbers for the access lists of a protocol to uniquely identifying each access list inside the protocol. The following table lists the protocols that can use numbers to specify access lists and the number ranges of access lists that can be used by each protocol.

Protocol	Number Range
Standard IP	1-99, 1300 - 1999
Extended IP	100-199, 2000 - 2699

## Guide to configure IP Access List

---

When you create an access list, defined rules will be applied to all packet messages on a switch. The switch decides whether to forward or block a packet messages by judging whether the packet matches a rule.

Basic Access Lists include standard access lists and extended access lists. The typical rules defined in access lists are the following:

- Source address
- Destination address
- Upper layer protocol
- Time range

Standard IP access lists (1 – 99, 1300 – 1999) forward or block packets according to source addresses. Extended IP access lists (100 – 199, 2000 – 2699) use the above four combinations to forward or block packets. Other types of access lists forward or block packets according to related codes.

A single access list can use multiple separate access list sentences to define multiple rules. Where, all sentences use a same number or name to bind these sentences to a same access list. However, the more the used sentences are, the more difficult to read and understand an access list.

## Implicating “Deny Any Data Flow” Rule Sentence

---

The ending part of each access list implicates a “Deny any data flow” rule sentence. Therefore, if a packet matches no rule, then it is denied, as shown in the following example:

```
access-list 1 permit host 192.168.4.12
```

This list allows only the message of host 192.168.4.12 and denies any other host. This is because the list contains the following rule statement at the end: **access-list 1 deny any**

Here is another example:

```
access-list 1 deny host 192.168.4.12
```

If the list contains the only statement above, the messages from any host will be denied on the port.

**Caution**

It is required to consider the routing update message when defining the access list. Since the end of the access list “denies all dataflow”, this may cause all routing update messages blocked.

## Order to Input Rule Sentences

Each added rule is appended to the access list. If a sentence is created, then you cannot delete it separately and can only delete the whole access list. Therefore, the order of access list sentences is very important. When deciding whether to forward or block packets, a switch compares packets and sentences in the order of sentence creation. After finding a matching sentence, it will not check other rule sentences.

If you have created a sentence and it allows all data flows to pass, then the following sentences will not be checked, as shown in the following example:

```
access-list 101 deny ip any any
access-list 101 permit tcp 192.168.12.0 0.0.0.255 eq telnet any
```

Because the first rule sentence denies all IP messages, the host telnet message of the 192.168.12.0/24 network will be denied. Because the switch discovers that the messages match the first rule sentence, it will not check other rule sentences.

## Configuring IP Access List

The configuration of the basic access list includes the following steps:

1. Define a basic access list
2. Apply the access list to a specific interface.

There are two methods to configure a basic access list.

Method 1: Run the following command in the global configuration mode:

Command	Function
Ruijie(config)# <b>access-list id {deny   permit} {src src-wildcard   host src   any   interface idx} [time-range tm-rng-name]</b>	Define an access list
Ruijie(config)# <b>interface interface</b>	Select the interface to which the access list is to be applied.
Ruijie(config-if)# <b>ip access-group id { in   out }</b>	Apply the access list to the specific interface

Method 2: Run the following command in the ACL configuration mode:

Command	Function
Ruijie(config)# <b>ip access-list { standard   extended } { id   name }</b>	Enter the access list configuration mode
Ruijie (config-xxx-nacl)# <b>[sn] { permit   deny } {src src-wildcard   host src   any } [time-range tm-rng-name]</b>	Add table entries for ACL. For details, please see command reference.

Command	Function
Ruijie(config-xxx-nacl)# <b>exit</b> Ruijie(config)# <b>interface</b> <i>interface</i>	Exit from the access control list mode and select the interface to which the access list is to be applied.
Ruijie(config-if)# <b>ip access-group</b> <i>id</i> { <b>in</b>   <b>out</b> }	Apply the access list to the specific interface

Method 1 only configures the numerical value ACL. Method 2 can configure names and numerical value ACL and specify the priorities of table entries (in the devices that support ACE priority levels).

(The following introduces the operation principle of the reflected ACL:



#### Note

- a. Router auto-generates a temporary access list according to the L3, L4 information of the beginning traffic in the internal network based on the principles of protocol is constant, the source and destination IP addresses, and the source and destination ports are rigidly exchanged.
- b. Routers allows the traffic to flow into the internal network only when the L3, L4 information of returned traffic is matched with the one in the temporary access list previously created based on the outputting traffic. )

## Showing IP ACL

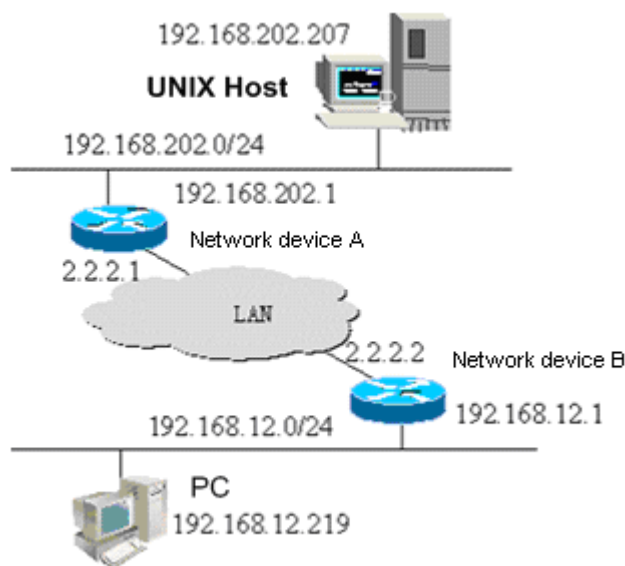
To monitor access lists, run the following command the in privileged user mode:

Command	Function
Ruijie# <b>show access-lists</b> [ <i>id</i>   <i>name</i> ]	Show the basic access list.

## IP ACL Example

### ■ Configuration requirements:

There are two network devices A and B, as shown in Figure 3:



**Figure-3 Basic Access List Example**

It is required to implement the following security functions by configuring access lists on device B.

1. Hosts at the 192.168.12.0/24 network section can only access the remote UNIX host TELNET service during the normal working time period and deny the PING service.
2. On the device B console, access to any of the services of hosts at the 192.168.202.0/24 network section is denied.



**Note**

The above case simplifies the application in the bank system. Namely, it only allows the hosts on the Local Area Network of branches or savings agencies to access the central host and disallows accessing the central host on the device.

## ■ Equipment Configuration

Device B configuration:

```
Ruijie(config)# interface GigabitEthernet 0/1
Ruijie(config-if)# ip address 192.168.12.1 255.255.255.0
Ruijie(config-if)# exit
Ruijie(config)# interface GigabitEthernet 0/2
Ruijie(config-if)# ip address 2.2.2.2 255.255.255.0
Ruijie(config-if)# ip access-group 101 in
Ruijie(config-if)# ip access-group 101 out
```

According to requirements, configure an extended access list numbered 101

```
access-list 101 permit tcp 192.168.12.0 0.0.0.255 any eq telnet time-range check
Ruijie(config)# access-list 101 deny icmp 192.168.12.0 0.0.0.255 any
Ruijie(config)# access-list 101 deny ip 2.2.2.0 0.0.0.255 any
Ruijie(config)# access-list 101 deny ip any any
```

Configure the time range

```
Ruijie(config)# time-range check
Ruijie(config-time-range)# periodic weekdays 8:30 to 17:30
```

**Note**

For access list 101, the last rule sentence "access-list 101 deny ip any" is not needed, for the ending part of the access list implicates a "deny any" rule sentence.

Device A configuration:

```
Ruijie(config)# hostname Ruijie
Ruijie(config)# interface GigabitEthernet 0/1
Ruijie(config-if)# ip address 192.168.202.1 255.255.255.0
Ruijie(config)# interface GigabitEthernet 0/2
Ruijie(config-if)# ip address 2.2.2.1 255.255.255.0
```

## Configuring Extended MAC Address-based Access Control List

To configure MAC address-based access control lists on a device, you must specify unique names or numbers for the access lists of a protocol to uniquely identifying each access list inside the protocol. The following table lists the range of the numbers that can be used to specify MAC access lists.

Protocol	Number Range
Extended MAC Access List	700-799

## Configuration Guide of Extended MAC Address-based Access Control List

When you create an expert access list, defined rules will be applied to all packet messages on a switch. The switch decides whether to forward or block a packet messages by judging whether the packet matches a rule.

The typical rules defined in MAC access lists are the following:

- Source MAC address
- Destination MAC address
- Ethernet protocol type
- Time-range

The MAC extended access list (number 700 – 799) forwards or blocks the packets based on the source and destination MAC addresses, and can also match the Ethernet protocol type.

A single MAC access list can use multiple separate access list sentences to define multiple rules. Where, all sentences use a same number or name to bind these sentences to a same access list.

## Configuring Extended MAC Address-based Access Control List

The configuration of an MAC access list includes the following steps:

1. Define an MAC access list
2. Apply the access list to a specific interface

There are two methods to configure an MAC access list.

Method 1: Run the following command in the global configuration mode:

Command	Function
Ruijie(config)# <b>access-list</b> id { <b>deny</b>   <b>permit</b> }{ <b>any</b>   <b>host</b> <i>src-mac-addr</i> } { <b>any</b>   <b>host</b> <i>dst-mac-addr</i> } [ <i>ethernet-type</i> ] [ <b>cos</b> <i>cos</i> ]	Define an access list. For details about commands, please see command reference.
Ruijie(config)# <b>interface</b> <i>interface</i>	Select the interface to which the access list is to be applied.
Ruijie(config-if)# <b>mac access-group</b> id { <b>in</b>   <b>out</b> }	Apply the access list to the specific interface

Method 2: Run the following command in the ACL configuration mode:

Command	Function
Ruijie(config)# <b>mac access-list extended</b> { <i>id</i>   <i>name</i> }	Enter the access list configuration mode
Ruijie (config-mac-nacl)# [ <i>sn</i> ] { <b>permit</b>   <b>deny</b> }{ <b>any</b>   <b>host</b> <i>src-mac-addr</i> } { <b>any</b>   <b>host</b> <i>dst-mac-addr</i> } [ <i>ethernet-type</i> ] [ <b>cos</b> <i>cos</i> ]	Add table entries for ACL. For details about commands, please see command reference.
Ruijie(config-mac-nacl)# <b>exit</b> Ruijie(config)# <b>interface</b> <i>interface</i>	Exit from the access control list mode and select the interface to which the access list is to be applied.
Ruijie(config-if)# <b>mac access-group</b> { <i>id</i>   <i>name</i> } { <b>in</b>   <b>out</b> }	Apply the access list to the specific interface



#### Note

Method 1 only configures the numerical value ACL. Method 2 can configure names and numerical value ACL and specify the priorities of table entries (they support priority ACE products).

## Showing Configuration of MAC Extended Access List

To monitor access lists, please run the following command the in privileged EXEC mode:

Command	Function
Ruijie# <b>show access-lists</b> [ <i>id</i>   <i>name</i> ]	Show the basic access list.

## MAC Extended Access List Example

It is required to implement the following security functions by configuring MAC access lists:

1. The 0013.2049.8272 host using the ipx protocol cannot access the giga 0/1 port of a device.
2. It can access other ports.



```
Ruijie> enable
Ruijie# configure terminal
Ruijie(config)# mac access-list extended mac-list
Ruijie(config-mac-nacl)# deny host 0013.2049.8272 any ipx
Ruijie(config-mac-nacl)# permit any any
Ruijie(config-mac-nacl)# exit
Ruijie(config)# interface gigabitEthernet 0/1
Ruijie(config-if)# mac access-group mac-list in
Ruijie(config-if)# end
Ruijie# show access-lists
mac access-list extended mac-list
deny host 0013.2049.8272 any ipx
permit any any
Ruijie#
```

**Note**

For access lists, "permit any any" cannot be discarded, for the ending part of an access list implicates a "deny any" rule sentence.

Extended MAC access list is not supported on the WAN interface (for example E1 interface).

## Configuring Expert Extended Access List

To configure expert extended access lists on a device, you must specify unique names or numbers for the access lists of a protocol to uniquely identifying each access list inside the protocol. The table below lists the number range of the Expert access list.

Protocol	Number Range
Expert extended access list	2700-2899

## Configuration Guide of Expert Extended Access List

When you create an expert extended access list, defined rules will be applied to all packet messages on a switch. The switch decides whether to forward or block a packet messages by judging whether the packet matches a rule.

The typical rules defined in expert access lists are the following:

All information in basic access lists and MAC extended access lists

VLAN ID

Expert extended access lists (2700 – 2899) are the syntheses of basic access lists and MAC extended access lists and can filter VLAN IDs.

A single expert access list can use multiple separate access list sentences to define multiple rules. Where, all sentences use a same number or name to bind these sentences to a same access list.

## Configuring Extended Expert ACL

The configuration of an expert access list includes the following steps:

1. Define an expert access list
2. Apply the access list to a specific interface (application particular case)

There are two methods to configure an expert access list.

Method 1: Run the following command in the global configuration mode:

Command	Function
Ruijie (config)# <b>access-list</b> <i>id</i> { <b>deny</b>   <b>permit</b> } [ <i>prot</i>   {[ <i>ethernet-type</i> ] [ <b>cos</b> <i>cos</i> ]}] [ <b>VID</b> <i>vid</i> ] { <b>src</b> <i>src-wildcard</i>   <b>host</b> <i>src</i>   <b>interface</b> <i>idx</i> } { <b>host</b> <i>src-mac-addr</i>   <b>any</b> } { <b>dst</b> <i>dst-wildcard</i>   <b>host</b> <i>dst</i>   <b>any</b> } { <b>host</b> <i>dst-mac-addr</i>   <b>any</b> } [ <b>precedence</b> <i>precedence</i> ] [ <b>tos</b> <i>tos</i> ] [ <b>dscp</b> <i>dscp</i> ] [ <b>fragment</b> ] [ <b>time-range</b> <i>tm-rng-name</i> ]	Define an access list. For details about commands, please see command reference.
Ruijie(config)# <b>interface</b> <i>interface</i>	Select the interface to which the access list is to be applied.
Ruijie(config-if)# <b>expert access-group</b> <i>id</i> { <b>in</b>   <b>out</b> }	Apply the access list to the specific interface

Method 2: Run the following command in the ACL configuration mode:

Command	Function
Ruijie(config)# <b>expert access-list extended</b> { <i>id</i>   <i>name</i> }	Enter the access list configuration mode
Ruijie (config-exp-nacl)# [ <i>sn</i> ]{ <b>permit</b>   <b>deny</b> } [ <i>prot</i>   {[ <i>ethernet-type</i> ] [ <b>cos</b> <i>cos</i> ]}] [ <b>VID</b> <i>vid</i> ] { <b>src</b> <i>src-wildcard</i>   <b>host</b> <i>src</i>   <b>interface</b> <i>idx</i> } { <b>host</b> <i>src-mac-addr</i>   <b>any</b> } { <b>dst</b> <i>dst-wildcard</i>   <b>host</b> <i>dst</i>   <b>any</b> } { <b>host</b> <i>dst-mac-addr</i>   <b>any</b> } [ <b>precedence</b> <i>precedence</i> ] [ <b>tos</b> <i>tos</i> ] [ <b>dscp</b> <i>dscp</i> ] [ <b>fragment</b> ] [ <b>time-range</b> <i>tm-rng-name</i> ]	Add table entries for ACL. For details about commands, please see command reference.
Ruijie(config-exp-nacl)# <b>exit</b> Ruijie(config)# <b>interface</b> <i>interface</i>	Exit from the access control list mode and select the interface to which the access list is to be applied.
Ruijie(config-if)# <b>expert access-group</b> { <i>id</i>   <i>name</i> } { <b>in</b>   <b>out</b> }	Apply the access list to the specific interface



#### Note

Method 1 only configures the numerical value ACL. Method 2 can configure names and the numerical value ACL. In a version supporting priority table entries, method 2 can also specify the priorities of table entries (the [*sn*] option in a command).

## Showing Configuration of Extended Expert ACL

To monitor access lists, please run the following command the in privileged user mode:

Command	Function
Ruijie# <b>show access-lists</b> [ <i>id</i>   <i>name</i> ]	Show the expert access list.

## Expert Extended Access List Example

It is required to implement the following security functions by configuring expert access lists:

The 0013.2049.8272 host using vlan 20 cannot access the giga 0/1 port of a device.

It cannot access other ports.

```
Ruijie> enable
Ruijie# config terminal
Ruijie(config)# expert access-list extended expert-list
Ruijie(config-exp-nacl)# permit ip vid 20 any host 0013.2049.8272 any any
Ruijie(config-exp-nacl)# deny any any any any
Ruijie(config-exp-nacl)# exit
Ruijie(config)# interface gigabitEthernet 0/1
Ruijie(config-if)# expert access-group expert-list in
Ruijie(config-if)# end
Ruijie# show access-lists
expert access-list extended expert-list
permit ip vid 20 any host 0013.2049.8272 any any
deny any any any any
```

## Configuring IPv6-based Extended Access List

### Configuring IPv6 Extended Access List

The configuration of an IPv6-based access list includes the following steps:

1. Define an IPv6 access list
2. Apply the access list to a specific interface (application particular case)

There is the following method to configure a basic access list. Run the following command in the ACL configuration mode:

Command	Function
Ruijie(config)# <b>ipv6 access-list</b> <i>name</i>	Enter the access list configuration mode
Ruijie (config-ipv6-nacl)# [sn] { <b>permit</b>   <b>deny</b> } prot { <i>src-ipv6-prefix/prefix-len</i>   <b>host</b> <i>src-ipv6-addr</i>   <b>any</b> } { <i>dst-ipv6-pfix/pfix-len</i>   <b>any</b>   <b>host</b> <i>dst-ipv6-addr</i> } [ <b>dscp</b> <i>dscp</i> ] [ <b>flow-label</b> <i>flow-label</i> ] [ <b>time-range</b> <i>tm-rng-name</i> ]	Add table entries for ACL. For details about commands, please see command reference.
Ruijie(config-exp-nacl)# <b>exit</b> Ruijie(config)# <b>interface</b> <i>interface</i>	Exit from the access control list mode and select the interface to which the access list is to be applied.

Command	Function
Ruijie(config-if)# <b>ipv6 traffic-filter</b> <i>name</i> {in   out}	Apply the access list to the specific interface

## Showing Configuration of IPv6 Extended Access List

To monitor access lists, please run the following command the in privileged user mode:

Command	Function
Ruijie# <b>show access-lists</b> [ <i>name</i> ]	Show the basic access list.

## IPv6 Extended Access List Example

It is required to implement the following security functions by configuring access lists:

The 192.168.4.12 host can access the gi 0/1 port of a device.

It cannot access other ports.

```
Ruijie> enable
Ruijie# config terminal
Ruijie(config)# ipv6 access-list v6-list
Ruijie(config-ipv6-nacl)# permit ipv6 ::192:68:4:12/24 any
Ruijie(config-ipv6-nacl)# deny ipv6 any any
Ruijie(config-ipv6-nacl)# exit
Ruijie(config)# interface gigabitEthernet 0/1
Ruijie(config-if)# ipv6 traffic-filter v6-list in
Ruijie(config-if)# end
Ruijie# show access-lists
ipv6 access-list extended v6-list
permit ipv6 ::192.168.4.12 any
deny any any
Ruijie#
```

## Configuring TCP Flag Filtering Control

The TCP Flag filtering feature provides a flexible mechanism. At present, TCP Flag filtering control supports the match-all option. Namely, when the TCP Flags in a received message exactly match those defined in the ACL table entry, the message will be checked by the ACL rule. A user can define any combination of TCP Flags to filter some messages with specific TCP Flags.

For example,

```
permit tcp any any match-all rst
```

Allow the messages with a TCP Flag RST set and 0 in other positions to pass



### Note

When the protocol number of the naming ACL and numerical value configuration is TCP, you can select to configure this filtering feature. MAC extended and IP standard ones do not have this function.

Please configure a TCP Flag by following these steps:

Command	Function
Ruijie(config)# <b>ip access-list extended</b> { id   name }	Enter the access list configuration mode
Ruijie(config-ext-nacl)# [sn] { <b>permit</b>   <b>deny</b> } <b>tcp</b> <b>source</b> source-wildcard [ operator port ] <b>destination</b> destination-wildcard [operator port] [match-all flag-name][precedence precedence]	Add table entries for ACL. For details about commands, please see command reference.
Ruijie(config-exp-nacl)# <b>exit</b>	Exit from the access control list mode and select the interface to which the access list is to be applied.
<b>Or</b>	
Ruijie(config)# <b>interface</b> interface	Exit from the access control list mode and select the interface to which the access list is to be applied.
Ruijie(config-if)# <b>ip access-group</b> {id   name} {in   out}	Apply the access list to the specific interface

The following example explains how to configure a TCP Flag

Enable permission and password

```
Ruijie> enable
Ruijie#
```

Enter the global configuration mode.

```
Ruijie# configure terminal
```

Enter the ACL configuration mode.

```
Ruijie(config)# ip access-list extended test-tcp-flag
```

Add an ACL entry

```
Ruijie(config-ext-nacl)# permit tcp any any match-all rst
```

Add a deny entry

```
Ruijie(config-ext-nacl)# deny tcp any any match-all fin
```

end

```
Ruijie(config-ext-nacl)# end
```

Show

```
Ruijie# show access-list test-tcp-flag
ip access-lists extended test-tcp-flag
10 permit tcp any any match-all rst
20 deny tcp any any match-all fin
```

## Configuring ACL Entries by Priority

To embody the ACE priority, there are standards for each ACL to normalize the ACE arranging method under the ACL by using the numbered start point – increment mode, as detailed below:

- ACE is sorted in the ascend order in the chain table by the sequential numbers.
- Starting from the start point number, if no number is specified, it increases by step on the basis of the previous ACE number.

- To specify number, the ACE is inserted in sorting mode, and the increment ensures new ACE can be inserted between two adjacent ACEs.
- The ACL specifies the start point number and the number increment.

The **ip access-list resequence** {acl-id/ acl-name} sn-start sn-inc command is available, with details in the related command reference.

Whenever the above command is run, the ACEs will be re-sorted under the ACL list. For example, the ACE numbers under the ACL named `tst_acl` is as follows:

In the beginning

```
ace1: 10
ace2: 20
ace3: 30
```

The ACE numbers are as follows after “**ip access-list resequence** `tst_acl 100 3`” is run:

```
Ruijie(config)# ip access-list resequence tst_acl 100 3
ace1: 100
ace2: 103
ace3: 106
```

When adding `ace4` without entering `sn-num`, the numbers are as follows:

```
Ruijie(config-std-nacl)# permit ...
ace1: 100
ace2: 103
ace3: 106
ace4: 109
```

When adding `ace5` by entering `seq-num = 105`, the numbers are as follows:

```
Ruijie(config-std-nacl)# 105 permit ...
ace1: 100
ace2: 103
ace5: 105
ace3: 106
ace4: 109
```

The reference of the numbers is to implement the priority adding ace mode.

Delete ACE

```
Ruijie(config-std-nacl)# no 106
ace1: 100
ace2: 103
ace5: 105
ace4: 109
```

The above numbers can also facilitate deleting ACE.

## Configuring ACL Based on Time-range

You can run the ACLs based on time, for example, make the ACL take effect during certain periods in a week. For this purpose, you must first set a Time-Range.

Time-Range implementation depends on the system clock. If you want to use this function, you must assure that the system has a reliable clock.

In the privileged configuration mode, you can create a time-range by performing the following steps:

Command	Function
Ruijie# <b>configure terminal</b>	Enter the global configuration mode.

Command	Function
Ruijie(config)# <b>time-range</b> <i>time-range-name</i>	Identify a time-range by using a meaningful display character string as its name
Ruijie(config-time-range)# <b>absolute</b> [ <b>start time date</b> ] <b>end time date</b>	Set the absolute time range (optional). For details, see the configuration guide of time-range.
Ruijie(config-time-range)# <b>periodic day-of-the-week time to</b> [ <i>day-of-the-week</i> ] <b>time</b>	Set the periodic time range (optional). For details, see the configuration guide of time-range.
Ruijie# <b>show time-range</b>	Verify the configurations.
Ruijie# <b>copy running-config startup-config</b>	Save the configuration.
Ruijie(config)# <b>ip access-list extended</b> <i>101</i>	Enter the ACL configuration mode.
Ruijie(config-ext-nacl)# <b>permit ip any any time-range</b> <i>time-range-name</i>	Configure the ACE of a time-range.

The length of the name should be 1-32 characters, which should not include any space.



#### Note

You can set one absolute time range at most. The application based on time-ranges will be valid only in this time range.

You can set one or more periodic intervals. If you have already set a running time range for the **time-range**, the application takes effect at periodic intervals in that time range.

The following example shows how to deny HTTP data streams during the working hours in a week by using the ACLs as example:

```
Ruijie(config)# time-range no-http
Ruijie(config-time-range)# periodic weekdays 8:00 to 18:00
Ruijie(config)# end
Ruijie(config)# ip access-list extended limit-udp
Ruijie(config-ext-nacl)# deny tcp any any eq www time-range no-http
Ruijie(config-ext-nacl)# exit
Ruijie(config)# interface gigabitEthernet 0/1
Ruijie(config-if)# ip access-group no-http in
Ruijie(config)# end
```

Example of displaying time range:

```
Ruijie# show time-range
time-range entry: no-http(inactive)
periodic Weekdays 8:00 to 18:00
time-range entry: no-udp
periodic Tuesday 15:30 to 16:30
```

## Configuring Security Tunnel

Applying a secure ACL globally means that the ACL is a security tunnel. A general ACL is installed on a

port or port map; a security tunnel is installed on an interface or globally. The difference between them arises in priority. The security tunnel takes precedence over port security (that is the IP binding under port security), 802.1x and secure ACL. The global security tunnel takes effect for all ports, unless you set a port as an exception port.



#### Note

- 1 A security tunnel supports permit and deny rules.
- 2 The global security tunnel takes no effect for an exception port.
- 3 The security tunnel policies enabled on an interface take precedence over the global security tunnel.
- 4 Without IP authorization, using a security tunnel in 802.1x will reduce the permitted authentication number at large extent, which is in accordance with the one under IP authorization.
- 5 It is strongly recommended to configure a security tunnel before authentication, so as to avoid the case that resource exhaustion causes the authenticated users cannot access the Interface due to the configuration of security tunnel midway.

You can use an exist ACL to configure a security tunnel

In the privileged configuration mode, execute the following commands to configure a global security tunnel:

Command	Function
Ruijie# <b>configure terminal</b>	Enter the global configuration mode.
Ruijie(config)# <b>security global access-group</b> <i>acl-name</i>	Configure a global security tunnel.

In the privileged configuration mode, execute the following commands to set an exception port:

Command	Function
Ruijie# <b>configure terminal</b>	Enter the global configuration mode.
Ruijie# <b>interface</b> <i>interface-id</i>	Enter the interface configuration mode.
Ruijie(config)# <b>security uplink enable</b>	Set the interface as an exception port..

If a security tunnel is configured under the interface, remove the security tunnel and then set the interface as the exception port.

In the privileged configuration mode, execute the following commands to configure a security tunnel on the interface:

Command	Function
Ruijie# <b>configure terminal</b>	Enter the global configuration mode.
Ruijie# <b>interface</b> <i>interface-id</i>	Enter the interface configuration mode.
Ruijie(config)# <b>security access-group</b> <i>acl-name</i>	Configure a security tunnel on the interface.

If the interface is set as an exception port, remove the setting and then configure the security tunnel on the interface.

The following example configures a security tunnel.

Set port 4 as security port and bind IP address and MAC address



```
Ruijie(config)#interface FastEthernet 0/4
Ruijie(config-if)#switchport port-security
Ruijie(config-if)#switchport port-security mac-address 0000.0000.0011 ip-address 192.168.6.3
```

Only the packets whose source IP address is 192.168.6.3 and MAC address is 0000.0000.0011 can flow in the device from port 4. To receive IPX packets, set a security tunnel as follows:

```
Ruijie#configure
Ruijie(config)#expert access-list extended safe_channel
Ruijie(config-exp-nacl)#permit ipx any any
Ruijie(config-exp-nacl)#exit
Ruijie(config)#security global access-group safe_channel
```

Or configure a security tunnel on the interface:

```
Ruijie#configure
Ruijie(config)#expert access-list extended safe_channel
Ruijie(config-exp-nacl)#permit ipx any any
Ruijie(config-exp-nacl)#exit
Ruijie(config)#interface FastEthernet 0/4
Ruijie(config-if)#security access-group safe_channel
```

## Configuring the List Remark

The ACL remark and ACE remark functions are provided for the ACL configuration and display.



### Note

- Up to one ACL remark and 2048 ACE remarks are configured in one ACL.
- The length of each remark is 100 bytes.
- The ACE remark is supported on the router only.

In the privileged configuration mode, execute the following commands to configure the ACL remark:

Command	Function
Ruijie# <b>configure terminal</b>	Enter the global configuration mode.
Ruijie(config)# <b>ip access-list standard id</b>	Enter the ACL configuration mode.
Ruijie(config-std-nacl)# <b>list-remark comment</b>	Configure the list remark.

You can also execute the following commands to set the ACL remark:

Command	Function
Ruijie# <b>configure terminal</b>	Enter the global configuration mode.
Ruijie(config)# <b>access-list id list-remark comment</b>	Set the ACL remark.

In the privileged configuration mode, execute the following commands to configure the ACE remark:

Command	Function
Ruijie# <b>configure terminal</b>	Enter the global configuration mode.
Ruijie(config)# <b>ip access-list standard id</b>	Enter the ACL configuration mode.
Ruijie(config-std-nacl)# <b>remark comment</b>	Configure the ACE remark.

You can also execute the following commands to set the ACE remark:

Command	Function
Ruijie# <b>configure terminal</b>	Enter the global configuration mode.
Ruijie(config)# <b>access-list</b> <i>id</i> <b>list-remark</b> <i>comment</i>	Set the ACE remark.

The following example configures the ACL remark and the ACE remark:

```
Ruijie(config)#ip access-list standard 1

Ruijie(config-std-nacl)#remark ace_remark_permit_62_start

Ruijie(config-std-nacl)#permit 192.168.197.62 0.0.0.0

Ruijie(config-std-nacl)#remark ace_remark_permit_62_end

Ruijie(config-std-nacl)#list-remark acl_remark_foo

Ruijie(config-std-nacl)#end

Ruijie#write

Ruijie#show access-lists 1

ip access-list standard 1

remark ace_remark_permit_62_start

10 permit host 192.168.197.62

remark ace_remark_permit_62_end

list-remark acl_remark_foo

Ruijie#
```

## Configuration Examples

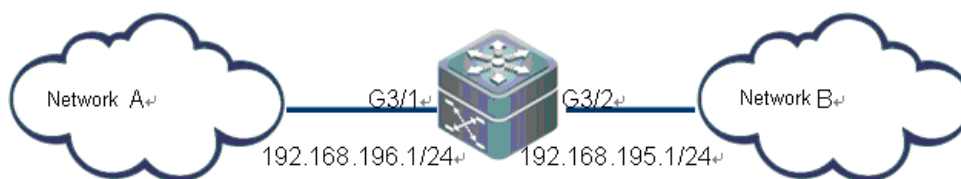
### Configuring Unidirectional TCP Connection

Configure TCP Flag filtering to enable unidirectional ACL.

### Configuration Requirements

For the security of network A, the hosts in network A are allowed to originate the TCP connection request to the hosts in network B. However, the hosts of network B are not allowed to originate the TCP communication requests to network A.

## Topology View



As shown in the above figure, two networks are connected through an intermediate device. Network A connects to the G3/1 port of the device and network B connects to the G3/2 port of the device.

## Analysis

By filtering the packets of TCP connection request originated by network B on the G3/2 port of the device, you can block the TCP connection request from hosts in network B to network A. According to the analysis of TCP connection, the SYN of the flag field in the TCP header of the initial TCP request packet is reset and the ACK is set to 0. Therefore, to enable network A to access network B in the one-way direction, configure the Match-all option of the extended ACL to set the SYN of the TCP header to 1 and ACK to 0 on the inbound direction of the G3/2 port.

## Configuration Steps

### 1) Define an Access Control List (ACL)

# Enter global configuration mode

```
Ruijie# configure terminal
```

# Create the extended ACL101 in the configuration mode

```
Ruijie(config)# ip access-list extended 101
```

# Deny the packets whose SYN is 1 and permit other packets whose SYN is 0 (including ACK)

```
Ruijie(config-ext-nacl)# deny tcp any any match-all SYN
```

# Permit other IP packets

```
Ruijie(config-ext-nacl)# permit ip any any
```

### 2) Apply the ACL at the interface

# Exit ACL mode

```
Ruijie(config-ext-nacl)# exit
```

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

```
Ruijie(config)# ip address 1.1.1.1 255.255.255.0
```

```
Ruijie(config)# interface gigabitEthernet 0/1
```

```
Ruijie(config-if)# ip access-group ifaddr in
```

# Enter the G3/2 port on which the ACL is applied

```
Ruijie(config)# interface gigabitEthernet 3/2
```

# Apply ACL 101 to the packet filtering at the inlet of G3/2

```
Ruijie(config-if)# ip access-group 101 in
```

### 3) Show the configuration of ACL

# In the privileged EXEC mode, use the **Show** command to display related configuration of ACL

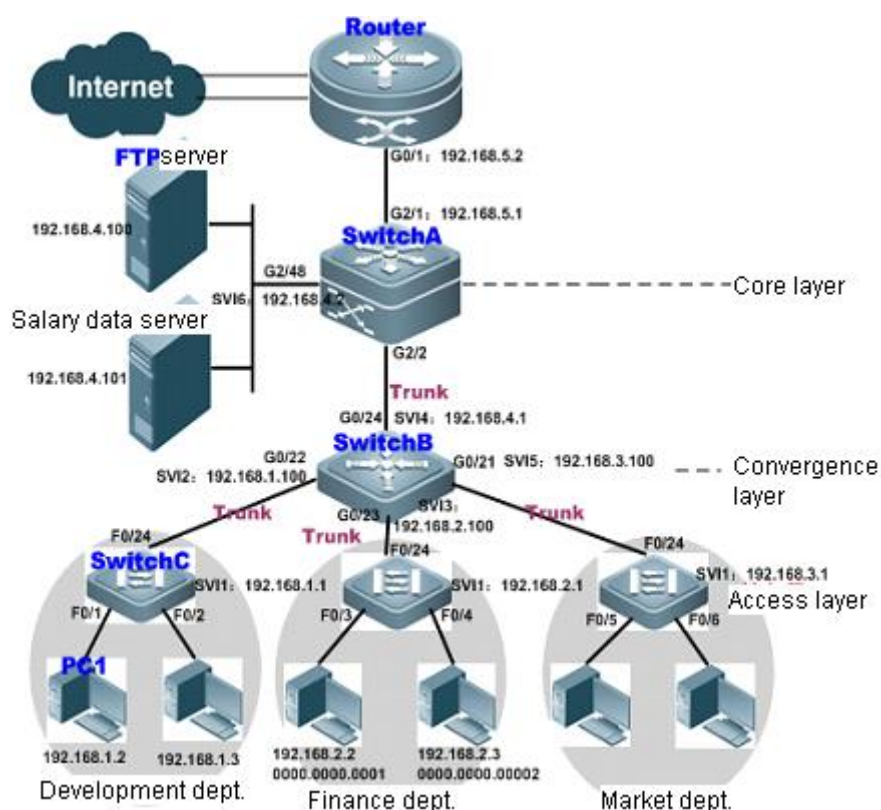
```

Ruijie# show access-lists 101
ip access-list extended 101
 10 deny tcp any any match-all syn
 20 permit ip any any

```

## Typical Application of Intranet ACL

### Networking Diagram



The above diagram shows the typical topology of an Intranet:

The access switch (SwitchC) connecting PCs of respective departments is connected to the convergence switch through 1000M optical fiber cable (trunk mode).

The convergence switch (SwitchB) assigns one VLAN for each department and is connected to the core switch through 10G optical fiber cable (trunk mode).

The core switch (SwitchA) is connected with multiple servers, such as FTP, HTTP server and etc, and is connected to Internet through firewall.

### Application Requirements

The above scenario of Intranet ACL application mainly involves the following needs:

1. Internet viruses are almost everywhere. Various vulnerable ports must be blocked in order to guarantee Intranet security.
2. Only the internal PCs can access the servers. External PCs are not allowed to access the servers.

3. PCs other than the finance department cannot access PCs of finance department; PCs other than the development department cannot access PCs of development department.
4. QQ, MSN and other IM applications cannot be used by the staff of development department during working hours (namely 9:00-18:00).

### Configuration Tips

---

1. The viruses can be avoided by configuring extended ACL on the router-connecting port (G2/1) of core switch (SwitchA) to filter packets destined for relevant ports.
2. As for the requirement that internal PCs can access the servers while external PCs are not allowed to access these servers, we can define the IP extended ACL and apply to ports (G2/2, SVI2) of the core switch (SwitchA) that connect with the convergence switch and server.
3. As for the requirement that specific departments cannot access each other, we can define the IP extended ACL (apply IP extended ACL to G0/22 and G0/23 of Switch B).
4. Configuring time & IP based extended ACL can prevent development departments from using QQ/MSN and other IM application during a specific period (applying time & IP based extended ACL to SVI2 of SwitchB).

### Configuration Steps

---

- Configure the core switch: SwitchA

#### Step 1: Define the virus-blocking ACL of "Virus\_Defence"

---

#### Configuration Guide

The worms viruses on the network will create a TFTP server on the local port of "udp/69" in order to transmit the binary virus program to other infected systems. While selecting the destination IP address, the worms will generally select the IP of subnet to which the infected system belongs, and then randomly select the attack target on Internet as per certain algorithm. Once the connection is established, the worms will send attack data to TCP ports (135, 445, 593, 1025, 5554, 9995, 9996), UDP ports (136, 445, 593, 1433, 1434) and UDP/TCP ports (135, 137, 138, 139) of targets. If the attack is successful, TCP/4444 port of target system will be used as the backdoor port. After that, worms will connect to this port and send tftp command in order to transmit virus file to the target system and run the file. The infected server will send substantive invalid data packets to the network, thus wasting network bandwidth and even causing failure of network devices and the network. In such a case, the extended ACL can be used to filter data packets destined for these ports.

---

```

SwitchA#configure terminal
SwitchA(config)#ip access-list extended Virus_Defence
! Block packets destined for internal and external TCP ports which may have been used by
viruses
SwitchA(config-ext-nacl)#deny tcp any any eq 135
SwitchA(config-ext-nacl)#deny tcp any eq 135 any
SwitchA(config-ext-nacl)#deny tcp any any eq 136
SwitchA(config-ext-nacl)#deny tcp any eq 136 any
SwitchA(config-ext-nacl)#deny tcp any any eq 137
SwitchA(config-ext-nacl)#deny tcp any eq 137 any
.....! The configuration is the same for other ports.
SwitchA(config-ext-nacl)#deny tcp any any eq 9996
SwitchA(config-ext-nacl)#deny tcp any eq 9996 any
! Block packets destined for internal and external UDP ports which may have been used by
viruses
SwitchA(config-ext-nacl)#deny udp any any eq 69
SwitchA(config-ext-nacl)#deny udp any eq 69 any
SwitchA(config-ext-nacl)#deny udp any any eq 135
SwitchA(config-ext-nacl)#deny udp any eq 135 any
SwitchA(config-ext-nacl)#deny udp any any eq 137
SwitchA(config-ext-nacl)#deny udp any eq 137 any
.....! The configuration is the same for other ports.
SwitchA(config-ext-nacl)#deny udp any any eq 1434
SwitchA(config-ext-nacl)#deny udp any eq 1434 any
! Block ICMP packets
SwitchA(config-ext-nacl)#deny icmp any any
! Permit all other IP packets
SwitchA(config-ext-nacl)#permit ip any any
SwitchA(config-ext-nacl)#exit

```

#### Step 2: Apply ACL "Virus\_Defence" to the router-connecting interface of core switch

```

SwitchA(config)#interface gigabitEthernet 2/1
SwitchA(config-if)#no switchport
SwitchA(config-if)#ip address 192.168.5.1 255.255.255.0
! Apply ACL "Virus_Defence" to the in direction of G2/1 to block virus packets from external
network
SwitchA(config-if)#ip access-group Virus_Defence in
SwitchA(config-if)#exit

```

#### Step 3: Define the ACL of "access\_server" to only permit Intranet PCs to access the server

```

SwitchA(config)#ip access-list extended access_server
! Only permit Intranet PCs to access the server (IP address being 192.168.4.100).
SwitchA(config-ext-nacl)#permit ip 192.168.2.0 0.0.0.255 host 192.168.4.100
SwitchA(config-ext-nacl)#permit ip 192.168.1.0 0.0.0.255 host 192.168.4.100
SwitchA(config-ext-nacl)#permit ip 192.168.3.0 0.0.0.255 host 192.168.4.100
SwitchA(config-ext-nacl)#deny ip any any

```

#### Step 4: Apply ACL "access\_server" to the interface connecting with convergence switch and server

```

SwitchA(config)#interface gigabitEthernet 2/2
SwitchA(config-if)#switch mode trunk
! Apply to the in direction on the interface of convergence switch
SwitchA(config-if)#ip access-group access_server in
SwitchA(config-if)#exit
! Create VLAN
SwitchA(config)#vlan 2
SwitchA(config-vlan)#exit
SwitchA(config)#interface gigabitEthernet 2/48

```

```

! The server-connecting interface of G2/48 belongs to vlan2
SwitchA(config-if)#switch access vlan 2
SwitchA(config-if)#exit
! Apply to the in direction of server-connecting interface
SwitchA(config)#interface vlan 2
SwitchA(config-if-VLAN 2)# ip access-group access_server in
SwitchA(config-if-VLAN 2)# ip address 192.168.4.2 255.255.255.0
SwitchA(config-ext-nacl)#end

```

## ● Configure the convergence switch: SwitchB

### Step 1: Create vlan2-4

```

SwitchB#configure terminal
! Create vlan2-4
SwitchB(config)#vlan range 2-4
SwitchB(config-vlan-range)#exit

```

### Step 2: Define ACL

#### ! Define IP extended ACL (vlan\_access1 and vlan\_access2)

```

SwitchB(config)#ip access-list extended vlan_access1

```

#### ! Prohibit finance department and market department from accessing the development department

```

SwitchB(config-ext-nacl)#deny ip 192.168.2.0 0.0.0.255 192.168.1.0 0.0.0.255
SwitchB(config-ext-nacl)#deny ip 192.168.3.0 0.0.0.255 192.168.1.0 0.0.0.255
SwitchB(config-ext-nacl)#permit ip any any
SwitchB(config)#ip access-list extended vlan_access2

```

#### ! Prohibit development department and market department from accessing the finance department

```

SwitchB(config-ext-nacl)#deny ip 192.168.1.0 0.0.0.255 192.168.2.0 0.0.0.255
SwitchB(config-ext-nacl)#deny ip 192.168.3.0 0.0.0.255 192.168.2.0 0.0.0.255
SwitchB(config-ext-nacl)#permit ip any any
SwitchB(config-ext-nacl)#exit

```

### Step 3: Apply ACLs of "vlan\_access1" and "vlan-access2" to the corresponding interfaces

```

! Configure G0/22 as a trunk port and apply vlan_access1
SwitchB(config)#interface GigabitEthernet 0/22
SwitchB(config-if)#switchport mode trunk
SwitchB(config-if)#ip access-group vlan_access1 in
! Configure G0/23 as a trunk port and apply vlan_access2
SwitchB(config)# interface GigabitEthernet 0/23
SwitchB(config-if)# switchport mode trunk
SwitchB(config-if)# ip access-group vlan_access2 in
! Configure G0/24 as a trunk port
SwitchB(config)#interface GigabitEthernet 0/24
SwitchB(config-if)#switchport mode trunk
! Configure IP address of SVI2.
SwitchB(config)#interface vlan 2
SwitchB(config-if)#ip address 192.168.1.100 255.255.255.0
! Configure IP address of SVI3.
SwitchB(config)#interface vlan 3
SwitchB(config-if)#ip address 192.168.2.100 255.255.255.0
! Configure IP address of SVI4.
SwitchB(config)#interface vlan 4
SwitchB(config-if)#ip address 192.168.4.1 255.255.255.0

```

### Step 4: Specify time range

```

! Define the time range of 9:00-18:00 from Monday to Friday
SwitchB#configure terminal

```

```
SwitchB(config)#time-range worktime
SwitchB(config-time-range)#periodic weekdays 9:00 to 18:00
```

### Step 5: Specify the traffic rule of development department

```
SwitchB#configure terminal
```

#### ! Create the extended ACL of "yanfa" in configuration mode

```
SwitchB(config)#ip access-list extended yanfa
```

#### ! Prohibit all hosts of development department from using QQ, MSN and other IM applications during 9:00-18:00 of every working day.

```
SwitchB(config-ext-nacl)#deny tcp 192.168.1.0 0.0.0.255 eq 8000 any time-range worktime
SwitchB(config-ext-nacl)#deny tcp 192.168.1.0 0.0.0.255 eq 8001 any time-range worktime
SwitchB(config-ext-nacl)#deny tcp 192.168.1.0 0.0.0.255 eq 443 any time-range worktime
SwitchB(config-ext-nacl)#deny tcp 192.168.1.0 0.0.0.255 eq 1863 any time-range worktime
SwitchB(config-ext-nacl)#deny tcp 192.168.1.0 0.0.0.255 eq 4000 any time-range worktime
SwitchB(config-ext-nacl)#deny udp 192.168.1.0 0.0.0.255 eq 8000 any time-range worktime
SwitchB(config-ext-nacl)#deny udp 192.168.1.0 0.0.0.255 eq 1429 any time-range worktime
SwitchB(config-ext-nacl)#deny udp 192.168.1.0 0.0.0.255 eq 6000 any time-range worktime
SwitchB(config-ext-nacl)#deny udp 192.168.1.0 0.0.0.255 eq 6001 any time-range worktime
SwitchB(config-ext-nacl)#deny udp 192.168.1.0 0.0.0.255 eq 6002 any time-range worktime
SwitchB(config-ext-nacl)#deny udp 192.168.1.0 0.0.0.255 eq 6003 any time-range worktime
SwitchB(config-ext-nacl)#deny udp 192.168.1.0 0.0.0.255 eq 6004 any time-range worktime
```

#### ! Permit all other IP traffic

```
SwitchB(config-ext-nacl)#permit ip any any
```

#### ! Apply ACL to the in direction of SVI2

```
SwitchB(config)#interface vlan 2
SwitchB(config-if)#ip access-group yanfa in
```

## Verifications

Step 1: Verify whether ACE entries are correct. The key is that whether the precedence order of entries is correct and whether entries are effective.

```
SwitchA#show access-lists
ip access-list extended Virus_Defence
10 deny tcp any any eq 135
20 deny tcp any eq 135 any
30 deny tcp any eq 4444 any
40 deny tcp any any eq 5554
50 deny tcp any eq 5554 any
60 deny tcp any any eq 9995
70 deny tcp any eq 9995 any
80 deny tcp any any eq 9996
90 deny tcp any eq 9996 any
100 deny udp any any eq tftp
110 deny udp any eq tftp any
120 deny udp any any eq 135
130 deny udp any eq 135 any
140 deny udp any any eq netbios-ns
150 deny udp any eq netbios-ns any
160 deny udp any any eq netbios-dgm
170 deny udp any eq netbios-dgm any
180 deny udp any any eq netbios-ss
190 deny udp any eq netbios-ss any
200 deny udp any any eq 445
```



```
210 deny udp any eq 445 any
220 deny udp any any eq 593
230 deny udp any eq 593 any
240 deny udp any any eq 1433
250 deny udp any eq 1433 any
260 deny udp any any eq 1434
270 deny udp any eq 1434 any
280 deny tcp any any eq 136
290 deny tcp any eq 136 any
300 deny tcp any any eq 137
310 deny tcp any eq 137 any
320 deny tcp any any eq 138
330 deny tcp any eq 138 any
340 deny tcp any any eq 139
350 deny tcp any eq 139 any
360 deny tcp any any eq 445
370 deny tcp any eq 445 any
380 deny tcp any any eq 593
390 deny tcp any eq 593 any
400 deny tcp any eq 1025 any
410 deny tcp any any eq 4444
420 deny icmp any any
430 permit tcp any any
440 permit udp any any
450 permit ip any any

ip access-list extended access_server
10 permit ip 192.168.2.0 0.0.0.255 host 192.168.4.100
20 permit ip 192.168.1.0 0.0.0.255 host 192.168.4.100
30 permit ip 192.168.3.0 0.0.0.255 host 192.168.4.100
40 deny ip any any
SwitchB#show access-lists
ip access-list extended vlan_access1
10 deny ip 192.168.2.0 0.0.0.255 192.168.1.0 0.0.0.255
20 deny ip 192.168.3.0 0.0.0.255 192.168.1.0 0.0.0.255
30 permit ip any any

ip access-list extended vlan_access2
10 deny ip 192.168.1.0 0.0.0.255 192.168.2.0 0.0.0.255
20 deny ip 192.168.3.0 0.0.0.255 192.168.2.0 0.0.0.255
30 permit ip any any

ip access-list extended yanfa
10 deny tcp 192.168.1.0 0.0.0.255 eq 8000 any time-range worktime (active)
20 deny tcp 192.168.1.0 0.0.0.255 eq 8001 any time-range worktime (active)
30 deny tcp 192.168.1.0 0.0.0.255 eq 443 any time-range worktime (active)
40 deny tcp 192.168.1.0 0.0.0.255 eq 1863 any time-range worktime (active)
50 deny tcp 192.168.1.0 0.0.0.255 eq 4000 any time-range worktime (active)
60 deny udp 192.168.1.0 0.0.0.255 eq 8000 any time-range worktime (active)
70 deny udp 192.168.1.0 0.0.0.255 eq 1429 any time-range worktime (active)
80 deny udp 192.168.1.0 0.0.0.255 eq 6000 any time-range worktime (active)
90 deny udp 192.168.1.0 0.0.0.255 eq 6001 any time-range worktime (active)
100 deny udp 192.168.1.0 0.0.0.255 eq 6002 any time-range worktime (active)
110 deny udp 192.168.1.0 0.0.0.255 eq 6003 any time-range worktime (active)
```

```
120 deny udp 192.168.1.0 0.0.0.255 eq 6004 any time-range worktime (active)
```

**Step 2: Verify whether ACL configurations are complete.** The key is that whether the correct ACL has been applied to the specified interface.

**SwitchA:**

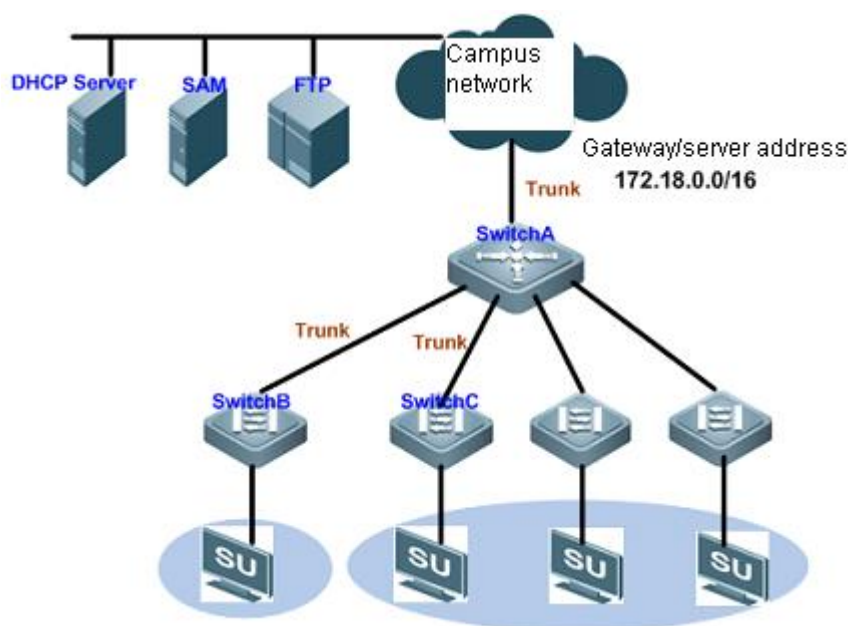
```
SwitchA#show run
interface GigabitEthernet 2/1
  no switchport
  no ip proxy-arp
  ip access-group Virus_Defence in
  ip address 192.168.5.1 255.255.255.0
!
interface GigabitEthernet 2/2
  switchport mode trunk
  ip access-group access_server in
!
interface VLAN 2
  no ip proxy-arp
  ip access-group access_server in
  ip address 192.168.4.2 255.255.255.0
```

**SwitchB:**

```
SwitchB#show run
!
interface GigabitEthernet 0/22
  switchport mode trunk
  ip access-group vlan_access1 in
!
interface GigabitEthernet 0/23
  switchport mode trunk
  ip access-group vlan_access2 in
!
interface VLAN 2
  no ip proxy-arp
  ip access-group yanfa in
  ip address 192.168.1.100 255.255.255.0
```

## Application of expert ACL & ACL80

### Networking Diagram



The above figure shows the simplified topology of campus network:

SwitchA is the convergence device assigning one VLAN for each faculty and is connected to the campus network through 10G optical fiber cable (trunk mode).

SwitchB and SwitchC are access devices connecting PCs of respective faculties, and are connected to the convergence switch through 1000M optical fiber cable (trunk mode).

SU client must be installed on each PC, which can only access network after passing 802.1x authentication.

### Application Requirements

SU software is not embedded in Windows. You must download and install SU client on the PC in order to pass authentication. However, the PC cannot download software without 802.1x authentication. To solve this problem, the following requirements must be met:

1. IP packets and ARP packets accessing the segment address of gateway/server (172.18.0.0/16) are allowed to pass through without authentication, so that the user PC can download software from the specified server or access gateway before authentication.
2. DHCP packets (UDP port number being 67/68) are allowed to pass through without authentication, so that the user PC can acquire the IP address in order to proceed with authentication.

### Configuration Tips

Configure ACL80 or expert ACL on the access device (SwitchB/SwitchC) and combine the feature of secure tunnel to permit certain packets without authentication.

In this case, ACL80 is configured on SwitchB and expert ACL is configured on SwitchC.

## Configuration Steps

---

### SwitchB

#### Configuration Guide

The customized ACL allows the user to define 64 bytes out of the first 80 bytes of packets to perform per-bit matching and filtering. The user-defined string will be compared with the string extracted from packet (1 means match and 0 means no match), so as to determine further action.

#### Step 1: Configure the customized ACL

```
SwitchB#configure terminal
```

! Create a customized ACL named "tongdao"

```
SwitchB(config)#expert access-list advanced tongdao
```

! Permit all ARP packets (protocol number being 0800, offset being 24) with source IP (the offset in the source IP of ARP packets is 40) falling within the network segment of 172.18.0.0 (hexadecimal value being ac12)

```
SwitchB(config-exp-dacl)#permit 0806 ffff 24 ac12 ffff 40
```

! Permit all IP packets (protocol number being 0800, offset being 24) with source IP (the offset in the source IP of IP packets is 38) falling within the network segment of 172.18.0.0 (hexadecimal value being ac12)

```
SwitchB(config-exp-dacl)#permit 0800 ffff 24 ac12 ffff 38
```

! Permit DHCP packets with UDP port being 67 (Bootstrap Protocol Server) and 68 (Bootstrap Protocol Client) (offset in protocol number being 35; hexadecimal value of 11 to indicate UDP; offset in port being 46; hexadecimal value of 43/44 corresponding to 67 and 68).

```
SwitchB(config-exp-dacl)# permit 11 ff 35 00440043 ffffffff 46
```

```
SwitchB(config-exp-dacl)#exit
```

#### Step 2: Globally configure the ACL for secure tunnel application

! Configure ACL "tongdao" for secure tunnel application

```
SwitchB(config)# security global access-group tongdao
```

### SwitchC

#### Step 1: Configure expert ACL

```
SwitchC#configure terminal
```

! In configuration mode, create an expert ACL named "tongdao1"

```
SwitchC(config)#expert access-list extended tongdao1
```

! Permit all IP packets with source IP falling within the network segment of 172.18.0.0

```
SwitchC(config-exp-dacl)#permit ip 172.18.0.0 0.0.255.255 any any any
```

! Permit all packets with UDP port number being 67 (Bootstrap Protocol Server) and 68 (Bootstrap Protocol Client)

```
SwitchC(config-exp-dacl)# permit udp any any eq bootpc any any eq bootps
```

```
SwitchC(config-exp-dacl)#exit
```

#### Step 2: Globally configure the ACL for secure tunnel application

! Configure ACL "tongdao1" for secure tunnel application

```
SwitchC(config)# security global access-group tongdao1
```

## Verifications

---

Step 1: Verify whether ACE entries are correct. The key is that whether the precedence order of entries is correct and whether entries are effective.

```
SwitchB# show access-lists
```

```

expert access-list advanced tongdao
10 permit 0806 FFFF 24 AC12 FFFF 40
20 permit 0800 FFFF 24 AC12 FFFF 38
30 permit 11 FF 35 00440043 FFFFFFFF 46
SwitchC# show access-lists
expert access-list extended tongdao1
10 permit ip 172.18.0.0 0.0.255.255 any any any
20 permit udp any any eq bootpc any any eq bootps

```

Execute the above command to verify whether the corresponding ACE entries are correct.

Step 2: Verify whether ACL configurations are complete. The key is that whether the correct ACL has been applied in the global configuration mode:

```

SwitchB#show run
!
expert access-list advanced tongdao
!
security global access-group tongdao
!
!
SwitchC#show run
!
expert access-list advanced tongdao1
!
security global access-group tongdao1
!
!

```

## Acl Configuration of Different Line Cards

Acl out has two processing methods:

When all the line cards online are the EB/EC line cards or the EA line cards, acl out can associate the outgoing port and takes effect for any packet, supporting associating svi, and router port with the outgoing port.

When there are other line cards among the line cards online, which are not the EA line cards, acl out takes effect only for known unicast packets and does not support router port. This principle is also appropriate for hot plugging/unplugging line cards, which prompts the users to reset line cards.

Note that when the non-E line cards are inserted in the chassis, ACL out association at the outbound direction on ACCESS port is valid for the known unicast packets forwarded in Layer2 only, but invalid for the broadcast packets and packets forwarded in Layer3.

If acl out is implemented on the exit port, then ip extension acl and expert acl will not support port matching. Besides, expert acl only supports ip packet matching, not other L2 packets, IPV6 does not support flow\_label, dscp and fragment matching.

If acl out is processed in the original way, then associating acl out with svi has lots of restrictions:

- 1) Changes the priority of in and out direction; the acl used in out direction is higher than that used in in direction.
- 2) When associating acl with svi in out direction, there is no **deny any any** option by default. But there is **deny any any** option in other acl application.

- 3) Associating acl with svi in Out direction can support ip standard, ip extension, mac extension, acl application of expert extension.
- 4) There are some restrictions for matching destination ip and destination mac in acl when associating acl with svi in Out direction. If you want to match destination mac in mac extension and expert acl and applicate the acl in out direction of svi, the entry will be set and not take effect.
- 5) The set acl will not take effect if you want to match destination ip, which is not within the subnet ip range of associated svi, in ip standard, ip extension and expert acl . For example, the address of vlan 1 is 192.168.64.1 255.255.255.0. And now, if you create an ip extended acl with ace deny udp any 192.168.65.1 0.0.0.255 eq 255, it will not take effect when applying this acl to the exit port of vlan 1, for the destination ip is not within the subnet ip range of vlan 1; but it will take effect if the ace is deny udp any 192.168.64.1 0.0.0.255 eq 255, for the destination ip is up to specification.
- 6) The priority of associating acl with svi in out direction is higher than that of all the other acl application.
- 7) Acl out does not support user-defined acl type.

# QoS Configuration

## QoS Overview

---

The fast development of the Internet results in more and more demands for multimedia streams. Generally, people have different service quality requirements for different multimedia, which requires the network to be able to allocate and dispatch resources according to the user demands. As a result, the traditional "best effort" forwarding mechanism cannot meet the user demands. So the QoS emerges.

The QoS (Quality of Service) is used to evaluate the ability for the service provider to meet the customer demands. In the Internet, the QoS mechanism is introduced to improve the network service quality, where the QoS is used to evaluate the ability of the network to deliver packets. The commonly-mentioned QoS is an evaluation on the service ability for the delay, jitter, packet loss and more core demands.

## Basic Framework of QoS

---

The devices that have no QoS function cannot provide the capability of transmission quality service, and will not ensure special forwarding priority for certain dataflow. When bandwidth is abundant, all the traffic can be well processed. But when congestion occurs, all traffic could be discarded. This kind of forwarding policy is otherwise called the service of best effect, since the device now is exerting its performance of data forwarding and the use of its switching bandwidth is maximized.

The device of this module features the QoS function to provide transmission quality service. This makes it possible to select specific network traffic, prioritize it according to its relative importance, and use congestion-management and congestion-avoidance techniques to provide preferential treatment. The network environment with QoS configured is added with predictability of network performance and allocates network bandwidth more effectively to maximize the use of network resources.

The QoS of this device is based on the DiffServ (Differentiated Service Mode) of the IETF Internet Engineering Task Force. According to the definitions in the DiffServ architecture, every transmission message is classified into a category in the network, and the classification information is included in the IP packet header. The first 6 bits in the ToS (Type of Service) field for IPv4 packet header or the Traffic Class field for IPv6 packet header carry the classification information of the message. The classification information can also be carried in the Link layer packet header. Below shows the special bits in the packet:

- Carried by the first 3 bits in the Tag Control Information of 802.1Q frame header, which contains the priority information of one of the 8 categories. These three bits are generally called User Priority bits.
- Carried by the first 3 bits of the ToS field for IPv4 packet header or Traffic Class field for IPv6 packet header, called IP precedence value; or carried by the first 6 bits of the ToS field for IPv4 packet header or Traffic Class field for IPv6 packet header, called Differentiated Services Code Point (DSCP) value.

In a DiffServ-compliant network, every device has the same transmission service policy for the messages with the same classification information, and vice versa. The class information in the packet can be assigned by all the systems along the way, such as hosts, devices, or other network devices. It's based on a policy set by a manager, or contents in the packet, or both. The assignment of class information in order

to identify packets usually consumes enormous resources of the network device. To reduce the processing overhead on the backbone network, such assignment is often used on the network edge. Based on the class information, the devices can provide different priorities for different traffic, or limit the amount of resources allocated per traffic class, or appropriately discard the packets of less important, or perform other operations as appropriate. This behavior of these independent devices is called per-hop behavior in the DiffServ architecture.

If all devices in the network are providing consistent per-hop behavior, this network forms the end-to-end QoS solution for the DiffServ architecture.

## QoS processing flow

---

### Classifying

---

The process of classifying involves putting the messages to the dataflow indicated with CoS value according to the trust policy or the analysis of the message contents. As a result, the core task of classifying is to determine the CoS value of a message. It happens when the port is receiving the inbound messages. When a port is associated with a policy-map that represents a QoS policy, the classification will take effect and be applied on all the messages input through that port.

For general non-IP messages, the switch classifies the messages according to the following criteria:

- If the message itself does not contain any QoS information, which means the layer-2 packet header has no User Priority bits, it gets the QoS information of the message by using the default CoS value of the message input port. Like the User Priority bits of the message, the default CoS value of the port ranges 0~7.
- If the message itself contains QoS information, which means the layer-2 packet header has User Priority bits, it gets the CoS information directly from the message.



#### Note

The above criteria take effect only when the QoS trust mode of the port is enabled. Enabling the QoS trust mode of a port does not mean getting the QoS information directly from the message or the input port of the message without analyzing the message contents.

- If the policy-map associated with the port is using the ACL classifying based on the MAC access-list extended, the associated ACLs will be matched by getting the source MAC address, destination MAC address and Ethertype domain of the message on that port, to determine the DSCP value of the message. Note that, if a port is associated with a policy-map but has no DSCP value set for it, the switch will assign the priority for the messages of this classification by performing the default behavior: following the priority information contained in the layer-2 packet header of the message or the default priority of the port.



**Note**

The above three criteria may apply simultaneously on the same port. In this case, they will take effect according to the sequence 3, then 2 and then 1. In other words, the ACLs work first for the classifying operation. When it fails, the criteria 2 will be used, and so on. Here, if the QoS trust mode of the port is enabled, criteria 2 and 1 will be used to get the QoS information directly from the message or the port; otherwise, default DSCP value 0 will be assigned for the messages failing the classifying operation.

For IP messages, the switch classifies the messages according to the following criteria:

- If the port trust mode is Trust ip-precedence, it extracts from the ip precedence field (3 bits) of the IP message and fills the CoS field (3 bits) of the output message.
- If the port trust mode is Trust cos, it extracts directly the CoS field (3 bits) of the message and overwrite the ip precedence field (3 bits) of the message. There are the following two cases. Case 1 is that the layer-2 packet header does not contain User Priority bits, and now the CoS value is got from the default CoS value of the message input port. Case 2 is that the layer-2 packet header contains User Priority bits, and now the CoS is got directly from the packet header.
- If the Policy-map associated with the port is using the ACLs classifying based on the ip access-list (extended), the associated ACLs will be matched by getting the source IP address, destination IP address, Protocol field and layer-4 TCP/UDP port field of the message, to determine the DSCP value of the message, and the CoS value is determined according to the mapping from DSCP to CoS. Note that, if a port is associated with a policy-map but has no DSCP value set for it, the switch will use the above criteria 1 and 2 to determine the priority.

Just like the criteria for non-IP message classifying, the above classifying criteria can apply on the same port at the same time. In this case, they will take effect according to the sequence 3, then 2 and then 1.

For the details of the CoS-to-DSCP map and IP-precedence-to-DSCP map, see the descriptions below.

## **Policing**

The Policing action happens after the data classifying is completed. It is used to constrain the transmission bandwidth occupied by the classified dataflow. The Policing action will check every message in the classified dataflow. If the message is occupying more bandwidth as allowed by the police that applies on that dataflow, the message will be treated specially, either to be discarded or assigned with another DSCP value.

In the QoS processing flow, the Policing action is optional. If no Policing action is enabled, the DSCP value of messages in the classified dataflow will remain unchanged, and no message will be discarded before the message is sent for the Marking action.

## **Marking**

After the Classifying and Policing actions, the Marking action will write the QoS information for the message to ensure the DSCP value of the classified message can be transferred to the next hop device in the network. Here, the QoS ACLs can be used to change the QoS information of the message, or the QoS information is reserved in the Trust mode. For example, the Trust DSCP can be selected to reserve the

DSCP information in the IP packet header.

## Queuing

---

The Queuing action is responsible for transferring the messages in the dataflow to an output queue of the port. The messages in different output queues will have transmission service policies of different levels and qualities.

Each port has 8 output queues. The two mapping tables DSCP-to-CoS Map and Cos-to-Queue Map configured on the switch convert the DSCP value of the message into output queue number so as to determine which output queue to transfer the messages into.

## Scheduling

---

The Scheduling action is the last cycle in the QoS process. After the messages are transferring into different output queues of the port, the switch works with WRR or another algorithm to transmit the messages in those 8 queues.

It is possible to set the weight in the WRR algorithm to configure the amount of messages to be transmitted in every cycle of message output, thus affecting the transmission bandwidth. Alternatively, it is possible to set the weight in the DRR algorithm to configure the amount of message bytes to be transmitted in every cycle of message output, thus affecting the transmission bandwidth.

## Switch Congestion Queue Number Control

---

Each port on the switch supports 8 output queues. The output buffer area resources shall be used when the queue is outputting the packets. The switch output buffer area resources are shared by all port queues, so if the output congestions of multiple queues on multiple ports occur at the same time, the output buffer area resources cannot address the satisfaction of all current output queues, leading to the inaccuracy of the congestion control policy (for example, the output scheduling algorithm is inaccurate.)

Ruijie switch provides the mechanism of output buffer area allocation of output congestion queues on the port. The following dynamic configuration mode and static configuration mode can be used:

### Dynamic Mode:

The device supports to plan the congestion queue number on all ports dynamically. Below are the rules:

- For the Gigabit interface, the buffer area resources shall be satisfied for the congestion of 8 queues at the same time.
- For the 100M ports, the remain buffer area resources are allocated on average.

### Static Mode:

The device supports to configure the congestion queue number on the ports statically/manually, ensuring that the output buffer area resources are enough to address the requirements of the output congestion control.

By using the staic configuration, you can configure the congestion queue number on each port according to the actual output queue number in the network plan to utilize the output buffer area resources more effectively.

**Note**

- The configuration takes effect only when the buffer control is in the QoS mode.
- Only Aggregated Ports and AP member ports support the congestion queue control.
- With one congestion queue configured, when the output congestion is generated on the port and the packets of each queue output, the priority difference is not displayed.

## QoS Logic Interface Group

A series of interface, which could be APs, or the physical ports, can be specified as one QoS logic interface group, and association the logic interface group with Policy-map for the QoS processing. Take the rate-limit for example, the packets that corresponds to the rate-limit condition share the bandwidth value limited by Policy-map on all ports within the same logic interface group.

**Note**

The member ports join the logic interface group must be physical ports or Aggregate Port.

The supported logic interface group number is up to 128.

## QoS Configuration

### Default QoS configuration

Make clear the following points of QoS before starting the configuration:

- One interface can be associated with at most one policy-map.
- One policy-map can have multiple class-maps.
- One class-map can be associated at most one ACL, and all ACEs in that ACL must have the same filter domain template.
- The amount of ACEs associated with one interface meets the constraint described in the section "Configuring secure ACL".

By default, the QoS function is disabled. That is, the device treats all messages equally. When you associate a Policy Map with a port and set the trust mode of the port, the QoS function of that port is enabled. To disable the QoS function of a port, you may remove the Policy Map setting and set the trust mode of the port as Off. Below is the default QoS configuration:

Default CoS value	0
Number of Queues	8
Queue Scheduling	WRR
QueueWeight	1:1:1:1:1:1:1:1
WRR Weight Range	1:15
DRR Weight Range	1:15

Trust mode	No Trust
Switch Buffer Management Mode	FC

Default mapping table from CoS value to queue

CoS Value	0	1	2	3	4	5	6	7
Queue	1	2	3	4	5	6	7	8

Default mapping table from CoS to DSCP

CoS Value	0	1	2	3	4	5	6	7
DSCP value	0	8	16	24	32	40	48	56

Default mapping table from IP-Precedence to DSC

IP-Precedence	0	1	2	3	4	5	6	7
DSCP	0	8	16	24	32	40	48	56

Default mapping table from DSCP to CoS

DSCP	0	8	16	24	32	40	48	56
CoS	0	1	2	3	4	5	6	7

## Configure the QoS trust mode of the interface

By default, the QoS trust mode of an interface is disabled.

Command	Description
Ruijie# <b>configure terminal</b>	Enter the configuration mode
Ruijie(config)# <b>interface</b> <i>interface</i>	Enter the interface configuration mode.
Ruijie(config-if)# <b>mls qos trust {cos   ip-precedence   dscp}</b>	Configure the QoS trust mode of the interface CoS, dscp or ip-precedence
Ruijie(config-if)# <b>no mls qos trust</b>	Restore the QoS trust mode of the interface to default



### Note

The QoS trust mode cannot be configured on the SVI port.

The command below set the trust mode of interface gigabitEthernet 0/4 to DSCP:

```
Ruijie(config)# interface gigabitEthernet 0/4
Ruijie(config-if)# mls qos trust dscp
Ruijie(config-if)# end
Ruijie# show mls qos interface g0/4
Interface GigabitEthernet 0/4
```

```
Attached input  policy-map:
Default COS: trust dscp
Default COS: 0
Ruijie#
```

## Configuring the Default CoS Value of an Interface

You may configure the default CoS value for every interface through the following steps. By default, the CoS value of an interface 0.

Command	Description
Ruijie# <b>configure terminal</b>	Enter the configuration mode
Ruijie(config)# <b>interface</b> <i>interface</i>	Enter the interface configuration mode.
Ruijie(config-if)# <b>mls qos cos</b> <i>cos</i> <b>default-cos</b>	Configure the default CoS value of the interface, where default-cos is the desired default CoS value, ranging 0~7.
Ruijie(config-if)# <b>no mls qos cos</b>	Restore to the default CoS value.

The example below set the default CoS value of interface g0/4 to 6:

```
Ruijie# configure terminal
Ruijie(config)# interface g 0/4
Ruijie(config-if)# mls qos cos 6
Ruijie(config-if)# end
Ruijie# show mls qos interface g 0/4
Interface GigabitEthernet 0/4
Attached input  policy-map:
Default COS: trust dscp
Default COS: 6
Ruijie#
```

## Configuring the Logic Interface Group

To configure the logic interface group, run the following command in the interface configuration mode:

Command	Description
Ruijie(config-if)# <b>[no] virtual-group</b> <i>virtual-group-number</i>	Add an interface to the logic interface group, or remove an interface from the logic interface group. <i>virtual-group-number</i> : the group number of the logic interfaces.

Use the **no virtual-group** *virtual-group-number* command to make a physical port to exit from the logic interface group.

The example below set the interface g0/1 to the member of logic interface group 5:

```
Ruijie# configure terminal
Ruijie(config)# interface gigabitEthernet 0/1
Ruijie(config-if)# virtual-group 5
Ruijie(config-if-range)# end
```

## Configuring Class Maps

You may create and configure Class Maps through the following steps:

Command	Description
Ruijie# <b>configure terminal</b>	Enter the configuration mode
Ruijie(config)# <b>ip access-list extended</b> {id name} ... Ruijie(config)# <b>ip access-list standard</b> {id name} ... Ruijie(config)# <b>mac access-list extended</b> {id name} ... Ruijie(config)# <b>expert access-list extended</b> {id name} ... Ruijie(config)# <b>ipv6 access-list extended</b> name ... Ruijie(config)# <b>access-list</b> id[...]	Create ACL Please refer to the chapter of ACL
Ruijie(config)# <b>[no] class-map</b> class-map-name	Create and enter into the class map configuration mode, where class-map-name is the name of the class map to be created. The no option will delete an existing class map
Ruijie(config-cmap)# <b>[no] match access-group</b> {acl-num   acl-name }	Set the matching ACL, where acl-name is the name of the created ACL, acl-num is the ID of the created ACL; the no option delete that match.

For example, the following steps creates a class-map named class1, which is associated with a ACL:acl\_1. This class-map will classify all TCP messages with port 80.

```
Ruijie(config)# ip access-list extended acl_1
Ruijie(config-ext-nacl)# permit tcp any any eq 80
Ruijie(config-ext-nacl)# exit
Ruijie(config)# class-map class1
Ruijie(config-cmap)# match access-group acl_1
Ruijie(config-cmap)# end
```

## Configuring Policy Maps

You may create and configure Policy Maps through the following steps:

Command	Description
Ruijie# <b>configure terminal</b>	Enter the configuration mode

Command	Description
Ruijie(config)# <b>[no] policy-map</b> <i>policy-map-name</i>	Create and enter into the policy map configuration mode, where <i>policy-map-name</i> is the name of the policy map to be created.  The <b>no</b> option will delete an existing policy map
Ruijie(config-pmap)# <b>[no] class</b> <i>class-map-name</i>	Create and enter into the data classifying configuration mode, where <i>class-map-name</i> is the name of the class map to be created.  The <b>no</b> option deletes that data classification
Ruijie(config-pmap-c)# <b>[no] set { ip dscp new-dscp   cos new-cos }</b>	Set new ip dscp value or new cos value for the IP messages in the dataflow. The ip dscp value does not take effect for non-IP messages.  <i>new-dscp</i> is the new DSCP value to be set, whose range varies with the specific product.  <i>new-cos</i> is the new CoS value to be set, whose range is 0 to 7.
Ruijie(config-pmap-c)# <b>police</b> <i>rate-bps burst-byte [exceed-action {drop   dscp dscp-value   cos cos-value}]</i>	Limit the bandwidth of the dataflow and specify the action for the excessive bandwidth part, where <i>rate-bps</i> is the limited bandwidth per second (kbps), <i>burst-byte</i> is the limited burst bandwidth (Kbyte), <b>drop</b> means dropping the message of the excessive bandwidth part, <b>dscp dscp-value</b> means changing the DSCP value of the message in excessive bandwidth part, and <i>dscp-value</i> value range varies with specific products. <b>cos cos-value</b> means changing the CoS value of the message in excessive bandwidth and <i>cos-value</i> value range is 0 to 7.  The effective range of the <i>burst-byte</i> is 4 to 2097152.
Ruijie(config-pmap-c)# <b>no police</b>	Cancel to limit the bandwidth of the dataflow and specify the action for the excessive bandwidth part

**Note**

The DENY action in the ACL, matched with the CLASS MAP will be ignored.

For example, the following steps create a policy-map named *policy1* and associate it with interface Gigabitethernet 1/1.

```
Ruijie(config)# policy-map policy1
Ruijie(config-pmap)# class class1
Ruijie(config-pmap-c)# set ip dscp 48
Ruijie(config-pmap-c)# exit
Router(config-pmap)# exit
```

```
Ruijie(config)# interface gigabitethernet 1/1
Ruijie(config-if)# switchport mode trunk
Ruijie(config-if)# mls qos trust cos
Ruijie(config-if)# service-policy input policy1
```

## Applying Policy Maps on the Interface

You may apply the Policy Maps to a port through the following steps:

Command	Description
<b>configure terminal</b>	Enter the configuration mode
<b>Interface</b> <i>interface</i>	Enter the interface configuration mode.
<b>[no] service-policy {input   output} <i>policy-map-name</i></b>	Apply the created policy map to the interface, where the <i>policy-map-name</i> is the name of the created policy map.

## Applying Policy Maps to the Logic Interface Group

To apply Policy Maps to the logic interface group, run the following commands:

Command	Description
<b>Ruijie#configure terminal</b>	Enter the configuration mode
<b>Ruijie(config)#virtual-group</b> <i>virtual-group-number</i>	<b>Enter the logic interface group configuration mode.</b>
<b>Ruijie(config)# [no] service-policy {input   output} <i>policy-map-name</i></b>	<b>Apply the created Policy Maps to the logic interface group.</b> <b><i>policy-map-name</i>: the name of created policy map;</b> input: <b>the input rate-limit;</b> output: <b>the output rate-limit.</b>



### Note

This function is not supported. Because it is necessary to associate the class map with acl, all restrictions of the acl configuration are applicable for the qos configuration. For the details, see the *ACL Configuration*.

## Configuring the Output Queue Scheduling Algorithm

You may schedule the algorithms for the output queue of a port: WRR, SP, RR and DRR. By default, the output queue algorithm is WRR (Weighted Round-Robin).

You may set the port priority queue scheduling method through the following steps. For details of the algorithm, see the overview of QoS.



Command	Description
Ruijie# <b>configure terminal</b>	Enter the configuration mode
Ruijie(config)# <b>mls qos scheduler {sp   rr   wrr   drr}</b>	Set the port priority queue scheduling method, where <b>sp</b> is absolute priority scheduling, <b>rr</b> is round-robin, <b>wrr</b> is weighted round-robin with frame quantity, and <b>drr</b> weighted round-robin with frame length
Ruijie(config)# <b>no mls qos scheduler</b>	Restore the default <b>wrr</b> scheduling

For example, the following steps set the port output algorithm to SP:

```
Ruijie# configure terminal
Ruijie(config)# mls qos scheduler sp
Ruijie(config)# end
Ruijie# show mls qos scheduler
Global Multi-Layer Switching scheduling
Strict Priority
Ruijie#
```

## Configuring Output Round-Robin Weight

You may set the output round-robin weight through the following steps:

Command	Description
Ruijie# <b>configure terminal</b>	Enter the configuration mode
Ruijie(config)# <b>{wrr-queue   drr-queue} bandwidth weight1...weightn</b>	weight1...weightn are the weight values specified for the output queues. For the count and value range, see the default QoS settings
Ruijie(config)# <b>no {wrr-queue   drr-queue} bandwidth</b>	The no option restores the default weight value.

The example below sets the wrr scheduling weight as 1:2:3:4:5:6:7:8

```
Ruijie# configure terminal
Ruijie(config)# wrr-queue bandwidth 1 2 3 4 5 6 7 8
Ruijie(config)# end
Ruijie# show mls qos queueing
Cos-queue map:
cos qid
--- ---
0 1
1 2
2 3
3 4
4 5
5 6
6 7
7 8
wrr bandwidth weights:
qid weights
```

```

--- -----
0  1
1  2
2  3
3  4
4  5
5  6
6  7
7  8
Ruijie(config)#

```

## Configuring Cos-Map

You may set cos-map to change which queue to select for the messages in output. The default value of cos-map is provided in the default QoS configuration section.

Command	Description
Ruijie# <b>configure terminal</b>	Enter the configuration mode
Ruijie(config)# <b>priority-queue</b> <b>Cos-Map qid cos0 [cos1 [cos2 [cos3</b> <b>[cos4 [cos5 [cos6 [cos7]]]]]]]</b>	<i>qid</i> is the queue id; <i>cos0..cos7</i> are the CoS values associated with that queue.
Ruijie(config)# <b>no priority-queue</b> <b>cos-map</b>	Restore default of cos-map

Below is the example of configuring CoS Map

```

Ruijie# configure terminal
Ruijie(config)# priority-queue Cos-Map 1 2 4 6 7 5
Ruijie(config)# end
Ruijie# show mls qos queueing
Cos-queue map:
cos qid
--- ---
0  1
1  2
2  1
3  4
4  1
5  1
6  1
7  1

wrr bandwidth weights:
qid weights
--- -----
0  1
1  2
2  3
3  4
4  5
5  6
6  7
7  8

```

## Configuring CoS-to-DSCP Map

CoS-to-DSCP Map is used to map the CoS value to internal DSCP value. You may follow these steps to set CoS-to-DSCP Map. The default value of CoS-to-DSCP is provided in the default QoS configuration section.

Command	Description
Ruijie# <b>configure terminal</b>	Enter the configuration mode
Ruijie(config)# <b>mls qos map cos-dscp dscp1...dscp8</b> Ruijie(config)# <b>no mls qos map cos-dscp</b>	Change the CoS-to-DSCP Map settings, where dscp1...dscp8 are the DSCP values corresponding to CoS values 0 ~ 7. The DSCP value range varies with specific products.

For Example:

```
Ruijie# configure terminal
Ruijie(config)# mls qos map cos-dscp 56 48 46 40 34 32 26 24
Ruijie(config)# end
Ruijie# show mls qos maps cos-dscp
cos dscp
--- ----
0 56
1 48
2 46
3 40
4 34
5 32
6 26
7 24
```

## Configuring DSCP-to-CoS Map

DSCP-to-CoS is used to map internal DSCP value to CoS value so that it is possible to select output queue for messages.

The default value of DSCP-to-CoS Map is provided in the default QoS configuration section. You may follow these steps to set DSCP-to-CoS Map:

Command	Description
Ruijie# <b>configure terminal</b>	Enter the configuration mode
Ruijie(config)# <b>mls qos map dscp-cos dscp-list to cos</b>	Set DSCP to COS Map, where dscp-list is the list of DSCP values to be set, DSCP values delimited by spaces, value range varying with specific products, cos means the CoS values corresponding to the DSCP values, ranging 0~7
Ruijie(config)# <b>no mls qos map dscp-cos</b>	Restore default

For example, the following steps set the DSCP values 0, 32 and 56 to map 6:

```
Ruijie# configure terminal
```

```

Ruijie(config)# mls qos map dscp-cos 0 32 56 to 6
Ruijie(config)# show mls qos maps dscp-cos
dscp cos      dscp cos      dscp cos      dscp cos
----
0 6           1 0           2 0           3 0
4 0           5 0           6 0           7 0
8 1           9 1          10 1          11 1
12 1          13 1          14 1          15 1
16 2          17 2          18 2          19 2
20 2          21 2          22 2          23 2
24 3          25 3          26 3          27 3
28 3          29 3          30 3          31 3
32 6          33 4          34 4          35 4
36 4          37 4          38 4          39 4
40 5          41 5          42 5          43 5
44 5          45 5          46 5          47 5
48 6          49 6          50 6          51 6
52 6          53 6          54 6          55 6
56 6          57 7          58 7          59 7
60 7          61 7          62 7          63 7

```

## Configuring Port Rate Limiting

You may follow these steps to limit the port rate:

Command	Description
Ruijie# <b>configure terminal</b>	Enter the configuration mode
Ruijie(config)# <b>interface</b> <i>interface</i>	Enter the interface configuration mode.
Ruijie(config-if)# <b>rate-limit output</b> <i>bps burst-size</i>	Port rate limit, where output is the output rate limit, bps is the bandwidth limit per second (kbps), and burst-size is the burst bandwidth limit (Kbyte)
Ruijie(config-if)# <b>no rate-limit</b>	Cancel port rate limiting

```

Ruijie# configure terminal
Ruijie(config)# interface gigabitEthernet 0/4
Ruijie(config-if)# rate-limit output 64 1024
Ruijie(config-if)# end
Ruijie#

```

## Configuring IPpre to DSCP Map

IPpre-to-Dscp is used to map the IPpre values of message to internal DSCP values. The default settings of IPpre-to-DSCP Map are provided in the default QoS configuration section. you may follow these steps to configure IPpre-to-Dscp Map:

Command	Description
Ruijie# <b>configure terminal</b>	Enter the configuration mode

Command	Description
Ruijie(config)# <b>mls qos map ip-precedence-dscp</b> <i>dscp1...dscp8</i>	Modify the setting of IP-Precedence-to-Dscp Map, where dscp1...dscp8 are the DSCP values corresponding to IP-Precedence values 0~7
Ruijie(config)# <b>no mls qos map ip-prec-dscp</b>	Restore default

For Example:

```
Ruijie# configure terminal
Ruijie(config)# mls qos map ip-precedence-dscp 56 48 46 40 34 32 26 24
Ruijie(config)# end
Ruijie# show mls qos maps ip-prec-dscp
ip-precedence dscp
-----
0      56
1      48
2      46
3      40
4      34
5      32
6      26
7      24
```

## Configuring the Switch Buffer

To manage the switch buffer in the state of 802.3x flow-control or QoS, run the following commands:

Command	Description
Ruijie# <b>configure terminal</b>	Enter the configuration mode
Ruijie(config)# <b>buffer management</b> <i>{fc/qos}</i>	Configure the buffer management mode. FC: 802.3xflow-control QoS: QoS mode
Ruijie(config)# <b>no buffer management</b>	Cancel the switch buffer management.

For Example:

```
Ruijie# configure terminal
Ruijie(config)# buffer management qos
Ruijie(config)# end
Ruijie# show buffer management
%current port's buffer management mode: qos
```

## Configuring the Switch Congestion Queue Number Control

To configure the switch congestion queue number, run the following commands:

Command	Description
Ruijie# <b>configure terminal</b>	Enter the configuration mode
Ruijie(config)# <b>interface interface</b>	Enter the interface configuration mode.
Ruijie(config-if)# <b>buffer management qos queue queue-number</b>	Configure the switch congestion queue number. <i>Queue-number:</i> the congestion queue number supported on the port, 1-8. <b>1</b> represents that the priorities are not differed for each queue when the congestion occurs; <b>8</b> represents that when the congestion of 8 queues occurs, the packets are output based on the priority level.
Ruijie(config-if)# <b>[no default]buffer management qos queue</b>	Set the congestion queue number on the port to the default value.

The following example shows how to set the congestion queue number for the interface fastEthernet 0/4 as 8:

```
Ruijie# configure terminal
Ruijie(config)# interface fastEthernet 0/4
Ruijie(config-if)# buffer management qos queue 8
Ruijie(config-if)# end
```

## QoS Displaying

### Showing class-map

You may show the contents of class-map through the following steps:

Command	Description
<b>show class-map [class-name]</b>	Show the contents of the class map entity

For example,

```
Ruijie# show class-map
Class Map cc
Match access-group 1
Ruijie#
```

### Showing policy-map

You may show the contents of policy-map through the following steps:

Command	Description
---------	-------------

Command	Description
<b>show policy-map</b> [ <i>policy-name</i> ] [ <b>class</b> <i>class-name</i> ]	Show QoS policy map, <i>policy-name</i> is the selected name of policy map, specified as <b>class</b> Show the class map bound with the policy map in case of <i>class-name</i>

For example,

```
Ruijie# show policy-map
Policy Map pp
Class cc
Ruijie#
```

## Showing mls qos interface

You may show the QoS information of all ports through the following steps:

Command	Description
<b>show mls qos interface</b> [ <i>interface</i> ] <i>policers</i>	Show the QoS information of the interface, The <b>Policers</b> option shows the policy map applied on the interface.

For example,

```
Ruijie# show mls qos interface gigabitEthernet 0/4
Interface GigabitEthernet 0/4
Attached input policy-map: pp
Default COS: trust dscp
Default COS: 6
Ruijie# show mls qos interface policers
Interface: GigabitEthernet 0/4
Attached input policy-map: pp
Ruijie#
```

## Showing mls qos virtual-group

You may show the QoS information on all interfaces through the following steps:

Command	Description
<b>show mls qos virtual-group</b> [ <i>virtual-group-number</i>   <b>policers</b> ]	Show the police information associated with the logic interface group. The <b>Policers</b> option displays the police associated with the logic interface group.

For example:

```
Ruijie# show mls qos virtual-group 1
Virtual-group: 1
Attached input policy-map: pp
Ruijie# show mls qos virtual-group policers
Virtual-group: 1
Attached input policy-map: pp
Ruijie#
```

## Showing mls qos queueing

You may show the QoS queue information through the following steps:

Command	Description
<b>Show mls qos queueing</b>	Show the QoS queue information, CoS-to-queue map, wrr weight and drr weight;

For example:

```
Ruijie# show mls qos queueing
```

```
Cos-queue map:
```

```
cos qid
```

```
--- ---
```

```
0 1
```

```
1 2
```

```
2 1
```

```
3 4
```

```
4 1
```

```
5 1
```

```
6 1
```

```
7 1
```

```
wrr bandwidth weights:
```

```
qid weights
```

```
--- -----
```

```
0 1
```

```
1 2
```

```
2 3
```

```
3 4
```

```
4 5
```

```
5 6
```

```
6 7
```

```
7 8
```

## Showing mls qos scheduler

You may show the QoS scheduling method through the following steps:

Command	Description
<b>Show mls qos scheduler</b>	Show the port priority queue scheduling method.

For example:

```
Ruijie# show mls qos scheduler
```

```
Global Multi-Layer Switching scheduling
```

```
Strict Priority
```

```
Ruijie#
```

## Showing mls qos maps

You may show the MLS QoS maps table through the following steps:

Command	Description
---------	-------------



Command	Description
<b>show mls qos maps [cos-dscp   dscp-cos   ip-prec-dscp]</b>	Show MLS QoS map.

For example:

```
Ruijie# show mls qos maps cos-dscp
```

```
cos dscp
```

```
--- ----
```

```
0 0
```

```
1 8
```

```
2 16
```

```
3 24
```

```
4 32
```

```
5 40
```

```
6 48
```

```
7 56
```

```
Ruijie# show mls qos maps dscp-cos
```

```
dscp cos    dscp cos    dscp cos    dscp cos
```

```
---- -
```

```
0 6      1 0      2 0      3 0
```

```
4 0      5 0      6 0      7 0
```

```
8 1      9 1     10 1     11 1
```

```
12 1     13 1     14 1     15 1
```

```
16 2     17 2     18 2     19 2
```

```
20 2     21 2     22 2     23 2
```

```
24 3     25 3     26 3     27 3
```

```
28 3     29 3     30 3     31 3
```

```
32 6     33 4     34 4     35 4
```

```
36 4     37 4     38 4     39 4
```

```
40 5     41 5     42 5     43 5
```

```
44 5     45 5     46 5     47 5
```

```
48 6     49 6     50 6     51 6
```

```
52 6     53 6     54 6     55 6
```

```
56 6     57 7     58 7     59 7
```

```
60 7     61 7     62 7     63 7
```

```
Ruijie# show mls qos maps ip-prec-dscp
```

```
ip-precedence dscp
```

```
-----
```

```
0      56
```

```
1      48
```

```
2      46
```

```
3      40
```

```
4      34
```

```
5      32
```

```
6      26
```

```
7      24
```

## Showing mls qos rate-limit

You may show the port rate limiting information through the following steps:

Command	Description
<b>show mls qos rate-limit</b> [ <i>interface interface</i> ]	Show the rate limit of [port]

```
Ruijie# show mls qos rate-limit
Interface GigabitEthernet 0/4
rate limit input bps = 100 burst = 100
```

## Showing the policy-map interface

You can show the configuration of port policy map by performing following steps

Command	Function
<b>show policy-map interface</b> <i>interface</i>	Showing the configuration of (port) policy map

```
Ruijie#show policy-map interface f0/1
FastEthernet 0/1 input (tc policy): pp
  Class cc
    set ip dscp 22
    mark count 0
```



The device currently does not support the statistic of mark count.

### Note

## Showing the buffer management mode

You can show the buffer management mode by performing following steps

Command	Function
<b>show buffer management</b>	Showing the configuration of buffer management mode.

```
Ruijie#show buffer management
%current port's buffer management mode: qos
```

## Showing the virtual-group

You can show the virtual-group configuration by performing following steps

Command	Function
<b>show virtual-group</b> [ <i>virtual-group-number</i>   <b>summary</b> ]	Showing the logic interface group information.

```
Ruijie#show virtual-group 1
virtual-group      member
-----
1                  Gi0/2 Gi0/3 Gi0/4 Gi0/5
                  Gi0/6 Gi0/7 Gi0/8 Gi0/9 Gi0/10
```

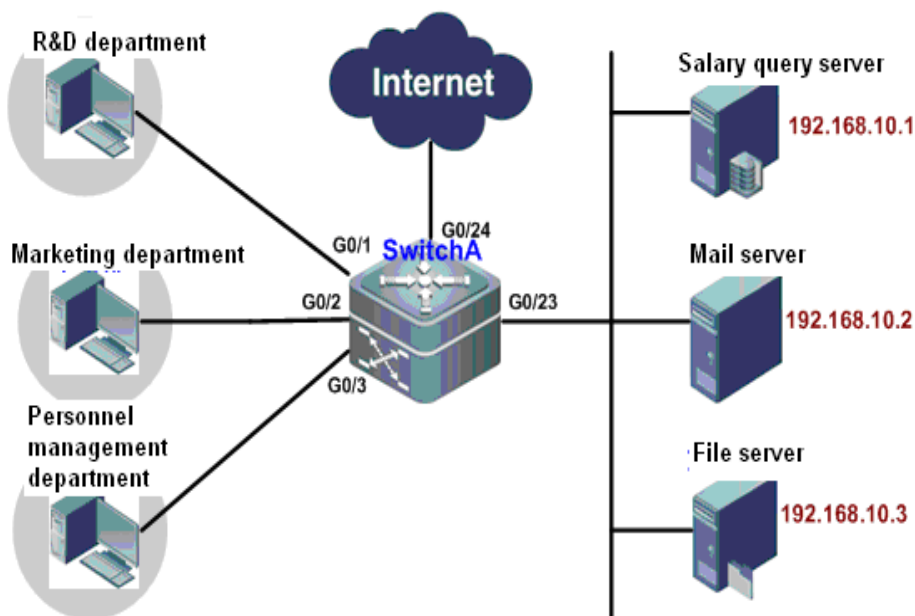
```
Ruijie#show virtual-group summary
```

virtual-group	member
1	Gi0/1 Gi0/2 Gi0/3 Gi0/4 Gi0/5 Gi0/6 Gi0/7 Gi0/8 Gi0/9
2	Gi0/11 Gi0/12 Gi0/13 Gi0/14 Gi0/15 Gi0/16 Gi0/17 Gi0/18 Gi0/19

## Typical QoS Configuration Examples

### Priority Remarking + Queue Scheduling

#### Networking Diagram



As shown below, the port Gi0/23 of the switch is connected to the salary query server, mail server and file server; while the Gi0/1, Gi0/2 and Gi0/3 are connected to the R&D department, marketing department and personnel management department respectively.

#### Configuration Requirements

The following requirements shall be met through the configurations:

- 1) When the R&D department and marketing department access the server, the priority of the server packets is: Mail server > File server > Salary query server
- 2) The switch will give priority to the Internet or server access of the personnel management department.
- 3) During the switch operation, the network congestion occurs frequently. To ensure the smooth operation, it is required to use the WRR queue scheduling, so that the IP packets accessing the mail database, file database, salary query database will be scheduled according to the ratio of 6:2:1.

## Configuration Tips

---

- 1) Configure the CoS value of data stream for different servers to handle and the priority of packets used to access different types of servers.
- 2) Configure the default CoS value of the interface to a specified value to give priority to the packets sent from the personnel management department.
- 3) Configure the output round robin weight for the WRR queue scheduling.

## Configuration Procedure

---

Step1: Create the ACL for accessing various servers.

```
SwitchA(config)#ip access-list extended salary
SwitchA(config-ext-nacl)#permit ip any host 192.168.10.1
SwitchA(config-ext-nacl)#exit
SwitchA(config)#ip access-list extended mail
SwitchA(config-ext-nacl)#permit ip any host 192.168.10.2
SwitchA(config-ext-nacl)#exit
SwitchA(config)#ip access-list extended file
SwitchA(config-ext-nacl)#permit ip any host 192.168.10.3
```

Step2: Create the class-map matching various server ACLs.

```
SwitchA(config)#class-map salary
SwitchA(config-cmap)#match access-group salary
SwitchA(config-cmap)#exit
SwitchA(config)#class-map mail
SwitchA(config-cmap)#match access-group mail
SwitchA(config-cmap)#exit
SwitchA(config)#class-map file
SwitchA(config-cmap)#match access-group file
```

Step3: Associate the policy-map with the corresponding class-map and configure the Cos value of accessing the server dataflow:

Mail server> File server > Salary query server

```
SwitchA(config)#policy-map toserver
SwitchA(config-pmap)#class mail
SwitchA(config-pmap-c)#set cos 4
SwitchA(config-pmap-c)#exit
SwitchA(config-pmap)#class file
SwitchA(config-pmap-c)#set cos 3
SwitchA(config-pmap-c)#exit
SwitchA(config-pmap)#class salary
SwitchA(config-pmap-c)#set cos 2
SwitchA(config-pmap-c)#end
```

Step4: Apply the policy-map to the corresponding port and configure the Qos trust mode of the port.

```
SwitchA(config)#interface gigabitEthernet 0/1
SwitchA(config-if-GigabitEthernet 0/1)#service-policy input toserver
SwitchA(config-if-GigabitEthernet 0/1)#mls qos trust cos
SwitchA(config-if-GigabitEthernet 0/1)#exit
SwitchA(config)#interface gigabitEthernet 0/2
SwitchA(config-if-GigabitEthernet 0/2)#service-policy input toserver
SwitchA(config-if-GigabitEthernet 0/2)#mls qos trust cos
SwitchA(config-if-GigabitEthernet 0/2)#exit
```

Step5: Configure the port priority queue scheduling mode to SP.

```
SwitchA(config)#mls qos scheduler sp
```

Step6: Configure the default Cos value of the interface connecting the personnel management department to 7 to give precedence to the packets sent from the personnel management department and configure the Qos trust mode of the port.

```
SwitchA(config)#interface gigabitEthernet 0/3
SwitchA(config-if-GigabitEthernet 0/3)#mls qos cos 7
SwitchA(config-if-GigabitEthernet 0/3)#mls qos trust cos
```

Step7: Configure the output round robin weight for the WRR queue scheduling.

```
Ruijie(config)#wrr-queue bandwidth 1 1 1 2 6 1 1 1
```

Step8: Configure the port priority queue scheduling mode to WRR.

```
SwitchA(config)#mls qos scheduler wrr
```

## Verification

Step1: Check whether the class-map configuration is correct.

```
SwitchA(config)#show class-map
Class Map salary
  Match access-group salary
Class Map mail
  Match access-group mail
Class Map file
  Match access-group file
```

Step2: Check whether the policy-map configuration is correct.

```
SwitchA(config)#show policy-map

Policy Map toserver
  Class mail
    set cos 4
  Class file
    set cos 3
  Class salary
    set cos 2
```

Step3: Check whether the QOS information of the corresponding port is correct.

```
SwitchA(config)#show mls qos interface gigabitEthernet 0/1
Interface: GigabitEthernet 0/1
Attached input policy-map: toserver
Attached output policy-map:
Default trust: cos
Default cos: 0
SwitchA(config)#show mls qos interface gigabitEthernet 0/2
Interface: GigabitEthernet 0/2
Attached input policy-map: toserver
Attached output policy-map:
Default trust: cos
Default cos: 0
```

**Step4: Check QOS queue information.**

```
SwitchA(config)#show mls qos queueing
```

```
Cos-queue map:
```

```
cos qid
```

```
--- ---
```

```
0 1
```

```
1 2
```

```
2 3
```

```
3 4
```

```
4 5
```

```
5 6
```

```
6 7
```

```
7 8
```

```
wrr bandwidth weights:
```

```
qid weights
```

```
--- -----
```

```
1 1
```

```
2 1
```

```
3 1
```

```
4 2
```

```
5 6
```

```
6 1
```

```
7 1
```

```
8 1
```

```
drp bandwidth weights:
```

```
qid weights
```

```
--- -----
```

```
1 1
```

```
2 1
```

```
3 1
```

```
4 1
```

```
5 1
```

```
6 1
```

```
7 1
```

```
8 1
```

## Reliability Configuration

---

1. CFM Configuration
2. REUP Configuration
3. RLDP Configuration
4. DLDP Configuration
5. TPP Configuration
6. BFD Configuration
7. RNS&Track Configuration
8. GRTD Configuration
9. SEM Configuration
10. VSU Configuration

# CFM Configuration

## Introduction to CFM

### Overview

The Ethernet technology was initially applied in LAN, which has comparatively low requirements on reliability and stability. Therefore, its support to OAM (Operations, Administration and Maintenance) has been very weak since the emergence of Ethernet, and this has become a severe barrier to large-scale application in the telecom network (such as Metropolitan Area Network and Wide Area Network). For this reason, there have emerged many Ethernet OAM standards. According to the scope of application, these standards can be classified into link-level OAM and network-level OAM. The link-level OAM refers to the OAM applied on the point-to-point single link, such as the EFM OAM defined in IEEE802.3ah. The OAM which can be used to monitor a virtual bridged network falls into network-level OAM.

According to the definition in IEEE 802.1ag, CFM (Connectivity Fault Management) is designed to detect network connectivity failures and falls into the category of network-level OAM. Through CFM, the network administrator can effectively detect, verify and isolate connectivity failures in the network. The operating environment of CFM can cross multiple nodes, thus providing end-to-end OAM monitoring and management services for the user.

### Basic Concepts/Features

#### Maintenance Domain

Maintenance Domain (MD) is used to define the range of network to be managed. In order to precisely locate the fault point, the concept of MD Level is introduced. There are 8 MD levels ranging from 0 to 7, while a higher number indicates a higher level and greater range of MD. 0 is the lowest level and 7 is the largest level. Domains may touch (as shown in Fig 1, MD1 borders on MD2) or nest (as shown in Fig 2, MD2 is nested in MD1), but domains should not intersect (as shown in Fig 3, MD1 intersects on MD2).

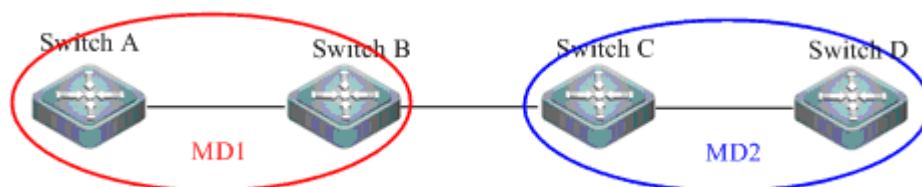


Fig 1



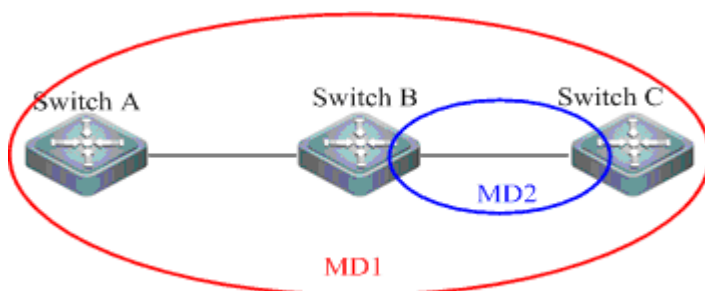


Fig 2

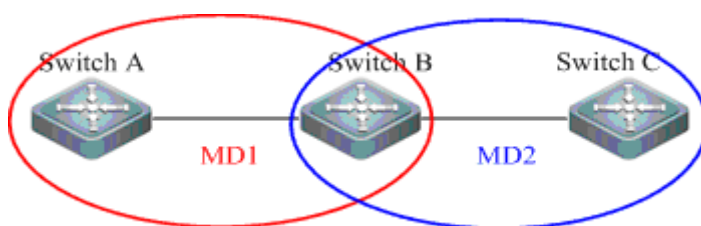


Fig 3

In addition, when two domains nest, the outer domain must have a higher maintenance level than the domain nested within it. Low-level CFM PDU will be discarded when entering into the high-level maintenance domain; high-level CRM PDU can pass through low-level maintenance domain; CFM PDUs with the same maintenance level cannot pass through each other.

## Maintenance Association

Multiple Maintenance Associations (MA) can be configured in one MD as required. Each MA is a set of maintenance end points within a specific MD. Please refer to subsequent paragraphs for descriptions about the maintenance end point. Generally, one MA serves a specific subnet, and thus MA is generally bound to a VLAN. MA is identified with the MAID consisting of MD name and MA name.

## Service Instance

Service instance represents the specified maintenance association in a specific maintenance domain. To facilitate configuration and expression of a subnet represented by a maintenance domain, the concept of service instance was introduced. Different service instances will expressed in a global-unique instance number.

## Maintenance Point

The Maintenance Point (MP) configured on the port belongs to a MA. MP is the main subject of CFM, which verifies network status by monitoring the connectivity between an MA and respective MPs. MP can also be divided into maintenance association end point and maintenance domain intermediate points:

## Maintenance Domain End Point

Maintenance association End Point (MEP) is used to determine the boundary and range of a maintenance domain (MD). It is a core unit of CFM, and is responsible for initiating all CFM PDU packets in order to carry out route discovery, error detection, fault isolation and error advertisement. MEP is the end point of MA, while major protocols of CRM are all running on MEP. The level of MD where the MEP is in determines the level of CFM PDU sent by MEP. If the level of CFM PDUs received is higher than that of local MD, MEP will forward the packets; if the level of CFM PDUs received is lower than that of local MD, MEP will discard the packets to avoid that CFM PDUs from low-level MD enter the high-level MD. Under normal circumstances, there will be either no MEP or at least two MEPs in one MD. If one MD has only one MEP, then the OAM packets it sends may leak into the maintenance domain.

MEP can be classified into Inward MEP and Outward MEP.

Inward MEP will not send out CFM PDUs from the local port. Instead, it sends out CFM PDUs from other ports on the device. As shown in Fig. 4, Port1 of Switch B and Port4 of Switch C are at the boundary of MD1. Configure a MEP for MD1 on these two ports respectively (MEP1 and MEP2). MEP1 will not send out CFM PDUs of MD1 from port1, because it is out of the range of MD1; MEP1 will only send out CFM PDUs of MD1 from port2. The rule is the same for MEP2. Both MEP1 and MEP2 are inward MEPs.

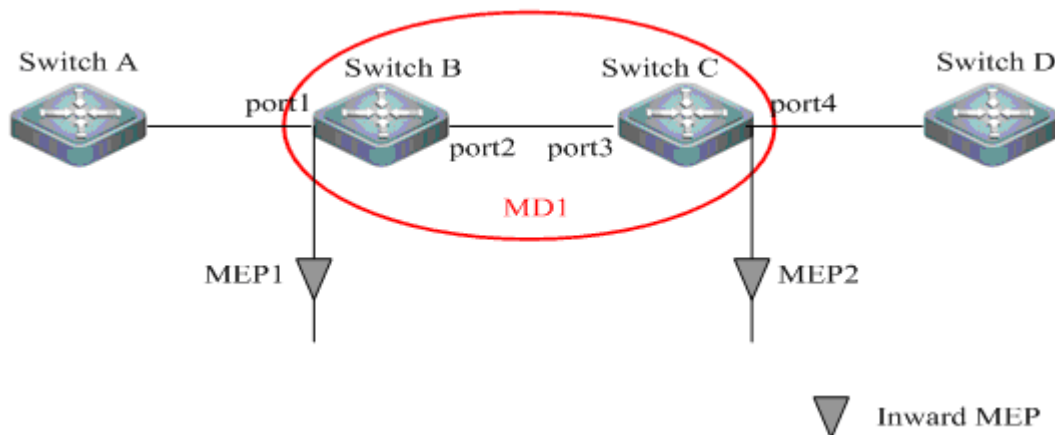


Fig 4

Outward MEP will send out CFM PDUs from the local port. As shown in Fig 5, port2 on Switch B and port3 on Switch C are at the boundary of MD2. Configure an Outward MEP for MD2 on these two port respectively (MEP1 and MEP2). There are called Outward MEPs because they will not send out CFM PDUs from other ports on the device, but from the port on which MEP is configured.

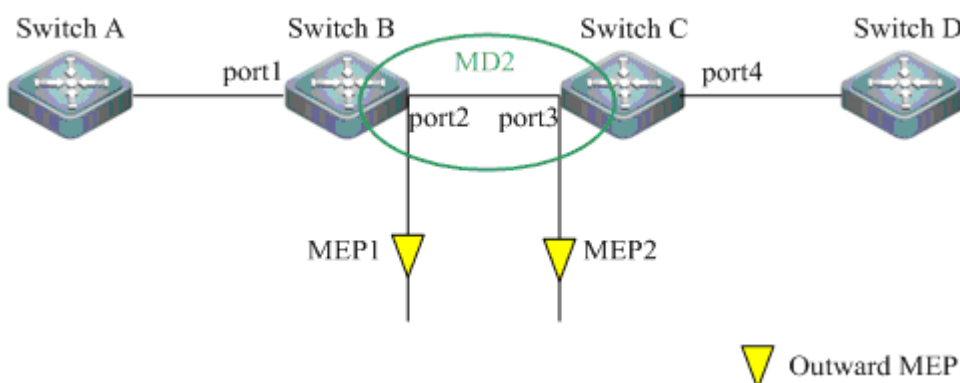




Fig 5

 <b>Note</b>	MEP is identified with an integer. The MD and MA with which the MEP is affiliated determine the VLAN ID carried by the CFM PDU packets sent by it.
 <b>Caution</b>	When configuring MEP, make sure the MEP to be created already exists in MEP list, or else the MEP cannot be created successfully.

### Maintenance Domain Intermediate Point

Maintenance domain Intermediate Point (MIP) is inside the MD. Different from MEP, it will initiate any CFM PDU, but process and respond to CFM PDUs. The MD and MA with which the MIP is affiliated determine the VLAN ID of CFM PDU packets that it can receive and respond. Similar to MEP, the level of MD where the MIP is in determines the level of CFM PDUs forwarded by MIP. If the level of CFM PDUs received is higher than that of local MD, MEP will forward the packets; if the level of CFM PDUs received is lower than or equal to that of local MD, MIP will process locally instead of forwarding the packets, so as to avoid that CFM PDUs from low-level MD enter the high-level MD.

### Working Principles

From the above descriptions, we can learn that the operation of CFM protocol involves the following factors: MD, MA and MP (including MEP and MIP). MD defines the scope of maintenance; MA defines a subnet in MD, and is usually bound to a VLAN. One MD may have multiple MAs, because there may be multiple subnets. MP defines a maintenance point in one MA, and network connectivity is monitored by exchanging CFM PDUs among these maintenance points. Therefore, we can say that these maintenance points are used to quickly locate fault points when network link fails. Specifically, CFM mainly provides the following three features:

- Continuity Check
- Linktrace
- Loopback

Their working principles will be introduced below in detail.

### Continuity Check

Continuity check is used to detect the connectivity between MEPs in a MA. These MEPs will periodically send CFM PDUs called CCM (Continuity Check Message) to each other. If one MEP doesn't receive the CCMs sent from remote MEP within 3.5 times of the CCM transmit interval, it means that this remote MEP is lost, and this link may have failed. As shown in Fig 6, there is a MA1 in MD1, and MA1 serves VLAN 100. The following figure assumes that the ports (Gi0/1 - Gi0/8) of all switches within the red circle have been added to VLAN 100. MEP1 and MEP2 are at the boundary of MD1. Assuming that the CCM transmit interval is 1s, when executing continuity check, CCMs carrying VLAN 100 ID will be sent

periodically every second between MEP1 and MEP2. Assuming that MEP1 doesn't receive the CCMs sent from MEP2 within 3.5 times of the transmit interval (3.5 seconds in this example), MEP1 will assume that the link between MEP1 and MEP2 have failed, namely the connectivity failure is detected in VLAN 100.

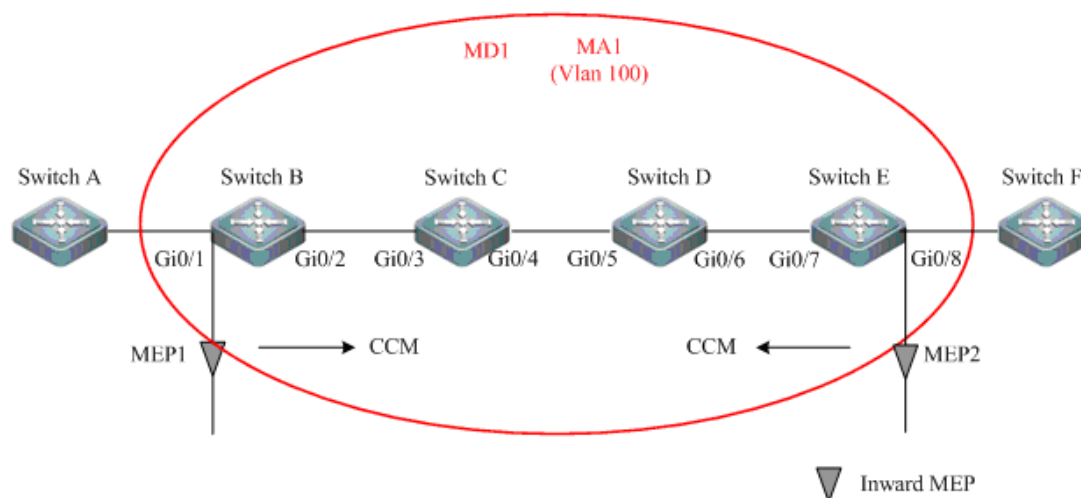


Fig 6

The following table lists the CCM transmit intervals supported by Ruijie switch products.

CCM transmit interval	Timeout time of remote MEP
10ms	35ms
100ms	350ms
1s	3.5s
10s	35s
60s	210s
600s	2100s

## Linktrace

Linktrace is similar to the "tracert" command used in Windows. By specifying the target MIP or MEP on one MEP, CFM PDUs called LTM (Linktrace Message) will be sent out, and all MIPs along the path will reply CFM PDUs called LTR (Linktrace Reply) to the source MEP, so that the path between source and target can be determined and fault points can be located. For example, Continuity Check may be able to detect the connectivity failure on the link between two MEPs, but it cannot locate the fault point, while Link Trace can locate the fault point to a specific MIP or MEP.

The working principle of Linktrace is shown in Fig 7. MA1 is configured in MD1 and serves VLAN 100. It is assumed that the ports (Gi0/1 - Gi0/8) of all switches within the red circle have been added to VLAN 100, and MEPs and MIPs have also been configured. Taking MEP1 as an example, the process of executing "Linktrace" is shown below: MEP1 sets MEP2 as its target. Since the direction is Inward, it sends out LTM from port Gi0/2. After MIP1 receives the message, it will reply a LTR to MEP1. Since MIP1 is not the target of LTM, it will forward the LTM to MIP2, which will also reply a LTR to MEP1. Since MIP2 is not the target of LTM, it will continue to forward the LTM until MEP2 receives the LTM and

replies a LTR to MEP1, so as to confirm that it is the target and end the transmission of LTM. Through the abovementioned process, MEP1 will get a detailed path diagram leading to MEP2.

Assuming that MEP1 doesn't receive the CCMs sent from MEP2 within 3.5 times of CCM transmit interval, which means that the link failure is detected between MEP1 and MEP2, we can then execute "Linktrace" to locate the fault point. If MIP1 doesn't reply with LTR, we can learn that the link between Switch B and Switch C has failed. Similarly, if MIP2 doesn't reply with LTR, we can learn that the link between Switch C and Switch D has failed...

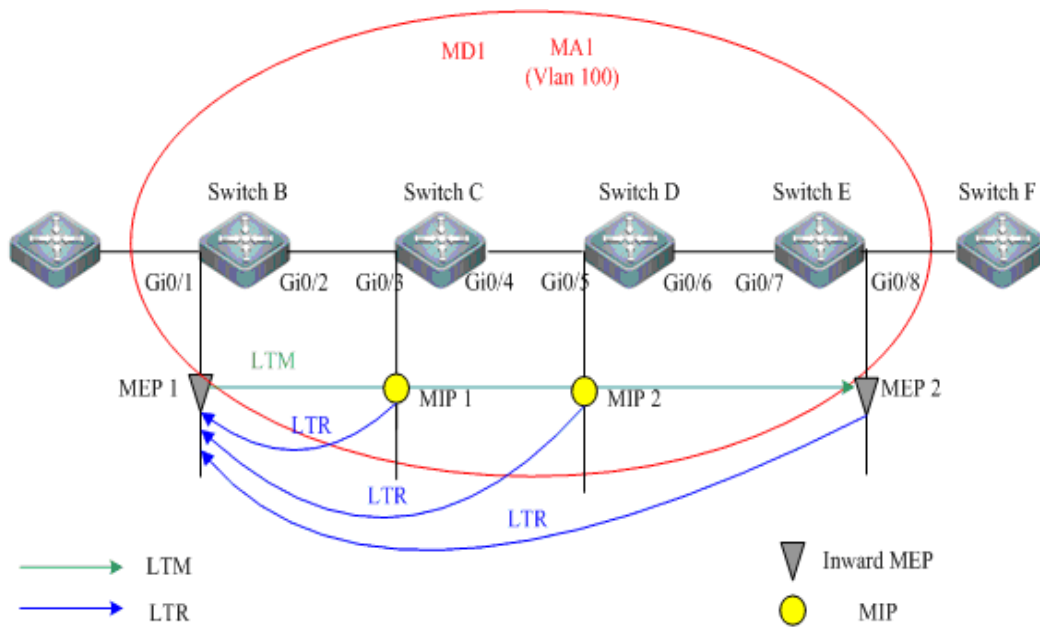


Fig 7

## Loopback

Loopback is similar to the "ping" command we use. As a feature provided by CFM, the MEP sends CFM PDUs called LBM (Loopback Message) to target MIP or MEP, which will reply with CFM PDUs called LBR (Loopback Response) after receiving such LBM. Therefore, this feature is similar the "ping" command we are familiar with. When Continuity Check detects connectivity failure on the link, we can use "Loopback" to verify this fault.

As shown in Fig 8, MA1 is configured in MD1 and serves VLAN 100. It is assumed that the ports (Gi0/1 - Gi0/8) of all switches within the red circle have been added to VLAN 100, and MEPs and MIPs have also been configured. This illustration involves two loopback examples (MIP and MEP).

In the case of MIP, assuming that the target is MIP2, execute "loopback" command and MEP1 will create a LBM (LBM1 in this example) with destination MAC Address being the MAC Address of MIP2, source MAC Address being that of MEP1. Since the direction of MEP1 is Inward, it will send out LBM1 from port Gi0/2, and MIP1 will receive and forward LBM1 after finding out that the destination MAC Address is not its own MAC Address. MIP2 will receive LBM1 and find out that the destination MAC Address is its own MAC Address. It will then generate a LBR (LBR1 in this example) with destination MAC Address being that of MEP1 and reply LBR1 to MEP1. The loopback process is then completed.

The loopback process in which MEP is the destination is same as the loopback process in which MIP is the destination.

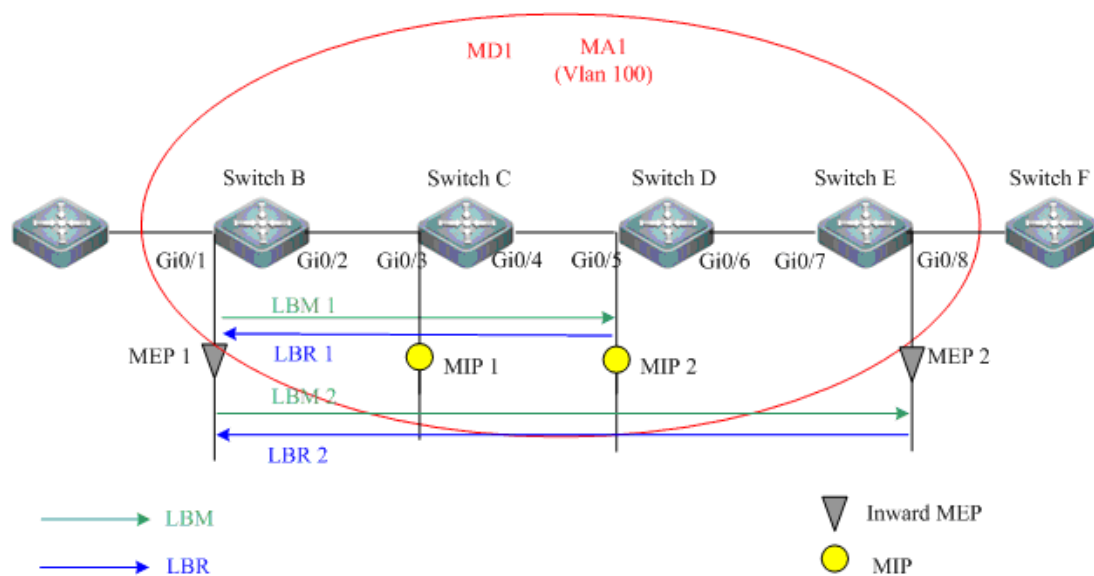


Fig 8

## Protocol Specifications

Related protocol specifications include:

- IEEE 802.1ag:Connectivity Fault Management

## Default configurations

The following table describes the default configurations of CFM.

Function	Default setting
CFM Enable State	CFM is disabled
MD	MD is not created
MA	MA is not created
Service-instance	Service-instance is not created
MEP	MEP is not created
MIP	MIP is not created
CCM transmit interval type	4, namely the transmit interval is 1s
Continuity Check Enable State	Continuity check is disabled
LTM TTL	64

## Configuring CFM

### Configuring to Enable CFM Protocol

By default, CFM protocol is disabled on device. Enter privilege mode and execute the following steps to enable CFM protocol:

Command	Function
Ruijie# <b>configure terminal</b>	Enter global configuration mode.
Ruijie(config)# <b>cfm enable</b>	Enable CFM protocol.
Ruijie(config)# <b>end</b>	Exit configuration mode.
Ruijie# <b>show cfm status</b>	Display the current status of CFM.

To disable CFM protocol, execute "no ethernet cfm enable" command in the global configuration mode.

Configuration example:

# Configure to enable CFM protocol on the switch

```
Ruijie# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Ruijie(config)# cfm enable
Ruijie(config)# end
Ruijie# show cfm status
CFM is enabled.
```

### Configuring Maintenance Domain

By default, no maintenance domain will be created on the device. Enter privilege mode and execute the following steps to create maintenance domain:

Command	Function
Ruijie# <b>configure terminal</b>	Enter global configuration mode.
Ruijie(config)# <b>cfm md md-name level level</b>	Create a maintenance domain and specify the domain name as "md-name" and domain level as "level". The maintenance domain name shall be a character string with length reaching 1-43; the domain level shall range between 0-7.
Ruijie(config)# <b>end</b>	Exit configuration mode.
Ruijie# <b>show cfm md</b>	Display all maintenance domains created on the device.

To delete one maintenance domain, execute "**no cfm md md-name**" global configuration command.

Configuration example:

## # Configure maintenance domain

```
Ruijie# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Ruijie(config)# cfm md md_test1 level 1
Ruijie(config)# end
Ruijie# show cfm md
CFM is enabled.
Total 1 MD(s) configured:
Level: 1    MD Name: md_test1
```

## Configuring Maintenance Association

By default, no maintenance association will be created on the device. Enter privilege mode and execute the following steps to create maintenance association:

Command	Function
Ruijie# <b>configure terminal</b>	Enter global configuration mode.
Ruijie(config)# <b>cfm ma</b> <i>ma-name</i> <b>vlan</b> <i>vlan-id</i>	Create a maintenance association and specify its name as "ma-name" and VLAN ID as "vlan-id". The MA name shall be a character string with length reaching 1-43; the VLAN ID shall range between 1-4094.
Ruijie(config)# <b>end</b>	Exit configuration mode.
Ruijie# <b>show cfm ma</b> <i>[[na-name]</i> <b>md</b> <i>md-name]</i>	Display all maintenance associations created on the device.

To delete one maintenance association, execute "**no cfm ma** *ma-name*" global configuration command.

Configuration example:

## # Configure maintenance association

```
Ruijie# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Ruijie(config)# cfm ma ma_test1 vlan 2
Ruijie(config)# end
Ruijie# show cfm ma
Total 2 MD(s) configured.
MD: md_test0
1 MA(s) belong(s) to MD md_test0:
MA: ma_test0
Service instance: 5    VLAN: 5    Level: 2

MD: md_test1
Total 1 MA(s) belong(s) to MD md_test1:
MA: ma_test1
```



Service instance: 1      VLAN: 2      Level: 1

**Caution**

The maintenance association can only be configured after configuring maintenance domain, and the sum of the length of MD name and the length of MA name must not exceed 44 characters.

## Configuring Service Instance

By default, no service instance will be created on the device. Enter privilege mode and execute the following steps to create service instance:

Command	Function
Ruijie# <b>configure terminal</b>	Enter global configuration mode.
Ruijie(config)# <b>cfm service-instance</b> <i>instance-id</i> <b>md</b> <i>md-name</i> <b>ma</b> <i>ma-name</i>	Create a service instance with id being "instance-id" and serving the maintenance association of "ma-name" in the maintenance domain of "md-name". The instance-id shall range between 1 and 32767.
Ruijie(config)# <b>end</b>	Exit configuration mode.
Ruijie# <b>show cfm md</b>	Display all maintenance domains created on the device.

To delete one service instance, execute "**no cfm service-instance** *instance-id*" global configuration command.

Configuration example:

### # Configure service instance

```
Ruijie# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Ruijie(config)# cfm service-instance 1 md md_test1 ma ma_test1
Ruijie(config)# end
Ruijie# show cfm service-instance 1
Service instance 1:
MD name: md_test1
MA name: ma_test1
Level: 1      VLAN: 2      MIP-rule: None      CCM interval: 1s
```

**Caution**

The service instance can only be configured after configuring maintenance association. Deleting service instance will only relieve the binding relation with maintenance association, which will not be deleted.

## Configuring MEP List

By default, no MEP list will be created on the device. Enter privilege mode and execute the following steps to configure MEP list:

Command	Function
Ruijie# <b>configure terminal</b>	Enter global configuration mode.
Ruijie(config)# <b>cfm mep-list</b> <i>mep-list</i> <b>service-instance</b> <i>instance-id</i>	Configure a MEP list for the service instance of "instance-id". The parameter of "mep-list" can be one MEP or a series of MEPs starting with the low MEP ID and ending with the high MEP ID and using "-" to link both IDs (i.e., 10-20). The MEP ID shall range between 1-8191.
Ruijie(config)# <b>end</b>	Exit configuration mode.
Ruijie# <b>show cfm mep</b> <i>mep-id</i> <b>service-instance</b> <i>instance-id</i>	Display the specified MEP list.

To delete one MEP, execute "**no cfm mep** *mep-id* **service-instance** *instance-id*" command in the interface configuration mode.

Configuration example:

# Configure MEP

```
Ruijie# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Ruijie(config)# cfm mep-list 1-3 service-instance 1
Ruijie(config)# end
Ruijie# show cfm mep-list service-instance 1
Service instance: 1
MEP list: 1 to 3.
```

## Configuring MEP

By default, no MEP will be created on the device. Enter privilege mode and execute the following steps to configure MEP:

Command	Function
Ruijie# <b>configure terminal</b>	Enter global configuration mode.
Ruijie(config)# <b>interface</b> <i>interface-name</i>	Enter interface configuration mode; MEP can be configured on physical interface or Aggregate Link.

Ruijie(config-if)# <b>cfm mep</b> <i>mep-id</i> <b>service-instance</b> <i>instance-id</i> <b>{ inward   outward }</b>	Configure a MEP with id being "mep-id" on the specified interface and specify the direction of MEP. This MEP shall belong to the service instance with id being "instance-id". MEP-ID shall range between 1 and 8191.
Ruijie(config)# <b>end</b>	Exit configuration mode.
Ruijie# <b>show cfm mep</b> <i>mep-id</i> <b>service-instance</b> <i>instance-id</i>	Display the specified MEP.

To delete one MEP, execute "**no cfm mep** *mep-id* **service-instance** *instance-id*" command in the interface configuration mode.

Configuration example:

#### # Configure MEP

Ruijie# **configure terminal**

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

Ruijie(config)# **interface** GigabitEthernet0/2

Ruijie(config-if)# **cfm mep** 1 **service-instance** 1 **inward**

Ruijie(config)# **end**

Ruijie# **show cfm mep** 1 **service-instance** 1

Interface: GigabitEthernet0/2

MD name: mdtest\_1

MA name: matest\_1

Level: 1      VLAN: 2      Direction: Inward

CCM send: Disable

FNG state: FNG\_RESET

CCM:

Current state: CCI\_IDLE

Interval: 1s      Send CCM: 0

Loopback:

NextTransId: 1

Send LBR: 0      Recv Ordered LBR: 0      Recv MisOrdered LBR: 0

Linktrace:

NextTransId: 1

SendLTR: 0      ReceiveLTM: 0



The MEP configured must already exist in the MEP list, or else MEP cannot be created successfully.

## Configuring MIP

By default, no MIP will be created on the device. After creating maintenance association, the device will not automatically create MIP. Enter privilege mode and execute the following steps to configure MIP:

Command	Function
Ruijie# <b>configure terminal</b>	Enter global configuration mode.
Ruijie(config)# <b>cfm mip-rule {default   explicit} service-instance <i>instance-id</i></b>	Create MIP generation rule for the specified service instance.
Ruijie(config)# <b>end</b>	Exit configuration mode.
Ruijie# <b>show cfm mp [interface <i>interface-name</i>]</b>	Display the specified maintenance point.

To delete MIP generation rule, execute "**no cfm mip-rule service-instance *instance-id***" command in the privilege mode.

Configuration example:

### # Configure MIP

```
Ruijie# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Ruijie(config)# cfm mip-rule default service-instance 1
Ruijie(config)# end
Ruijie# show cfm mp
Interface GigabitEthernet0/2  VLAN 2
MEP ID: 2    Level: 2    Service instance: 2    Direction: Inward
MD name: md_test10
MA name: ma_test10

MIP    Level: 1    Service instance: 1
MD name: md_test1
MA name: ma_test1
```

## Configuring to Enable Continuity Check

By default, continuity check will not be enabled after one MEP has been created on the device. Enter privilege mode and execute the following steps to enable continuity check:

Command	Function
Ruijie# <b>configure terminal</b>	Enter global configuration mode.
Ruijie(config)# <b>interface <i>interface-name</i></b>	Enter interface configuration mode.
Ruijie(config-if)# <b>cfm cc service-instance <i>instance-id</i> enable</b>	Enable continuity check on the specified service instance.
Ruijie(config)# <b>end</b>	Exit configuration mode.

Ruijie# <b>show cfm mep</b> <i>mep-id</i> <b>service-instance</b> <i>instance-id</i>	Display the specified MEP.
---	----------------------------

To disable continuity check, execute "**no cfm cc service-instance** *instance-id* **enable**" command.

Configuration example:

# Configure to enable continuity check

Ruijie# **configure terminal**

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

Ruijie(config)# **interface** Gi0/1

Ruijie(config-if)# **cfm cc service-instance** 1 **enable**

Ruijie(config)# **end**

Ruijie# **show cfm mep** 1 **service-instance** 1

Interface: GigabitEthernet0/2

MD name: md\_test1

MA name: ma\_test1

Level: 1      VLAN: 2      Direction: Inward

CCM send: Enable

FNG state: FNG\_RESET

CCM:

Current state: CCI\_IDLE

Interval: 1s      Send CCM: 0

Loopback:

NextTransId: 1

Send LBR: 0      Recv Ordered LBR: 0      Recv MisOrdered LBR: 0

Linktrace:

NextTransId: 1

SendLTR: 0      ReceiveLTM: 0

No CCM from some remote MEPs is received.

One or more error CCMs is received. The last-received CCM:

MD name :md\_test3

MA name :ma\_test3

MEPID :5      TransId :8000

Received Time: 02/3/6 13:01:34

One or more cross-connect CCMs is received. The last-received CCM:

MD name :md\_test4

MA name :ma\_test4

MEPID :6      TransId : 8009

Received Time: 02/3/6 13:01:34

Some other MEPs are transmitting the RDI bit

## Configuring CCM Transmit Interval

By default, the CCM transmit interval is 1s. Enter privilege mode and execute the following steps to configure CCM transmit interval:

Command	Function														
Ruijie# <b>configure terminal</b>	Enter global configuration mode.														
Ruijie(config)# <b>interface</b> <i>interface-name</i>	Enter interface configuration mode.														
Ruijie(config-if)# <b>cfm cc interval</b> <i>interval-type</i> <b>service-instance</b> <i>instance-id</i>	Configure CCM transmit interval type for the specified service instance. The parameter of "interval-type" shall range between 2-7. CCM transmit intervals represented by various interval types are shown below: <table> <tr> <td>Interval-type</td><td>CCM transmit interval</td></tr> <tr> <td>2</td><td>10ms</td></tr> <tr> <td>3</td><td>100ms</td></tr> <tr> <td>4</td><td>1s</td></tr> <tr> <td>5</td><td>10s</td></tr> <tr> <td>6</td><td>60s</td></tr> <tr> <td>7</td><td>600s</td></tr> </table>	Interval-type	CCM transmit interval	2	10ms	3	100ms	4	1s	5	10s	6	60s	7	600s
Interval-type	CCM transmit interval														
2	10ms														
3	100ms														
4	1s														
5	10s														
6	60s														
7	600s														
Ruijie(config)# <b>end</b>	Exit configuration mode.														
Ruijie# <b>show cfm mep</b> <i>mep-id</i> <b>service-instance</b> <i>instance-id</i>	Display the specified MEP.														

To restore the CCM transmit interval of all MEPs in one service instance to the default value, execute "**no cfm cc interval service-instance** *instance-id*" command.

Configuration example:

# Configure CCM transmit interval

```
Ruijie# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Ruijie(config)# interface GigabitEthernet0/2
Ruijie(config)# cfm cc interval 5 service-instance 1
Ruijie(config)# end
Ruijie(config)# show cfm mep 1 service-instance 1
Interface: GigabitEthernet0/2
MD name: md_test1
MA name: ma_test1
Level: 1      VLAN: 2      Direction: Inward
CCM send: Enable
```

FNG state: FNG\_RESET

CCM:

Current state: CCI\_IDLE

Interval: 10s      Send CCM: 0

Loopback:

NextTransId: 1

Send LBR: 0      Recv Ordered LBR: 0      Recv MisOrdered LBR: 0

Linktrace:

NextTransId: 1

SendLTR: 0      ReceiveLTM: 0

No CCM from some remote MEPs is received.

One or more error CCMs is received. The last-received CCM:

MD name :md\_test3

MA name :ma\_test3

MEPID :5      TransId :8000

Received Time: 02/3/6 13:01:34

One or more cross-connect CCMs is received. The last-received CCM:

MD name :md\_test4

MA name :ma\_test4

MEPID :6      TransId : 8009

Received Time: 02/3/6 13:01:34

Some other MEPs are transmitting the RDI bit



#### Note

IEEE 802.1ag has defined 7 types of CCM transmit intervals, namely 3.3ms, 10ms, 100ms, 1s, 10s, 60s, , 100ms, 1s, 10s, 60s and 600s CCM transmit intervals, while other switch products can only support 1s or above CCM transmit interval.

## Configuring Linktrace

By default, the device will not automatically execute linktrace function. Enter privilege mode and execute the following steps to execute linktrace:

Command	Function
Ruijie# <b>configure terminal</b>	Enter global configuration mode.

Ruijie(config)# <b>cfm linktrace service-instance</b> <i>instance-id</i> <b>mep</b> <i>mep-id</i> [ <b>remote-mep</b> <i>remote-mep-id</i>   <b>remote-mac</b> <i>mac-address</i> ] [ <b>ttl</b> <i>ttl-value</i> ] [ <b>hw-only</b> ]	Execute linktrace on the specified MEP in the specified service instance. Specify the MEP ID if the target is a MEP or MIP MAC Address if the target is a MIP.
Ruijie(config)# <b>end</b>	Exit configuration mode.
Ruijie# <b>show cfm linktrace-info</b> [ <b>service-instance</b> <i>instance-id</i> [ <b>mep</b> <i>mep-id</i> ]]	Display the result of linktrace.

Configuration example:

# Configure linktrace function

Ruijie# **configure terminal**

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

Ruijie(config)# **cfm linktrace service-instance 1 mep 1 remote-mep 2**

Linktrace to MEP 2 with the sequence number 1-1001

MAC Address	TTL	Last MAC	Relay Action
0010-FC00-6512	63	0010-FC00-6500	Hit

Ruijie(config)# **end**

Ruijie(config)# **show cfm linktrace-info service-instance 1**

Service instance: 1 MEP ID: 1

MAC Address	TTL	Last MAC	Relay Action
0010-FC00-6512	63	0010-FC00-6500	Hit

## Configuring Linktrace Auto-Detection

By default, if the CCM sent from the remote MEP is not received within 3.5 times of the CCM transmit interval, the local MEP will not automatically execute linktrace function. Enter privilege mode and execute the following steps to configure linktrace auto-detection when the remote MEP is lost:

Command	Function
Ruijie# <b>configure terminal</b>	Enter global configuration mode.
Ruijie(config)# <b>cfm linktrace auto-detection size</b> <i>entries-count</i>	Enable linktrace auto-detection on the device. You can specify the number of linktrace result entries to be saved.
Ruijie(config)# <b>end</b>	Exit configuration mode.
Ruijie# <b>show cfm linktrace-info auto-detection</b> [ <b>size</b> <i>entries-count</i> ]	Display the result of linktrace auto-detection.

Configuration example:

# Configure linktrace auto-detection

Ruijie# **configure terminal**

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

Ruijie(config)# **cfm linktrace auto-detection**

Ruijie(config)# **end**



```

Ruijie# show cfm linktrace-info auto-detection
Service instance: 1      MEP ID: 1      Time: 2010/02/27 20:10:10
Target MEP ID: 3      TTL: 64
MAC Address      TTL      Last MAC      Relay Action
0010-FC00-6505    63      0000-FC00-6504  MPDB
0010-FC00-A852    62      0000-FC00-6505  FDB
0000-FC00-6508    61      0010-FC00-A852  Hit
Service instance: 2      MEP ID: 2      Time: 2010/02/27 21:10:10
Target MEP ID: 4      TTL: 64
MAC Address      TTL      Last MAC      Relay Action
0010-FC00-6508    61      0010-FC00-A852  Hit

```

## Configuring Loopback

By default, the device will not automatically execute loopback function. Enter privilege mode and execute the following steps to execute loopback function:

Command	Function
Ruijie# <b>cfm loopback service-instance <i>instance-id</i> mep <i>mep-id</i> {remote-mep <i>remote-mep-id</i>   remote-mac <i>mac-address</i>} [count <i>count</i>]</b>	Execute loopback on the specified MEP in the specified service instance. Specify the MEP ID if the target is a MEP or MIP MAC Address if the target is a MIP.

Configuration example:

# Configure loopback function

```

Ruijie# ethernet cfm loopback service-instance 1 mep 1 remote-mep 2
Loopback to 0010-FC00-6512 with the sequence number start from 1-1017:
Reply from 0010-FC00-6512: sequence number=1-1017
Reply from 0010-FC00-6512: sequence number=1-1018
Reply from 0010-FC00-6512: sequence number=1-1019
Reply from 0010-FC00-6512: sequence number=1-1020
Reply from 0010-FC00-6512: sequence number=1-1021
Loopback Message Sent:5 Received:5 Lost:0 (%0 loss)

```

## Displaying Configurations

CFM has provided the following commands to display various configurations and status information. Their descriptions are given below:

Command	Function
<b>show cfm md</b>	Display the maintenance domains configured on the device.

<b>show cfm ma</b> [ <i>ma-name</i> ] <b>md</b> <i>md-name</i> ]	Display the maintenance associations configured on the device.
<b>show cfm mep</b> <i>mep-id</i> <b>service-instance</b> <i>instance-id</i>	Display the detailed configurations and operational information of MEP.
<b>show cfm mp</b> [ <b>interface</b> <i>interface-id</i> ]	Display the MP configured, including information about MEP and MIP.
<b>show cfm remote-mep service-instance</b> <i>instance-id</i> <b>mep</b> <i>mep-id</i>	Display the information of remote MEP.
<b>show cfm service-instance</b> [ <i>instance-id</i> ]	Display service instance.
<b>show cfm linktrace-info</b> [ <b>service-instance</b> <i>instance-id</i> [ <b>mep</b> <i>mep-id</i> ] ]	Display the result of linktrace.
<b>show cfm linktrace-info auto-detection</b> [ <b>size</b> <i>entries-count</i> ]	Display the result of linktrace auto-detection.
<b>show cfm status</b>	Display CFM status.

## Typical CFM Configuration Examples

To accomplish complete CFM functions, this configuration example will be divided into the following steps:

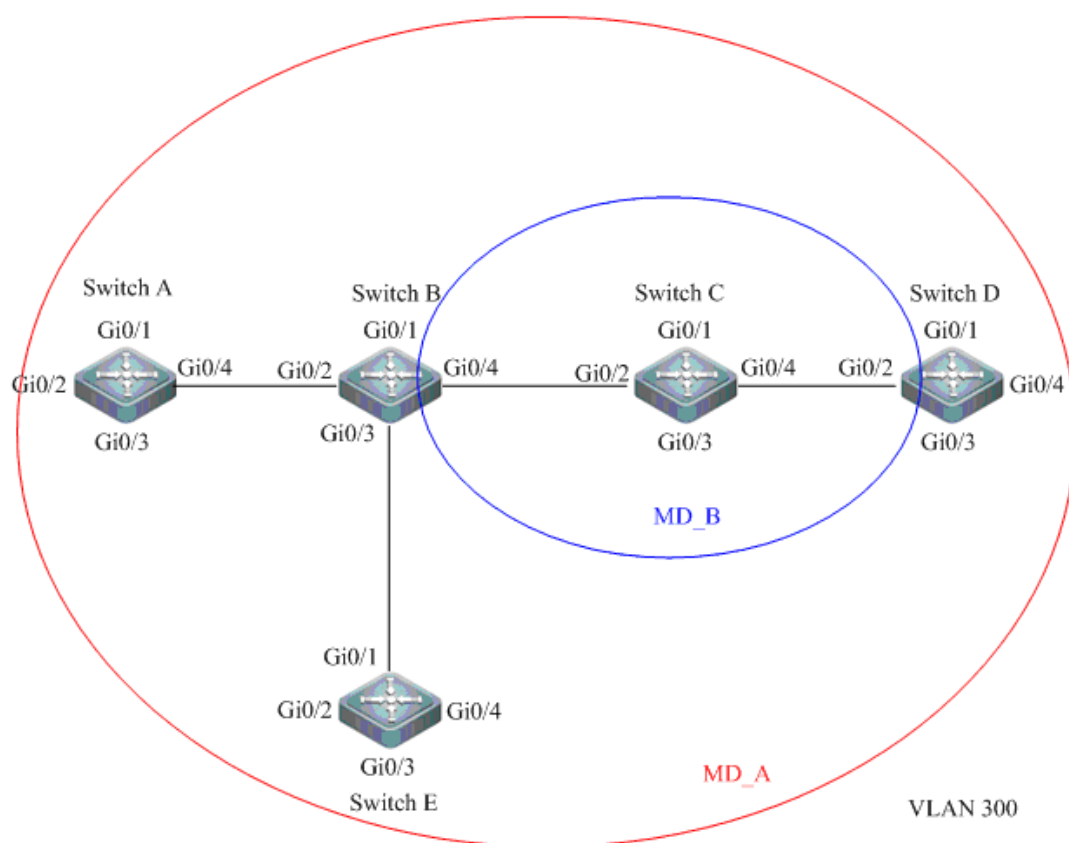
- Configure service instance
- Configure MEP and enable continuity check
- Configure MIP
- Configure MEP linktrace
- Configure MEP loopback

### Configuring Service Instance

#### Networking Requirements

- 1) Four devices are connected in a straight line, while another device is connected to any of two intermediate devices.
- 2) Plan two maintenance domains among these five devices: MD\_A and MD\_B. MD\_A will have 3 MEPs, while MD\_B will have 2 MEPs. The level of MD\_A is 6, while the level of MD\_B is 2. MD\_B is nested in MD\_A.
- 3) Each maintenance association in the maintenance domain serves the same VLAN of "VLAN 100".

## Network Topology



**Fig 9 Layout of maintenance domains**

### Configuration Tips

According to the location of end points in the maintenance domains as shown in Figure 9, the following configurations shall be executed:

Configure maintenance domain of "MD\_A" on Switch A and Switch E.

Configure maintenance domain of "MD\_B" on Switch C.

Configure maintenance domain of "MD\_A" and "MD\_B" on Switch B and Switch D.

Configure a maintenance association (MA) on each device for their respective maintenance domains.

Configure a corresponding service instance for each maintenance association.

### Configuration Steps

#### 1) Switch A

# Configure a maintenance domain of "MD\_A" with level being 6; configure a maintenance association of "MA\_A" serving VLAN 300; create a service instance with ID being 1 and serving MA\_A in MD\_A.

Ruijie# **configure terminal**

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

Ruijie(config)# **cfm enable**

Ruijie(config)# **cfm md MD\_A level 6**

```
Ruijie(config)# cfm ma MA_A vlan 300
Ruijie(config)# cfm service-instance 1 md MD_A ma MA_A
```

## 2) Switch B

# Configure a maintenance domain of "MD\_A" with level being 6; configure a maintenance association of "MA\_A" serving VLAN 300; create a service instance with ID being 1 and serving MA\_A in MD\_A. Configure a maintenance domain of "MD\_B" with level being 2; configure a maintenance association of "MA\_B" serving VLAN 300; create a service instance with ID being 2 and serving MA\_B in MD\_B.

```
Ruijie# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Ruijie(config)# cfm enable
Ruijie(config)# cfm md MD_A level 6
Ruijie(config)# cfm ma MA_A vlan 300
Ruijie(config)# cfm service-instance 1 md MD_A ma MA_A
Ruijie(config)# cfm md MD_B level 2
Ruijie(config)# cfm ma MA_B vlan 300
Ruijie(config)# cfm service-instance 2 md MD_B ma MA_B
```

## 3) Switch C

# Configure a maintenance domain of "MD\_B" with level being 2; configure a maintenance association of "MA\_B" serving VLAN 300; create a service instance with ID being 2 and serving MA\_B in MD\_B.

```
Ruijie# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Ruijie(config)# cfm enable
Ruijie(config)# cfm md MD_B level 2
Ruijie(config)# cfm ma MA_B vlan 300
Ruijie(config)# cfm service-instance 2 md MD_B ma MA_B
```

## 4) Switch D

# Configure a maintenance domain of "MD\_A" with level being 6; configure a maintenance association of "MA\_A" serving VLAN 300; create a service instance with ID being 1 and serving MA\_A in MD\_A. Configure a maintenance domain of "MD\_B" with level being 2; configure a maintenance association of "MA\_B" serving VLAN 300; create a service instance with ID being 2 and serving MA\_B in MD\_B.

```
Ruijie# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Ruijie(config)# cfm enable
Ruijie(config)# cfm md MD_A level 6
Ruijie(config)# cfm ma MA_A vlan 300
Ruijie(config)# cfm service-instance 1 md MD_A ma MA_A
Ruijie(config)# cfm md MD_B level 2
```

```
Ruijie(config)# cfm ma MA_B vlan 300
Ruijie(config)# cfm service-instance 2 md MD_B ma MA_B
```

## 5) Switch E

# Configure a maintenance domain of "MD\_A" with level being 6; configure a maintenance association of "MA\_A" serving VLAN 300; create a service instance with ID being 1 and serving MA\_A in MD\_A.

```
Ruijie# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Ruijie(config)# cfm enable
Ruijie(config)# cfm md MD_A level 6
Ruijie(config)# cfm ma MA_A vlan 300
Ruijie(config)# cfm service-instance 1 md MD_A ma MA_A
```

## Verification

After the aforementioned configurations, execute the following commands on the Switch A-E to verify the configurations. Here we will take Switch A as an example, and the verification process is also applicable to other devices.

### 1) Verify whether CFM has been enabled.

```
Ruijie# show cfm status
```

CFM is enabled.        //+ indicates that CFM protocol has been enabled, while "disabled" indicates that CFM is not enabled.

### 2) Verify the maintenance domain

```
Ruijie(config)# show cfm md
CFM is enabled.
Total 1 MD(s) configured:
Level: 6    MD name: MD_A
```

### 3) Verify the maintenance association

```
Ruijie# show cfm ma
Total 1 MD(s) configured.
MD: MD_A
1 MA(s) belong(s) to MD MD_A:
MA: MA_A
Service instance: 1    VLAN: 300    Level: 6
```

### 4) Verify the service instance

```
Ruijie# show cfm service-instance 1
Service instance 1:
MD name: MD_A
MA name: MA_A
Level: 6    VLAN: 300    MIP: None    CCM interval: 1s
```

//+MIP:None indicates that MIP is not configured.

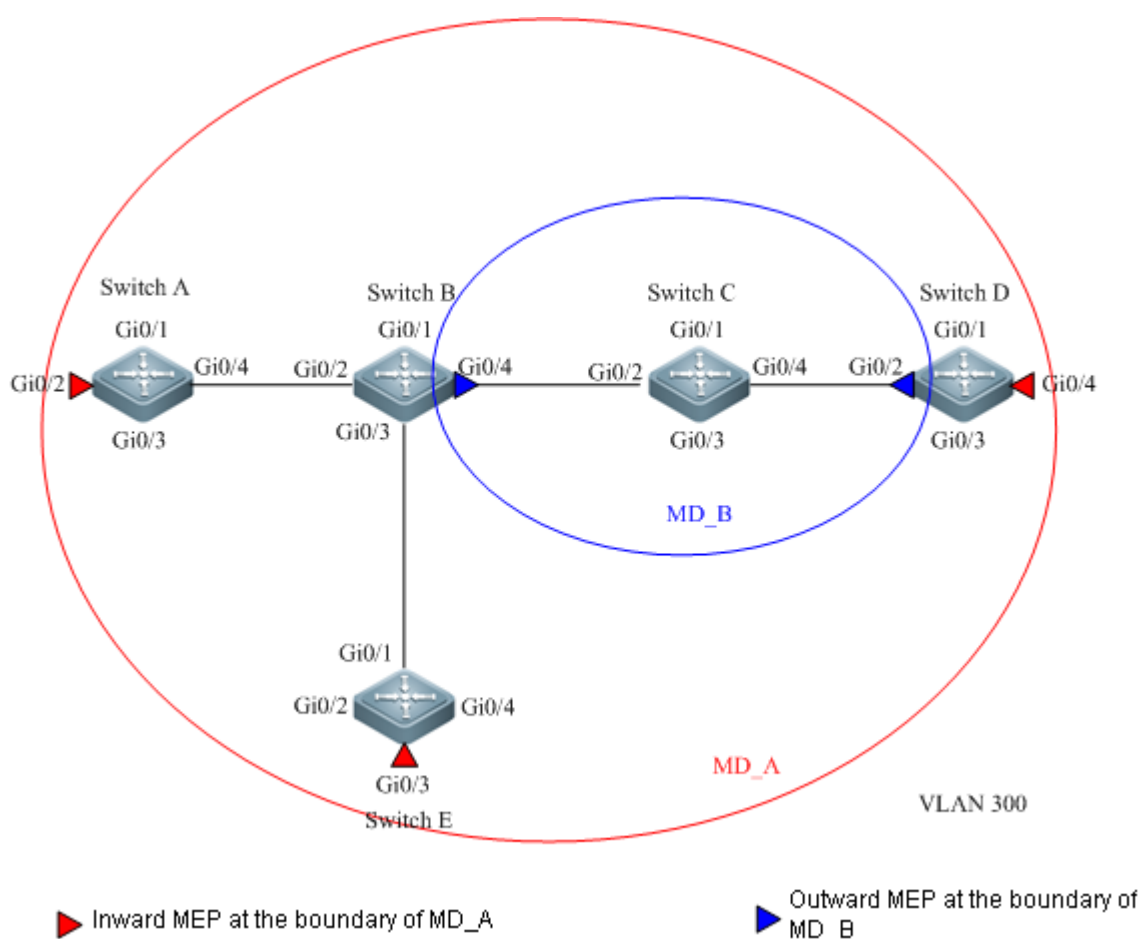
## Configuring MEP and Enabling Continuity Check

### Networking Requirements

After the configuration of service instance, we shall proceed with MEP configuration. MEP is used to define the boundary of maintenance domain, so it must be configured on the boundary port of maintenance domain:

- 1) Determine all boundary ports of each maintenance domain;
- 2) Determine the direction of MEP configured on each boundary port according to the location of maintenance domain;
- 3) Determine the unique ID in the maintenance association for each MEP;
- 4) Determine the remote MEP to be detected by each MEP.

### Network Topology



**Fig 10 Maintenance domains and maintenance end points**

## Configuration Tips

According to the location of end points in the maintenance domains as shown in Figure 10, the following configurations shall be executed:

MD\_A has three boundary ports, namely Gi0/2 on Switch A, Gi0/4 on Switch D and Gi0/3 on Switch E. Since they will not send CFM PDUs at MD\_A level on local ports, Inward MEPs must be configured on these ports.

MD\_B has two boundary ports, namely Gi0/4 on Switch B and Gi0/2 on Switch D. Since they will send CFM PDUs at MD\_B level on local ports, Outward MEPs must be configured on these ports.

For one domain, a MEP list must be configured on each device with a boundary port, indicating that only CFM PDUs sent from these MEPs will be processed.

Enable continuity check on all MEPs configured.

## Configuration Steps

### 1) Switch A

# Configure a MEP list on this device, including all MEPs to be configured in MD\_A, and configure one Inward MEP on Gi0/2 and enable continuity check function.

Ruijie# **configure terminal**

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

Ruijie(config)# **cfm mep-list 1-3 service-instance 1**

Ruijie(config)# **interface Gi0/2**

Ruijie(config-if)# **cfm mep 1 service-instance 1 inward**

Ruijie(config-if)# **cfm cc service-instance 1 enable**

### 2) Switch B

# Configure a MEP list on this device, including all MEPs to be configured in MD\_B, and configure one Outward MEP on Gi0/4 and enable continuity check function.

Ruijie# **configure terminal**

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

Ruijie(config)# **cfm mep-list 4-5 service-instance 2**

Ruijie(config)# **interface Gi0/4**

Ruijie(config-if)# **cfm mep 4 service-instance 2 outward**

Ruijie(config-if)# **cfm cc service-instance 2 enable**

### 3) Switch D

# Gi0/2 on this device is the boundary port of MD\_B, while Gi0/4 is the boundary port of MD\_A. The configurations shall be:

# First configure a MEP list on this device, including all MEPs to be configured in MD\_A, and configure one Inward MEP on Gi0/4 and enable continuity check function.

Further configure a MEP list on this device, including all MEPs to be configured in MD\_B, and configure one Outward MEP on Gi0/2 and enable continuity check function.

Ruijie# **configure terminal**

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

Ruijie(config)# **cfm mep-list 1-3 service-instance 1**

Ruijie(config)# **interface Gi0/4**

Ruijie(config-if)# **cfm mep 2 service-instance 1 inward**

Ruijie(config-if)# **cfm cc service-instance 1 enable**

Ruijie(config-if)#**end**

Ruijie(config)# **cfm mep-list 4-5 service-instance 2**

Ruijie(config)# **interface Gi0/2**

Ruijie(config-if)# **cfm mep 5 service-instance 2 outward**

Ruijie(config-if)# **cfm cc service-instance 2 enable**

#### 4) Switch E

# Configure a MEP list on this device, including all MEPs to be configured in MD\_A, and configure one Inward MEP on Gi0/3 and enable continuity check function.

Ruijie# **configure terminal**

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

Ruijie(config)# **cfm mep-list 1-3 service-instance 1**

Ruijie(config)# **interface Gi0/3**

Ruijie(config-if)# **cfm mep 3 service-instance 1 inward**

Ruijie(config-if)# **cfm cc service-instance 1 enable**

## Verification

After the aforementioned configurations, execute the following commands on the Switch A, Switch B, Switch D and Switch E to verify the configurations. Here we will take Switch A as an example, and the verification process is also applicable to other devices.

#### 1) Verify MEP list

Ruijie# **show cfm mep-list service-instance 1**

Service instance: 1

MEP list: 1 to 3. //+ indicates that a MEP list has been configured on the device for service instance 1

#### 2) Verify MEP

Ruijie# **show cfm mep 1 service-instance 1**

Interface: GigabitEthernet0/2

MD name: MD\_A

MA name: MA\_A

Level: 6 VLAN: 300 Direction: Inward //+ level of local MD, VLAN ID and MEP direction

CCM send: Enable //+ Enable continuity check

FNG state: FNG\_DEFECT\_REPORTED

CCM:

Current state: CCI\_WAITING



Interval: 1s    Send CCM: 12    //+ CCM transmit interval, and the number of CCMs sent

Loopback:

NextTransId: 120

Send LBR: 0    Recv Ordered LBR: 0    Recv MisOrdered LBR: 0

Linktrace:

NextTransId: 10

SendLTR: 0    ReceiveLTM: 0

## Configuring MIP

### Networking Requirements

After the configuration of MEP, CFM function is now active. However, when there are multiple hops between two MEPs in one maintenance domain and if no MIP is configured between these two MEPs, the fault cannot be located to a specific device if there is link failure between them. Therefore, this section will carry on with MIP planning.

### Network Topology

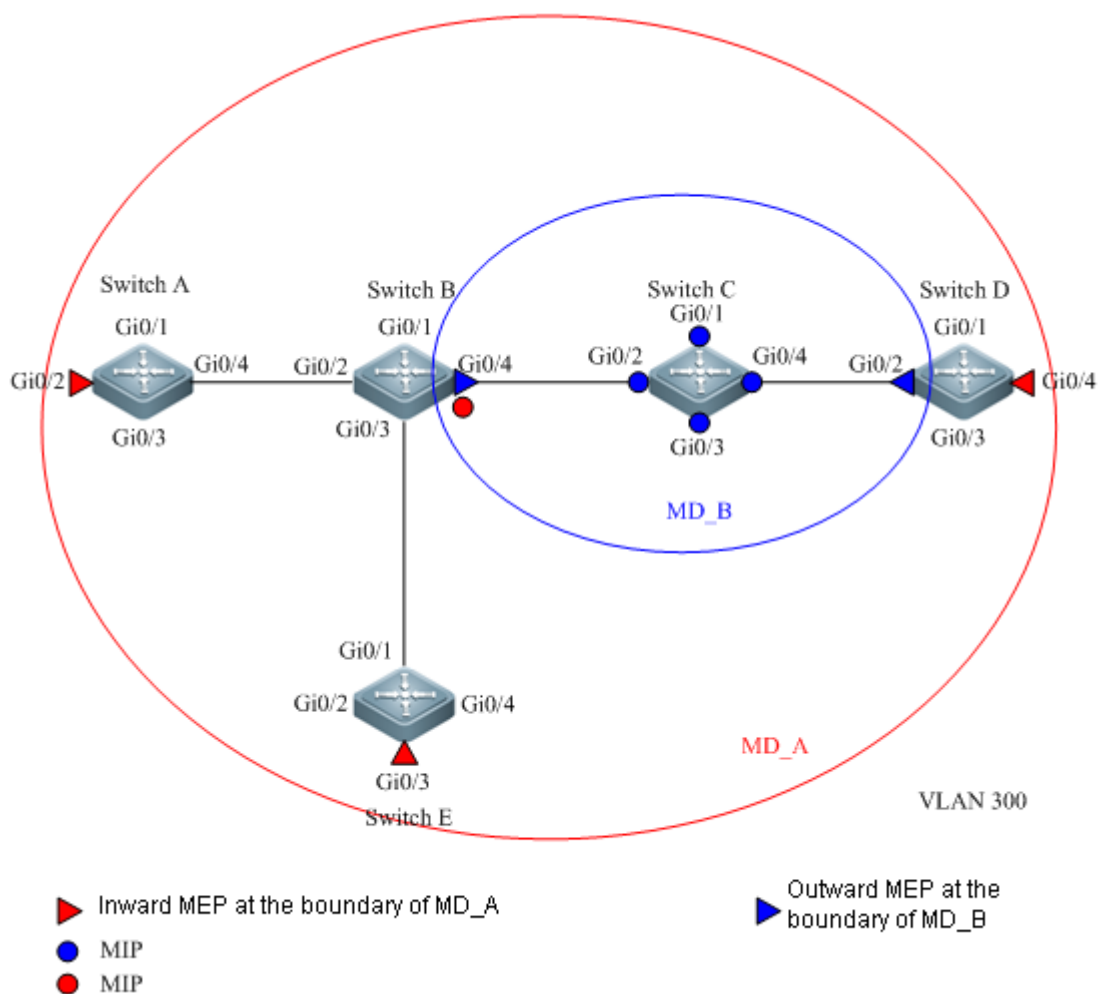


Fig Maintenance domains and maintenance intermediate points

## Configuration Tips

There are two rules to generate MIP: default rule and explicit rule.

If the default rule is configured on the device, MIP will be generated on the port meeting the following two conditions:

Lower level MA is not configured on the device.

If lower level MA is configured on the device, then MIP will be generated only on the port configured with lower level MEP.

If explicit rule is configured on the device, then MIP will be generated only on the port configured with MEP of lower level MD.

According to the aforementioned MIP generation rules, the configuration tips are shown below:

Configure MIP of MD\_A on Switch B. Since lower level MD\_B has been configured on Switch B and MEP of MD\_B has been configured on Gi0/4, MIP shall be generated on this device using explicit rule.

Configure MIP of MD\_B on Switch C. Since there is no lower level MD on Switch C, the default rule must be used in order to generate MIP. In this way, a MIP will be generated on all ports.

## Configuration Steps

### 1) Switch B

# Use explicit rule on this device to generate MIP for MD\_A.

Ruijie# **configure terminal**

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

Ruijie(config)# **cfm mip-rule explicit service-instance 1**

### 2) Switch C

# Use explicit rule on this device to generate MIP for MD\_B.

Ruijie# **configure terminal**

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

Ruijie(config)# **cfm mip-rule explicit service-instance 2**

## Verification

After the aforementioned configurations, execute the following commands on the Switch B and Switch C to verify the configurations. Here we will take Switch B as an example, and the verification process is also applicable to Switch C.

### 1) Verify the MIP generation rule configured on Switch B

Ruijie# **show cfm service-instance 1**

Service instance 1:

MD name: MD\_A

MA name: MA\_A

Level: 6      VLAN: 300      MIP-rule: Explicit      CCM interval: 1s

//+ we can see that the MIP generation rule is Explicit

## 2) Verify the MIP generation rule configured on Switch C

```
Ruijie# show cfm service-instance 2
```

Service instance 2:

MD name: MD\_B

MA name: MA\_B

Level: 2      VLAN: 300      MIP-rule: Default      CCM interval: 1s

//+ we can see that the MIP generation rule is Default

## Configuring MEP Linktrace

### Networking Requirements

Through CFM continuity check, the MEP on device can acquire information about other MEPs in this maintenance domain, and the maintenance point (MP) can be created together with the MIP configured. We can use linktrace to have the detailed path to other MEPs in the maintenance domain.

### Network Topology

See Fig 11

### Configuration Tips

According to the MEPs configured in Fig 11, in order to learn the path between MEP on Switch A and the MEP on Switch D, we will need to initiate linktrace on Switch A, and then the MEP on Switch A will send LTM to the MEP on Switch D.

### Configuration Steps

#### 1) Switch A

# Initiate linktrace on this device. The source MEP is MEP1 and the target is the MEP on Switch D. According to the aforementioned configurations, we can learn that its MEP ID is 2.

```
Ruijie# configure terminal
```

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

```
Ruijie(config)# cfm linktrace service-instance 1 mep 1 remote-mep 2
```

### Verification

After executing linktrace on Switch A, an entry of linktrace result will be formed and saved. Execute the following command on this device to display linktrace result.

#### 1) Display linktrace result on Switch A

```
Ruijie# show cfm linktrace-info service-instance 1
```

Service instance: 1      MEPID: 1

MAC Address	TTL	PreHop MAC	Relay Action
-------------	-----	------------	--------------

00d0-F800-6505	63	00d0-F800-6504	FDB
00d0-F800-A852	62	00d0-F800-6505	Hit

## Configure MEP loopback

### Networking requirements

You can use loopback function to verify whether a link on the network is connected.

### Network topology

See Fig 11

### Configuration tips

According to the MEPs configured in Fig 11, in order to verify whether the link between Switch A and Switch D is connected, we will need to initiate loopback on Switch A, and then the MEP on Switch A will send LBM to the MEP on Switch D.

### Configuration steps

#### 1) Switch A

# Initiate loopback on this device. The source MEP is MEP1 and the target is the MEP on Switch D. According to the aforementioned configurations, we can learn that its MEP ID is 2.

Ruijie# configure terminal

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

Ruijie#cfm loopback service-instance 1 mep 1 remote-mep 2

Loopback to 00d0-F800-8612 with the sequence number start from 2-1000:

Reply from 00d0-F800-8612: sequence number=2-1000

Reply from 00d0-F800-8612: sequence number=2-1001

Reply from 00d0-F800-8612: sequence number=2-1002

Reply from 00d0-F800-8612: sequence number=2-1003

Reply from 00d0-F800-8612: sequence number=2-1004

Loopback Message Sent:5 Received:5 Lost:0 (%0 loss)

### Verification

Please refer to the above command for the execution result of loopback. There is no special command to verify the result of loopback.

# REUP Configuration

## REUP Overview

### Understanding REUP

The Rapid Ethernet Uplink Protection protocol (REUP) protects Ethernet uplink rapidly.

Ports are configured in pair on the ends of an uplink, with one being active and the other being standby. When two ports are up, one of them is set to be backup. For details, refer to section Configure REUP Preemption Mode and Delay.

By default, the standby port is in backup status, which cannot forward packets. When the port in forward status is down, the backup port transfers to health status and forwards packets. Moreover, the REUP advertises address update messages to upstream devices for updating MAC address, so that data interruption can be restored in 50ms in case of a link failure.

The REUP and STP are mutually exclusive on a port. In this case, the STP runs on downstream and the REUP runs on upstream for uplink backup and problem protection. The REUP offers basic link redundancy even if the STP is disabled while enabling millisecond-level fault recovery.

### Default REUP Configuration

The following table shows default REUP configuration:

Item	Default value
REUP	Disabled
Preemption mode	Off
Preemption delay	35 seconds
Mac update transit	Disable
Mac update receive	Disabled

### REUP Configuration Guide

Before configuring the REUP, note that:

- A port belongs to only one REUP pair. Each active link has only one standby link and vice versa. The active link and the standby link must be different ports.
- The REUP supports Layer2 physical port and Layer2 AP port, not AP member port.
- The primary port can be of different type than the secondary port. So do their rates. For example, you can set the AP port as the primary port and the physical port as the secondary port.

- The STP is disabled on the port with the REUP enabled. The port with the REUP configured does not participate in STP. BPDU penetrate transmission is supported when the STP is disabled.
- A device can be configured with up to 16 REUP pairs and 8 address update groups. Each address update group has up to four member ports. A port belongs to only one address update group.
- It is necessary to disable modifying the attributes of a port after the REUP is configured successfully on it.

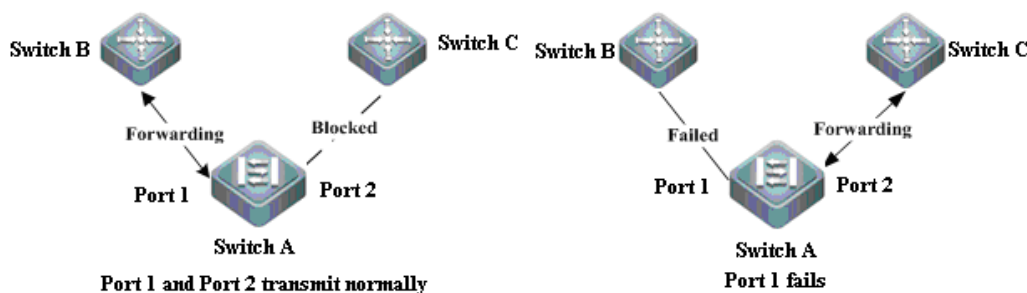
## Configuring REUP

### Configuring Dual Link Backup

You can configure a REUP pair by specifying one port as the standby port of another port. When two links are up, one is active (forwarding packets), and the other is standby (not forwarding packets). If the active link fails, the standby link becomes active and begins to forward packets. After the active link recovers from the fault, it becomes standby and does not forward any packets. Certainly, you can set the link recovered from the fault to preempt the currently active link.

As shown in Figure-1, for example, Switch A's port 1 and port 2 are connected to the upstream switches B and C. REUP is enabled on port 1 and port 2. Port 1 is active for forwarding packets; port 2 is backup. Switch C does not forward any packets from Switch A. Once port 1 fails, port 2 starts to forward packets. If port 1 recovers from the fault, it becomes backup.

**Figure-1 REUP topology**



In the privileged EXEC configuration mode, execute the following command to configure a REUP pair:

Command	Function
Ruijie # <b>configure terminal</b>	Enter the global configuration mode.
Ruijie (config) # <b>interface interface-id</b>	Enter the interface configuration mode.
Ruijie (config-if) # <b>switchport backup interface interface-id</b>	Configure a Layer 2 physical port or a layer 2 AP port as a backup port
Ruijie(config-if)# <b>end</b>	Return to the privileged EXEC mode.

Ruijie# <b>show interfaces</b> [ <i>interface-id</i> ] <b>switchport backup</b> [detail]	Show the configuration.
Ruijie# <b>copy running-config startup-config</b>	Save the configuration.

For example:

```
Ruijie# configure
Enter configuration commands, one per line. End with CNTL/Z.
Ruijie(config)# interface gigabitEthernet 0/1
Ruijie(config-if)# switchport backup interface gigabitEthernet 0/2
Ruijie(config-if)# show interface switchport backup
Switch Backup Interface Pairs:
Active Interface      Backup Interface      State
-----
GigabitEthernet 0/1   GigabitEthernet 0/2   Active Up/Backup Down
```

## Configuring the Preemption Mode and Delay

By configuring the preemption mode, you can determine the best available link. For bandwidth mode, the REUP will use a link of larger bandwidth. For forced mode, the REUP will forcibly use a reliable and stable link.

To avoid frequent active-standby link switching, you can define preemption delay. After two links recover, link switching occurs after the delay.

In the privileged Exec mode, execute the following commands to configure the preemption mode and delay:

Command	Function
Ruijie # <b>configure terminal</b>	Enter the global configuration mode.
Ruijie (config) # <b>interface</b> <i>interface-id</i>	Enter the interface configuration mode.
Ruijie (config-if) # <b>switchport backup interface</b> <i>interface-id</i>	Configure a Layer 2 physical port or a layer 2 AP port as a backup port.
Ruijie(config-if)# <b>switchport backup interface</b> <i>interface-id</i> <b>preemption mode</b> { forced bandwidth off }	Configure the preemption mode: Forced: The primary port always preempts the secondary port. Bandwidth: Use the port of higher bandwidth. Off: Disable preemption.
Ruijie(config-if)# <b>switchport backup interface</b> <i>interface-id</i> <b>preemption delay</b> <i>delay-time</i>	Configure preemption delay, which takes effect only in forced and bandwidth modes.
Ruijie(config-if)# <b>end</b>	Return to the privileged EXEC mode.
Ruijie# <b>show interfaces</b> [ <i>interface-id</i> ] <b>switchport backup</b> [detail]	Show the configuration.

Ruijie# <b>copy</b> <b>running-config</b> <b>startup-config</b>	Save the configuration.
---	-------------------------

For example:

```
Ruijie# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Ruijie (config) # interface gigabitEthernet 0/1
Ruijie (config-if) # switchport backup interface gigabitEthernet 0/2 preempt mode forced
Ruijie (config-if) # switchport backup interface gigabitEthernet 0/2 preempt delay 50
Ruijie (config-if) # show interfaces switchport backup detail
Switch Backup Interface Pairs:
Active Interface      Backup Interface      State
-----
GigabitEthernet 0/1   GigabitEthernet 0/2   Active Up/Backup Down
Interface Pair : Gi0/1, Gi0/2
Preemption Mode : forced
Preemption Delay : 50 seconds
Bandwidth : Gi0/1(1000 Mbits), Gi0/2(10 Mbits)
```

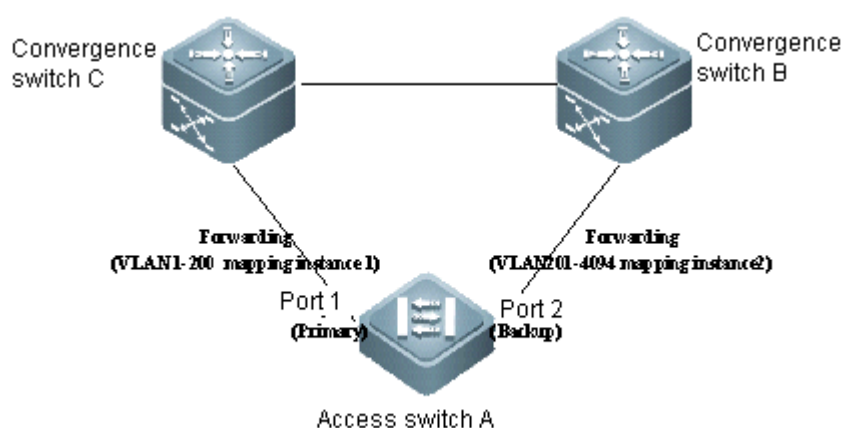


#### Note

1. The bandwidth of an AP port is the number of its members whose link is up multiplying the speed of the members.
2. Once the STP is enabled on the uplink, the preemption delay should be larger than 35 seconds.

## Configuring the VLAN Load Balancing

VLAN load balancing allows two ports of REUP pair to forward data packets of mutually exclusive VLANs, thus making maximum use of link bandwidth.

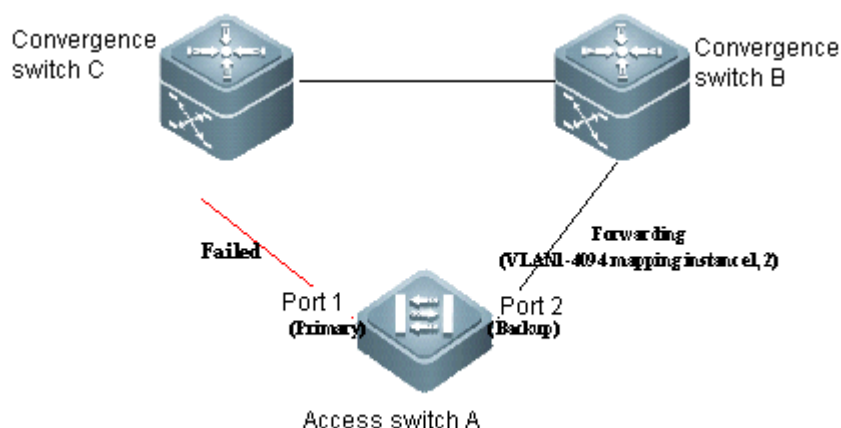


**Fig 3 Topology in which both links for load balancing are normal**

As shown in Fig 3: REUP is configured on Port 1 and Port 2 of Switch A; REUP VLAN load balancing is enabled to map VLAN 1-200 to instance 1 and other VLANs to instance 2; the



packets of VLAN 1-200 (instance 1) will be transmitted via Port 1, and packets of all other VLANs (instance 2) will be transmitted via Port 2.



**Fig 4 Topology in which one link for load balancing is failed**

When one of the ports is failed, the other port will be responsible for forwarding packets of all VLANs. After the failed port has recovered and functions normally within the preemption delay, it will take over the packets of its responsible VLANs from another port.

In privileged EXEC mode, execute the following steps to configure REUP VLAN load balancing.

Command	Function
Ruijie# <b>configure terminal</b>	Enter the global configuration mode.
Ruijie(config)# <b>interface</b> <i>interface-id</i>	Enter the interface configuration mode.
Ruijie(config-if)# <b>switchport backup interface</b> <i>interface-id</i> <b>prefer</b> <i>instance</i> <i>standby-interface-instance-range</i>	Configure a layer-2 port as the backup port, and specify the packets of which VLAN mapping instance will be forwarded by the backup port.
Ruijie(config-if)# <b>end</b>	Return to privileged EXEC mode.
Ruijie# <b>show interface</b> [ <i>interface-id</i> ] <b>switchport backup</b>	Show the configurations.
Ruijie# <b>copy running-config startup-config</b>	Save configurations.

For example:

```

Ruijie# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Ruijie(config)#spanning-tree mst configuration
Ruijie(config-mst)#instance 1 vlan 1-200
Ruijie(config-mst)#exit
Ruijie(config)#show spanning-tree mst configuration
Multi spanning tree protocol : Enable
Name      :
Revision : 0
Instance  Vlans Mapped
-----
0          : 201-4094

```

1 : 1-200

-----  
Ruijie(config)# **interface gigabitEthernet 0/1**

Ruijie(config-if)# **switchport backup interface gigabitEthernet 0/2 prefer instance 1**

Ruijie(config-if)# **end**

Ruijie# **show interfaces switchport backup**

Ruijie(config-if)#show interfaces switchport backup

Switch Backup Interface Pairs:

Active Interface	Backup Interface	State
------------------	------------------	-------

-----  
GigabitEthernet 0/1    GigabitEthernet 0/2    Active Up/Backup Down

Instances Preferred on Active Interface:Instance 0,2-64

Mapping VLAN 201-4094

Instances Preferred on Backup Interface:Instance 1

Mapping VLAN 1-200



---

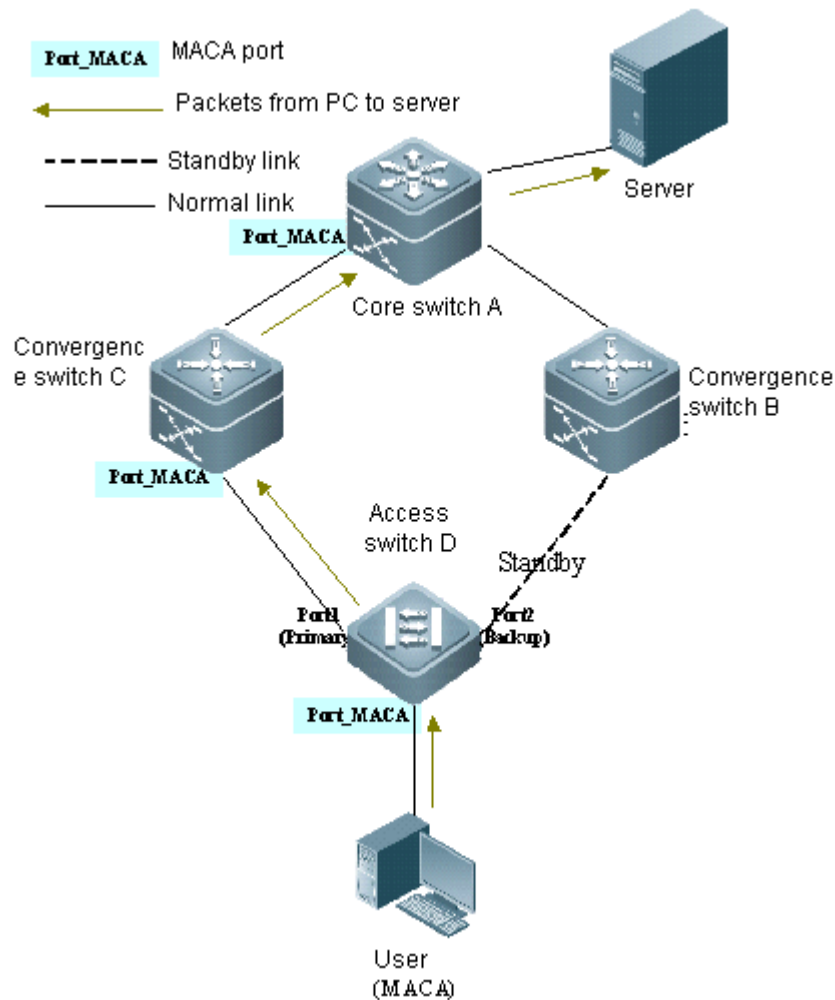
**Note**

The instance mapping in REUP VLAN load balancing is centrally controlled by the MSTP module. For details about instance configuration, please refer to "MSTP Configuration Guide" (MSTP-SCG.doc).

---

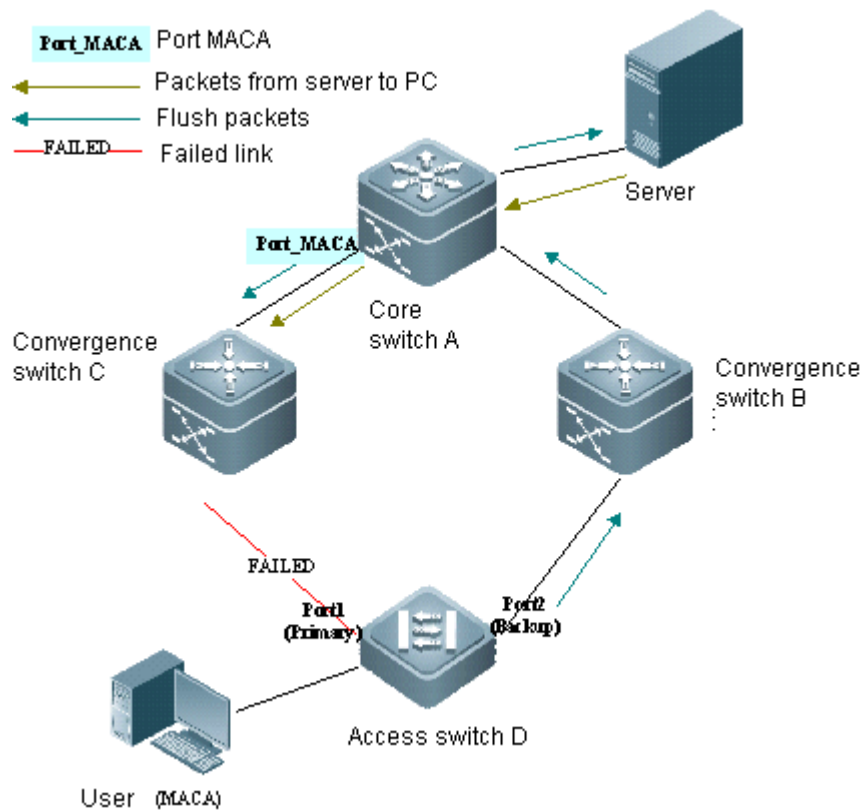
## Configuring MAC Address Updating

### Introduction to MAC Address Updating



**Fig 5 Normal working state of REUP**

As shown in Fig 5, REUP dual-link backup is enabled on Gi0/1 and Gi0/2 of Switch D. Port Gi0/1 is the active port. During the process of normal communication, Switch A will learn the MAC address of PC from the port (Gi0/3) connected to Switch C.



**Fig 6 Failed state during the switchover**

After port Gi0/1 of Switch D fails, port Gi0/2 will instantly become active and start to forward data packets. By this time, Switch A is temporarily unable to learn the MAC address of PC from port Gi0/4 connected to Switch B, and packets sent by the server to PC will be forwarded by Switch A to Switch C, causing packet loss.

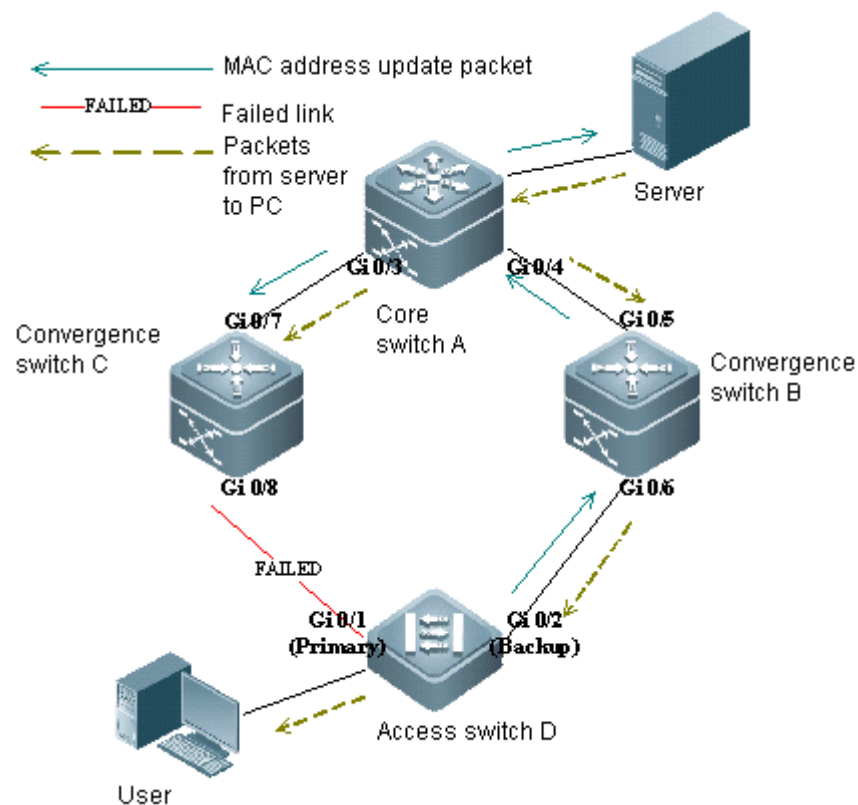


Fig 7 State after REUP sends MAC address updating message

To avoid the aforementioned defect, we need to enable MAC address updating on Switch D. While Gi0/2 starts to forward packets, Switch D will send MAC update message on Gi0/2. After Switch A receives such MAC address updating message, it will clear the MAC address on port Gi0/3, so that Switch A can forward the packets transmitted from server to PC to the port connected to Switch B, thus quickening the convergence of packet forwarding.

To reduce the side effect of flooding caused by MAC address updating, we have introduced the MAC address update group, which means that multiple ports will be included in the group. When one port in this group receives the MAC address updating message, it will update the MAC address information on other ports within this group.

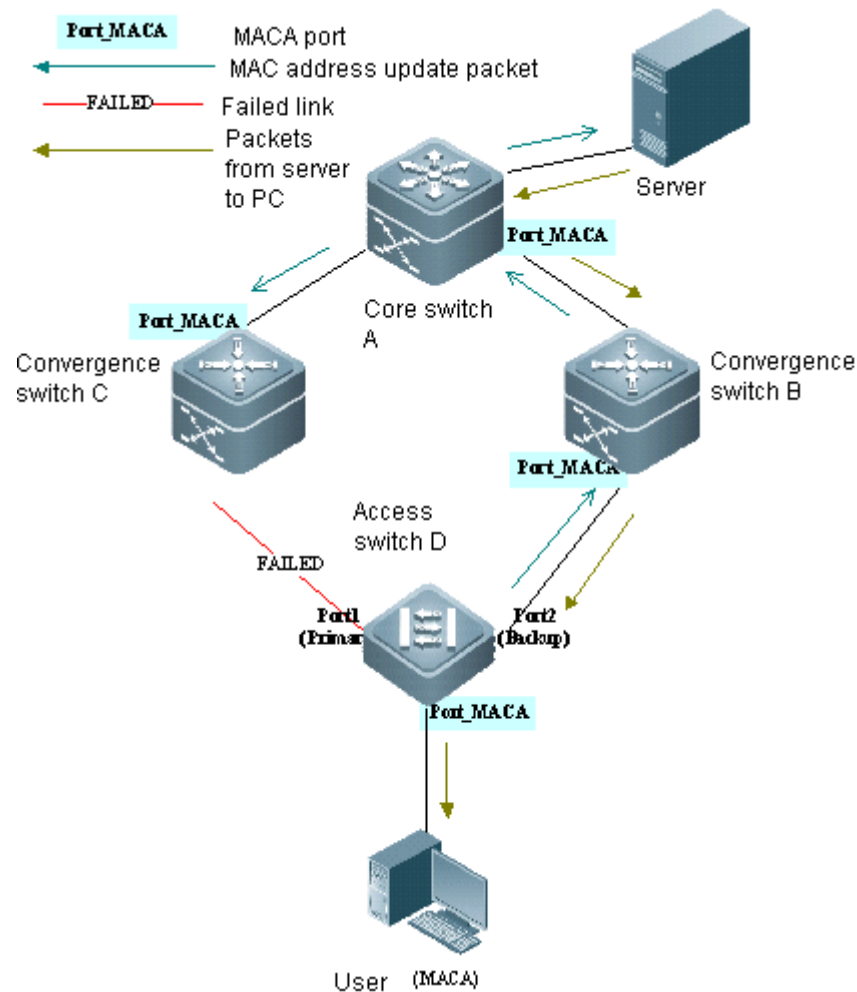


Fig 8 State after REUP sends MAC address updating packet

To support up-stream devices which don't support MAC address updating message, when Gi0/2 changes to forwarding state, Switch D will send MAC address updating packet on behalf of user PC, so that Switch A can update the MAC address of user PC to Gi0/4, thus recovering downlink data transmission on Switch A.

## Configuring MAC Address Updating

To enable the MAC address updating function, enable the function of sending MAC address message on the switch.

In the privileged EXEC configuration mode, follow these steps to function of sending MAC address message on the switch:

Command	Function
Ruijie # <b>configure terminal</b>	Enter the global configuration mode.
Ruijie (config) # <b>mac-address-table move update transit</b>	Enable the function of sending the MAC address updating message.
Ruijie(config)# <b>mac-address-table move update max-update-rate</b> <i>pkts-per-second</i>	(Optional) Configure the maximum number of MAC address updating packets sent per second. Range: 0-32000; default: 150.
Ruijie(config)# <b>interface</b> <i>interface-id</i>	Enter the interface configuration mode.
Ruijie(config-if)# <b>mac-address-table move update transit vlan</b> <i>vlanid</i>	(Optional) Configure the VID for the interface to send MAC address update message. By default, MAC address updating message is sent in the default VLAN of port.
Ruijie(config-if)# <b>end</b>	Return to privileged EXEC mode.
Ruijie# <b>show mac-address-table move update</b>	Show the configuration.
Ruijie# <b>copy running-config startup-config</b>	Save the configuration.

Meanwhile, enable all switches on the switched path to receive MAC address updating messages, and join all ports on the switched path to the same MAC address updating group. In privileged EXEC mode, execute the following steps to enable the switch to receive MAC address updating message and address updating group.

Command	Function
Ruijie # <b>configure terminal</b>	Enter the global configuration mode.
Ruijie (config) # <b>mac-address-table move update receive</b>	Enable the function of receiving the MAC address updating message.
Ruijie(config)# <b>no mac-address-table move update receive vlan</b> <i>vlan-range</i>	(Optional) Configure the VLAN range for the device to handle MAC address updating message. By default, MAC address updating message is handled in all VLANs.
Ruijie(config)# <b>interface</b> <i>interface-id</i>	Enter the interface configuration mode.
Ruijie(config-if)# <b>mac-address-table update group</b> [ <i>number</i> ]	Add the port to the MAC address updating group. By default, add the port to the first MAC address updating group.
Ruijie(config-if)# <b>end</b>	Return to the privileged EXEC mode.
Ruijie# <b>show mac-address-table update group</b>	Show the configuration.
Ruijie# <b>copy running-config startup-config</b>	Save the configuration.

For example, as shown in Fig 5, enable the REUP dual link backup function on port 1 and port 2 of switch D.

```
Ruijie # configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Ruijie (config)# interface gigabitEthernet 0/1
Ruijie (config-if)# switchport backup interface gigabitEthernet 0/2
Ruijie (config-if)# end
Ruijie # show interface switchport backup detail
Switch Backup Interface Pairs:
Active Interface      Backup Interface      State
GigabitEthernet 0/1  GigabitEthernet 0/2   Active Up/Backup Standby
Interface Pair : Gi0/1, Gi0/2
Preemption Mode : off
Preemption Delay : 35 seconds
Bandwidth : 100000 Kbit (Gi0/1), 100000 Kbit (Gi0/2)
```

Enable the function of sending the MAC address updating on Switch D.

```
Ruijie # configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Ruijie (config)# mac-address-table move update transit
Ruijie (config)# end
Ruijie # show mac-address-table move update
Mac address table move update status:
Transit:enable
Receive:disable
Pair: Gi0/2,Gi0/1
Members      Status      Transit Count      Last Transit Time
-----
Gi0/2        Up          0
Gi0/1        Down        0
```

Enable the function of receiving the MAC address updating message on Switches B, C and A, and add all ports on the switched path to the same MAC address updating group.

Apply the following configurations on Switch A

```
Ruijie # configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Ruijie (config)# mac-address-table move update receive
Ruijie (config)# interface range gigabitEthernet 0/3-4
Ruijie (config-if-range)# mac-address-table update group
Ruijie (config-if-range)# end
Ruijie # show mac-address-table update group detail
Mac-address-table Update Group:1
Received mac-address-table update message count:0
Group member  Receive Count  Last Receive Switch-ID  Receive Time
-----
Gi0/3         0              0000.0000.0000
Gi0/4         0              0000.0000.0000
```

Apply the following configurations on Switch B:

```
Ruijie # configure terminal
```

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

```
Ruijie (config)# mac-address-table move update receive
```

```
Ruijie (config)# interface range gigabitEthernet 0/5-6
```

```
Ruijie (config-if-range)# mac-address-table update group
```

```
Ruijie (config-if-range)# end
```

Apply the following configurations on Switch C:

```
Ruijie # configure terminal
```

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

```
Ruijie (config)# mac-address-table move update receive
```

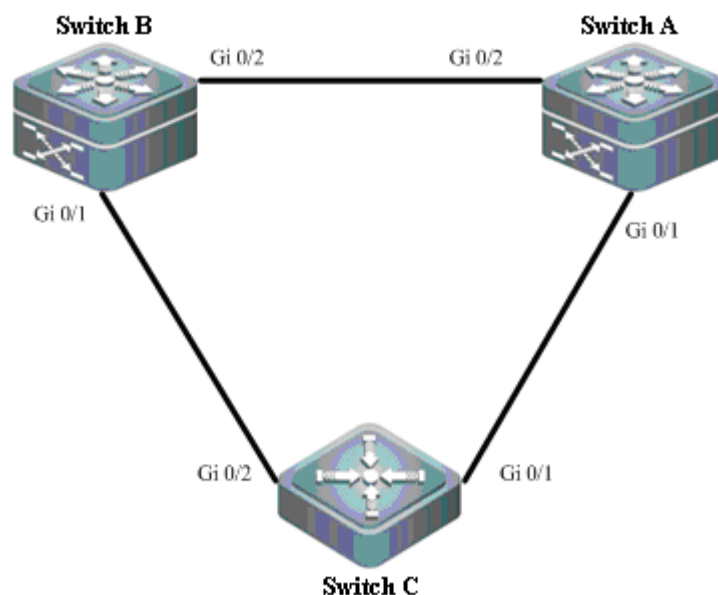
```
Ruijie (config)# interface range gigabitEthernet 0/7-8
```

```
Ruijie (config-if-range)# mac-address-table update group
```

```
Ruijie (config-if-range)# end
```

## Typical REUP Applications

**Figure-5 Typical REUP application topology**



As shown in the above figure, Switch C connects to Switch A and Switch B through Gi0/1 and Gi0/2. To enable rapid bi-directional convergence, enable the dual link backup function on Switch C, enable the function of receiving the MAC address updating message on Switch A and Switch B, and add the ports along the switching path to the MAC address updating group.

Configuration on Switch C:

```
Ruijie # configure terminal
```

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

```
Ruijie(config)# interface gigabitEthernet 0/1
```

```
Ruijie(config-if)# switchport backup interface gigabitEthernet 0/2
```

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

```
Ruijie(config)# mac-address-table move update transit
```

```
Ruijie(config)# end
```

```
Ruijie# show mac-address-table move update
```

Mac address table move update status:

Transit:enable



```

Receive:disable
Pair: Gi0/1,Gi0/2
Members          Status    Transit Count    Last Transit Time
-----
Gi0/1            Standby    0
Gi0/2            Up         1                Wed Aug 20 10:51:34 2008

```

### Configuration on Switch A and Switch B:

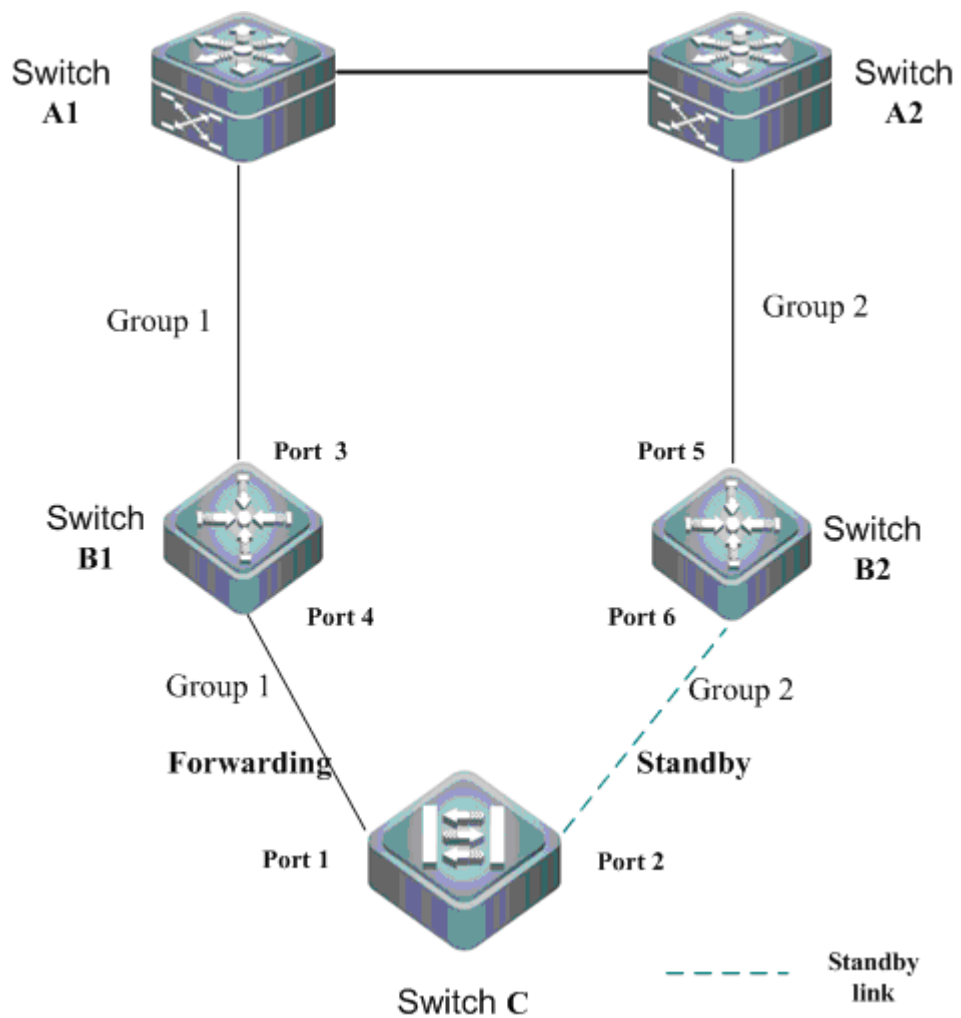
```

Ruijie # configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Ruijie(config)# mac-address-table move update receive
Ruijie(config)# interface range gigabitEthernet 0/1 - 2
Ruijie(config-if-range)# mac-address-table update group
Ruijie(config-if-range)# end
Ruijie# show mac-address-table update group detail
Mac-address-table Update Group:1
Received mac-address-table update message count:0
Group member      Receive Count    Last Receive Switch-ID    Receive Time
-----
Gi0/1              0                0000.0000.0000
Gi0/2              0                0000.0000.0000

```

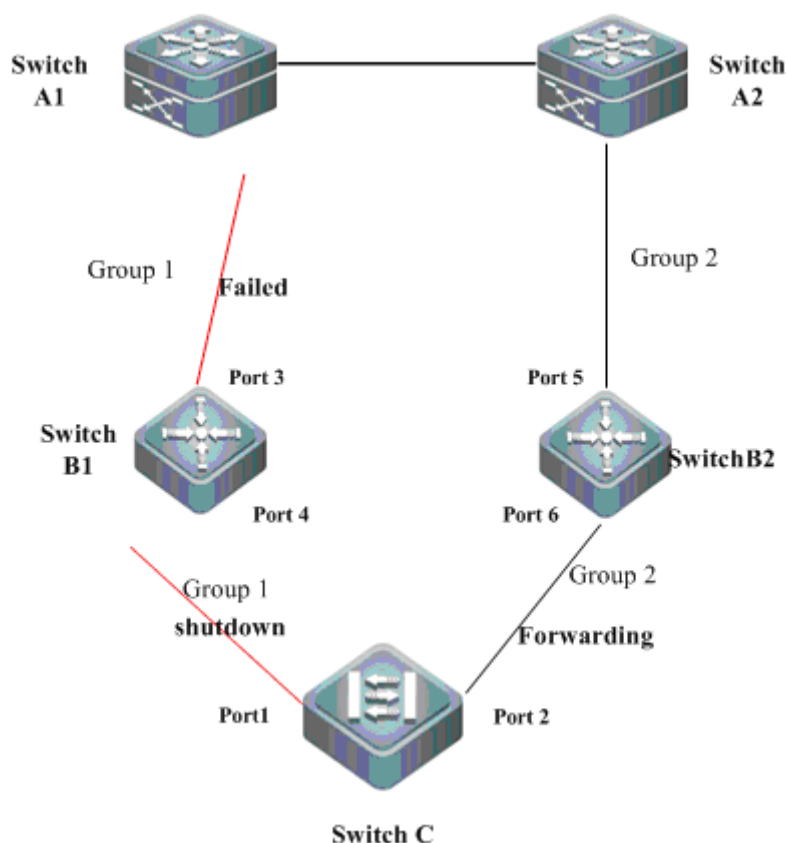
## Configuring Link State Tracking

With Link State Tracking, when upstream links have failed, the downstream devices can be advertised to switch over the link. By configuring upstream ports and downstream ports of link state tracking group, Link State Tracking binds the link state of multiple downstream ports to multiple upstream ports. When all upstream links in the tracking group have failed, the downstream ports will be shut down, so that the packet transmission over upstream link can be switched from primary link to the backup link.



**Fig 10 Link state tracking configuration example**

As shown in Fig 10: port 4 of Switch B1 is configured as the downstream port of group 1, and port 3 is configured as the upstream port; port 6 of Switch B2 is configured as the downstream port of group 2, and port 5 is configured as the upstream port; REUP dual-link backup is enabled on port 1 and port 2 of Switch C.



**Fig 11 Topology in which the upstream links on primary link are failed**

Fig 11 Topology in which the upstream links on primary link are failed

When upstream link of Switch B1 is failed, Link State Tracking will instantly shut down the downstream port 4, so that the packet transmission on the upstream link of Switch C can be switched to Switch B2.

In privileged EXEC mode, execute the following steps to configure Link State Tracking.

Command	Function
Ruijie # <b>configure terminal</b>	Enter the global configuration mode.
Ruijie(config)# <b>link state track</b> [number]	Enable a link state group. The range of "number" is 1-2. By default, the first link state group will be enabled (default number is 1).
Ruijie(config)# <b>interface</b> interface-id	Enter the interface configuration mode.
Ruijie(config-if)# <b>link state group</b> [number] {upstream   downstream}	Configure the upstream ports and downstream ports of link state group. The range of "number" is 1-2. By default, the first link state group will be joined (default number is 1).
Ruijie(config-if)# <b>end</b>	Return to the privileged EXEC mode.
Ruijie# <b>show mac-address-table update group</b>	Show the configuration.
Ruijie# <b>copy running-config startup-config</b>	Save the configuration.

For example: On Switch B1, configure port 4 as the downstream port and port 3 as the upstream port of link state group 1.

```
Ruijie# configure terminal
Ruijie(config)# link state track 1
Ruijie(config)# interface fastethernet 0/4
Ruijie(config-if)# link state group 1 downstream
Ruijie(config)# exit
Ruijie(config-if)# interface fastethernet 0/3
Ruijie(config-if)# link state group 1 upstream
Ruijie(config-if)# end
```

Verify the state of Link State Group.

```
Ruijie# show link state group detail
Link State Group:1  Status: Enabled, UP
Upstream Interfaces :Gi0/3(Up)
Downstream Interfaces : Gi0/4(Up)
Link State Group:2  Status: Disabled, Down
Upstream Interfaces :
Downstream Interfaces :
(Up):Interface up   (Dwn):Interface Down   (Dis):Interface disabled
```

## REUP Configuration Example

### Topological Diagram

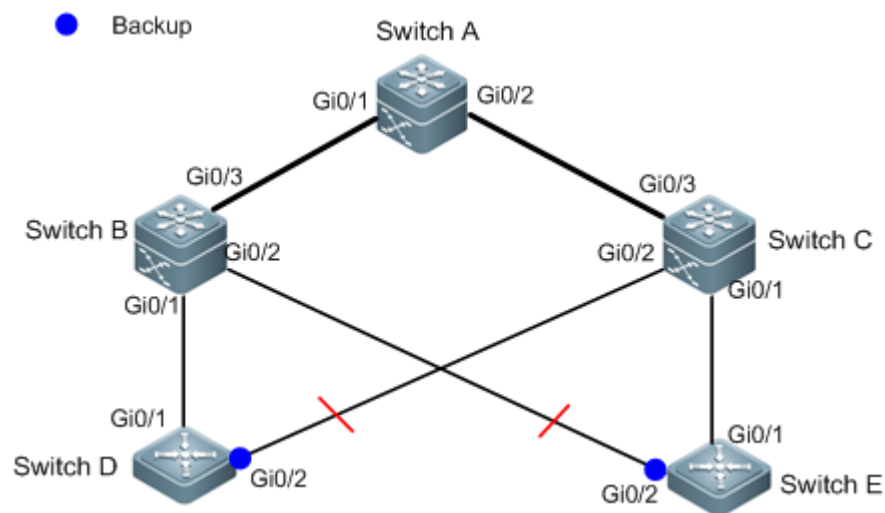


Fig 12 Topological diagram for REUP configuration

### Application Requirements

When downstream devices are connected to upstream devices, service interruption may be easily caused by the single point failure on the single upstream link. Generally, dual upstream links are used. One downstream device (Switch D/E) is connected to two upstream devices

(Switch B and Switch C) to furthest avoid single point failure and enhance network reliability. The specific requirements are shown below:

1. Downstream devices (Switch D/E) reach the upstream device (Switch A) through two upstream links to realize redundant backup of the link.
2. Downstream devices (Switch D/E) shall allow rapid bidirectional convergence in the case of link failure.
3. G0/2 of Switch E is a 100M interface, and G0/1 is a 1000M interface. When the failed link is restored, the upstream link with greater bandwidth shall be selected.

## Configuration Tips

Applying REUP will meet all the above application needs:

1. Configure REUP dual-link backup on downstream devices (Switch D/E) to allow redundant backup of the primary link and backup link.
2. Configure REUP MAC address update on the corresponding devices to achieve rapid bidirectional convergence of the network: enable the downstream devices (Switch D/E) to send MAC address update messages; enable the upstream devices (Switch A/B/C) to receive MAC address update messages and join all ports into the same address update group.
3. Configure REUP preemption mode to enable the priority use of upstream link with greater bandwidth.

## Configuration Steps

Trunk links are used to connect devices. For interface related configurations, please refer to "Interface Configuration" section in this manual.

### ➤ Configurations on Switch D

Step 1: Configure REUP pair (Gi0/1 is the primary port and Gi0/2 is the secondary port)

```
SwitchD > enable
SwitchD # configure terminal
SwitchD (config)# interface GigabitEthernet 0/1
SwitchD(config-if-GigabitEthernet 0/1)# switchport mode trunk
SwitchD(config-if-GigabitEthernet 0/1)#switchport backup interface GigabitEthernet 0/2
SwitchD(config-if-GigabitEthernet 0/1)# exit
```

Step 2: Enable Switch D to send MAC address update message

```
SwitchD (config)# mac-address-table move update transit
```

### ➤ Configurations on Switch E

Step 1: Configure REUP pair (port 1 is the primary port and port 2 is the secondary port)

```
SwitchE> enable
SwitchE # configure terminal
SwitchE (config)# interface GigabitEthernet 0/1
```

```
SwitchE (config-if-GigabitEthernet 0/1)# switchport mode trunk
```

```
SwitchE (config-if-GigabitEthernet 0/1)# switchport backup interface GigabitEthernet 0/2
```

### Step 3: Configure preemption mode

#### ! Configure preemption mode as bandwidth mode

```
SwitchE (config-if-GigabitEthernet 0/1)# switchport backup interface gigabitEthernet 0/2 preemption mode bandwidth
```

#### ! Configure preemption delay as 40 seconds

```
SwitchE (config-if-GigabitEthernet 0/1)# switchport backup interface gigabitEthernet 0/2 preemption delay 40
```

```
SwitchE (config-if-GigabitEthernet 0/1)# exit
```

### Step 2: Enable Switch E to send MAC address update message

```
Ruijie(config)# mac-address-table move update transmit
```

## ➤ Configurations on Switch B

### Step 1: Enable Switch B to send MAC address update message

```
SwitchB # configure terminal
```

```
SwitchB (config)# mac-address-table move update receive
```

### Step 2: Join all ports on REUP switched path to the same MAC address update group

In this example, Gi0/1 and Gi0/3 are interfaces on the upstream switched path of SwitchD, and Gi0/3 and Gi0/2 are interfaces on the upstream switched path of SwitchE. Since one interface can only join one address update group, we can join Gi0/1, Gi0/2 and Gi0/3 into the same address update group.

```
Ruijie(config)# interface range gigabitEthernet 0/1 – 3
```

```
SwitchB(config-if-range)#switchport mode trunk
```

```
SwitchB (config-if-range)# mac-address-table update group 1
```

```
SwitchB (config-if-range)# end
```

## ➤ Configurations on Switch C

Same as the configurations on Switch B.

## ➤ Configurations on Switch A

### Step 1: Enable Switch A to send MAC address update message

```
SwitchA # configure terminal
```

```
SwitchA (config)# mac-address-table move update receive
```

### Step 2: Join all ports on REUP switched path to the same MAC address update group

```
SwitchA (config)# interface range gigabitEthernet 0/1 – 2
```

```
SwitchA (config-if-range)# switchport mode trunk
```

```
SwitchA (config-if-range)# mac-address-table update group 1
```

```
SwitchA (config-if-range)# end
```

## Verify configurations

## ➤ Displaying REUP configurations on Switch D

### Step 1: Display the dual-link backup state of ports on Switch D

```
SwitchD#show interfaces switchport backup detail
```

```
Switch Backup Interface Pairs:
```

```
Active Interface    Backup Interface    State
```

```
-----
```

```

Gi4/1          Gi4/2          Active Up/Backup Standby
Interface Pair : Gi4/1, Gi4/2
Preemption Mode : Off          //REUP preemption mode is disabled
Preemption Delay : 35 seconds
Bandwidth : Gi4/1(1000 Mbits), Gi4/2(1000 Mbits)

```

As shown above, when links function normally (both primary and secondary ports of Switch D are Link Up), the secondary port of Switch D will maintain Standby state.

**Step 2: Disconnect the uplink on the primary port of Switch D and then verify device state**

```

SwitchD#show interfaces switchport backup detail
Switch Backup Interface Pairs:
Active Interface  Backup Interface  State
-----
Gi4/1            Gi4/2            Active down/Backup up
Interface Pair : Gi4/1, Gi4/2
Preemption Mode : Off
Preemption Delay : 35 seconds
Bandwidth : Gi4/1(1000 Mbits), Gi4/2(1000 Mbits)

```

As shown above, when the uplink on primary port of Switch D is failed, the backup port will switch to forwarding state (UP) to transmit packets.

**Step 3: Restore the uplink on the primary port of Switch D and then verify device state**

```

SwitchD#show interfaces switchport backup detail
Switch Backup Interface Pairs:
Active Interface  Backup Interface  State
-----
Gi4/1            Gi4/2            Active Standby /Backup up
Interface Pair : Gi4/1, Gi4/2
Preemption Mode : Off
Preemption Delay : 35 seconds
Bandwidth : Gi4/1(1000 Mbits), Gi4/2(1000 Mbits)

```

As shown above, since REUP preemption mode hasn't been configured on Switch D, when the uplink on primary port is restored, the secondary port will still maintain forwarding state and the primary port will go into standby state.

### ➤ Displaying REUP configurations on Switch E

**Step 1: Display the dual-link backup state of ports on Switch E**

```

SwitchE#show interfaces switchport backup detail
Switch Backup Interface Pairs:
Active Interface  Backup Interface  State
-----
Gi0/1            Gi0/2            Active Up/Backup Standby

Interface Pair : Gi0/1, Gi0/2
Preemption Mode : bandwidth          //REUP bandwidth based preemption mode
Preemption Delay : 40 seconds
Bandwidth : Gi0/1(1000 Mbits), Gi0/2(100 Mbits)

```

As shown above, when links function normally (both primary and secondary ports of Switch E are Link Up), the secondary port of Switch E will maintain Standby state.

Step 2: Disconnect the uplink on the primary port of Switch E and then verify device state

```
SwitchD#show interfaces switchport backup detail
Switch Backup Interface Pairs:
Active Interface   Backup Interface   State
-----
Gi0/1             Gi0/2             Active down/Backup up
Interface Pair : Gi0/1, Gi0/2
Preemption Mode : bandwidth
Preemption Delay : 40 seconds
Bandwidth : Gi0/1(1000 Mbits), Gi0/2(100 Mbits)
```

As shown above, when the uplink on primary port of Switch E is failed, the backup port will switch to forwarding state (UP) to transmit packets.

Step 3: Restore the uplink on the primary port of Switch D and then verify device state

After the uplink is restored and before the delay time runs out, immediately verify the dual-link backup state of device. The primary port goes into Standby state, and the secondary port remains in forwarding state, as shown below:

```
SwitchE#show interfaces switchport backup
Switch Backup Interface Pairs:
Active Interface   Backup Interface   State
-----
Gi0/1             Gi0/2             Active Standby/Backup Up
```

After the 40-second delay time runs out, CLI will print the following LOG information:

```
*Apr 14 22:08:45: %REUP_INTF-5-PREEMPT: Preempting interface Gi0/2 in reup pair (Gi0/1, Gi0/2), preemption mode is bandwidth
```

Verify the dual-link backup state of device again. Since REUP bandwidth based preemption mode is configured, REUP will preempt the link with greater bandwidth (namely the uplink on Gi0/1).

```
SwitchE#show interfaces switchport backup
Switch Backup Interface Pairs:
Active Interface   Backup Interface   State
-----
Gi0/1             Gi0/2             Active Up/Backup Standby
Interface Pair : Gi0/1, Gi0/2
Preemption Mode : bandwidth
Preemption Delay : 40 seconds
Bandwidth : Gi0/1(1000 Mbits), Gi0/2(100 Mbits)
```

### ➤ Displaying REUP configurations on the upstream devices

Display information about MAC address update group on Switch A

```
SwitchA#show mac-address-table update group detail
Mac-address-table Update Group:1
Received mac-address-table update message count:5
Group member Receive Count   Last Receive Switch-ID   Receive Time
```



```

-----
Gi0/1      2      00d0.f822.35aa  Thu Aug 20 13:42:16 2009
Gi0/2      3      00d0.f822.33ad  Thu Aug 20 13:43:55 2009

```

### Display information about MAC address update group on Switch B

SwitchB#show mac-address-table update group detail

Mac-address-table Update Group:1

Received mac-address-table update message count:5

Group member	Receive Count	Last Receive Switch-ID	Receive Time
-----	-----	-----	-----
Gi0/1	1	00d0.f822.35ad	Thu Aug 20 13:43:50 2009
Gi0/2	1	00d0.f822.33aa	Thu Aug 20 13:42:44 2009
Gi0/3	3	00d0.f822.35ad	Thu Aug 20 13:43:32 2009

### Display information about MAC address update group on Switch C

SwitchC#show mac-address-table update group detail

Mac-address-table Update Group:1

Received mac-address-table update message count:6

Group member	Receive Count	Last Receive Switch-ID	Receive Time
-----	-----	-----	-----
Gi0/1	1	00d0.f822.35aa	Thu Aug 20 13:43:51 2009
Gi0/2	1	00d0.f822.33ad	Thu Aug 20 13:42:43 2009
Gi0/3	3	00d0.f822.35aa	Thu Aug 20 13:43:31 2009

# RLDP Configuration

## RLDP Overview

### Understanding RLDP

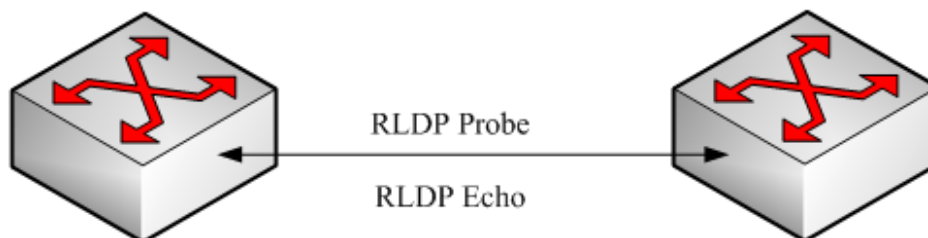
The Rapid Link Detection Protocol (RLDP) is one of Ruijie's proprietary link protocol designed to detect Ethernet link fault quickly.

General Ethernet link detection mechanism only makes use of the status of the physical connections and detects the connectivity of the link via the auto-negotiation of the physical layer. This detection mechanism has restrictions and sometimes cannot provide reliable link detection information for the user. For example, if the optical fiber receiving line pair on the optical interface is misconnected, due to the existence of the optical converter, the related port of the device is "linkup" physically but actually the corresponding layer-2 link cannot work for communications. Here is another example. There is an intermediate network between two Ethernet devices. Due to the existence of the network transmission relay devices, the same problem may occur if those relay devices are faulty.

The RLDP enables easy detection of Ethernet device link fault, including the one-way link fault, two-way link fault and loop link fault.

The RLDP implements the detection by exchanging the RLDP messages at the two ends of the link, as shown in Figure-1:

**Figure-1:**



The RLDP defines two protocol messages: Probe message and Echo message. The RLDP sends the Probe message of this port to the port with RLDP configured and in linkup status on regular basis, and waits for the Echo message from the neighbor port and waits for the Probe message sent by the neighbor ports. If a link is correct both physically and logically, a port shall be able to receive the Echo message of the neighbor port as well as the Probe message of the neighbor port. Otherwise, the link is considered abnormal.



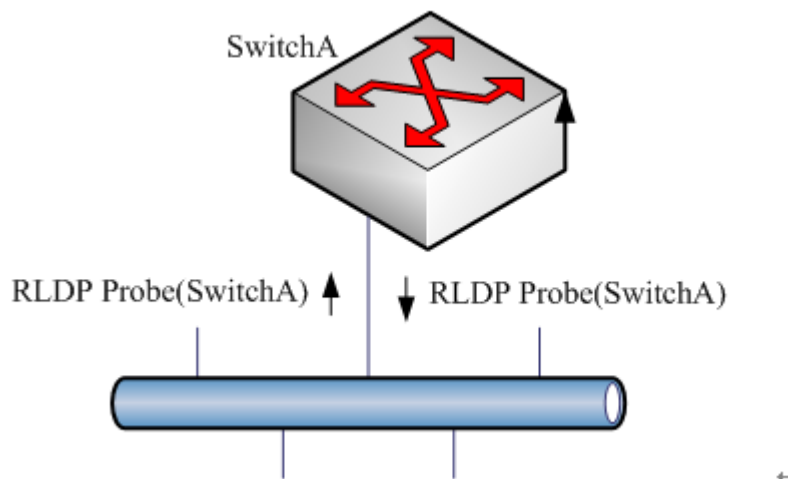
**Note**

To make use of the one-way detection and two-way detection functions of the RLDP, it is necessary to ensure the RLDP is enabled on the ports at both ends of the link. And, it is not allowed for a port with RLDP enabled to connect multiple neighbor ports. Otherwise, the RLDP cannot detect the health conditions of every neighbor link.

## Typical Application

### Loop detection:

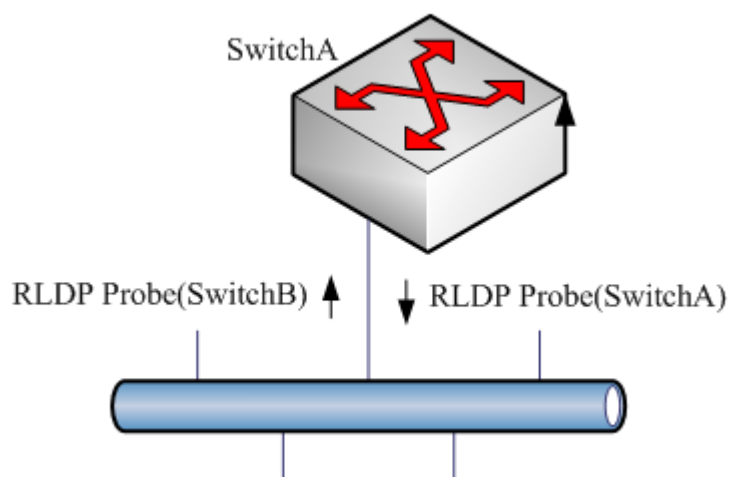
**Figure-2: Loop detection**



The so-called loop fault means that a loop appears on the links connected with the port. As shown above, on a port the RLDP receives the RLDP message sent from its machine, so the port is considered as loop fault. So, the RLDP deals with the fault according to the user configurations, including alarming, setting port violation, turning off the SVI with that port, turning off the port learning forwarding, and more.

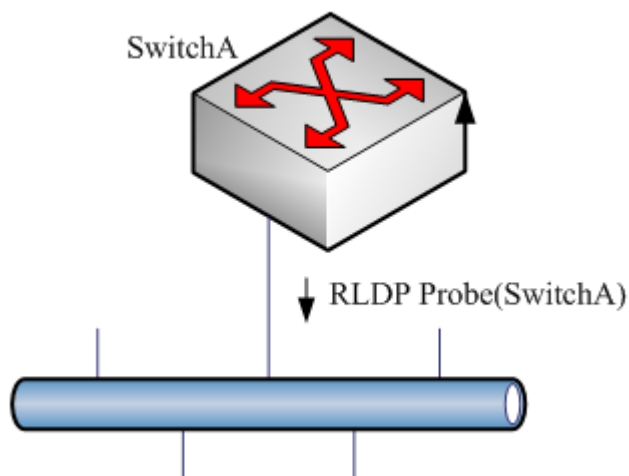
### One-way link detection:

**Figure-3: One-way link detection**



The so-called one-way link detection means the link connected with the port can receive message only or send messages only (due to misconnection of the optical receiving line pair, for example). As shown above, the RLDP only receives the detection message from the neighbor port on a port, so it is considered one-way link fault. So, the RLDP deals with the fault accordingly according to the user configurations. In addition, if the port cannot receive any RLDP detection message, it is also considered one-way link fault.

### Two-way link detection:

**Figure-4:Two-way link detection**

This means that fault occurs at the frame transmission/receiving at both ends of the link. As shown above, the port of the device sends the RLDP probe message but has never received the Echo message or the Probe message from the neighbors. So, it is considered two-way link fault. From the nature of the fault, the two-way fault actually includes the one-way fault.

**Note**

If the party at one of the two link ends has not enabled the RLDP, the diagnosis also shows two-way or one-way link fault. So, in configuring two-way link detection or one-way link detection, the administrator shall make sure that the RLDP is enabled at both ends to avoid the incorrect diagnosis information.

## Configuring RLDP

The following sections describe how to configure RLDP.

- RLDP defaults
- Configure global RLDP
- Configure port RLDP
- Configure RLDP detection interval
- Configure the RLDP maximum detection times
- Restore the RLDP status of the port

### RLDP defaults

Global RLDP status	DISABLE
Port RLDP status	DISABLE
Detection interval	2S
Maximum detection times	3

**Caution**

- The RLDP can be configured only on the basis of the switching interface (including AP) and the routing interface.
- All RLDP frames are untagged.
- In the RLDP fault processing type, the block function and the STP are mutually exclusive. In other words, if the fault processing type configured on the port is "block", it is recommended to disable STP; otherwise, since the STP cannot recognize one-way link, possibly the STP allows port forwarding but the RLDP is configured with port blocking.

## Configuring RLDP Globally

The RLDP works on the port only when the global RLDP is enabled.

In the global configuration mode, follow these steps to enable RLDP:

Command	Function
Ruijie(config)# <b>rldp enable</b>	Turn on the global RLDP function switch.
Ruijie(config)# <b>end</b>	Return to the privileged EXEC mode.

The **no** option of the command turns off the global *RLDP*.

## Configuring RLDP on the Port

The RLDP operation is port-based, so the user needs to explicitly configure which ports shall run RLDP. In configuring the port RLDP, it is required to specify the diagnosis type and the troubleshooting method for the port at the same time. The diagnosis types include unidirection-detect, bidirection-detect and loop-detect. The troubleshooting methods include warning, block, shutdown-port, and shutdown-svi.

In the configuration mode, follow these steps to configure the RLDP on the port:

Command	Function
Ruijie(config)# <b>interface interface-id</b>	Enter the interface mode.
Ruijie(config-if)# <b>rldp port</b> {unidirection-detect bidirection-detect   loop-detect } {warning shutdown-svi   shutdown-port block}	Enable the RLDP on the port and configure the diagnosis type and troubleshooting method at the same time.
Ruijie(config-if)# <b>end</b>	Return to the privileged EXEC mode.

The **no** option of the command disables the RLDP on the port and the configured detection types one by one.

In the example below, the RLDP is configured on GigabitEthernet 0/5, and multiple diagnosis types and troubleshooting methods are specified:

```
Ruijie# configure terminal
Ruijie(config)# interface gigabitEthernet 0/5
Ruijie(config-if)# rldp port unidirection-detect
shutdown-svi
Ruijie(config-if)# rldp port bidirection-detect warning
Ruijie(config-if)# rldp port loop-detect block
Ruijie(config-if)# end
Ruijie# show rldp interface gigabitEthernet 0/5
```

```

port state      : normal
local bridge    : 00d0.f822.33ac
neighbor bridge : 0000.0000.0000
neighbor port   :
unidirection detect information:
action : shutdown svi
state  : normal
bidirection detect information :
action : warnning
state  : normal
loop detect information      :
action : block
state  : normal

```

Several precautions in configuring port detection:

- The routing interface does not support the shutdown-svi error handling method, so this method is not executed in case of the occurring of detection error.
- In configuring loop detection, the neighbor devices downward connected with the port cannot enable the RLDP detection; otherwise, the port cannot have correct detection.
- If the block method is configured on the aggregated port and the link detection error happens, do not change the member port relations of the aggregate port before the port reset detection; otherwise, the forwarding status of the member interface may have unexpected effects of forwarding status.
- If the RLDP detects link error, alarm information will be given. The user can send the alarm information to the log server by configuring the log function. At least 3 levels of log shall be ensured.
- You are recommended to specify the diagnosis type of the loop detection to shutdown-port for the reason that for some devices, even if the device detects the loop and specifies the block port, a large amount of packets will be sent to the CPU for the hardware chip limitation.
- If you configure RLDP with port blocking after enabling the port, ERPS, RERP and REUP protocols cannot be run on this port. If you want to run these protocols on this port, you are recommended to specify the diagnosis type of loop detection to shutdown-port.

## Configuring RLDP Detection Interval

The port with the RLDP function enabled will send the RLDP Probe messages on a regular basis.

In the global configuration mode, follow these steps to configure the RERP detection interval:

Command	Function
Ruijie(config)# <b>rl dp detect-interval</b> interval	Configure the detection interval within the range 2-15s, 3s by default.
Ruijie(config)# <b>end</b>	Return to the privileged EXEC mode.

The **no** option of the command restores the value to its default.

## Configuring the Maximum RLDP Detection Times

If the port with RLDP enabled cannot receive messages from neighbors in the maximum detection period (maximum detection times X detection interval), that port will be diagnosed as faulty. See the Overview for details of the fault types.

In the global configuration mode, follow these steps to configure the RERP maximum detection times:

Command	Function
Ruijie(config)# <b>rldp detect-max</b> Num	Configure the maximum detection times, num range 2-10, 2 by default.
Ruijie(config)# <b>end</b>	Return to the privileged EXEC mode.

The **no** option of the command restores the value to its default.



### Note

The maximum detection times only take effect in the unidirectional link detection and bidirectional link detection, and will not take effect if only loop detection is enabled on a port.

## Restoring the RLDP Status of the Port

The port with shutdown-port troubleshooting method configured cannot resume the RLDP detection actively after a fault occurs. If the user confirms the fault removed, run the recovery command to restart the RLDP on the shutdown port. This command sometimes may make the other ports with detection errors resume.

In the privileged EXEC mode, follow these steps to resume the RLDP detection of the port:

Command	Function
Ruijie# <b>rldp reset</b>	Make any port with RLDP detection failure resume the detection.



### Note

The **errdisable recover** command can be used in the global configuration mode to restart, instantly or at fixed time, the RLDP detection of the port that is set violation by RLDP. It is worth mentioning that when there are some relay devices between rldp ports, if you use **errdisable recover interval** to restore the fault timely, you need to set the value of rldp detection time greater than that of **errdisable recover interval**, that is, the value of detect-interval\* detect-max total time is greater than that of **errdisable recover interval** to prevent error judgment.

## Viewing RLDP Information

The following RLDP-related information can be viewed:

- View the RLDP status of all ports
- View the RLDP status of the specified port

## Viewing the RLDP Status of All Ports

In the privileged EXEC mode, run the following commands to view the RLDP global configuration and the port detection information with RLDP detection configured:

Command	Function
Ruijie# <b>show rldp</b>	View the RLDP global configuration and the port detection information with RLDP detection configured

In the example below, the **show rldp** command is used to view the detection information of all RLDP ports:

```
Ruijie# show rldp
rldp state           : enable
rldp hello interval  : 2
rldp max hello       : 3
rldp local bridge    : 00d0.f8a6.0134
-----
interface GigabitEthernet 0/1
port state:normal
neighbor bridge      : 00d0.f800.41b0
neighbor port        : GigabitEthernet 0/2
unidirection detect information:
action               : shutdown svi
state                : normal

interface GigabitEthernet 0/24
port state:error
neighbor bridge      : 0000.0000.0000
neighbor port        :
bidirection detect information :
action               : warnning
state                : error
```

As shown above, port GigabitEthernet 0/1 is configured with unidirection detection. No error is detected now, and the port status is normal. Port GigabitEthernet 0/24 is configured with bidirection detection, and bidirection fault is detected.

## Viewing the RLDP Status of the Specified Port

In the privileged EXEC mode, run the following command to view the RLDP detection information of the specified port:

Command	Function
Ruijie# <b>show rldp interface interface-id</b>	View the RLDP detection information of interface-id.

In the example below, the **show rldp interface GigabitEthernet 0/1** command is used to view the RLDP detection information of port fas0/1:

```
Ruijie# show rldp int GigabitEthernet 0/1
port state           :error
local bridge         : 00d0.f8a6.0134
neighbor bridge      : 00d0.f822.57b0
neighbor port        : GigabitEthernet 0/1
unidirection detect information:
action: shutdown svi
```



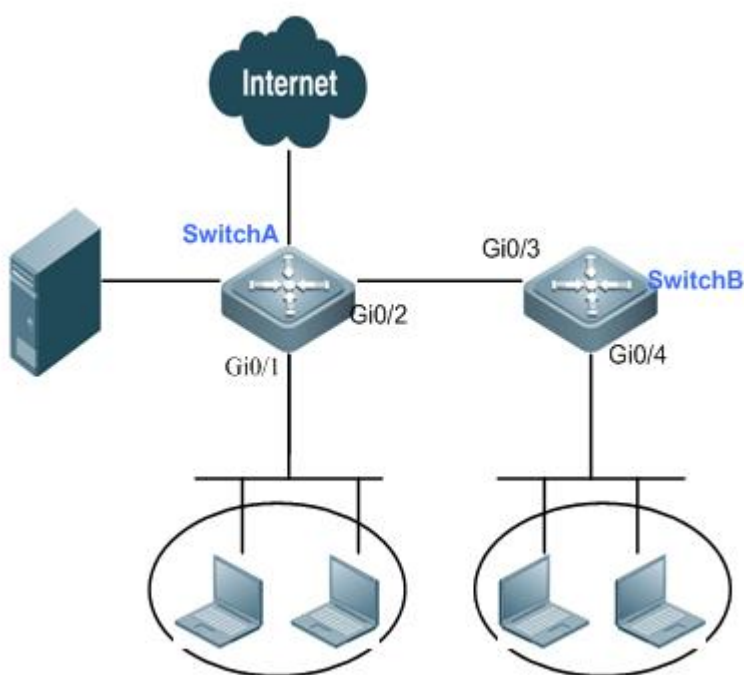
```
state : normal
bidirection detect information :
action : warnning
state : normal
loop detect information :
action: shutdown svi
state : error
```

As shown above, the port GigabitEthernet 0/1 is configured with three detection types: unidirection detection, bidirection detection and loop detection. The troubleshooting methods are shutdown-svi and warning. Error is found in loop detection so the current port status is error. Accordingly, the SVI of the port is shutdown.

## Typical RLDP Configuration Example

### RLDP Fault Detection and Handling

#### Topological Diagram



Topological diagram for RLDP application

#### Application Requirements

As shown above, users from respective departments of the enterprise access network through Switch A and Switch B. Due to network interruption caused by link failure or such non-device factors as the contrived network loop, RLDP loop detection and unidirectional/bidirectional link detection must be configured to instantly locate and handle faults, so that the network can be recovered instantly and the losses caused by network failure can be reduced. Major needs include:

- The loop error or unidirectional/bidirectional link failure detected can be handled as per the fault-handling method configured.
- If the port configured with "shutdown-port" fault-handling is failed, the RLDP detection can be recovered and all failed ports can start detection again.

## Configuration Tips

1. After enabling global RLDP, enable RLDP on the port and configure diagnosis type and fault-handling method.

Note: For loop detection, RLDP cannot be enabled on the downlink port (the port connecting with department users or servers); for unidirectional/bidirectional link detection, RLDP must be enabled on the port connecting with peer device. If the port is a routing port, only the fault-handling method of warning, block or shutdown-port can be used, and shutdown-svi is not supported.

2. In privilege mode, use "rldp reset" command to enable all failed ports to start RLDP detection again.

## Configuration Steps

Step 1: Enable RLDP on the device.

! Enable global RLDP on Switch A.

```
SwitchA#configure terminal
```

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

```
SwitchA(config)#rldp enable
```

! Configurations of Switch B are the same as above.

Step 2: Configure diagnosis type and fault-handling method on the port.

! Enable RLDP on the ports of Switch A; configure loop detection and fault-handling method as "block" on port Gi 0/1 and configure unidirectional link detection and fault-handling method as "warning" on port Gi 0/2.

```
SwitchA(config)#interface gigabitEthernet 0/1
```

```
SwitchA(config-if)#rldp port loop-detect block
```

```
SwitchA(config-if)#exit
```

```
SwitchA(config)#interface gigabitEthernet 0/2
```

```
SwitchA(config-if)#rldp port unidirection-detect warning
```

```
SwitchA(config-if)#exit
```

! Enable RLDP on the ports of Switch B; configure loop detection and fault-handling method as "block" on port Gi 0/4 and configure bidirectional link detection and fault-handling method as "shutdown-port" on port Gi 0/3.

```
SwitchB(config)#interface gigabitEthernet 0/4
```

```
SwitchB(config-if)#rldp port loop-detect block
```

```
SwitchB(config-if)#exit
```

```
SwitchB(config)#interface gigabitEthernet 0/3
```

```
SwitchB(config-if)#rldp port bidirection-detect shutdown-port
```

```
SwitchB(config-if)#exit
```

Step 3: Restore RLDP detection on the port.

! Execute "rldp reset" command on Switch A.

```
SwitchA#rldp reset
```

! Configurations of Switch B are the same as above.

## Verify Configurations

Display RLDP information about all ports on the device.

! RLDP information of all ports on Switch A

```
SwitchA#show rldp
rldp state          : enable
rldp hello interval: 3
rldp max hello      : 2
rldp local bridge   : 00d0.f822.33aa
-----
Interface GigabitEthernet 0/2
port state          : normal
neighbor bridge     : 00d0.f800.41b0
neighbor port       : GigabitEthernet 0/3
unidirection detect information:
    action: warning
    state : normal

Interface GigabitEthernet 0/1
port state          : normal
neighbor bridge     : 0000.0000.0000
neighbor port       :
loop detect information :
    action: block
    state : normal
```

! RLDP information of all ports on Switch B

```
SwitchB#show rldp
rldp state          : enable
rldp hello interval: 3
rldp max hello      : 2
rldp local bridge   : 00d0.f800.41b0
-----
Interface GigabitEthernet 0/3
port state          : normal
neighbor bridge     : 00d0.f822.33aa
neighbor port       : GigabitEthernet 0/2
bidirection detect information:
    action: shutdown-port
    state : normal

Interface GigabitEthernet 0/4
port state          : normal
neighbor bridge     : 0000.0000.0000
neighbor port       :
```

loop detect information :

action: block

state : normal

# DLDP Configuration

## Overview

---

Based on the SDH platform, the MSTP supports access, processing, and transmission of multiple services, such as TDM, ATM, and Ethernet, providing a multi-service node for the unified network management system. Because Ethernet lacks in the link keep-alive protocol, Ethernet access is always used at user access points. As a result, link protocol status is still normal even if lines for Ethernet to access the MSTP network are disconnected. In this case, route convergence slows down and the difficulty in locating a fault is increased.

The major procedure for device link detection can be divided into the following stages:

### 1. Initialization stage

When DLDP is enabled on the interface, DLDP is changed into initialization status, and then an ARP request is sent to obtain the MAC address of the peer device. If DLDP cannot obtain the peer MAC address, DLDP is in the initialization stage unless users prohibit this function and DLDP status is changed into deleted. After the peer MAC address is obtained, DLDP status is changed into link succeeded.

### 2. Link succeeded status

In this state, DLDP can send a link detection request to detect line connectivity. After DLDP responses are received, the interface is marked UP. If responses are not received, requests are sent until the number of requests exceed the maximum number. In this case, the link is marked failed and DLDP status is changed into initialization. If users delete this function during this process, DLDP status is changed into deleted.

### 3. Deleted status

In deleted state, the interface status is not analyzed by the link detection function. In this case, the interface status is consistent with the physical channel status.

The devices on both sides detected by DLDP can be set to work in active/passive mode. In the passive mode, DLDP detection packets are not sent actively and only the DLDP detection packets from the peer end are detected and replied to for link detection. When multi-channel DLDP detection is configured on a convergence router, the passive mode can greatly reduce processing load of the convergence device and traffic load of lines.

In the passive mode, the peer end must be set to active mode so that the devices on both sides can normally work with each other.

## Configuring Device Link Detection

---

### Task List

Follow the task list below to configure Ethernet link detection:

- Configuring Ethernet link detection function
- Configuring the next-hop IP address
- Configuring interval
- Configuring retry times
- Configuring resume times
- Clearing the records of the times when DLDP status is changed from UP to DOWN
- Checking the times when DLDP status is changed from UP to DOWN within a period of time

## Configuring Ethernet Link Detection Function

This command can be configured on the Ethernet port only. By default, this function is not enabled. To activate it, run the following command:

Command	Function
Ruijie(config-if)# <b>dldp ip</b> [ <i>nexthopip</i> ]	It is used to activate the link detection protocol.



### Note

- 1) This function is implemented with the help of ICMP ECHO packets. The peer device should enable the ICMP response function.
- 2) The precondition of enabling this function is that the interface is in UP state.
- 3) After this function is enabled, if the interface is in down state, the IP address of the interface cannot be modified.
- 4) In the case of detection across network segments, the next-hop IP address should be configured. For example, the local interface IP address is 10.1.1.1 needs to detect 30.1.1.1 through the 20.1.1.1 gateway, the next-hop IP address 20.1.1.1 should be configured.

## Configuring Interval

Setting heartbeat intervals can change the frequency of sending handshaking packets for link detection.

Command	Function
Ruijie(config-if)# <b>dldp ip interval</b> <i>val</i>	It is used to set the interval for device link detection.

## Configuring Retry Times

Command	Function
Ruijie(config-if)# <b>dldp ip retry</b> val	It is used to set the threshold of error times during device link detection.

## Configuring Active/Passive Mode

Command	Function
Ruijie(config-if)# <b>dldp passive</b>	It is used to set device link detection to work in passive mode.

## Configuring Resume Times

Command	Function
Ruijie(config-if)# <b>dldp ip resume</b> val	It is used to set the threshold of resuming the device link. The threshold indicates that the times for receiving continuous DLDP detection packet responses before the link status is changed from DOWN to UP. The resumption time is related to the interval for sending link detection packets set by running the <b>dldp ip interval</b> command. That is, line resumption time = resume times * dldp ip interval.



### Note

This function is used to avoid device link oscillation. For example, when users run the **ping** command to detect link status and the results show that some links are not connected all the time, links are oscillated all the time. That is, link status is always changed between UP and DOWN or ARP is always switched over. Setting a greater resume value can avoid this problem. Only when the number of detection packet responses received by the link reached the threshold set by using the **resume** command, link status is changed from DOWN to UP.

## Clearing the Records of the Times when DLDP Status is Changed from UP to DOWN

Command	Function
Ruijie(config-if)# <b>clear-dldp</b> [all] [ip [nexthopip]]	Ruijie routers can record the times of UP and DOWN status of device links. Running the <b>clear-dldp</b> command can clear the recorded times and begin to record the times.



### Note

- 1) Running the **clear-dldp all** command to clear the times when all links on an interface are changed from UP to DOWN within a period of time and to record the times from 0.
- 2) Running the **clear-dldp ip [nexthopip]** command to clear the times when the specified link is changed from UP to DOWN within a period of time and to record the times from 0.

## Checking the Times when Ethernet Link Status is UP and DOWN Within a Period of Time

Command	Function
Ruijie(config-if)# <b>show dldp</b> interface [ ] [FastEthernet/GigabitEthernet number]	It is used to check the times when Ethernet links are changed from UP to DOWN within a period of time on the configured DLDP-enabled interface.



### Note

- 1) Run the **show dldp interface** command to check the times of all Ethernet links when their status is UP and DOWN and the time for beginning to record the times.
- 2) Run the **show dldp interface FastEthernet/GigabitEthernet number** command to check the times when links are UP and DOWN on the Ethernet interface and the time for beginning to record the times.



# TPP Configuration

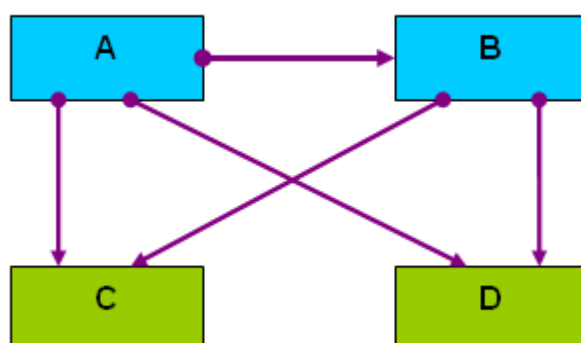
## TPP Overview

The Topology Protection Protocol (TPP) is a topology stability protection protocol. The network topology is rather fragile. Illegal attacks in the network may cause abnormal CPU utilization on network devices, frame path blocked, etc. These are apt to cause network topology oscillation. The topology protection aims to stabilize the network topology by detecting the abnormalities (high CPU utilization, frame buffer abnormal, etc.) and detecting the abnormalities of neighbor devices. The interaction with neighbor devices is implemented by sending specific abnormality advertisement. This function has rather high priority and can effectively prevent network topology oscillation.

## TPP Application

The topology protection is generated to address the network topology turbulence that may be caused in the MSTP or VRRP and other distributed network protocol. The MSTP, VRRP and other protocols work with the message notification mechanism to automatically maintain the network topological structure and automatically adapt to the topological change in the network. This on the other hand results in the aptness to attacks. When malicious network attacks arrive, transient interruption of timed messages may be caused due to high CPU utilization or frame path blocking, causing error fluctuation of the network topology and great harm to the normal communication in the network. The topology protection function minimizes such unnecessary fluctuations. It works with the other distributed protocols (MSTP, VRRP, etc.) to make the network more stable and reliable.

**Figure-1:**



As shown in the above dual-core topology, A and B are the L3 convergence devices, and C and D are the L2 access devices. A is the MSTP root bridge. The topology protection functions of all the devices are enabled.

The CPU of the L3 convergence device A is extremely busy due to network attack, resulting in that the BPDU packets cannot be sent. The topology protection function detects the exception

and sends the exception advertisement packet to its neighbors. B, C, and D all receive the advertisement and adopt the anti-vibration measures.

The CPU of B is extremely busy under the attack of a large number of packets and cannot send or receive packets normally. After detecting the exception, B sends the exception advertisement to all its neighbors. A receives the exception advertisement but does not process it further because B finds the exception has not effect on B according to its source. The downstream C and D receive the exception advertisement and perform further defense activities to ensure the reliability of the network topology, because they find the exception will affect the topology calculation.

## TPP Configuration

Configuring TPP involves global function configuration and port function configuration. The global function configuration is used to enable the topology protection function of the device. By default, the global topology protection function is enabled. Here, it will detect the running conditions of the local and neighbor devices and perform treatment for the abnormalities that occur. However, it does not notify the local running conditions to neighbor devices. The port function configuration is used to enable the topology protection function of the port. When the topology protection function is enabled on the port, it indicates that the opposite neighbor device is concerning about the running conditions of this machine. When the local device becomes abnormal, this will be notified to the opposite neighbor device of the port. By default, the topology protection function is disabled on all ports.



### Note

The topology protection function is suitable for the point-to-point link network, and adjacent network devices must enable the topology protection function. Besides, during the TPP configuration, you often need to use `cpu topology-limit` to configure the threshold for CPU utilization detection. When the CPU utilization exceeds the threshold, the system generates the topology protection advertisement. We suggest a middle to high value, such as 50–70, so that the TPP can judge the network conditions more accurately. If the value is too small, the network topology may not switch when it should to switch due to TPP alarm. If the value is too large, the system may be too busy to generate the TPP alarm, causing the TPP invalid.

## Configuring Topology Protection Globally

The global topology protection function is enabled by default. The **no** option of the command disables the global topology protection.

The configuration commands are as follows:

Command	Function
Ruijie> <b>enable</b>	Enter the privileged EXEC mode.
Ruijie# <b>config terminal</b>	Enter the global configuration mode.
Ruijie(config)# <b>topology guard</b>	Enable the global topology protection
Ruijie(config)# <b>end</b>	Exit to the privileged EXEC mode.

Command	Function
Ruijie# <b>copy running-config startup-config</b>	Save the configuration.

The **no topology guard** command disables the global topology protection function on the device.

## Configuring Topology Protection on the Port

The configuration commands are as follows:

Command	Function
Ruijie> <b>enable</b>	Enter the privileged EXEC mode.
Ruijie# <b>config terminal</b>	Enter the global configuration mode.
Ruijie(config)# <b>interface gi 0/1</b>	Enter the interface configuration mode.
Ruijie(config-if)# <b>tp-guard port enable</b>	Enable the port topology protection function.
Ruijie(config-if)# <b>end</b>	Exit to the privileged EXEC mode.

The **no tp-guard port enable** command disables the topology protection on the port. This command is suitable only on layer-2 switching ports and routing ports. It is inapplicable to AP member ports.



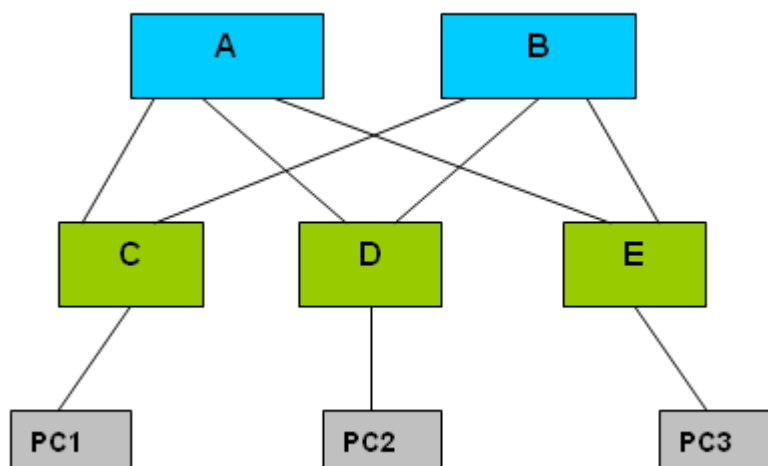
### Note

The global topology protection is the global switch for the topology protection. When it is enabled, the device detects the running parameters of its own and monitors the running parameters of neighbor devices at the same time. When abnormality appears locally, it sends abnormality notification messages to the neighbor devices. When the port topology protection function is enabled, if abnormality occurs locally, it sends abnormality notification message to neighbor devices.

## Typical TPP Configuration Examples

The figure below shows a dual-core networking topology:

**Figure-2:**



As shown in the figure, A and B are L3 convergence devices, while C, D and E are L2 access devices.

The MSTP enabled on A, B, C, D, and E, and VRRP enabled on A and B. The topology protection function enables the MSTP and VRRP to operate more reliable, avoiding unnecessary vibration of the network topology.

The global topology protection function is enabled on A, B, C, D, and E, and the topology protection function is enabled on all the ports..

## View TPP information

The following TPP-related information can be viewed:

- View the TPP configuration and status of the device

## Viewing the TPP configuration and status of the device

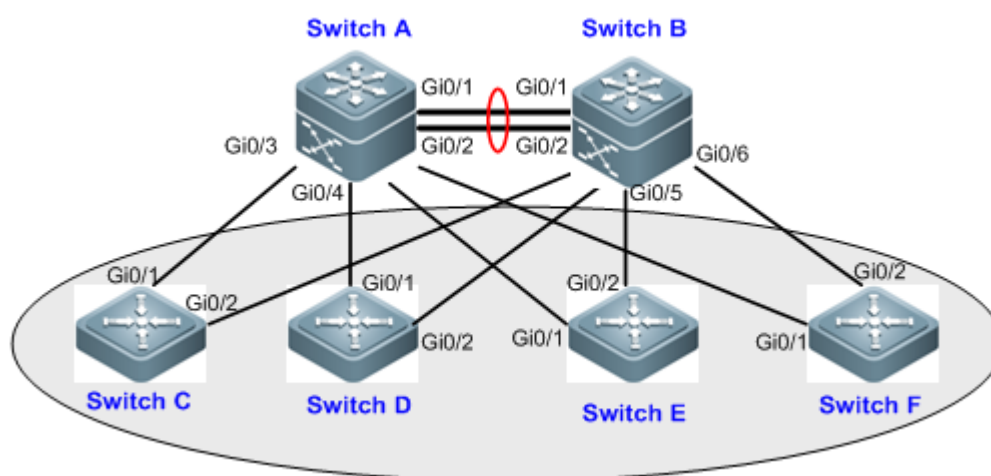
In the privileged EXEC mode, run the following command to view the TPP configuration and status of the device:

Command	Function
Ruijie# <b>show tpp</b>	View the TPP configuration and status of the device

```
Ruijie #show tpp
tpp state          : enable
tpp local bridge   : 00d0.f822.35ad
```

## Typical TPP Configuration Example

### Topology Diagram



Topology diagram for typical TPP application

## Application Requirements

As shown above, the core layer of a park network adopts the typical MSTP+VRPP topological structure. The illegal attacks existing in the network may result in abnormal CPU utilization on network devices, frame path blocked and etc, thus leading to the network topology oscillation.

By applying TPP, MSTP and VRRP can operate more stably, thus avoiding unnecessary network topology oscillation.

## Configuration Tips

Configure the following features on layer-3 core devices (Switch A/B) and layer-2 access devices (Switch C/D/E/F):

- Enable topology protection globally. This feature is enabled by default.
- Enable topology protection on the port connecting with devices, so that any local abnormality can be advertised to the neighbors in order to maintain topological stability.
- Configure the threshold for CPU utilization detection on each device. When CPU utilization of the device exceeds this threshold, the system will generate topology protection advertisement.



### Note

It is suggested to configure this value to an above-average ratio, such as 50-70, so that TPP can precisely estimate the network situation. If this value is too low, the network topology cannot be switched due to the alert of TPP when it becomes necessary; if this value is too high, the system may be too busy to generate TPP alert, resulting in the failure of TPP function.

## Configuration Steps

Only TPP configurations will be introduced below. For relevant configurations of MSTP+VRPP, please refer to "MSTP Configuration" and "VRRP Configuration" in the manual.

### ➤ Configurations on Switch A/B

Step 1: Global topology protection is enabled by default. If it is disabled, use the following command to enable this function.

```
Ruijie# config terminal
Ruijie(config)# topology guard
```

Step 2: Enable topology protection on the interface.

! Enable topology protection on the AP ports connecting core devices.

```
Ruijie(config)#interface aggregateport 1
Ruijie(config-if-AggregatePort 1)#tp-guard port enable
```

! Enable topology protection on the ports connecting downlink devices.

```
Ruijie(config)#interface range gigabitEthernet 0/3-6
Ruijie(config-if-range)#tp-guard port enable
```

Step 3: Configure the threshold for detecting CPU utilization.

! When CPU utilization exceeds 60%, the system will generate topology protection advertisement.

```
Ruijie(config)#cpu topology-limit 60
```

### ➤ Configurations on Switch C/D/E/F

Step 1: Global topology protection is enabled by default. If it is disabled, use the following command to enable topology protection.

```
Ruijie# config terminal
Ruijie(config)# topology guard
```

Step 2: Enable topology protection on the interface.

```
Ruijie(config)#interface range gigabitEthernet 0/1-2
Ruijie(config-if-range)#tp-guard port enable
```

Step 3: Configure the threshold for detecting CPU utilization.

! When CPU utilization exceeds 60%, the system will generate topology protection advertisement.

```
Ruijie(config)#cpu topology-limit 60
```

## Verification

### ➤ Display TPP configurations

Take the Switch A as the example for viewing TPP configurations. Key points: TPP state, TPP information of interface.

```
Ruijie#show tpp
tpp state          : enable          //Global TPP is enabled by default
tpp local bridge   : 00d0.f822.33aa
-----
interface GigabitEthernet 0/3
port tpp state     : enable
interface GigabitEthernet 0/4
port tpp state     : enable
interface GigabitEthernet 0/5
port tpp state     : enable
interface GigabitEthernet 0/6
port tpp state     : enable
interface AggregatePort 1
port tpp state     : enable
```

### ➤ Verification of TPP function

When spanning tree topology is stable, SwitchA is the root bridge, and the Gi 0/2 interface of Switch C is in Block state.

Step 1: To simulate the scenario that Switch C is attacked by the downlink illegal users, we have configured BPDU Filter on port Gi0/3 of Switch B, so that port Gi0/2 of Switch C

cannot receive BPDU packets. When TPP is not configured, port Gi0/2 of Switch C turns into Forwarding state, and the topology changes.

```
Ruijie#show spanning-tree sum
```

```
Spanning tree enabled protocol mstp
```

```
MST 0 vlans map : 1-9, 11-19, 21-29, 31-39, 41-4094
```

```
Root ID    Priority    4096
           Address    00d0.f834.56f0
           this bridge is root
           Hello Time  2 sec Forward Delay 15 sec Max Age 20 sec
```

```
Bridge ID  Priority    32768
           Address    00d0.f822.33aa
           Hello Time  2 sec Forward Delay 15 sec Max Age 20 sec
```

Interface	Role	Sts Cost	Prio	Type	OperEdge
Gi0/2	Desg FWD	20000	128	P2p	True
Gi0/1	Root FWD	20000	128	P2p	False

```
MST 1 vlans map : 10, 20
```

```
Region Root Priority    4096
           Address    00d0.f834.56f0
           this bridge is region root
```

```
Bridge ID  Priority    32768
           Address    00d0.f822.33aa
```

Interface	Role	Sts Cost	Prio	Type	OperEdge
Gi0/2	Desg FWD	20000	128	P2p	True
Gi0/1	Root FWD	20000	128	P2p	False

Step 2: After completing TPP related configurations as per the steps shown herein, we simulates the scenario that Switch C is attacked by downlink illegal users who send excessive ARP packets to Switch C, causing CPU utilization to exceed the configured threshold. By this time, further configure BPDU Filter on port Gi0/3 of Switch B, so that the Gi0/2 of Switch C cannot receive BPDU packets. By displaying the state of spanning tree interface on Switch C, it can be found that the interface maintains the Block state. TPP has taken effect.

```
Ruijie#show spanning-tree summary
```

```
Spanning tree enabled protocol mstp
```

```
MST 0 vlans map : 1-9, 11-19, 21-29, 31-39, 41-4094
```

```
Root ID    Priority    4096
```

Address 00d0.f834.56f0  
this bridge is root  
Hello Time 2 sec Forward Delay 15 sec Max Age 20 sec

Bridge ID Priority 32768  
Address 00d0.f822.33aa  
Hello Time 2 sec Forward Delay 15 sec Max Age 20 sec

Interface	Role Sts Cost	Prio	Type	OperEdge
-----	-----	-----		
Gi0/2	Altn BLK 20000	128	P2p	False
Gi0/1	Root FWD 20000	128	P2p	False

MST 1 vlans map : 10, 20

Region Root Priority 4096  
Address 00d0.f834.56f0  
this bridge is region root

Bridge ID Priority 32768  
Address 00d0.f822.33aa

Interface	Role Sts Cost	Prio	Type	OperEdge
-----	-----	-----		
Gi0/2	Altn BLK 20000	128	P2p	False
Gi0/1	Root FWD 20000	128	P2p	False



# BFD Configuration

## Understanding BFD

### BFD Overview

Bidirectional forwarding detection (BFD) provides low-overhead, short-duration detection of the connectivity in the forwarding path between adjacent routers. The fast detection of failures in the forwarding path speeds up enabling the backup forwarding path and improves the network performance.

### BFD Packet Format

The two types of BFD packets are control packets and echo packets. The local end sends echo packets to the peer, which returns the received echo packets back without processing. Therefore, no BFD echo packet format is defined. Only BFD control packet format is defined. There are two versions for the BFD control packet: version 0 and version 1. By default, the BFD session establishment adopts the version 1. However, if one end receives the version 0 control packets from the peer, the default version 1 will automatically switch to version 0 to establish the BFD session. You can use the **show bfd neighbors** command to view the version member. The format of the version 1 packet is shown as follows:

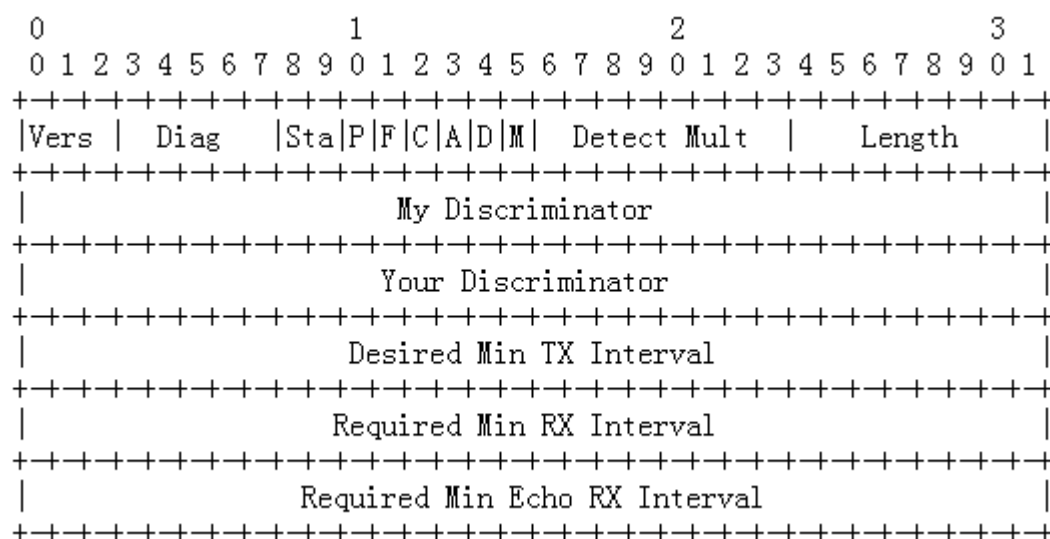


Figure-1 BFD Control Packet Format

- Vers: BFD version. The current version is 1.
- Diag: The reasons for the last transition of the local protocol from UP to some other state, including:
  1. no diagnostic information
  2. detection timeout of the control packets
  3. echo failure
  4. adjacency advertisement session is Down
  5. reset the forwarding panel
  6. channel failure
  7. channel connection failure
  8. AdminDown

- Sta: Current BFD session state. Its value can be 0 for AdminDown, 1 for Down, 2 for Init and 3 for Up.
- P: When the parameter changes, the sender offsets the Poll(P) bit in the BFD packet and the receiver must response to this packet immediately.
- F: It must be offset in the echo packet of responding the Poll(P) bit offset.
- C: The forwarding/control separation bit. Once it is offset, the change of control panel has no influence on the BFD detect. For example, BFD is able to go on detecting the link state if OSPF(the control panel) reloads/GR.
- A: Authentication identifier. Offset means the session needs to be verified. If it is set to 1, the control packet contains the authentication field and the session is authenticated.
- D: Inquiry demand. Offset means the sender expects to detect the links in the inquiry demand mode.
- M: Used in the one-to-multiple application and must be set to 0.
- Detect Mult: Detect the timeout multiplier, used to calculate the detection timeout time for the detector.
- Length: the packet length.
- My Discriminator: the local discriminator connecting the BFD session.
- Your Discriminator: the peer discriminator connecting the BFD session.
- Desired Min Tx Interval: the minimum BFD packets sending interval for the local protocol.
- Required Min Rx Interval: the minimum BFD packets receiving interval for the local protocol.
- Required Min Echo Rx Interval: the minimum Echo packets receiving interval for the local protocol (if the Echo function is not supported for the local protocol, set the value to 0)
- Auth Type: the authentication type(optional), including:
  1. Simple Password
  2. Keyed MD5
  3. Meticulous Keyed MD5
  4. Keyed SHA1
  5. Meticulous Keyed SHA1
- Auth Length: the authentication data length
- Authentication Data: the authentication data field

**Caution**

Since v10.3(4b3), RGOS support the packet format in version 1 and version 0. By default, version 1 is used for the packet sending of BFD session. If the packets sent from the peer with version 1 are received, it will automatically switch to the version 0 to establish the session.

## BFD Operation Mechanism

The BFD detection mechanism is independent from the applied interface media type, the encapsulation format and the associated upper-layer protocols such as OSPF, BGP, RIP. The BFD establishes a session between adjacent routers, enables the route protocols to re-calculate the route table by rapidly sending the detection fault to the running route protocols and decreases the network convergence time sharply. The BFD itself can not discover the neighbors, so it needs the upper-layer protocols to notify the neighbors of which the session is established.

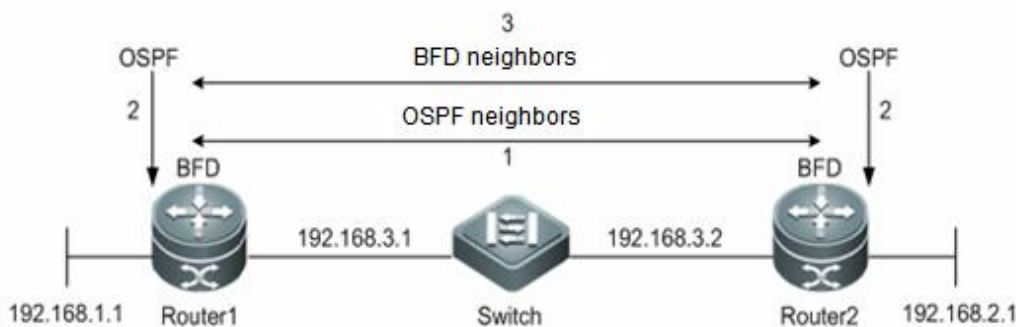


Figure-2 BFD Session Establishment

As the Figure-2 shows, two routers are connected via a L2 switch. OSPF and BFD are running in the two routers at the same time. The BFD session establishment process is:

- Step 1: OSPF discovers neighbors and establish neighbor relationships.
- Step 2: OSPF notifies BFD of establishing the session with the neighbors.
- Step 3: BFD establishes the session with the neighbors.

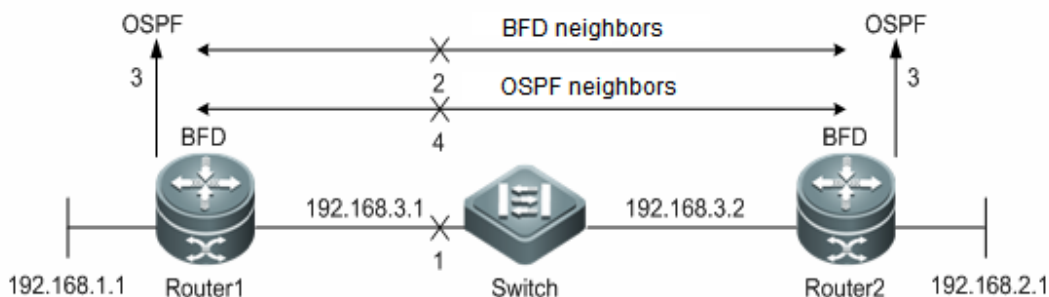


Figure-3 BFD Fault Detection Process

As the Figure-3 shows, the BFD fault detection process is:

- Step 1: A link communication failure between Router1 and Router2 occurs.
- Step 2: BFD session between the Router1 and Router2 detects the fault.
- Step 3: BFD notifies the fault of the OSPF reachability to the forwarding path of the neighbor.
- Step 4: OSPF deals with the process of the neighborDown. If the backup forwarding path exists and the convergence is about to happen, the backup forwarding path will be enabled.

## Related Protocols and Regulations

The related BFD protocols and regulations are:

- draft-ietf-bfd-base-09:Bidirectional Forwarding Detection
- draft-ietf-bfd-generic-05:Generic Application of BFD
- draft-ietf-bfd-mib-06:Bidirectional Forwarding Detection Management Information Base
- draft-ietf-bfd-v4v6-1hop-09:BFD for IPv4 and IPv6 (Single Hop)
- draft-ietf-bfd-multihop-07:BFD for IPv4 and IPv6 (Multihop)
- draft-ietf-bfd-mpls-07:BFD For MPLS LSPs

## BFD Features

This section describes the BFD features.

## BFD Session Establishment Mode

The BFD session is established in the following modes:

1. Active Mode: Before a session is established, BFD actively sends the BFD control packets regardless of whether any BFD control packet is received from the peer.
2. Passive Mode: Before a session is established, no BFD control packet is sent until a BFD control packet is received from the peer.

## BFD Detection Mode

The BFD detection modes are as follows:

1. Asynchronous Mode

In the asynchronous mode, the BFD control packets are sent periodically among the systems. If one system receives no BFD control packet from the peer within the BFD interval, the BFD session will be down.

2. Demand Mode

In the demand mode, suppose that every system has an independent method to confirm whether it has been connected to other systems, once a BFD session is established, the system stops sending the BFD control packets unless a system needs the connection verification. If the connection verification is necessary, the system will send a BFD control packet with the short sequence. If no returned packet is received within the detection interval, the BFD session will be down. If the echo packet is received from the peer, the forwarding path is normal.

3. Echo Mode

The local system sends the BFD echo packet periodically. The peer system loops back the echo packet via the forwarding channel. The BFD session will be down if the continuous echo packets are not received within the detection interval. The echo mode can be co-used with the above-mentioned two detection modes. In the echo mode, the packets are forwarded back via the forwarding panel of the peer system rather than the control panel, reducing the delay and speeding up the fault detection in comparison to the control packet sending. In the asynchronous mode, the control packet sending will be decreased with the echo function enabled, for the echo function processes the detection. If the echo function is enabled in the demand mode, the control packet sending can be cancelled after the BFD session establishment. The echo function must be enabled in the BFD session, otherwise the echo function will be invalid.



The **no ip redirects** command must be executed to disable the redirect function of the IP packets and the **no ip deny land** command must be executed to disable the function of anti-attack of the Land-based DDOS before configuring the echo mode. The BFD echo function works on the condition that the version of the BFD control packet is version 1.

## BFD Session Parameter

The BFD session parameters(for example, Desired Min Tx Interval, Required Min Rx Interval, Detect Mult, ect) can be modified after the BFD session is established. The modified BFD session will

renegotiate and use the newest parameter value to detect the session. During the modification, the session keeps in the UP state.

## BFD Authentication Method

The BFD authentication methods include:

1. Simple Password
2. Keyed MD5
3. Meticulous Keyed MD5
4. Keyed SHA1
5. Meticulous Keyed SHA1

## BFD for Dynamic Route Protocols

Configuring BFD for the route protocols improves the convergence performance of the protocol by taking advantages of the faster fault detection of the BFD in comparison to the HELLO mechanism of the protocol. Generally, the fault detection time can be decreased to less than 1s. RGOSv10.4(1), v10.3(4b3) and v10.3(5) support the following route protocols:

1. RIPv1, RIPv2
2. OSPFv2
3. BGP

RGOSv10.4E also supports the OSPFv3 route protocol. Make sure that the BFD for corresponding protocol is enabled on all BFD session neighbors, or the BFD session cannot be established. However, if the dynamic route protocol or other applications have already notify the BFD of establishing the session with the corresponding neighbor, the BFD for this protocol will be established automatically.

## BFD for Static Route

Configuring BFD for static route prevents the static route from being the forwarding path when the router selects the routing under the circumstances that the configured static route is unreachable. It can rapidly switch to the backup forwarding path if the backup forwarding path exists.

Being different from the dynamic route protocol, the static route protocol has no mechanism of discovering the neighbor. Therefore, when configuring the BFD for static route, the reachability of the next-hop of the static route is dependent on the BFD session state. If the BFD session detects the fault, which means that next-hop of the static route is unreachable, the static route can not be installed into the RIB. Make sure that the BFD for static route is enabled on all BFD session neighbors, or the BFD session cannot be established. However, if the dynamic route protocol or other applications have already notify the BFD of establishing the session with the corresponding neighbor, the BFD for static route will be enabled automatically.

If the BFD session is removed from the peer in the process of the BFD session establishment, the BFD session will be down. And under this circumstance, the static route forwarding shall be ensured.

## BFD for PBR

Configuring BFD for PBR prevents the PBR from being the forwarding path when the router selects the routing under the circumstances that the configured PBR is unreachable. It can rapidly switch to the backup forwarding path if the backup forwarding path exists.

The method of BFD for PBR is similar to the BFD for static route. If the BFD session detects the fault by following the forwarding path of the specified neighbor, the PBR will be notified of the unreachability to the corresponding next-hop. The PBR reaching the next-hop is ineffective.

Make sure that the BFD for PBR is enabled on all BFD session neighbors, or the BFD session cannot be established. However, if the dynamic route protocol or other applications have already notify the BFD of establishing the session with the corresponding neighbor, the BFD for PBR will be enabled automatically.

If the BFD session is removed from the peer in the process of the BFD session establishment, the BFD session will be down. And under this circumstance, the PBR forwarding shall be ensured.

## BFD for VRRP

BFD for VRRP configuration can replace the HELLO mechanism of VRRP itself to realize the fast detection of running state of the master and backup routers and improve the network performance. Generally, the time of failure detection can be shortened to less than 1s.

Make sure that the BFD for VRRP is enabled on the router at both ends, or the BFD session cannot be established. However, if the dynamic route protocol or other applications have already notify the BFD of establishing the session with the corresponding neighbor, the BFD for VRRP will also be configured.

VRRP can also use BFD to follow the specified neighbor. If the BFD session detects the fault of the forwarding path to the neighbor, it will reduce the VRRP priority automatically and trigger the switchover between the master and backup routers. The BFD can be established only when the dynamic route protocol or other applications notify BFD of establishing the session with corresponding neighbor.

## BFD for VRRP+

BFD for VRRP+ can replace the BVF detection by BVG of VRRP+, allowing quick detection of BVF operating state and accelerating the switchover of forwarding entity during failure. Under general circumstances, the fault detection time can be shortened to less than 1 second.

Since VRRP+ is based on VRRP protocol, no extra configuration will be needed during its association with BFD. You only need to make sure VRRP has been enabled on the devices at both ends and BFD session has been correctly associated.

## BFD supports to change the State of Layer3 Interfaces

BFD supports to change the state of layer-3 interface. In configuration mode, execute "bfd bind peer-ip" to detect the directly connected address of the specified layer-3 interface. The BFD session state established by this CLI command will generate the BFD state of the corresponding interface, such as BFD-DOWN/BFD-UP. In various types of FRR, BFD is used to detect interface state and perform fast FRR switchover.

## BFD for MPLS-LSP

BFD for MPLS mainly refers to the case that LSP (Label Switched Path) uses BFD to carry out quick neighbor detection. The detection modes supported include:

1. Configure BFD for detecting static LSP;
2. Configure BFD for detecting the LSP generated by LDP;
3. Configure BFD for detecting backward LSP with IP

## BFD for VRF

The BFD supports VPN Routing and Forwarding(VRF) and detects the connectivity of the forwarding path between the Provider Edge(PE) and the Customer Edge(CE).

## Supported BFD Interfaces

For the switches, it is allowed to configure the BFD on the Routed Port and SVI only. Besides, it fails to set the BFD session on the SVI L2AP member port.

For the routers, it is allowed to configure the BFD on the synchronous port, the asynchronous port, ATM, the serial port, the frame relay, POS, CPOS, the dialed port, Ethernet port and its sub-port, E1, channelized ATM, channelized CPOS.

## Configuring BFD

This section describes how to configure the BFD features.

### Default Configurations

Function	Defaults
BFD session creation mode	Active mode, can not be set.
BFD detection mode	Asynchronous mode, the echo function is enabled by default.
BFD session parameter	No default value, must be set.
BFD authentication method	Disabled, can not be set.
BFD for dynamic route protocol	Disabled
BFD for static route	Disabled
BFD for PBR	Disabled
BFD for VRRP	Disabled
BFD for VRF	Disabled

### Configuring the BFD Session Parameter

The BFD session parameter has no default value and must be configured. The following are the configuration steps:

Command	Function
Ruijie> <b>enable</b>	Enter the privileged EXEC mode.
Ruijie# <b>configure terminal</b>	Enter the global configuration mode.
Ruijie(config)# <b>interface type number</b>	Enter the interface configuration mode.

Command	Function
Ruijie(config-if)# <b>bfd interval</b> <i>milliseconds</i> <b>min_rx</b> <i>milliseconds</i> <b>multiplier</b> <b>interval-multiplier</b>	Configure the BFD parameters on the specified interface. Interval <i>milliseconds</i> : configure the minimum sending interval, in millisecond; min_rx <i>milliseconds</i> : configure the minimum receiving interval, in millisecond; multiplier <i>interval-multiplier</i> : configure the detection timeout multiplier.
Ruijie(config-if)# <b>end</b>	Exit the interface configuration mode and return to the privileged EXEC mode.

Use the **no bfd interval** command in the interface configuration mode to remove the BFD session parameter configurations.

The following example shows how to configure the BFD session parameter on the Routed Port FastEthernet 0/2:

Ruijie# **configure terminal**

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

Ruijie(config)# **interface** *fastEthernet 0/2*

Ruijie(config-if)# **bfd interval** 100 **min\_rx** 100 **multiplier** 3



#### Caution

The difference of the bandwidth transmitted on different interfaces should be considered when configuring the parameters. If the minimum sending and receiving intervals are too low, it may result in the oversized bandwidth of the BFD and the influence of the data transmission.

## Configuring the BFD Echo Function

By default, the BFD echo function is enabled. Enabling the echo function does not influence the established session state. With the echo function disabled, the echo packets will not be sent, and not be received on the forwarding panel.

Follow the following steps to configure the BFD echo function:

Command	Function
Ruijie> <b>enable</b>	Enter the privileged EXEC mode.
Ruijie# <b>configure terminal</b>	Enter the global configuration mode.
Ruijie(config)# <b>interface</b> <i>type number</i>	Enter the interface configuration mode.
Ruijie(config-if)# <b>bfd echo</b>	Enable the echo function.
Ruijie(config-if)# <b>end</b>	Exit the interface configuration mode and return to the privileged EXEC mode.

Use the **no bfd echo** command in the interface configuration mode to disable the BFD echo function.



The following example shows how to configure the BFD echo function on the Routed Port FastEthernet 0/2:

Ruijie# **configure terminal**

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

Ruijie(config)# **interface fastEthernet 0/2**

Ruijie(config-if)# **bfd echo**

After enabling the echo function in the BFD asynchronous mode, the slower frequency can be adopted to send the BFD control packets.

Follow the following steps to configure this parameter:

Command	Function
Ruijie> <b>enable</b>	Enter the privileged EXEC mode.
Ruijie# <b>configure terminal</b>	Enter the global configuration mode.
Ruijie(config)# <b>bfd slow-timer milliseconds</b>	Configure the time of the slow-timer, in milliseconds, ranging from 1000 to 30000. The default value is 1000.
Ruijie(config)# <b>end</b>	Exit the global configuration mode.

Use the **no bfd slow-timer** command in the global configuration mode to restore it to the default value.

The following example shows how to configure the time of the slow-timer to 1400 milliseconds:

Ruijie# **configure terminal**

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

Ruijie(config)# **bfd slow-timer 1400**



#### Caution

The local end sends the BFD echo packet to the peer, which returns the received packets with processing on the forwarding panel. In this process, the BFD session detection may fail for the peer has been congested resulting in the loss of the echo packets. Under these circumstances, the corresponding QoS policy is necessary to be configured to make sure that the echo packets take the precedence to be processed or the echo function is disabled.

## Configuring the BFD UP-Dampening Time

The BFD up-dampening time configuration solves the problem that due to the line instability, BFD session state frequent switchover between DOWN and UP occurs, which results in the frequent forwarding path switchover of the associated application(for example, the static route) and the abnormal operation.

Follow the following steps to configure the BFD up-dampening time:

Command	Function
Ruijie> <b>enable</b>	Enter the privileged EXEC mode.
Ruijie# <b>configure terminal</b>	Enter the global configuration mode.
Ruijie(config)# <b>interface type number</b>	Enter the interface configuration mode.
Ruijie(config-if)# <b>bfd up-dampening milliseconds</b>	Configure the up-dampening time.

Command	Function
Ruijie(config)# <b>end</b>	Exit the interface configuration mode and return to the privileged EXEC mode.

Use the **no bfd up-dampening** command in the interface configuration mode to restore to the default value.

The following example shows how to configure the BFD up-dampening time as 60,000ms:

Ruijie# **configure terminal**

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

Ruijie(config)# **interface fastEthernet 0/2**

Ruijie(config-if)# **bfd up-dampening 60000**

## Configuring the BFD Protection Policy

BFD protocol is so sensitive that if the device with BFD function enabled suffers from attack (for example, a large amount of Ping packets attack the device), which lead to the BFD session turbulence, the device can be protected by enabling the BFD protection policy. However, if the BFD function and the BFD protection policy are enabled at the same time, the loss of BFD packets on the attacked device occurs when the packets sent from the last-hop device go through this device, influencing the BFD session establishment between the last-hop device and other devices. This function is valid only for the switches.

Follow the following steps to configure the BFD protection policy:

Command	Function
Ruijie> <b>enable</b>	Enter the privileged EXEC mode.
Ruijie# <b>configure terminal</b>	Enter the global configuration mode.
Ruijie(config)# <b>bfd cpp</b>	Enable the BFD protection policy.
Ruijie(config)# <b>end</b>	Exit the global configuration mode.

By default, the BFD CPP is enabled. Use the **no bfd cpp** command in the global configuration mode to disable the BFD CPP.

The following example shows how to enable the BFD CPP:

Ruijie# **configure terminal**

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

Ruijie(config)# **bfd cpp**

## Configuring the BFD for RIP

RIP sends the route updating information periodically. A route is invalid and RIP cannot rapidly respond to the link failure when no route updating information is received within the specified time.

After enabling the BFD for RIP, the BFD session will be established for the RIP route information source(the source address for RIP route updating packet). Once BFD detects that a neighbor is invalid, RIP route information will directly be in the invalid state and not join in the route forwarding no longer. The convergence time can be decreased from 180s(the default RIP timer) to less than 1s.

Use the **bfd all-interfaces** command to configure the BFD for RIP on all interfaces. Or use the **ip rip bfd [disable]** command in the interface configuration mode to enable or disable the BFD for RIP on the specified interface.

Command	Function
Ruijie> <b>enable</b>	Enter the privileged EXEC mode.
Ruijie# <b>configure terminal</b>	Enter the global configuration mode.
Ruijie(config)# <b>router rip</b>	Enter the Router configuration mode.
Ruijie(config-router)# <b>bfd all-interfaces</b>	Enable the BFD for RIP on all interfaces.
Ruijie(config-router)# <b>exit</b>	(Optional) Exit the Router configuration mode and return to the global configuration mode.
Ruijie(config)# <b>interface</b> <i>type number</i>	(Optional) Enter the interface configuration mode.
Ruijie(config-if)# <b>ip rip bfd [disable]</b>	(Optional) Enable or disable the BFD for RIP on a specified interface.
Ruijie(config-if)# <b>end</b>	(Optional) Exit interface configuration mode.
Ruijie# <b>show bfd neighbor [details]</b>	(Optional) Show the information of the BFD session establishment and whether RIP is associated to the specified session.

Use the **no bfd all-interfaces** command in the Router configuration mode to disable the BFD for RIP on all interfaces.

The following example shows how to enable the BFD for RIP on all interfaces excluding the FastEthernet 0/2:

```
Ruijie# configure terminal
```

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

```
Ruijie(config)# router rip
```

```
Ruijie(config-router)# bfd all-interfaces
```

```
Ruijie(config-router)# exit
```

```
Ruijie(config)# interface FastEthernet 0/2
```

```
Ruijie(config-if)# ip rip bfd disable
```

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

**Caution**

When configuring BFD for IPv4 PBR, the route information source (source address for RIP route updating packet) of two devices with RIP enabled shall be in the same network segment to establish the BFD session between adjacent routers.

Before enabling BFD for IPv4 PBR, the BFD session parameter must be configured, or it is ineffective.

For the non-unnumbered interface, if the neighbor end and the local end are not connected directly, the BFD for IPv4 PBR fails to be enabled.

The BFD session cannot be established if the specified interface and the actual outbound interface for the BFD packets are inconsistent because of the IP routing.

The BFD session cannot be established if the specified interface and the actual incoming interface for the BFD packets are inconsistent.

## Configuring the BFD for OSPF

OSPF protocol dynamically discovers the neighbors by the Hello packets. With BFD for OSPF configured, the BFD session for the neighbors in FULL relationship will be established and the neighbor state will be detected by the BFD mechanism. Once BFD neighbor is invalid, OSPF processes the network convergence. The convergence time could be from 120s (by default, the sending interval of the OSPF Hello packet in non-broadcast network is 30s, which is a quarter of the invalid time for the adjacency router, namely, 120s) to less than 1s.

Use the **bfd all-interfaces** command to configure the BFD for OSPF on all interfaces. Or use the **ip rip bfd [disable]** command in the interface configuration mode to enable or disable the BFD for OSPF on the specified interface.

Command	Function
Ruijie> <b>enable</b>	Enter the privileged EXEC mode.
Ruijie# <b>configure terminal</b>	Enter the global configuration mode.
Ruijie(config)# <b>router ospf process-id</b>	Enter the Router configuration mode.
Ruijie(config-router)# <b>bfd all-interfaces</b>	Enable the BFD for OSPF on all interfaces.
Ruijie(config-router)# <b>exit</b>	(Optional) Exit the Router configuration mode and return to the global configuration mode.
Ruijie(config)# <b>interface type number</b>	(Optional) Enter the interface configuration mode.
Ruijie(config-if)# <b>ip rip bfd [disable]</b>	(Optional) Enable or disable the BFD for OSPF on a specified interface.
Ruijie(config-if)# <b>end</b>	(Optional) Exit interface configuration mode.

Command	Function
Ruijie# <b>show bfd neighbor [details]</b>	(Optional) Show the information of the BFD session establishment and whether OSPF is associated to the specified session.
Ruijie# <b>show ip ospf</b>	(Optional) Verify whether OSPF is associated to the specified session.

Use the **no bfd all-interfaces** command in the Router configuration mode to disable the BFD for OSPF on all interfaces.

The following example shows how to enable the BFD for OSPF on all interfaces excluding the FastEthernet 0/2:

Ruijie# **configure terminal**

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

Ruijie(config)# **router ospf 123**

Ruijie(config-router)# **bfd all-interfaces**

Ruijie(config-router)# **exit**

Ruijie(config)# **interface FastEthernet 0/2**

Ruijie(config-if)# **ip rip bfd disable**

Ruijie(config-if)#**end**



**Caution**

Before enabling BFD for OSPF, the BFD session parameter must be configured, or it is ineffective.

The BFD session cannot be established if the specified interface and the actual outbound interface for the BFD packets are inconsistent because of the IP routing.

The BFD session cannot be established if the specified interface and the actual incoming interface for the BFD packets are inconsistent.

BFD monitoring is not supported in the virtual link of OSPFv2/OSPFv3.

## Configuring the BFD for BGP

Being similar to OSPF, by configuring the BFD for BGP, BGP protocol rapidly detects the faults, realizes the rapid detection of the neighbor relationship and fastens the protocol convergence. By default, the BGP keepalive interval is 60s and the holdtime is 180s. The minimum value of the keepalive interval and holdtime are 1s and 3s respectively. It is slow to detect the neighbor relationship. A large amount of the packets will be lost on the interface that receives and sends the packets at the fast speed.

Use the **neighbor ip-address fall-over bfd** command to enable the BFD for BGP.

Command	Function
Ruijie> <b>enable</b>	Enter the privileged EXEC mode.
Ruijie# <b>configure terminal</b>	Enter the global configuration mode.
Ruijie(config)# <b>router bgp as-tag</b>	Enter the Router configuration mode.

Command	Function
Ruijie(config-router)# <b>neighbor ip-address fall-over bfd</b>	Configure the BFD for BGP to detect the fault of the specific neighbor.
Ruijie(config-router)# <b>end</b>	(Optional) Exit router configuration mode.
Ruijie# <b>show bfd neighbor [details]</b>	(Optional) Show the information of the BFD session establishment and whether BGP is associated to the specified session.
Ruijie# <b>show ip bgp neighbors</b>	(Optional) Verify whether BGP is associated to the specified session.

Use the **no neighbor ip-address fall-over bfd** command in the Router configuration mode to disable the BFD for BGP.

The following example shows how to enable the BFD for BGP, and detect the forwarding path with the neighbor 172.16.0.2

#### Ruijie# **configure terminal**

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

```
Ruijie(config)# interface FastEthernet 0/1
```

```
Ruijie(config-if)# no switchport
```

```
Ruijie(config-if)# ip address 172.16.0.1 255.255.255.0
```

```
Ruijie(config-if)# bfd interval 50 min_rx 50 multiplier 3
```

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

```
Ruijie(config)# router bgp 44000
```

```
Ruijie(config-router)# bgp log-neighbors-changes
```

```
Ruijie(config-router)# neighbor 172.16.0.2 remote-as 45000
```

```
Ruijie(config-router)# neighbor 172.16.0.2 fall-over bfd
```

```
Ruijie(config-router)# end
```



#### Caution

If BGP establishes the session using the loopback address and enables BFD to detect the neighbors, the outbound interface for the BFD packets will be specified according to the result of IP routing. In this situation, before configuring the BFD for BGP, the **bfd interval** command is necessary to be used to configure the BFD session parameter on the possible outbound interface, or it may fail to establish the session.

The BFD session cannot be established if the specified interface and the actual incoming interface for the BFD packets are inconsistent.

## Configuring the BFD for Static Route

Execute the following steps to configure the BFD for static route.

Command	Function
Ruijie> <b>enable</b>	Enter the privileged EXEC mode.
Ruijie# <b>configure terminal</b>	Enter the global configuration mode.
Ruijie(config)# <b>ip route static bfd</b> [vrf vrf-name] interface-type interface-number gateway [source ip-address]	Configure the session neighbors of the BFD for static route. interface-type interface-number: the neighbor interface; gateway: the IP address for the neighbor ; In the circumstances of multi-hopping, use the source ip-address command to configure the source IP address for the session. Make sure that the BFD session parameter for the interface has been configured before configuration. For details, see Configuring the BFD Session Parameter.
Ruijie(config)# [ <b>ip ipv6</b> ] route prefix mask {ip-address   interface-type interface-number [ip-address]}	Configure the static route. In order to ensure the BFD for static route configuration, the input parameters of interface-type interface-number and ip-address and the ones configured in step3 must be consistent.
Ruijie(config)# <b>end</b>	(Optional) Exit global configuration mode.
Ruijie# <b>show bfd neighbor</b> [details]	(Optional) Show the information of the BFD session establishment and whether the static route is associated to the specified session.

Use the **no ip route static bfd** [vrf vrf-name] interface-type interface-number gateway command in the interface configuration mode to disable the BFD for static route.

The following example shows how to enable the BFD for static route, and detect the forwarding path with the neighbor 172.16.0.2:

Ruijie# **configure terminal**

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

Ruijie(config)# **interface** FastEthernet 0/1

Ruijie(config-if)# **no switchport**

Ruijie(config-if)# **ip address** 172.16.0.1 255.255.255.0

Ruijie(config-if)# **bfd interval** 50 **min\_rx** 50 **multiplier** 3

Ruijie(config-if)# **ip route static bfd** FastEthernet 0/1 172.16.0.2

Ruijie(config-if)# **ip route** 10.0.0.0 255.0.0.0 **FastEthernet** 0/1 172.16.0.2

Ruijie(config-if)# **end**

## Configuring the BFD for PBR

Execute the following steps to configure the BFD for PBR.

Command	Function
Ruijie> <b>enable</b>	Enter the privileged EXEC mode.
Ruijie# <b>configure terminal</b>	Enter the global configuration mode.
Ruijie(config)# <b>route-map</b> <i>route-map-name</i> <b>[permit   deny]</b> <i>sequence</i>	Define the route map and enter the route-map configuration mode.
Ruijie(config-route-map)# <b>match ip address</b> <i>access-list-number</i>	Configure the matched access list.
Ruijie(config-route-map)# <b>set ip next-hop verify-availability</b> <i>next-hop-address</i> <b>{track number   bfd [vrf vrf-name] interface-type interface-number gateway}</b>	Configure the session neighbor of the BFD for PBR. <i>interface-type interface-number</i> : the neighbor interface; <i>gateway</i> : the IP address for the neighbor ; Make sure that the BFD session parameter for the interface has been configured before configuration. For details, see <i>Configuring the BFD Session Parameter</i> . If the BFD session faults are detected, the next-hop specified by the <i>next-hop-address</i> is unreachable. Use the no form of this command to remove the configuration.
Ruijie(config-route-map)# <b>exit</b>	Exit the route-map configuration mode.
Ruijie(config)# <b>interface</b> <i>type number</i>	Enter the interface configuration mode.
Ruijie(config-if)# <b>ip policy route-map</b> <i>route-map</i>	Configure the BFD for the PBR.
Ruijie(config-if)# <b>end</b>	(Optional) Exit interface configuration mode.
Ruijie# <b>show bfd neighbor [details]</b>	(Optional) Show the information of the BFD session establishment and whether PBR is associated to the specified session.
Ruijie# <b>show route-map</b>	(Optional) Verify whether PBR is associated to the specified session.

Use the **no set ip next-hop verify-availability** [*next-hop-address* **[track number|bfd [vrf vrf-name] interface-type interface-number gateway]**] command in the route-map configuration mode to disable the BFD for PBR.

The following example shows how to enable the BFD for PBR, and detect the forwarding path with the neighbor 172.16.0.2:

Ruijie# **configure terminal**



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

```
Ruijie(config)# route-map Example1 permit 10
Ruijie(config-route-map)# match ip address 1
Ruijie(config-route-map)# set ip precedence priority
Ruijie(config-route-map)#set ip next-hop verify-availability 172.16.0.2 bfd FastEthernet 0/1
172.16.0.2
Ruijie(config-route-map)#exit
Ruijie(config)#interface FastEthernet 0/1
Ruijie(config-if)#no switchport
Ruijie(config-if)#ip address 172.16.0.1 255.255.255.0
Ruijie(config-if)#bfd interval 50 min_rx 50 multiplier 3
Ruijie(config-if)#ip policy route-map Example1
Ruijie(config-if)#exit
```

## Configuring the BFD for VRRP

Execute the following steps to configure the BFD for VRRP to detect the master and slave routers.

Command	Function
Ruijie> <b>enable</b>	Enter the privileged EXEC mode.
Ruijie# <b>configure terminal</b>	Enter the global configuration mode.
Ruijie(config)# <b>interface</b> type number	Enter the interface configuration mode.
Ruijie(config-if)# <b>vrrp</b> group-number <b>ip</b> [ip-address[ <b>secondary</b> ]]	Create the VRRP group and virtual Ip address on the specified interface.
Ruijie(config-if)# <b>vrrp</b> group-number <b>bfd</b> ip-address	Configure the BFD for VRRP. ip-address: the IP address for the specified neighbor.
Ruijie(config)-if# <b>end</b>	(Optional) Exit interface configuration mode.
Ruijie# <b>show bfd neighbor [details]</b>	(Optional) Show the information of the BFD session establishment and whether VRRP is associated to the specified session.
Ruijie# <b>show vrrp</b>	(Optional) Verify whether VRRP is associated to the specified session.

Use the **no vrrp group-number bfd** command in the interface configuration mode to disable the BFD for VRRP and the application of the master and slave router detection.

The following example shows how to enable the BFD for VRRP, and detect the forwarding path between the master and slave routers:

```
Ruijie# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Ruijie(config)#interface FastEthernet 0/1
Ruijie(config-if)#no switchport
Ruijie(config-if)#ip address 192.168.201.11 255.255.255.0
Ruijie(config-if)#bfd interval 50 min_rx 50 multiplier 3
```

```
Ruijie(config-if)#vrrp 1 priority 120
Ruijie(config-if)#vrrp 1 ip 192.168.201.1
Ruijie(config-if)#vrrp 1 bfd 192.168.201.12
Ruijie(config-if)#end
```

Execute the following steps to configure the BFD for VRRP to follow the specified neighbor IP.

Command	Function
Ruijie> <b>enable</b>	Enter the privileged EXEC mode.
Ruijie# <b>configure terminal</b>	Enter the global configuration mode.
Ruijie(config)# <b>interface</b> <i>type number</i>	Enter the interface configuration mode.
Ruijie(config-if)# <b>vrrp</b> <i>group-number</i> <b>ip</b> [ <i>ip-address</i> ][ <b>secondary</b> ]	Create the VRRP group and virtual Ip address on the specified interface.
Ruijie(config-if)# <b>vrrp</b> <i>group-number</i> <b>track</b> <b>bfd</b> <i>interface-type interface-number ip-address</i> [ <i>priority</i> ]	Specify the VRRP group to follow the neighbor IP address of the specified interface. Use the <b>no</b> form of this command to remove this configuration.
Ruijie(config)-if# <b>end</b>	(Optional) Exit interface configuration mode.
Ruijie# <b>show bfd neighbor</b> [ <b>details</b> ]	(Optional) Show the information of the BFD session establishment and whether VRRP is associated to the specified session.
Ruijie# <b>show vrrp</b>	(Optional) Verify whether VRRP is associated to the specified session and follows the specified neighbor IP.

Use the **no vrrp group-number track bfd interface-type interface-number ip-address** command in the interface configuration mode to disable the BFD for VRRP and the application of following the specified neighbor IP.

The following example shows how to specify the VRRP to follow the specified neighbor 192.168.1.3:

```
Ruijie# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Ruijie(config)#interface FastEthernet 0/1
Ruijie(config-if)#no switchport
Ruijie(config-if)#ip address 192.168.1.1 255.255.255.0
Ruijie(config-if)#bfd interval 50 min_rx 50 multiplier 3
Ruijie(config)#interface FastEthernet 0/2
Ruijie(config-if)#no switchport
Ruijie(config-if)#ip address 192.168.201.17 255.255.255.0
Ruijie(config-if)#vrrp 1 priority 120
Ruijie(config-if)#vrrp 1 ip 192.168.201.1
Ruijie(config-if)#vrrp 1 track bfd FastEthernet 0/1 192.168.1.3 30
Ruijie(config-if)#end
```

## Configuring the BFD for VRRP+

Since VRRP+ relies on VRRP, after configuring BFD for VRRP, VRRP+ will automatically associate with BFD.

## Configuring BFD to Support Changing the State of Layer 3 Interfaces

Generally, it will take a long time for link communication failure or link failure to change the interface state. For various FRRs relying on interface state, high-performance switchover cannot be achieved. Therefore, BFD is generally associated with the layer-3 interface state to realize fast detection of interface state. Execute the following configurations to associate BFD and layer 3 interface states.

Command	Function
Ruijie> <b>enable</b>	Enter privileged EXEC mode
Ruijie# <b>configure terminal</b>	Enter global configuration mode
Ruijie(config)# <b>interface</b> <i>type number</i>	Enter a specific layer-3 interface
Ruijie(config-if)# <b>bfd bind peer-ip</b> <i>ip-address</i> [ <b>source-ip</b> <i>ip-adress</i> ] <b>process-pst</b>	Configure the neighbor detected by BFD Source-IP is used to specify the source IP of BFD packets to prevent such packets from being discarded due to the failure of uRPF check while uRPF is enabled at the same time. Process-pst refers to the BFD state of the interface generating BFD session.
Ruijie(config-if)# <b>end</b>	(Optional) Exit interface configuration mode.
Ruijie# <b>show bfd neighbors</b> [ <b>details</b> ]	(Optional) Display the information about BFD session establishment and whether the interface has been associated to the relevant session.

To disable BFD on the interface, execute "**no bfd bind peer-ip ip-address**" in the configuration mode.

Configuration example:

# Configure to enable BFD on interface FastEthernet 0/2

Ruijie#**configure terminal**

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

Ruijie(config)# **interface FastEthernet 0/2**

Ruijie(config-if)#**no sw**

Ruijie(config-if)#**ip address 1.1.1.1 255.255.255.0**

Ruijie(config-if)#**bfd bind peer-ip 1.1.1.2 source-ip 1.1.1.1 process-pst**

Ruijie(config-if)#**end**

## Configuring BFD For MPLS

BFD for MPLS mainly uses BFD to quickly detect the LSPs on MPLS network in order to enhance the reliability of MPLS network.

## Configuring BFD for Detecting Static LSP

Command	Function
Ruijie> <b>enable</b>	Enter privileged EXEC mode
Ruijie# <b>configure terminal</b>	Enter global configuration mode
Ruijie# <b>mpls router ldp</b>	Enter LDP configuration mode
Ruijie(config)# <b>bfd bind static-lsp peer-ip</b> <i>ip-address source-ip ip-address</i> <b>[local-discriminator</b> <i>discr-value</i> <b>remote-discriminator</b> <i>discr-value]</i> <b>[process-state]</b>	Configure BFD for detecting static LSP and handle BFD session state. You can configure the peer IP address, the next-hop address and the egress interface of LSP. If no local discriminator is configured, the system will automatically select the local discriminator. If no remote discriminator is configured, the system will use auto-configuration to learn the remote discriminator.

## Configuring BFD for Detecting Dynamic LSP

Command	Function
Ruijie> <b>enable</b>	Enter privileged EXEC mode
Ruijie# <b>configure terminal</b>	Enter global configuration mode
Ruijie# <b>mpls router ldp</b>	Enter LDP configuration mode
Ruijie(config-mpls-router)# <b>bfd bind</b> <b>ldp-lsp peer-ip</b> <i>ip-address nexthop</i> <i>ip-address [interface interface-type</i> <i>interface-number] source-ip ip-address</i> <b>[local-discriminator</b> <i>discr-value</i> <b>remote-discriminator</b> <i>discr-value]</i> <b>[process-state]</b>	Configure BFD for detecting dynamic LSP and handle BFD session state. You can configure the peer IP address, the next-hop address and the egress interface of LSP. If no local discriminator is configured, the system will automatically select the local discriminator. If no remote discriminator is configured, the system will use auto-configuration to learn the remote discriminator.

## Configuring BFD for Detecting Backward LSP with IP

Command	Function
Ruijie> <b>enable</b>	Enter privileged EXEC mode
Ruijie# <b>configure terminal</b>	Enter global configuration mode

Command	Function
<pre>Ruijie(config)#          bfd          bind backward-lsp-with-ip peer-ip ip-address [vrf vrf-name] interface interface-type interface-number [source-ip ip-address] {local-discriminator      discr-value remote-discriminator discr-value}</pre>	<p>Configure BFD for detecting backward LSP with IP. You can configure the source IP address, peer IP address and the egress interface of LSP.</p> <p>The local discriminator and remote discriminator must be configured manually.</p>

To learn more details about BFD for MPLS-LSP and the command reference, please refer to the documents named "MPLD-CERF" and "MPLS-SCG".

## Displaying BFD Configuration and State

BFD offers the following displaying commands to view various configurations and running information. The functions of each command are explained as follows:

Command	Function
<pre>show bfd neighbors [vrf vrf-name] [ipv4 ip-address [details]] [ipv6 ipv6-address [details]   client {bgp ospf rip vrrp static-route pbr} [ipv4 ip-address [details]   ipv6 ipv6-address [details]] details]]</pre>	<p>Show the BFD session information. For details, see the field description in Table-1.</p>
<b>show vrrp</b>	Show the configuration of BFD for VRRP.
<b>show route-map</b>	Show the configuration of BFD for PBR.
<b>show ip route static bfd</b>	Show the configuration of BFD for static route.
<b>show ip bgp neighbors</b>	Show the configuration of BFD for BGP.
<b>show ip ospf neighbor</b>	Show the configuration of BFD for OSPF.
<b>show ip rip peer</b>	Show the configuration of BFD for RIP.



### Caution

The displaying commands above can be configured in any configuration mode except for the user mode.

## Configuration Examples

### Example of Configuring BFD for RIP

#### Network Requirement

RouterA and RouterB are interconnected through a L2 switch. Both routers run the RIP protocol and enable the BFD for RIP on the interface. After a link failure between RouterB and L2 switch occurs, BFD detects the failure and notifies the RIP of the failure, triggering the rapid convergence.

#### Network Topology

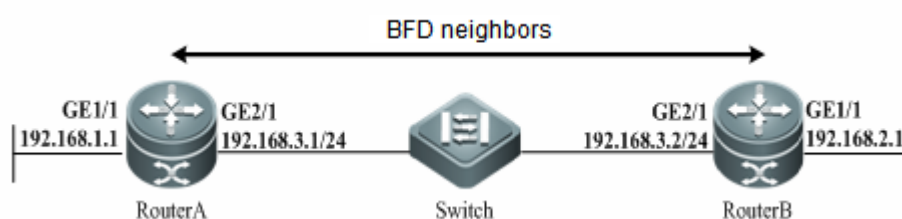


Figure-4 Topology of Configuring BFD for RIP

#### Configuration Steps

##### 1) RouterA Configuration

# Configure the Routed Port *gi 2/1*, the IP address, the BFD session parameter for Router A:

Ruijie# **configure terminal**

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

Ruijie(config)# **interface GigabitEthernet 2/1**

Ruijie(config-if)# **no switchport**

Ruijie(config-if)# **ip address 192.168.3.1 255.255.255.0**

Ruijie(config-if)# **bfd interval 200 min\_rx 200 multiplier 5**

# Configure the Routed Port *gi1/1*:

Ruijie(config-if)# **exit**

Ruijie(config)# **interface GigabitEthernet 1/1**

Ruijie(config-if)# **no switchport**

Ruijie(config-if)# **ip address 192.168.1.1 255.255.255.0**

# Enable RIP and configure the BFD for RIP to detect the neighbor 192.168.3.2:

Ruijie(config-if)# **exit**

Ruijie(config)# **router rip**

Ruijie(config-router)# **version 2**

Ruijie(config-router)# **network 192.168.3.0**

Ruijie(config-router)# **network 192.168.1.0**

Ruijie(config-router)# **passive-interface GigabitEthernet 2/1**

Ruijie(config-router)# **bfd all-interfaces**

##### 2) RouterB Configuration

# Configure the Routed Port, the IP address, the BFD session parameter for Router B:

Ruijie# **configure terminal**

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

Ruijie(config)# **interface GigabitEthernet 2/1**

Ruijie(config-if)# **no switchport**

Ruijie(config-if)# **ip address 192.168.3.1 255.255.255.0**

Ruijie(config-if)# **bfd interval 50 min\_rx 50 multiplier 5**

# Configure the Routed Port *gi1/1*:

Ruijie(config-if)# **exit**

Ruijie(config)# **interface GigabitEthernet 1/1**

Ruijie(config-if)# **no switchport**

Ruijie(config-if)# **ip address 192.168.1.1 255.255.255.0**

# Enable RIP and configure the BFD for RIP to detect the neighbor 192.168.3.1:

Ruijie(config-if)# **exit**

Ruijie(config)# **router rip**

Ruijie(config-router)# **version 2**

Ruijie(config-router)# **network 192.168.3.0**

Ruijie(config-router)# **network 192.168.2.0**

Ruijie(config-router)# **passive-interface GigabitEthernet 2/1**

Ruijie(config-router)# **bfd all-interfaces**

Ruijie(config-router)# **end**

## Configuration Verification

1) View the BFD session of RouterA

Ruijie# **show bfd neighbors details**

OurAddr	NeighAddr	LD/RD	RH	Holdown(mult)	State	Int
192.168.3.1	192.168.3.2	1/2	1	532 (3 )	Up	Ge2/1

Local Diag: 0, Demand mode: 0, Poll bit: 0

MinTxInt: 200000, MinRxInt: 200000, Multiplier: 5

Received MinRxInt: 50000, Received Multiplier: 3

Holdown (hits): 600(22), Hello (hits): 200(84453)

Rx Count: 49824, Rx Interval (ms) min/max/avg: 208/440/332

Tx Count: 84488, Tx Interval (ms) min/max/avg: 152/248/196

Registered protocols: RIP

Uptime: 02:18:49

Last packet: Version: 1 - Diagnostic: 0

I Hear You bit: 1 - Demand bit: 0

Poll bit: 0 - Final bit: 0

Multiplier: 3 - Length: 24

My Discr.: 2 - Your Discr.: 1

Min tx interval: 50000 - Min rx interval: 50000

Min Echo interval: 0

Field	Description
-------	-------------

Field	Description
OurAddr	IP address for the session on the local end.
NeighAddr	IP address for the adjacent session.
LD/RD	The session discriminator on the local and peer end.
RH	Whether the peer session responds to the local session or not.
Holdown(mult)	The time of not receiving the Hello packets on the local end and the detected timeout time of the session.
State	Current session state.
Int	The interface number for the session.
Session state is UP and using echo function with 50 ms interval	Whether the session is in echo mode and the interval of sending frames. This information is shown only in the echo mode.
Local Diag	The diagnostic information of the session.
Demand mode	Whether the demand mode is enabled or not.
Poll bit	Whether the session configuration is modified.
MinTxInt	The minimum sending interval of the session on the local end.
MinRxInt	The minimum receiving interval of the session on the local end.
Multiplier	The timeout times detected on the local end.
Received MinRxInt	The minimum sending interval of the session on the peer end.
Received Multiplier	The timeout times detected on the peer end.
Holdown (hits)	Session detection time and the detected timeout times.
Hello (hits)	The minimum interval of receiving the Hello packet after the session negotiation.
Rx Count	The count of BFD packets received on the local end.
Rx Interval (ms) min/max/avg	The minimum/maximum/average interval of receiving the session on the local end.



Field	Description
Tx Count	The count of BFD packets sent on the local end.
Tx Interval (ms) min/max/avg	The minimum/maximum/average interval of sending the session on the local end.
Registered protocols	Type of protocol registered to the session
Uptime	Time of keeping the session UP.
Last packet	Last BFD packet received on the local end.

Table-1 Filed Description of the Session Displaying

2) View the BFD session of RouterB

Ruijie# **show bfd neighbors details**

```
OurAddr      NeighAddr    LD/RD  RH  Holdown (mult)  State  Int
192.168.3.2  192.168.3.1  2/1    1   532 (5 )        Up     Ge2/1
```

Local Diag: 0, Demand mode: 0, Poll bit: 0

MinTxInt: 50000, MinRxInt: 50000, Multiplier: 3

Received MinRxInt: 200000, Received Multiplier: 5

Holdown (hits): 600(22), Hello (hits): 200(84453)

Rx Count: 49824, Rx Interval (ms) min/max/avg: 209/440/332

Tx Count: 84488, Tx Interval (ms) min/max/avg: 153/249/197

Registered protocols: RIP

Uptime: 02:18:49

Last packet: Version: 1 - Diagnostic: 0

I Hear You bit: 1 - Demand bit: 0

Poll bit: 0 - Final bit: 0

Multiplier: 5 - Length: 24

My Discr.: 1 - Your Discr.: 2

Min tx interval: 200000 - Min rx interval: 200000

Min Echo interval: 0

## Example of Configuring BFD for OSPF

### Network Requirement

RouterA and RouterB are interconnected through a L2 switch. Both routers run the OSPF protocol and enable the BFD for OSPF on the interface. After a link failure between RouterB and L2 switch occurs, BFD detects the failure and notifies the OSPF of the failure, triggering the rapid convergence.

## Network Topology

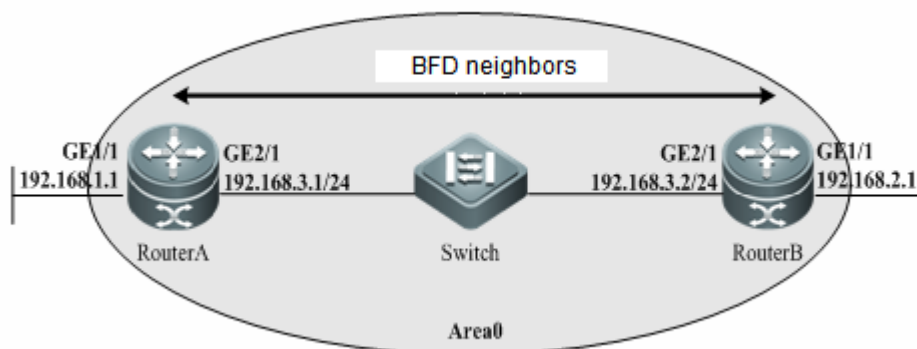


Figure-5 Topology of Configuring BFD for OSPF

## Configuration Steps

### 1) RouterA Configuration

# Configure the Routed Port, the IP address, the BFD session parameter for Router A:

Ruijie# configure terminal

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

Ruijie(config)# interface GigabitEthernet2/1

Ruijie(config-if)# no switchport

Ruijie(config-if)# ip address 192.168.3.1 255.255.255.0

Ruijie(config-if)# bfd interval 200 min\_rx 200 multiplier 5

# Configure the Routed Port *gi1/1*:

Ruijie(config-if)# exit

Ruijie(config)# interface GigabitEthernet1/1

Ruijie(config-if)# no switchport

Ruijie(config-if)# ip address 192.168.1.1 255.255.255.0

# Enable RIP and configure the BFD for OSPF to detect the neighbor 192.168.3.2:

Ruijie(config-if)# exit

Ruijie(config)# router ospf 123

Ruijie(config-router)# log-adj-changes detail

Ruijie(config-router)# network 192.168.3.0 0.0.0.255 area 0

Ruijie(config-router)# network 192.168.1.0 0.0.0.255 area 0

Ruijie(config-router)# bfd all-interfaces

Ruijie(config-router)# end

### 2) RouterB Configuration

# Configure the Routed Port, the IP address, the BFD session parameter for Router B:

Ruijie# configure terminal

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

Ruijie(config)# interface GigabitEthernet2/1

Ruijie(config-if)# no switchport

Ruijie(config-if)# ip address 192.168.3.2 255.255.255.0

```

Ruijie(config-if)# bfd interval 50 min_rx 50 multiplier 3
# Configure the Routed Port gi1/1:
Ruijie(config-if)# exit
Ruijie(config)# interface GigabitEthernet1/1
Ruijie(config-if)# no switchport
Ruijie(config-if)# ip address 192.168.2.1 255.255.255.0
# Enable OSPF and configure the BFD for OSPF to detect the neighbor 192.168.3.1:
Ruijie(config-if)# exit
Ruijie(config)# router ospf 123
Ruijie(config-router)# log-adj-changes detail
Ruijie(config-router)# network 192.168.3.0 0.0.0.255 area 0
Ruijie(config-router)# network 192.168.1.0 0.0.0.255 area 0
Ruijie(config-router)# bfd all-interfaces
Ruijie(config-router)# end

```

## Configuration Verification

### 1) View the BFD session of RouterA

```
Ruijie# show bfd neighbors details
```

OurAddr	NeighAddr	LD/RD	RH	Holdown(mult)	State	Int
192.168.3.1	192.168.3.2	1/2	1	532 (3 )	Up	Ge2/1

Local Diag: 0, Demand mode: 0, Poll bit: 0

MinTxInt: 200000, MinRxInt: 200000, Multiplier: 5

Received MinRxInt: 50000, Received Multiplier: 3

Holdown (hits): 600(22), Hello (hits): 200(84453)

Rx Count: 49824, Rx Interval (ms) min/max/avg: 208/440/332

Tx Count: 84488, Tx Interval (ms) min/max/avg: 152/248/196

Registered protocols: OSPF

Uptime: 02:18:49

Last packet: Version: 1 - Diagnostic: 0

I Hear You bit: 1 - Demand bit: 0

Poll bit: 0 - Final bit: 0

Multiplier: 3 - Length: 24

My Discr.: 2 - Your Discr.: 1

Min tx interval: 50000 - Min rx interval: 50000

Min Echo interval: 0

### 2) View the BFD session of RouterB

```
Ruijie# show bfd neighbors details
```

OurAddr	NeighAddr	LD/RD	RH	Holdown(mult)	State	Int
192.168.3.2	192.168.3.1	2/1	1	532 (5 )	Up	Ge2/1

Local Diag: 0, Demand mode: 0, Poll bit: 0

MinTxInt: 50000, MinRxInt: 50000, Multiplier: 3

Received MinRxInt: 200000, Received Multiplier: 5

Holdown (hits): 600(22), Hello (hits): 200(84453)

Rx Count: 49824, Rx Interval (ms) min/max/avg: 209/440/332 last: 66 ms ago

Tx Count: 84488, Tx Interval (ms) min/max/avg: 153/249/197 last: 190 ms ago

Registered protocols: OSPF

Uptime: 02:18:49

Last packet: Version: 1 - Diagnostic: 0

I Hear You bit: 1 - Demand bit: 0

Poll bit: 0 - Final bit: 0

Multiplier: 5 - Length: 24

My Discr.: 1 - Your Discr.: 2

Min tx interval: 200000 - Min rx interval: 200000

Min Echo interval: 0

## Example of Configuring BFD for BGP

### Network Requirement

RouterA and RouterB are interconnected through a L2 switch. Both routers run the BGP protocol and enable the BFD for BGP on the interface. After a link failure between RouterB and L2 switch occurs, BFD detects the failure and notifies the BGP of the failure, triggering the rapid convergence.

### Network Topology

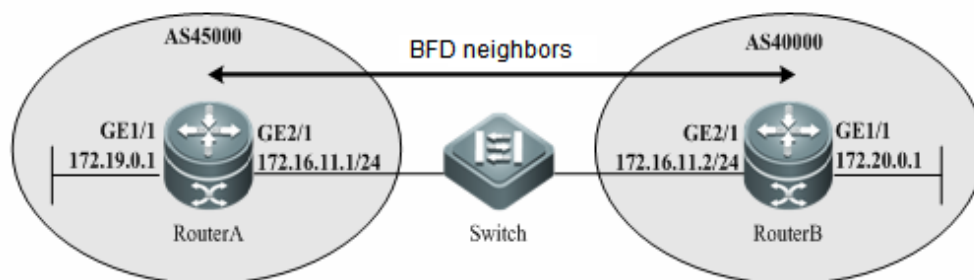


Figure-6 Topology of Configuring BFD for BGP

### Configuration Steps

#### 1) RouterA Configuration

# Configure the Routed Port, the IP address, the BFD session parameter for Router A:

Ruijie# configure terminal

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

Ruijie(config)# interface GigabitEthernet2/1

Ruijie(config-if)# no switchport

Ruijie(config-if)# ip address 172.16.11.1 255.255.255.0

Ruijie(config-if)# bfd interval 200 min\_rx 200 multiplier 5

# Configure the Routed Port *gi1/1*:

Ruijie(config-if)# exit

Ruijie(config)# interface GigabitEthernet1/1

Ruijie(config-if)# no switchport

```

Ruijie(config-if)# ip address 172.19.0.1 255.255.255.0
# Enable BGP and configure the BFD for BGP to detect the neighbor 172.16.11.2:
Ruijie(config-if)# exit
Ruijie(config-router)# router bgp 45000
Ruijie(config-router)# bgp log-neighbor-changes
Ruijie(config-router)# neighbor 172.16.11.2 remote-as 40000
Ruijie(config-router)# neighbor 172.16.11.2 fall-over bfd
Ruijie(config-router)# address-family ipv4
Ruijie(config-router-af)# neighbor 172.16.11.2 activate
Ruijie(config-router-af)# no auto-summary
Ruijie(config-router-af)# no synchronization
Ruijie(config-router-af)# network 172.19.0.0 mask 255.255.255.0
Ruijie(config-router-af)# exit-address-family
Ruijie(config-router)# end

```

## 2) RouterB Configuration

# Configure the Routed Port, the IP address, the BFD session parameter for Router B:

```

Ruijie# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Ruijie(config)# interface GigabitEthernet2/1
Ruijie(config-if)# no switchport
Ruijie(config-if)# ip address 172.16.11.2 255.255.255.0
Ruijie(config-if)# bfd interval 50 min_rx 50 multiplier 3
# Configure the Routed Port gi1/1:
Ruijie(config-if)# exit
Ruijie(config)# interface GigabitEthernet1/1
Ruijie(config-if)# no switchport
Ruijie(config-if)# ip address 172.20.0.1 255.255.255.0
# Enable BGP and configure the BFD for BGP to detect the neighbor 172.16.11.1:
Ruijie(config-if)# exit
Ruijie(config-router)# router bgp 40000
Ruijie(config-router)# bgp log-neighbor-changes
Ruijie(config-router)# neighbor 172.16.11.1 remote-as 45000
Ruijie(config-router)# neighbor 172.16.11.1 fall-over bfd
Ruijie(config-router)# address-family ipv4
Ruijie(config-router-af)# neighbor 172.16.11.1 activate
Ruijie(config-router-af)# no auto-summary
Ruijie(config-router-af)# no synchronization
Ruijie(config-router-af)# network 172.20.0.0 mask 255.255.255.0
Ruijie(config-router-af)# exit-address-family
Ruijie(config-router)# end

```

## Configuration Verification

View the BFD session of RouterA

```
Ruijie# show bfd neighbors details
```

OurAddr	NeighAddr	LD/RD	RH	Holdown(mult)	State	Int
---------	-----------	-------	----	---------------	-------	-----

172.16.11.1 172.16.11.2 1/2 1 532 (3 ) Up Ge2/1

Local Diag: 0, Demand mode: 0, Poll bit: 0

MinTxInt: 200000, MinRxInt: 200000, Multiplier: 5

Received MinRxInt: 50000, Received Multiplier: 3

Holdown (hits): 600(22), Hello (hits): 200(84453)

Rx Count: 49824, Rx Interval (ms) min/max/avg: 208/440/332

Tx Count: 84488, Tx Interval (ms) min/max/avg: 152/248/196

Registered protocols: BGP

Uptime: 02:18:49

Last packet: Version: 1 - Diagnostic: 0

I Hear You bit: 1 - Demand bit: 0

Poll bit: 0 - Final bit: 0

Multiplier: 3 - Length: 24

My Discr.: 2 - Your Discr.: 1

Min tx interval: 50000 - Min rx interval: 50000

Min Echo interval: 0

View the BFD session of RouterB

Ruijie# show bfd neighbors details

OurAddr	NeighAddr	LD/RD	RH	Holdown(mult)	State	Int
172.16.11.2	172.16.11.1	2/1	1	532 (5 )	Up	Ge2/1

Local Diag: 0, Demand mode: 0, Poll bit: 0

MinTxInt: 50000, MinRxInt: 50000, Multiplier: 3

Received MinRxInt: 200000, Received Multiplier: 5

Holdown (hits): 600(22), Hello (hits): 200(84453)

Rx Count: 49824, Rx Interval (ms) min/max/avg: 209/440/332 last: 66 ms ago

Tx Count: 84488, Tx Interval (ms) min/max/avg: 153/249/197 last: 190 ms ago

Registered protocols: BGP

Uptime: 02:18:49

Last packet: Version: 1 - Diagnostic: 0

I Hear You bit: 1 - Demand bit: 0

Poll bit: 0 - Final bit: 0

Multiplier: 5 - Length: 24

My Discr.: 1 - Your Discr.: 2

Min tx interval: 200000 - Min rx interval: 200000

Min Echo interval: 0

## Example of Configuring BFD for Static Route

### Network Requirement

RouterA and RouterB are interconnected through a L2 switch. Both routers run the static route protocol and enable the BFD for static route on the interface. After a link failure between RouterB and L2 switch occurs, BFD detects the failure and notifies the static route of the failure, triggering the static route removal from RIB and preventing the routing error.

## Network Topology

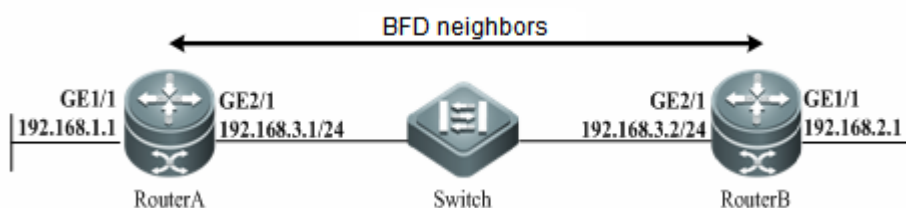


Figure-7 Topology of Configuring BFD for Static Route

## Configuration Steps

### 1) RouterA Configuration

# Configure the Routed Port, the IP address, the BFD session parameter for Router A:

Ruijie# configure terminal

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

Ruijie(config)# interface GigabitEthernet2/1

Ruijie(config-if)# no switchport

Ruijie(config-if)# ip address 192.168.3.1 255.255.255.0

Ruijie(config-if)# bfd interval 200 min\_rx 200 multiplier 5

# Configure the Routed Port *gi1/1*:

Ruijie(config-if)# exit

Ruijie(config)# interface GigabitEthernet1/1

Ruijie(config-if)# no switchport

Ruijie(config-if)# ip address 192.168.1.1 255.255.255.0

# Configure the BFD for static route to detect the neighbor 192.168.3.2:

Ruijie(config-if)# exit

Ruijie(config)# ip route static bfd GigabitEthernet 2/1 192.168.3.2

Ruijie(config)# ip route 192.168.2.0 255.255.255.0 GigabitEthernet 2/1 192.168.3.2

Ruijie(config)# end

### 2) RouterB Configuration

# Configure the Routed Port, the IP address, the BFD session parameter for Router B:

Ruijie# configure terminal

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

Ruijie(config)# interface GigabitEthernet2/1

Ruijie(config-if)# no switchport

Ruijie(config-if)# ip address 192.168.3.2 255.255.255.0

Ruijie(config-if)# bfd interval 50 min\_rx 50 multiplier 3

# Configure the Routed Port *gi1/1*:

Ruijie(config-if)# exit

Ruijie(config)# interface GigabitEthernet1/1

Ruijie(config-if)# no switchport

Ruijie(config-if)# ip address 192.168.2.1 255.255.255.0

# Configure the BFD for static route to detect the neighbor 192.168.3.1:

Ruijie(config-if)# exit

```
Ruijie(config)# ip route static bfd GigabitEthernet 2/1 192.168.3.1
Ruijie(config)# ip route 192.168.1.0 255.255.255.0 GigabitEthernet 2/1 192.168.3.1
Ruijie(config)# end
```

## Configuration Verification

### 1) View the BFD session of RouterA

```
Ruijie# show bfd neighbors details
```

OurAddr	NeighAddr	LD/RD	RH	Holdown(mult)	State	Int
192.168.3.1	192.168.3.2	1/2	1	532 (3 )	Up	Ge2/1

Local Diag: 0, Demand mode: 0, Poll bit: 0

MinTxInt: 200000, MinRxInt: 200000, Multiplier: 5

Received MinRxInt: 50000, Received Multiplier: 3

Holdown (hits): 600(22), Hello (hits): 200(84453)

Rx Count: 49824, Rx Interval (ms) min/max/avg: 208/440/332

Tx Count: 84488, Tx Interval (ms) min/max/avg: 152/248/196

Registered protocols: STATIC ROUTE

Uptime: 02:18:49

Last packet: Version: 1 - Diagnostic: 0

I Hear You bit: 1 - Demand bit: 0

Poll bit: 0 - Final bit: 0

Multiplier: 3 - Length: 24

My Discr.: 2 - Your Discr.: 1

Min tx interval: 50000 - Min rx interval: 50000

Min Echo interval: 0

### 2) View the BFD session of RouterB

```
Ruijie# show bfd neighbors details
```

OurAddr	NeighAddr	LD/RD	RH	Holdown(mult)	State	Int
192.168.3.2	192.168.3.1	2/1	1	532 (5 )	Up	Ge2/1

Local Diag: 0, Demand mode: 0, Poll bit: 0

MinTxInt: 50000, MinRxInt: 50000, Multiplier: 3

Received MinRxInt: 200000, Received Multiplier: 5

Holdown (hits): 600(22), Hello (hits): 200(84453)

Rx Count: 49824, Rx Interval (ms) min/max/avg: 209/440/332 last: 66 ms ago

Tx Count: 84488, Tx Interval (ms) min/max/avg: 153/249/197 last: 190 ms ago

Registered protocols: STATIC ROUTE

Uptime: 02:18:49

Last packet: Version: 1 - Diagnostic: 0

I Hear You bit: 1 - Demand bit: 0

Poll bit: 0 - Final bit: 0

Multiplier: 5 - Length: 24

My Discr.: 1 - Your Discr.: 2

Min tx interval: 200000 - Min rx interval: 200000

Min Echo interval: 0



## Example of Configuring BFD for PBR

### Network Requirement

RouterA and RouterB are interconnected through a L2 switch. Both routers run the PBR protocol and enable the BFD for PBR on the interface. After a link failure between RouterB and L2 switch occurs, BFD detects the failure and notifies the PBR of the failure, triggering the PBR removal preventing the routing error.

### Network Topology

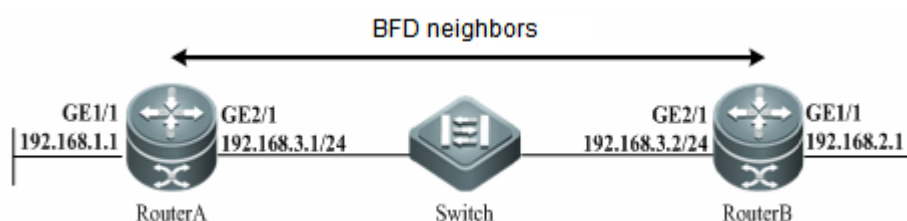


Figure-8 Topology of Configuring BFD for PBR

### Configuration Steps

#### 1) RouterA Configuration

# Configure the Routed Port, the IP address, the BFD session parameter for Router A:

Ruijie# configure terminal

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

Ruijie(config)# interface GigabitEthernet2/1

Ruijie(config-if)# no switchport

Ruijie(config-if)# ip address 192.168.3.1 255.255.255.0

Ruijie(config-if)# bfd interval 200 min\_rx 200 multiplier 5

# Configure the Routed Port *gi1/1*:

Ruijie(config-if)# exit

Ruijie(config)# interface GigabitEthernet1/1

Ruijie(config-if)# no switchport

Ruijie(config-if)# ip address 192.168.1.1 255.255.255.0

# Configure the BFD for PBR to detect the neighbor 192.168.3.2:

Ruijie(config)# ip access-list extended 100

Ruijie(config-ext-nacl)# permit ip any 192.168.2.0 0.0.0.255

Ruijie(config-ext-nacl)# deny ip any any

Ruijie(config-ext-nacl)# exit

Ruijie(config)# route-map Example1 permit 10

Ruijie(config-route-map)# match ip address 100

Ruijie(config-route-map)# set ip precedence priority

Ruijie(config-route-map)#set ip next-hop verify-availability 192.168.3.2 bfd GigabitEthernet 0/1  
192.168.3.2

Ruijie(config)# end

## 2) RouterB Configuration

# Configure the Routed Port, the IP address, the BFD session parameter for Router B:

Ruijie# configure terminal

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

Ruijie(config)# interface GigabitEthernet2/1

Ruijie(config-if)# no switchport

Ruijie(config-if)# ip address 192.168.3.2 255.255.255.0

Ruijie(config-if)# bfd interval 50 min\_rx 50 multiplier 3

# Configure the Routed Port *gi1/1*:

Ruijie(config-if)# exit

Ruijie(config)# interface GigabitEthernet1/1

Ruijie(config-if)# no switchport

Ruijie(config-if)# ip address 192.168.2.1 255.255.255.0

# Configure the BFD for PBR to detect the neighbor 192.168.3.1:

Ruijie(config)# ip access-list extended 100

Ruijie(config-ext-nacl)# permit ip any 192.168.1.0 0.0.0.255

Ruijie(config-ext-nacl)# deny ip any any

Ruijie(config-ext-nacl)# exit

Ruijie(config)# route-map Example1 permit 10

Ruijie(config-route-map)# match ip address 100

Ruijie(config-route-map)# set ip precedence priority

Ruijie(config-route-map)#set ip next-hop verify-availability 192.168.3.1 bfd GigabitEthernet 2/1  
192.168.3.1

Ruijie(config)# end

## Configuration Verification

View the BFD session of RouterA

Ruijie# show bfd neighbors details

OurAddr	NeighAddr	LD/RD	RH	Holdown(mult)	State	Int
192.168.3.1	192.168.3.2	1/2	1	532 (3 )	Up	Ge2/1

Local Diag: 0, Demand mode: 0, Poll bit: 0

MinTxInt: 200000, MinRxInt: 200000, Multiplier: 5

Received MinRxInt: 50000, Received Multiplier: 3

Holdown (hits): 600(22), Hello (hits): 200(84453)

Rx Count: 49824, Rx Interval (ms) min/max/avg: 208/440/332

Tx Count: 84488, Tx Interval (ms) min/max/avg: 152/248/196

Registered protocols: PBR

Uptime: 02:18:49

Last packet: Version: 1 - Diagnostic: 0

I Hear You bit: 1 - Demand bit: 0

Poll bit: 0 - Final bit: 0

Multiplier: 3 - Length: 24

My Discr.: 2 - Your Discr.: 1

Min tx interval: 50000 - Min rx interval: 50000

Min Echo interval: 0

View the BFD session of RouterB

Ruijie# show bfd neighbors details

OurAddr	NeighAddr	LD/RD	RH	Holdown(mult)	State	Int
192.168.3.2	192.168.3.1	2/1	1	532 (5 )	Up	Ge2/1

Local Diag: 0, Demand mode: 0, Poll bit: 0

MinTxInt: 50000, MinRxInt: 50000, Multiplier: 3

Received MinRxInt: 200000, Received Multiplier: 5

Holdown (hits): 600(22), Hello (hits): 200(84453)

Rx Count: 49824, Rx Interval (ms) min/max/avg: 209/440/332 last: 66 ms ago

Tx Count: 84488, Tx Interval (ms) min/max/avg: 153/249/197 last: 190 ms ago

Registered protocols: PBR

Uptime: 02:18:49

Last packet: Version: 1 - Diagnostic: 0

I Hear You bit: 1 - Demand bit: 0

Poll bit: 0 - Final bit: 0

Multiplier: 5 - Length: 24

My Discr.: 1 - Your Discr.: 2

Min tx interval: 200000 - Min rx interval: 200000

Min Echo interval: 0

## Example of Configuring BFD for VRRP

### Network Requirement

RouterA and RouterB are interconnected through a L2 switch. Both routers run the VRRP protocol and enable the BFD for PBR on the interface to detect the master and backup routers. After a link failure between RouterB and L2 switch occurs, BFD detects the failure, notifies VRRP of the failure, and triggers the priority level decline of the VRRP master router resulting in the switchover between the master and backup routers, which enables the backup router rapidly.

RouterA and RouterB access the Internet through RouterC and RouterD respectively. Configure the static routes to establish the forwarding path between RouterA and RouterC, RouterB and RouterD and enable the BFD to detect the neighbor. At the same time, RouterA and RouterB are configured the BFD for VRRP to detect the forwarding path between the RouterA and RouterC, RouterB and RouterD. The detection failure triggers the decline of priority for VRRP master router and switchover between the master and backup routers, which enables the backup router rapidly.

## Network Topology

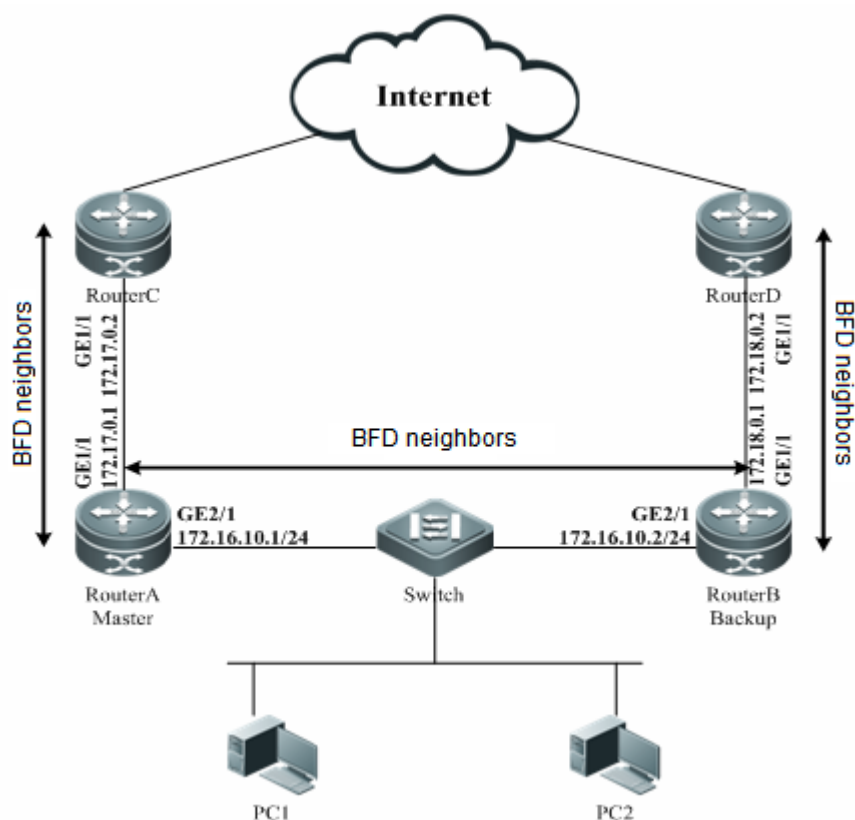


Figure-9 Topology of Configuring BFD for VRRP

## Configuration Steps

1) RouterC Configuration (Omitted)

2) RouterD Configuration (Omitted)

3) RouterA Configuration

# Configure the Routed Port, the IP address, the BFD session parameter for Router A:

Ruijie# configure terminal

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

Ruijie(config)# interface GigabitEthernet2/1

Ruijie(config-if)# no switchport

Ruijie(config-if)# ip address 172.16.10.1 255.255.255.0

Ruijie(config-if)# bfd interval 200 min\_rx 200 multiplier 5

# Configure the Routed Port *gi1/1*:

Ruijie(config-if)# exit

Ruijie(config)# interface GigabitEthernet1/1

Ruijie(config-if)# no switchport

Ruijie(config-if)# ip address 172.17.0.1 255.255.255.0

Ruijie(config-if)# bfd interval 200 min\_rx 200 multiplier 5

# Enable VRRP and configure the BFD for VRRP to detect the neighbor 172.16.10.2 and 172.17.0.2 at the same time:

```

Ruijie(config-if)# interface GigabitEthernet2/1
Ruijie(config-if)# vrrp 1 timers advertise 3
Ruijie(config-if)# vrrp 1 ip 172.16.10.3
Ruijie(config-if)# vrrp 1 priority 120
Ruijie(config-if)# vrrp 1 bfd 172.16.10.2
Ruijie(config-if)# vrrp 1 track bfd GigabitEthernet 1/1 172.17.0.2 30
# Configure the static route and associate the BFD to detect the neighbor 172.17.0.2:
Ruijie(config-if)# exit
Ruijie(config)# ip route static bfd GigabitEthernet 1/1 172.17.0.2
Ruijie(config)# ip route 0.0.0.0 0.0.0.0 GigabitEthernet 1/1 172.17.0.2
Ruijie(config)# end
2) RouterB Configuration
# Configure the Routed Port, the IP address, the BFD session parameter for Router B:
Ruijie# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Ruijie(config)# interface GigabitEthernet2/1
Ruijie(config-if)# no switchport
Ruijie(config-if)# ip address 172.16.10.2 255.255.255.0
Ruijie(config-if)# bfd interval 50 min_rx 50 multiplier 3
# Configure the Routed Port gi1/1:
Ruijie(config-if)# exit
Ruijie(config)# interface GigabitEthernet1/1
Ruijie(config-if)# no switchport
Ruijie(config-if)# ip address 172.18.0.1 255.255.255.0
Ruijie(config-if)# bfd interval 200 min_rx 200 multiplier 5
# Enable VRRP and configure the BFD for VRRP to detect the neighbor 172.16.10.1 and 172.18.0.2 at
the same time:
Ruijie(config-if)# interface GigabitEthernet2/1
Ruijie(config-if)# vrrp 1 timers advertise 3
Ruijie(config-if)# vrrp 1 ip 172.16.10.3
Ruijie(config-if)# vrrp 1 priority 120
Ruijie(config-if)# vrrp 1 bfd 172.16.10.1
Ruijie(config-if)# vrrp 1 track bfd GigabitEthernet 1/1 172.18.0.2 30
# Configure the static route and associate the BFD to detect the neighbor 172.18.0.2:
Ruijie(config-if)# exit
Ruijie(config)# ip route static bfd GigabitEthernet 1/1 172.18.0.2
Ruijie(config)# ip route 0.0.0.0 0.0.0.0 GigabitEthernet 1/1 172.18.0.2
Ruijie(config)# end

```

## Configuration Verification

View the BFD session of RouterA

```
Ruijie# show bfd neighbors details
```

OurAddr	NeighAddr	LD/RD	RH	Holdown(mult)	State	Int
172.16.10.1	172.16.10.2	1/2	1	532 (3 )	Up	Ge2/1

Local Diag: 0, Demand mode: 0, Poll bit: 0

MinTxInt: 200000, MinRxInt: 200000, Multiplier: 5  
 Received MinRxInt: 50000, Received Multiplier: 3  
 Holdown (hits): 600(22), Hello (hits): 200(84453)  
 Rx Count: 49824, Rx Interval (ms) min/max/avg: 208/440/332  
 Tx Count: 84488, Tx Interval (ms) min/max/avg: 152/248/196  
 Registered protocols: VRRP  
 Uptime: 02:18:49  
 Last packet: Version: 1 - Diagnostic: 0  
 I Hear You bit: 1 - Demand bit: 0  
 Poll bit: 0 - Final bit: 0  
 Multiplier: 3 - Length: 24  
 My Discr.: 2 - Your Discr.: 1  
 Min tx interval: 50000 - Min rx interval: 50000  
 Min Echo interval: 0

OurAddr	NeighAddr	LD/RD	RH	Holdown(mult)	State	Int
172.17.0.1	172.17.0.2	2/3	1	532 (3 )	Up	Ge2/1

Local Diag: 0, Demand mode: 0, Poll bit: 0

MinTxInt: 200000, MinRxInt: 200000, Multiplier: 5  
 Received MinRxInt: 50000, Received Multiplier: 3  
 Holdown (hits): 600(22), Hello (hits): 200(84453)  
 Rx Count: 49824, Rx Interval (ms) min/max/avg: 208/440/332 last: 68 ms ago  
 Tx Count: 84488, Tx Interval (ms) min/max/avg: 152/248/196 last: 192 ms ago  
 Registered protocols: VRRP,STATIC ROUTE  
 Uptime: 02:18:49  
 Last packet: Version: 1 - Diagnostic: 0  
 I Hear You bit: 1 - Demand bit: 0  
 Poll bit: 0 - Final bit: 0  
 Multiplier: 3 - Length: 24  
 My Discr.: 2 - Your Discr.: 1  
 Min tx interval: 50000 - Min rx interval: 50000  
 Min Echo interval: 0

View the BFD session of RouterB

Ruijie# show bfd neighbors details

OurAddr	NeighAddr	LD/RD	RH	Holdown(mult)	State	Int
172.16.10.2	172.16.10.1	2/1	1	532 (3 )	Up	Ge2/1

Local Diag: 0, Demand mode: 0, Poll bit: 0

MinTxInt: 50000, MinRxInt: 50000, Multiplier: 3  
 Received MinRxInt: 200000, Received Multiplier: 5  
 Holdown (hits): 600(22), Hello (hits): 200(84453)  
 Rx Count: 49824, Rx Interval (ms) min/max/avg: 208/440/332 last: 68 ms ago  
 Tx Count: 84488, Tx Interval (ms) min/max/avg: 152/248/196 last: 192 ms ago  
 Registered protocols: VRRP  
 Uptime: 02:18:49  
 Last packet: Version: 1 - Diagnostic: 0  
 I Hear You bit: 1 - Demand bit: 0

Poll bit: 0                      - Final bit: 0  
 Multiplier: 3                    - Length: 24  
 My Discr.: 1                    - Your Discr.: 2  
 Min tx interval: 200000       - Min rx interval: 200000  
 Min Echo interval: 0

OurAddr	NeighAddr	LD/RD	RH	Holdown(mult)	State	Int
172.18.0.1	172.18.0.2	1/3	1	532 (3 )	Up	Ge2/1

Local Diag: 0, Demand mode: 0, Poll bit: 0

MinTxInt: 200000, MinRxInt: 200000, Multiplier: 5

Received MinRxInt: 50000, Received Multiplier: 3

Holdown (hits): 600(22), Hello (hits): 200(84453)

Rx Count: 49824, Rx Interval (ms) min/max/avg: 208/440/332 last: 68 ms ago

Tx Count: 84488, Tx Interval (ms) min/max/avg: 152/248/196 last: 192 ms ago

Registered protocols: VRRP,STATIC ROUTE

Uptime: 02:18:49

Last packet: Version: 1                      - Diagnostic: 0

I Hear You bit: 1                    - Demand bit: 0

Poll bit: 0                      - Final bit: 0

Multiplier: 3                    - Length: 24

My Discr.: 2                    - Your Discr.: 1

Min tx interval: 50000       - Min rx interval: 50000

Min Echo interval: 0

## Example of Associating Layer 3 Interface with BFD

Layer 3 interface and BFD association is commonly applied in FRR, and separate use is not recommended. For related information, refer to the description given in *MPLS-SCG.doc*.

## Example of Configuring BFD for MPLS

Please refer to the descriptions given in *MPLS-SCG.doc*.

## Example of Configuring BFD for VRRP+

Please refer to the descriptions given in *VRRP-PLUS-SCG.doc*.

# RNS & Track Configuration

## Introduction to RNS

RNS (Ruijie Network Service) monitors the integrity of end-to-end connection by detecting whether the reply message is sent by the peer device. Based on the detection result of RNS, users can diagnose and locate network failures. At present, Ruijie products support two detection types: ICMP-echo and DNS.

To increase reliability of communication, some application modules need to track link status on an interface or network reachability in time. Adding the track module between the monitoring module that is responsible for interface link status and network reachability and application modules can shield differences between different monitoring modules and simplify processing application modules. One track object can track whether an IP address is reachable or the status of an interface is up. The track function separates the object to be tracked and modules interested in the status of this object, for example, PBR (Policy Based Routing) and VRRP (Virtual Router Redundancy Protocol). They can take different actions when the status of the object changes.

## List of RNS configuration tasks

General steps:

Configure a RNS object to send ICMP echo packets

1. **enable**
2. **configure terminal**
3. **ip rns** *operation-number*
4. **icmp-echo destination-hostname** [*source-ipaddr ip-address*]
5. **frequency seconds**
6. **exit**

Command	Function
Ruijie# <b>configure terminal</b>	Enter global configuration mode
Ruijie(config)# <b>ip rns</b> <i>operation-number</i>	Enter IP RNS configuration mode
Ruijie(config-ip-rns)# <b>icmp-echo destination-hostname</b> [ <b>source-ipaddr</b> <i>ip-address</i> ]	Configure an IP RNS object to send ICMP packets

Configuration example:

```
Ruijie> enable
Ruijie# configure terminal
Ruijie(config)# ip rns 1
Ruijie(config-ip-rns)# icmp-echo 10.1.1.1
```

Display the configurations of RNS object:



```
Ruijie# show ip rns configuration
Ip rns id:1
Type of operation to perform: icmp-echo
Target address/Source address:10.1.1.1/0.0.0.0
Operation timeout (milliseconds):1000
Vrf Name:
Operation frequency (milliseconds):1000
```

Display statistics of RNS object:

```
Ruijie# show ip rns statistics
IP rns index      1
Number of successes:0
Number of failures:174
Round-trip min/avg/max = 0/0/0 ms
```

## Introduction to Track

A track object can track whether an IP address is reachable and whether an interface is UP. The track feature separates a tracked object from the modules which are interested in this object, such as PBR and VRRP. When the state of track object changes, they can take different actions.

## List of track configuration tasks

To configure track, configure as per the tasks described below.

- Track the link state of an interface
- Track the state of a RNS object

### Track the link state of an interface

Execute this task to track the link state of an interface. A layer-2 interface is considered UP as long as the interface is powered up; a layer-3 interface is considered UP as long as the layer-2 interface of this interface-3 interface is UP; a logic interface like loopback interface is considered UP as long as it is not shut down.

General steps:

1. **enable**
2. **configure terminal**
3. **track object-number interface type number line-protocol**
4. **delay {up seconds [down seconds] | [up seconds] down seconds}**
5. **end**
6. **show track object-number**

Detailed steps:

Command	Function
---------	----------

Ruijie> <b>enable</b>	Enter privilege mode
Ruijie# <b>configure terminal</b>	Enter global configuration mode
Ruijie(config)# <b>track</b> <i>object-number</i> <b>interface</b> <i>type number line-protocol</i>	Track the state of an interface and enter track mode
Ruijie(config-track)# <b>delay</b> { <b>up</b> <i>seconds</i> [ <b>down</b> <i>seconds</i> ]   [ <b>up</b> <i>seconds</i> ] <b>down</b> <i>seconds</i> }	(Optional) Specify a delay time after which the state of track object will change when interface state changes. There is no delay by default.
Ruijie(config-track)# <b>show track</b> [ <i>object-number</i> ]	(Optional) Display the information about track object. You can use this command to verify whether the configurations are correct.

Configuration example:

```
Ruijie> enable
Ruijie# configure terminal
Ruijie(config)# track 3 interface FastEthernet 1/0 line-protocol
Ruijie(config-track)# delay up 30
Ruijie(config-track)# show track 3
```

Configure a track object to track the state of an interface. The following example shows relevant information:

```
Ruijie# show track 3
Track 3
interface FastEthernet 1/0
The state is Up
1 change,current state last:11 secs
Delay up 10 secs,down 10 secs
```

## Track the state of a RNS object

We use a track object to track the state of RNS object; If the RNS object receives the reply packets, then the state of track object is UP; otherwise, the state of track object is DOWN.



When track object is used to track a nonexistent RNS object, the state of this track object is UP.

General steps:

First configure an IP RNS object

1. **enable**
2. **configure terminal**
3. **ip rns** *operation-number*
4. **icmp-echo destination-hostname** [*source-ipaddr ip-address*]
5. **frequency** *seconds*

6. **exit**

Then configure a track object:

1. **enable**
2. **configure terminal**
3. **track** *object-number* **rns** *entry-number*
4. **delay up** *seconds* **down** *seconds*
5. **end**
6. **show track object-number**

Configure a route-map and apply the aforementioned track object:

1. **route-map** *map-tag* [**permit** | **deny**] [*sequence-number*]
2. **set ip next-hop verify-availability** [*next-hop-address* *sequence* **track** *object*]

Apply policy-based routing to an interface:

1. **interface** *type number*
2. **ip address** *ip-address* **mask** [*secondary*]
3. **ip policy route-map** *map-tag*
4. **exit**

Detailed steps:

Command	Function
Ruijie(config)# <b>track</b> <i>object-number</i> <b>rns</b> <i>entry-number</i>	Track the state of an IP RNS object and enter track mode.
Ruijie(config-track)# <b>delay</b> { <b>up</b> <i>seconds</i> [ <b>down</b> <i>seconds</i> ]   [ <b>up</b> <i>seconds</i> ] <b>down</b> <i>seconds</i> }	(Optional) Specify a delay time after which the state of track object will change when its state changes. There is no delay by default.
Ruijie(config-track)# <b>exit</b>	Return to global configuration mode.
Ruijie(config)# <b>interface</b> <i>type number</i>	Enter interface configuration mode.
Ruijie(config-if)# <b>ip</b> <b>address</b> <i>ip-address</i> <b>mask</b> [ <i>secondary</i> ]	Configure an IP address for the interface.
Ruijie(config-if)# <b>ip policy route-map</b> <i>map-tag</i>	Apply policy-based routing to this interface.
Ruijie(config-if)# <b>exit</b>	Return to global configuration mode.
Ruijie(config)# <b>route-map</b> <i>map-tag</i> [ <b>permit</b>   <b>deny</b> ] [ <i>sequence-number</i> ]	Configure a route-map.
Ruijie(config-route-map)# <b>set ip</b> <b>next-hop</b> <b>verify-availability</b> [ <i>next-hop-address</i> <i>sequence</i> <b>track</b> <i>object</i> ]	The route map configured is used to track the state of a track object

Configuration example:

```
Ruijie(config)# track 123 rns 1
```

```

Ruijie(config-track)# delay up 30
Ruijie(config-track)# exit
Ruijie(config)# interface ethernet 0
Ruijie(config-if)# ip address 10.1.1.11 255.0.0.0
Ruijie(config-if)# ip policy route-map alpha
Ruijie(config-if)# exit
Ruijie(config)# route-map alpha
Ruijie(config-route-map)# set ip next-hop verify-availability 10.1.1.1 10 track 123

```

Display the state of a track object:

```

Track 2
Ruijie Network Service 1
The state is Down
1 change,current state last:7 secs
Delay up 30 secs,down 0 secs

```

## Application of track feature

We can achieve the following function by tracking the UP/DOWN state of track object:

Associate the next hop of PBR with a track object

### Associate the next hop of PBR with a track object

In policy-based routing, we can associate the next hop of PBR with a track object. When the state of track object becomes DOWN, this next hop will be disabled, namely PBR will not use this next hop as the next hop for packets.

General steps:

First configure an IP RNS object (please refer RNS configurations given above).

Then configure a track object (please refer to track configurations given above).

Configure a route-map and apply the track object configured above:

1. **route-map map-tag [permit | deny] [sequence-number]**
2. **set ip next-hop verify-availability track object**

Apply policy-based routing to an interface:

1. **interface type number**
2. **ip address ip-address mask [secondary]**
3. **ip policy route-map map-tag**
4. **exit**

Detailed steps:

Command	Function
Ruijie(config)# <b>interface type number</b>	Enter interface configuration mode.

Ruijie(config-if)# <b>ip address</b> <i>ip-address mask [secondary]</i>	Configure an IP address for the interface.
Ruijie(config-if)# <b>ip policy route-map</b> <i>map-tag</i>	Apply policy-based routing to this interface.
Ruijie(config-if)# <b>exit</b>	Return to global configuration mode.
Ruijie(config)# <b>route-map</b> <i>map-tag</i> [ <b>permit</b>   <b>deny</b> ]	Configure a route-map.
Ruijie(config-route-map)# <b>set ip next-hop verify-availability track</b> <i>object</i>	The route map configured is used to track the state of a track object.

Configuration example:

```
Ruijie(config)# interface ethernet 0
Ruijie(config-if)# ip address 10.1.1.11 255.0.0.0
Ruijie(config-if)# ip policy route-map alpha
Ruijie(config-if)# exit
Ruijie(config)# route-map alpha
Ruijie(config-route-map)# set ip next-hop verify-availability 10.1.1.1 track 123
```

The policy-based routing to be achieved: When packets are received by fa 0/0 and the IP address of 10.1.1.1 is reachable, the next hop of packets is configured as 10.1.1.1 (IP address of the interface on router 2). If 10.1.1.1 is unreachable, the next hop of packets is configured as 10.2.2.2 (IP address of the interface on router 3). If 10.2.2.2 is also unreachable, PBR fails. Packets will be forwarded as per ordinary route according to the query result of core routing table.

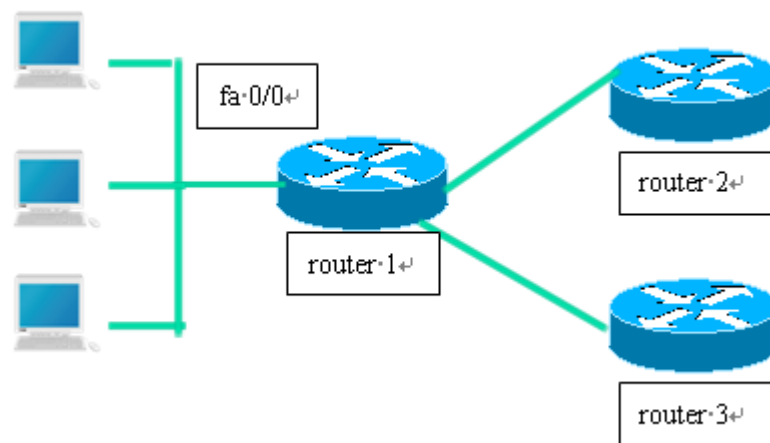


Figure 1

Configurations of Router 1:

# Define two IP RNS objects to track whether the remote IP address is reachable.

```
ip rns 1
icmp-echo 10.1.1.1
ip rns 2
```

```
icmp-echo 10.2.2.2
```

### # Define track object

```
track 123 rns 1
```

```
track 124 rns 2
```

### # Apply PBR to the interface

```
interface FastEthernet 0/0
```

```
ip address 10.4.4.4 255.255.255.0
```

```
ip policy route-map alpha
```

### # 10.1.1.1 is the following interface

```
interface fa 0/1
```

```
ip address 10.1.1.254 255.255.255.0
```

### # 10.2.2.2 is the following interface

```
interface fa 0/2
```

```
ip address 10.2.2.254 255.255.255.0
```

### # Configure a route-map; the availability of next hop depends on the reachability of track object.

```
route-map alpha
```

```
set ip next-hop verify-availability 10.1.1.1 track 123
```

```
set ip next-hop verify-availability 10.2.2.2 track 124
```

# GRTD Configuration

## Introduction to GRTD

### Overview

GRTD (Generic Real-Time Detections) subsystem provides a real-time fault detection mechanism. With this feature, the user can detect whether there is any hardware failure before and during the operation of network devices. GRTD provides four hardware failure diagnosis modes: background monitoring test, system boot-up self-test, scheduled test and CLI command line test. The function of hardware test is mainly aimed to detect whether all hardware components on system management link and data forwarding link works normally, so as to ensure that the system is free from any hardware failure on the management plane and data forwarding plane. GRTD fault detection items can be classified into items affecting normal system operation (disruptive) and items not affecting normal system operation (non-disruptive). For example, line card port loop back test and complete memory test are disruptive test items, while the channel test between management board and line card is a non-disruptive test item.

### Diagnosis Scope

---

GRTD can detect faults related to the following:

- Hardware components
- Interface (Ethernet ports and etc)
- Connector (the connector between backboard and management board or line card)
- Storage unit (memory, flash, chip and etc)

### Working Principle

GRTD is mainly used to detect hardware failure, with working principle as shown below:

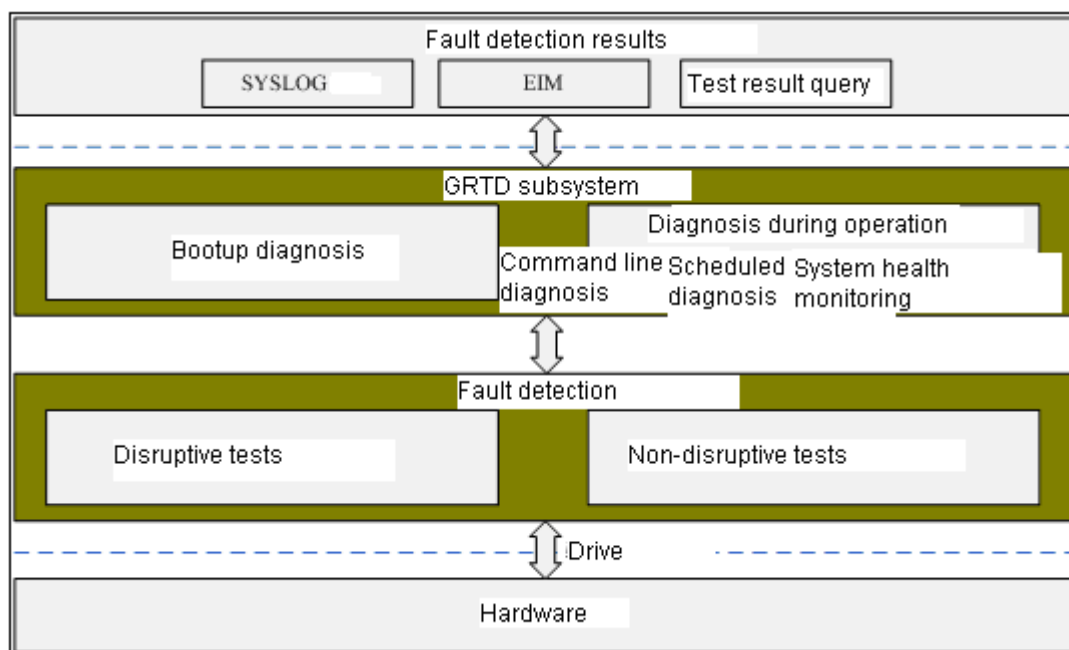


Fig 1 GRTD frame diagram

From GRTD frame diagram, we can learn that GRTD is mainly divided into three parts:

- Fault detection: According to the specific detection terms related to hardware structure, fault detection items can be classified into disruptive test items and non-disruptive test items.
- GRTD subsystem: core module of test function, providing four test modes.
- Fault detection result: detection result handling module, mainly used to handle fault detection results, including SYSLOG, SEM module linkage and result query.

GRTD subsystem provides four test modes:

1. Boot-up diagnosis: running at system initiation stage, used to detect whether there is any fault with the device before use.
2. Command line diagnosis: utilize CLI to detect faults as necessary.
3. Scheduled diagnosis: test detection items at the time scheduled by the user.
4. Monitoring test: running in system background; only non-disruptive test items can be taken as background monitoring test items.

To ensure high reliability of the network, real-time diagnosis can be utilized to reduce the impacts caused by failed devices on network operation. Highly reliable network requires real-time detection of hardware failure during the operation of devices on the network and that proper measures are taken in order to reduce the impacts caused by hardware failure on the network. GRTD is developed to accomplish this goal.

## Protocol Specification

GRTD is mainly related to hardware detection; there is no protocol specification.



## GRTD Features

The following sections describe the features of GRTD:

- GRTD test modes
- GRTD test items
- GRTD test result handling

### GRTD Test Modes

GRTD involves the following four test modes:

#### Boot-up self-test

During the process of management board or line card initialization, all hardware components on the management board or line card will be subject to self-test. The boot-up self-test can be classified into three levels: Complete boot-up level test, Minimal boot-up level test and no test. The difference between complete boot-up level test and minimal boot-up level test lies in the difference in the number of test items participating in boot-up self-test, and the complete boot-up level test includes the minimal boot-up level test. The user can execute the **show diagnostic content** command to query which test items will participate in the complete boot-up level test and which items will participate in the minimal boot-up level test, as shown below:

```
1) OutbandSelfTest-----> M**DX***** not config NA
2) InbandSelfTest-----> C**DX***** not config NA
```

One attribute of OutbandSelfTest is M, indicating that it will participate in the minimal boot-up level test. One attribute of InbandSelfTest is C, indicating that it will participate in the complete boot-up level test. If the current system is configured to complete boot-up level test, then it will execute OutbandSelfTest and InbandSelfTest during system initiation; if the current system is configured to minimal boot-up level test, then it will only execute OutbandSelfTest during system initiation.



#### Caution

In the current version, the boot-up self-test results of master management board will be displayed during the initialization process, while the test results of slave management board or line card can only be displayed by executing query command after normal running of the device.

#### Command line test

In command line test, the CLI is utilized to test a certain test item as required. After the test, the user needs to execute relevant command to view the test results.

#### Monitoring test

Monitor test runs in system background, and all test non-disruptive test items can be taken as monitoring test items. You can configure SYSLOG in case the monitoring test fails. You can activate or deactivate the monitoring test items, configure the monitoring interval, or configure the threshold of consecutive failures in monitoring test.



#### Caution

Disruptive test items cannot be covered in monitoring test. The minimum interval of monitoring test is 1 second.

#### Scheduled test

Scheduled test refers to the boot-up test items scheduled by the user. Three types of test times are supported:

1. on: Test at a particular time
2. daily: Test at a specific time each day
3. weekly: Test at a specific time on a certain day every week



You cannot configure different test modes with the same scheduled time. For example, if a certain test item is scheduled to run at 12:00 on a certain day, then you cannot configure a daily test schedule to be executed at 12:00.

## GRTD Test Items

The test items supported can be acquired by executing **show diagnostic content** command, as shown below:

- Test items supported by the management board

```
*****
*Diagnostic test suite attributes:
M/C*/-Minimal bootup level test / Complete bootup level test / NA
P/V*/-Per port test / Per device test / NA
D/N*/-Disruptive test / Non-disruptive test / NA
  X*/-Not a health monitoring test / NA
  F*/-Fixed monitoring interval test / NA
  E*/-Always enabled monitoring test / NA
A/I*/-Monitoring in active / Monitoring in inactive / NA
Y/O*/-Key test / Non-key test / NA
  B*/-Basic ondemand test / NA
  R*/-Power-down line cards and need reload mainbord / NA
  K*/-Require resetting the line card after the test completed / NA
*****

                                test interval Thre-
ID  Test Name                      Attributes day hh:mm:ss  shold
===  =====
1)  InBandChannelTest----->  **N*F*I****  0   00:00:30  10
2)  OutBandChannelTest----->  **N*F*I****  0   00:00:30  10
3)  OutbandSelfTest----->    **DX*****  not config  N/A
4)  InbandSelfTest----->    **DX*****  not config  N/A
5)  MacSelfTest----->      C*DX*****  not config  N/A
6)  TestCpld----->        C*DX*****  not config  N/A
7)  TestNandFlash----->    **DX*****  not config  N/A
8)  TestNorFlash----->    **DX*****  not config  N/A
9)  TestI2C----->        C*DX*****  not config  N/A
10) TestPCI----->        C*DX*****  not config  N/A
11) TestDdr----->        **DX****B**  not config  N/A
```

## ● Test items supported by the line card

```
*****
*Diagnostic test suite attributes:
M/C*/-Minimal bootup level test / Complete bootup level test / NA
P/V*/-Per port test / Per device test / NA
D/N*/-Disruptive test / Non-disruptive test / NA
  X*/-Not a health monitoring test / NA
  F*/-Fixed monitoring interval test / NA
  E*/-Always enabled monitoring test / NA
A/I*/-Monitoring in active / Monitoring in inactive / NA
Y/O*/-Key test / Non-key test / NA
  B*/-Basic ondemand test / NA
  R*/-Power-down line cards and need reload mainbord / NA
  K*/-Require resetting the line card after the test completed / NA
*****
```

ID	Test Name	Attributes	test interval	Thre-	day hh:mm:ss	shold
1)	PortLoopbackTest----->	MPDX*****	not config			N/A
2)	InbandSelfTest----->	**DX*****	not config			N/A
3)	MacSelfTest----->	C*DX*****	not config			N/A
4)	TestCpld----->	C*DX*****	not config			N/A
5)	TestNandFlash----->	**DX*****	not config			N/A
6)	TestNorFlash----->	**DX*****	not config			N/A
7)	TestI2C----->	C*DX*****	not config			N/A
8)	TestPCI----->	C*DX*****	not config			N/A
9)	TestDdr----->	**DX****B**	not config			N/A

If the MAC chip in the module supports extension storages (such as SSDRAM and TCAM), there will exist the test items of extension storages, such as MPLS card.

```
*****
*Diagnostic test suite attributes:
M/C*/-Minimal bootup level test / Complete bootup level test / NA
P/V*/-Per port test / Per device test / NA
D/N*/-Disruptive test / Non-disruptive test / NA
  X*/-Not a health monitoring test / NA
  F*/-Fixed monitoring interval test / NA
  E*/-Always enabled monitoring test / NA
A/I*/-Monitoring in active / Monitoring in inactive / NA
Y/O*/-Key test / Non-key test / NA
  B*/-Basic ondemand test / NA
  R*/-Power-down line cards and need reload mainbord / NA
  K*/-Require resetting the line card after the test completed / NA
*****
```

		test interval Thre-		
ID	Test Name	Attributes	day hh:mm:ss	shold
===	=====	=====	=====	=====
1)	InbandSelfTest----->	**DX*****	not config	N/A
2)	MacSelfTest----->	C*DX*****	not config	N/A
3)	TestCpld----->	C*DX*****	not config	N/A
4)	TestNandFlash----->	**DX*****	not config	N/A
5)	TestNorFlash----->	**DX*****	not config	N/A
6)	TestI2C----->	C*DX*****	not config	N/A
7)	TestPCI----->	C*DX*****	not config	N/A
8)	MacExtRamTest----->	**DX*****B*K	not config	N/A
9)	TestDdr----->	**DX*****B**	not config	N/A

#### Attributes of test items:

1. M/C: to participate in minimal boot-up level test / complete boot-up level test
2. P/V: per port test / per device test
3. D/N: Disruptive test / Non-disruptive test
4. X :X: Cannot be taken as a monitoring test item
5. F: Monitoring test with fixed test interval
6. E: Always enabled monitoring test
7. A/I: Monitoring test state is active / inactive
8. Y/O: Key test / non-key test
9. B: For the command line test only
10. R: the line card and management board need to be rebooted after the test
11. K: require resetting the line card after the test is completed

#### Detailed descriptions:

##### 1. PortLoopbackTest

Port loopback test refers to the process of executing loopback on the line card port (loopback test via loopback adapter or configuring chip MAC/PHY loopback) and then executing packet switching test on this port. If the test fails, you will need to check whether the corresponding hardware has failed. **Before the test, you need to specify the ID and the loopback mode of ports to be tested. Otherwise, the ID will be assumed as all ports on the line card and the loopback mode will be MAC loopback.**

Configure port ID and loopback mode:

Command	Function
Ruijie>enable	Enter privileged EXEC mode

Ruijie# <b>loopback-test</b> <i>device_num</i> <b>slot</b> <i>slot_id</i> <b>port</b> {all   range <i>potr_range</i>   port_id} <b>loopback</b> {mac   phy   none}	<b>diagnostic</b> <b>[device</b> Configure relevant parameters of port loopback test, including port ID and loopback mode <b>device</b> <i>device_num</i> Only effective for stacked and VSU devices.
Ruijie#	End

We can first use the loopback adapter to execute loopback test, and a successful test can indicate that the port is free from hardware failure. If the test fails, then you can configure the port to PHY loopback mode and execute the test again. If the test is successful, it means that a fault exists between PHY and RJ45. If the test fails, you need to configure the port to MAC loopback mode and execute the test again. If the test is successful, it means that a hardware fault exists between MAC and PHY. If the test fails again, it means that a hardware link fault exists between CPU and MAC.

For example: to execute MAC loopback test on port 1-24 on line card 1.

```
Ruijie# diagnostic port-test slot 1 port range 1-24 loopback mac
```

```
Ruijie#
```

Major application example: During the use of device, if any port fails, you can use this test function to verify whether the port suffers from hardware failure.



#### Caution

The port loopback test only applies to the line cards and BOX devices, and it doesn't apply to the management board. The port loopback test will affect the normal packet forwarding on the port. If you re-configure the port test parameters after the port test instead of querying test results immediately, the port test results will be set to untested. During the port PHY loopback test, the port to be tested must be in no shut down state, or else the test will fail. On the BOX devices, the reflector ports for NLB and the stack ports (the port is configured to stack on) cannot be tested.

## 2. InbandSelfTest

Inband channel self-test refers to the loopback test of inband channel, during which Higi is configured to loopback mode in order to send test frames. It is mainly used to detect whether the inband data channel (on the management board or line card) works normally.

Major application example: During the use of device, if the communication between slots or layer-3 data forwarding seems abnormal, you can use this command to verify whether the relevant inband channel has failed. Since the channels involved in cross-slot communication and layer-3 data forwarding include the inband data channel on the management board, forwarding channel on the backboard and the data channel on the line card. This feature is mainly used to detect whether any inband data channel on the board/card has failed.



#### Caution

Inband channel self-test will result in abnormal packet forwarding on the inband data channel, thus affecting normal services.

### 3. MacSelfTest

MAC chip self-test refers to MAC chip type self-test and the test to verify whether the channel between MAC chip and MAC buffer (such as SDRAM, SSRAM and TCAM) works normal. It will also test whether the MAC buffer works normal.

Major application example: During the use of device, the data packets sometimes cannot be forwarded normally. In such a case, we can use this function to detect whether the PCI bus can normally read and write in the MAC chip, or for MAC chip with external memory, whether MAC chip can normally read and write in the external memory.



**Caution**

The self-test of MAC chip with external memory will not compromise the normal operation of the device. However, if the MAC chip has external memory, the test will compromise the normal forwarding of data packets.

### 4. TestCpld

It is mainly used to detect whether the channel between CPU and CPLD works normally, namely whether the CPU can access CPLD. If the test fails, it means that the channel between CPU and CPLD is abnormal, which may compromise the normal communication between CPU and CPLD and the normal functioning of CPLD, such as abnormal indicator LED.

Major application example: During the use of device, if the indicator LED is found abnormal and the device cannot reboot normally, you can use this function to verify whether there is a fault with CPLD.



**Caution**

n

During CPLD test, the read-write operation will be performed on the CPLD register and the CPLD may not function well.

### 5. TestPCI

It is mainly used to detect the fault on PCI and PCIE bus. Failure of PCI/PCIE bus self-test may result in read error of components connected to PCI/PCIE bus and abnormal outband and inband data channels. Major application example: During the use of device, if the bus cannot detect devices, there is parity check error on the bus or there is Link failure on PCIE, you can use this function to verify whether there is any fault with PCI/PCIE bus.

### 6. TestNandFlash

It is mainly used to detect whether there is any fault with the serial flash. Flash fault detection includes: 1) testing of flash data bus and address bus; 2) sweep test of internal storage space of the flash. Generally, flash test will first proceed with data bus and address bus test. Since internal storage space test will generally take a long time, full space sweep test is not supported currently.

### 7. TestNorFlash

It is mainly used to detect whether there is any fault with the parallel flash.



**Caution**

Electricity failure is not allowed during the parallel flash test as it may lead to the loss of information saved in the parallel flash.

## 8. TestI2C

It is used to test the fault on I2C bus. Failure of I2c test may result in read error of information about the components connected to I2C, such as temperature, optical module and etc.

Major application example: During the use of device, if the temperature information or information about optical module or monitoring module cannot be read, you can use this function to verify whether there is any fault with the I2C bus.



**Caution**

For the I2C test on the BOX device, you need to check whether the extension slot is inserted with the extension modules (excluding the stack module) before using the command line test. If no, the test will fail.

## 9. TestDdr

It is used to detect whether there is any fault with read/write for the memory data cable, address cable and memory inner space.

Major application example: If the device fails to boot up or restarts exceptionally without reason, you can use this function to verify whether there is any fault with the memory hardware.



**Caution**

As device reboot is required by memory test, individual CLI test can only be executed for memory test. Memory test will be omitted if it is set as scheduled test or CLI test with the remaining test items. You can use the **show diagnostic event** command to view related information.

The memory test is performed in BOOT. Before the test, you need to check whether the BOOT version supports memory test. If no, this function will become invalid. In this case, please upgrade the BOOT version to the one that supports memory test. In the condition of dual BOOT, during memory test reboot, the device will not perform memory test if it boots from the BOOT.

```
Diagnostic events <storage for 500 events, 27 events
recorded>
```

```
Event Type (ET): I - Info, W - Warning, E - Error
```

```
Time Stamp      ET Slot Event Message
```

```
-----
```

```
-----
```

```
2010-08-27 09:03:24 I 1/0 Diagnostic Pass
2010-08-27 09:49:02 I 1/0 PortLoopbackTest Pass
2010-08-27 09:49:02 I 1/0 MacSelfTest Pass
2010-08-27 09:49:02 E 1/0 TestCpld Fail
2010-08-27 09:49:02 I 1/0 TestNandFlash Pass
2010-08-27 09:49:04 I 1/0 TestNorFlash Pass
2010-08-27 09:49:04 I 1/0 TestI2C Pass
2010-08-27 09:49:04 I 1/0 TestPCI Pass
2010-08-27 09:49:04 I 1/0 TestDdr Escape
```

## 10. InbandPingTest

Inband data channel ping test will detect whether the backboard forwarding channel between management board and line card works normally. Since the inband channel self-test will test the forwarding channel between management board and line card, **all line cards in the chassis will be tested.**

If the inband channel ping test fails, you can use inband channel self-test to verify whether the inband channel between line card and management board works normally, so as to find out which part of the inband channel fails.

## 11. OutbandPingTest

Outband data channel ping test will detect whether the outband management link between management board and line card is normally connected. Since the outband channel self-test will test the management channel between management board and line card, **all line cards in the chassis will be tested.**

## 12. OutbandSelfTest

Outband channel self-test refers to the loopback test of outband channel, and it only takes place on the management board. Similar to inband channel self-test, outband channel self-test will only detect whether the outband channel within the board works normally. No matter which part of outband channel works abnormally, the line card will be unable to receive the control commands sent from the management board, and the outband channel self-test is thus impossible. Therefore, outband channel self-test only takes places on the side of management board.



### Caution

Outband channel self-test will result in abnormal packet forwarding on the outband data channel, thus affecting control data forwarding between boards.

## GRTD Test Result Handling

GRTD test results will be handled in three ways:

1. If the test fails, the SYSLOG will be generated.

Mainly applicable to the monitoring test. You can configure whether to generate such logs or not.

2. Test result query

Query all test results through the command line.

3. Generate test events. The total number of test events about management board or line card is configurable.

There are three types of test events:

- 1) Info: test message, generally indicating a successful management board or line card test.
- 2) Warning: warning message generated in the event of test timeout or monitoring test error.
- 3) Error: error message generated in case of the error of test items other than the monitoring test.



### Caution

Currently, all tests are conducted against the hardware. Once any fault is detected, it means that a certain hardware component fails. Please contact the technical support engineer of Ruijie for details about device repair.



#### 4. Linkage between test results and SEM.

- 1) severity-major level: The errors detected by the test items except the InBandChannelTest and OutBandChannelTest items are at the severity-major level.
- 2) severity-minor level: The errors detected by the InBandChannelTest and OutBandChannelTest test items are at the severity-minor level.
- 3) severity-normal level: The errors of this level are not involved in current version.

## Configuring GRTD

### Default Configurations

Function	Default setting
GRTD boot-up level test	Minimal: minimal boot-up level test
GRTD scheduled test time	NA
GRTD monitoring test activation	The default setting differs from test to test. Currently the ping test is activated by default.
GRTD monitoring interval	The default setting differs from test to test. Currently the interval of ping test is 30 seconds by default.
SYSLOG of GRTD monitoring test	By default, SYSLOG is generated when the monitoring test fails.
The maximum threshold of consecutive failures in GRTD monitoring test	10 times by default
The number of GRTD diagnosis event logs	500 logs for each line card and management board

### Configuring GRTD Boot-up Level Test

The default GRTD boot-up level test is minimal. You can configure to complete, minimal and bypass. Complete means complete boot-up level test, minimal means minimal boot-up level test, while bypass means that no boot-up self-test will be executed. The configuration steps are shown below:

Command	Function
Ruijie> <b>enable</b>	Enter privileged EXEC mode
Ruijie# <b>configure terminal</b>	Enter global configuration mode
Ruijie(config)# <b>diagnostic bootup level {complete   minimal   bypass}</b>	Configure boot-up level test
Ruijie(config)#	End

To restore to the default GRTD boot-up level test setting, execute the **no diagnostic bootup level** command in the global configuration mode.

Configuration example:

# Configure GRTD boot-up self-test to complete boot-up level test.

```
Ruijie#config terminal
```

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

```
Ruijie(config)#diagnostic bootup level complete
```

```
Ruijie(config)#
```



### Caution

After configuration, you can execute the **show diagnostic bootup level** command to display the configuration result. This configuration will apply to all management boards and line cards, and the current configuration will only take effect after system reboot.

```
Ruijie#show diagnostic bootup level
```

```
Current bootup diagnostic level: complete
```

```
Ruijie#
```

## Configuring GRTD Command Line Test

The command line diagnosis utilizes CLI to carry out certain tests. Since some test items may affect the result of other tests after execution, the command line test shall pay attention to the problem of test sequencing. For example, the channel test must be executed before the memory test.

During command line test, the following testing sequence shall be followed.

1. First execute non-disruptive tests; execute "show diagnostic content" to obtain the attributes of all test items related to the management board or line card.
2. Execute port loopback test, channel test and similar tests. These tests are disruptive test items, but will not influence the test results of the subsequent tests.
3. Execute PCI/PCIE bus test, CPLD test, MAC self-test and etc.
4. Finally, execute complete memory test.

After executing complete memory test, reset the corresponding management board or line card. You must not proceed with the remaining tests without resetting.

Start test:

Command	Function
Ruijie> <b>enable</b>	Enter privileged EXEC mode
Ruijie# <b>diagnostic start</b> [ <b>device</b> <i>device-num</i> ] <b>module</b> { <b>mboard</b> <i>mboard_index</i>   <b>slot</b> <i>slot_id</i> } <b>test</b> { <b>all</b>   <b>range</b> <i>test_range</i>   <i>test_id</i> }	Start test (Optional) <b>device</b> <i>device-num</i> Only effective for stacked and VSU devices.
Ruijie#	End

The command line test must strictly follow the aforementioned testing sequence.

Example of command line test:

# Carry out command line test on the line card in slot 1.

Ruijie# **diagnostic start module slot 1 test range 4,5**

Ruijie#

End test:

Command	Function
Ruijie> <b>enable</b>	Enter privileged EXEC mode
Ruijie# <b>diagnostic stop</b> <b>[device device-num] module</b> <b>{mboard mboard_index   slot</b> <b>slot_id }</b>	End test (Optional) <b>device device-num</b> Only effective for stacked and VSU devices.
Ruijie#	End

Example of ending command line test:

# End command line test on the line card in slot 1.

Ruijie# **diagnostic stop module slot 1**

Ruijie#

Test result query:

Command	Function
Ruijie> <b>enable</b>	Enter privileged EXEC mode
Ruijie# <b>show diagnostic</b> <b>result [device device-num]</b> <b>module {mboard</b> <b>mboard_index   slot slot_id  </b> <b>all} [test {all   range</b> <b>test_range   test_id}]</b>	Query test result (Optional) <b>device device-num</b> Only effective for stacked and VSU devices.
Ruijie#	End

Example of ending command line test:

# Display the test results of all tests on the line card in slot 1.

Ruijie# **show diagnostic result slot 1 test all**

Current bootup diagnostic level: complete

Overall Diagnostic Result for Module 1: PASS

Test result: (P = Pass, F = Fail, U = Untested)

Ruijie#show diagnostic result slot 5 test all

Current bootup diagnostic level: minimal

Overall Diagnostic Result for Module: PASS

Test result: (P = Pass, F = Fail, U = Untested)

1) PortLoopbackTest(loop mode: Mac):

port 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24

P P

2) InbandSelfTest-----> P

3) MacSelfTest-----> P

4) TestCpld-----> P

5) TestNandFlash-----> P

6) TestNorFlash-----> P

```

7) TestI2C-----> U
8) TestPCI-----> U
9) TestDdr-----> U
Ruijie#
Ruijie#

```

## Configuring GRTD Scheduled Test

You can configure a particular time, a specific time each day, and a specific time on a certain day every week for performing the test. The configuration steps are shown below:

Command	Function
Ruijie> <b>enable</b>	Enter privileged EXEC mode
Ruijie# <b>configure terminal</b>	Enter global configuration mode
Ruijie(config)# <b>diagnostic schedule</b> [ <b>device</b> <i>device-num</i> ] <b>module</b> { <b>mboard</b> <i>mboard_index</i>   <b>slot</b> <i>slot_id</i> } <b>test</b> { <b>all</b>   <b>range</b> <i>test_range</i>   <b>test_id</b> { <b>daily</b> <i>hh:mm</i>   <b>on</b> <i>year month day_of_month</i> <i>hh:mm</i>   <b>weekly</b> <i>day_of_week</i> <i>hh:mm</i> }}	Configure the scheduled test time. (Optional) <b>device</b> <i>device-num</i> Only effective for stacked and VSU devices.
Ruijie(config)#	End

To delete the scheduled test time configured, execute the **no diagnostic schedule** command in the global configuration mode.

Configuration example:

# Run all tests on management board M1 at 12:00 each day.

```
Ruijie#config terminal
```

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

```
Ruijie(config)#diagnostic schedule module mboard m1 test all daily 12:00
```

```
Scheduling test(s) [1 2 3 6] may disrupt normal system operation
```

```
Ruijie(config)#
```

After configuration, execute "**show diagnostic schedule**" command to display configuration result.

```
Ruijie#*May 4 18:04:57: %SYS-5-CONFIG_I: Configured from console by console
```

```
Ruijie#show diagnostic schedule module mboard m1
```

```
Diagnostic for Module m1:
```

```
Schedule #1:
```

```
To be run on daily 12:0
```

```
Test ID(s) to be executed : 1 2 3 4 5 6
```

```
Ruijie#
```

Remove test 1 and test 2 from the daily test plan scheduled at 12:00

```
Ruijie#config terminal
```

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

```
Ruijie(config)#no diagnostic schedule module mboard m1 test range 1,2 daily 12:00
Ruijie(config)#
```

## Display results

```
Ruijie#*May 4 18:04:57: %SYS-5-CONFIG_I: Configured from console by console
Ruijie#show diagnostic schedule module mboard m1
Diagnostic for Module m1:
Schedule #1:
    To be run on daily 12:0
    Test ID(s) to be executed : 3 4 5 6
Ruijie#
```



### Caution

Once you have configured a test plan to be run at a particular time, you cannot configure other test plans to be run at the same time. For example:

```
Ruijie#show diagnostic schedule module mboard m1
Diagnostic for Module m1:
Schedule #1:
    To be run on daily 12:00
    Test ID(s) to be executed : 3 4 5 6
Ruijie#
Ruijie#configure terminal
Ruijie(config)# diagnostic schedule module mboard m1 test all on 2010
February 20 12:00
Schedule time (12:00) is conflict
Ruijie(config)#
```

## Activating GRTD Monitoring Test

For a certain monitoring test, you can activate or deactivate its monitoring test status.

Command	Function
Ruijie> <b>enable</b>	Enter privileged EXEC mode
Ruijie# <b>configure terminal</b>	Enter global configuration mode
Ruijie(config)# <b>diagnostic monitor active</b>	Activate monitoring test
Ruijie(config)# <b>diagnostic monitor active</b> [device device-num] <b>module</b> {mboard mboard_index   slot slot_id} <b>test</b> {all   range test_range   test_id}	Activate certain monitoring test items (Optional) <b>device</b> device-num Only effective for stacked and VSU devices.
Ruijie(config)#	End

To deactivate the monitoring test status of certain test items, execute the **no diagnostic monitor active** command in the global configuration mode.

Configuration example:

# Activate all monitoring tests on line card 1.

Ruijie#**config terminal**

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

Ruijie(config)#**diagnostic monitor active module slot 1 test all**

The test[1] can not be used as health monitoring test

The test[2] can not be used as health monitoring test

The test[3] can not be used as health monitoring test

The test[6] can not be used as health monitoring test

Ruijie(config)#



### Caution

To verify whether the test can be taken as a monitoring test item, execute "show diagnostic content" command, as shown below:

```
1) OutbandSelfTest-----> M**D***** not config NA
2) InbandSelfTest-----> C**D***** not config NA
3) InBandChannelTest -----> ***N***** 0 00:00:10 10
```

As long as the test item has the attribute of D, it means that this test is a disruptive one that cannot be taken as a monitoring test item. If the test item has the attribute of N, it means that this test can be taken as a monitoring test item.

## Configuring the Interval of GRTD Monitoring Test

Execute the following commands to configure monitoring interval:

Command	Function
Ruijie> <b>enable</b>	Enter privileged EXEC mode
Ruijie# <b>configure terminal</b>	Enter global configuration mode
Ruijie(config)# <b>diagnostic monitor interval</b>	Enter to configure the interval of monitoring test
Ruijie(config)# <b>diagnostic monitor interval</b> [ <b>device device-num</b> ] <b>module</b> { <b>mboard mboard_index</b>   <b>slot slot_id</b> } <b>test</b> { <b>all</b>   <b>range test_range</b>   <b>test_id</b> } <b>hh:mm:ss day day_count</b>	Configure the interval of monitoring test (Optional) <b>device device-num</b> Only effective for stacked and VSU devices.
Ruijie(config)#	End

For test items with default monitoring interval, if you need to restore to the default monitoring interval, execute the **no diagnostic monitor interval** command in the global configuration mode.

Configuration example:

# Configure the monitoring interval of all test items on line card 1 to 10 seconds.

Ruijie#**config terminal**

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

Ruijie(config)#**diagnostic monitor interval module slot 1 test all 00:00:10 day 0**

The test[1] can not be used as health monitoring test

The test[2] can not be used as health monitoring test

The test[3] can not be used as health monitoring test

The test[6] can not be used as health monitoring test

Ruijie(config)#



**Caution**

The minimal unit of monitoring interval is second. However, we can configure the monitoring interval to 0. When the monitoring interval of monitoring test item is 0, this monitoring test will not be executed.

## Configuring the Maximum Threshold of Consecutive Failures in GRTD Monitoring Test

The maximum threshold of consecutive failures in monitoring test means that the monitoring test will not be performed after the number of monitoring test failures reaches this threshold.

Command	Function
Ruijie> <b>enable</b>	Enter privileged EXEC mode
Ruijie# <b>configure terminal</b>	Enter global configuration mode
Ruijie(config)# <b>diagnostic monitor threshold</b>	Enter to configure the maximum threshold of consecutive failures in monitoring test
Ruijie(config)# <b>diagnostic monitor threshold</b> [ <b>device device-num</b> ] <b>module</b> { <b>mboard mboard_index</b>   <b>slot slot_id</b> } <b>test</b> { <b>all</b>   <b>range test_range</b>   <b>test_id</b> } <b>failure-count threshold_value</b>	Configure the maximum threshold of consecutive failures in monitoring test (Optional) <b>device device-num</b> Only effective for stacked and VSU devices.
Ruijie(config)#	End

For test items with default maximum threshold of consecutive failures in monitoring test, if you need to restore to the default value, execute the **no diagnostic monitor threshold** command in the global configuration mode.

Configuration example:

# Configure the maximum threshold of consecutive failures in all monitoring tests on line card 1 to 6 times.

Ruijie#**config terminal**

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

Ruijie(config)#**diagnostic monitor threshold module slot 1 test all failure-count 6**

The test[1] can not be used as health monitoring test

The test[2] can not be used as health monitoring test

The test[3] can not be used as health monitoring test

The test[6] can not be used as health monitoring test

Ruijie(config)#



**Caution**

The maximum threshold of consecutive failures in monitoring test ranges between 1 and 99.

## Configuring the Syslog of GRTD Monitoring Test

Specifying that whether SYSLOG will be generated when the monitoring test fails.

Command	Function
Ruijie> <b>enable</b>	Enter privileged EXEC mode
Ruijie# <b>configure terminal</b>	Enter global configuration mode
Ruijie(config)# <b>diagnostic monitor syslog</b>	Specifying the SYSLOG generated when the monitoring test fails.
Ruijie(config)#	End

To disable SYSLOG function, execute the **no diagnostic monitor syslog** command in the global configuration mode.

## Configuring the number of GRTD diagnosis event logs

Configure the number of event logs during management board or line card diagnosis.

Command	Function
Ruijie> <b>enable</b>	Enter privileged EXEC mode
Ruijie# <b>configure terminal</b>	Enter global configuration mode
Ruijie(config)# <b>diagnostic event-log size size_value</b>	Configure the number of diagnostic logs: 1 to 1000.
Ruijie(config)#	End

To restore to the default number of diagnosis event logs, execute the **no diagnostic event-log size** command in the global configuration mode.

## Boot-up Level Test Configuration Example

### Networking Requirements

NA

### Network Topology

NA

### Configuration Tips

This configuration doesn't apply to any specific line card or management board. After configuration, the boot-up level test of all management boards and line cards will adopt the value configured.

```
Ruijie# configure terminal
```

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

```
Ruijie(config)# diagnostic bootup level complete
```

```
Ruijie(config)#
```



## Verification

```
Ruijie# show diagnostic bootup level
Current bootup diagnostic level: complete
Ruijie#
```

## Example of Monitoring Test Configuration

### Networking Requirements

NA

### Network Topology

NA

### Configuration Tips

To start a certain monitoring test, you need to configure the monitoring interval and the maximum threshold of consecutive failures in monitoring test before activating this monitoring test item. Only non-disruptive tests can be taken as the monitoring test items.

- 1) Display all test items related to line card 1, so as to determine which tests are non-disruptive test items.

```
Ruijie# show diagnostic content slot M1
*****
*Diagnostic test suite attributes:
M/C*/-Minimal bootup level test / Complete bootup level test / NA
P/V*/-Per port test / Per device test / NA
D/N*/-Disruptive test / Non-disruptive test / NA
X*/-Not a health monitoring test / NA
F*/-Fixed monitoring interval test / NA
E*/-Always enabled monitoring test / NA
A/I*/-Monitoring in active / Monitoring in inactive / NA
Y/O*/-Key test / Non-key test / NA
B*/-Basic ondemand test / NA
R*/-Power-down line cards and need reload mainbord / NA
K*/-Require resetting the line card after the test completed / NA
*****

                                test interval  Thre-
ID   Test Name                  Attributes day hh:mm:ss  shold
===  =====
1) InBandChannelTest----->  **N*F*|****  0   00:00:30   10
2) OutBandChannelTest----->  **N*F*|****  0   00:00:30   10
3) OutbandSelfTest----->    **DX*****  not config   N/A
4) InbandSelfTest----->     **DX*****  not config   N/A
5) MacSelfTest----->        C*DX*****  not config   N/A
```

```

6) TestCpld-----> C*DX***** not config N/A
7) TestNandFlash-----> **DX***** not config N/A
8) TestNorFlash-----> **DX***** not config N/A
9) TestI2C-----> C*DX***** not config N/A
10) TestPCI-----> C*DX***** not config N/A
11) TestDdr-----> **DX****B** not config N/A

```

- 2) Test 1 and test 2 are non-disruptive test items. Configure the monitoring interval and the maximum threshold of consecutive failures for test 1 and test 2 (To facilitate operation, you can configure the monitoring interval and maximum threshold of consecutive failures for all test items. In the event of disruptive tests, the system will prompt that these tests cannot be taken as monitoring test items and thus will not proceed with the corresponding configurations.)

```
Ruijie(config)# diagnostic monitor interval slot M1 test range 1,2 00:00:20 day 0
```

The test[1] is used as fixed interval test

The test[2] is used as fixed interval test

```
Ruijie(config)#
```

```
Ruijie(config)# diagnostic monitor threshold slot M1 test range 1,2 failure-count 6
```

```
Ruijie(config)#
```

```
Ruijie(config)# diagnostic monitor active slot M1 test range 1,2
```

```
Ruijie(config)#
```

- 3) Configure the SYSLOG generated when the monitoring test fails.

```
Ruijie(config)# diagnostic monitor syslog
```

```
Ruijie(config)#
```

## Verification

```
Ruijie# show diagnostic content slot M1
```

```
*****
```

\*Diagnostic test suite attributes:

M/C\*/-Minimal bootup level test / Complete bootup level test / NA

P/V\*/-Per port test / Per device test / NA

D/N\*/-Disruptive test / Non-disruptive test / NA

X\*/-Not a health monitoring test / NA

F\*/-Fixed monitoring interval test / NA

E\*/-Always enabled monitoring test / NA

A/I\*/-Monitoring in active / Monitoring in inactive / NA

Y/O\*/-Key test / Non-key test / NA

B\*/-Basic ondemand test / NA

R\*/-Power-down line cards and need reload mainbord / NA

K\*/-Require resetting the line card after the test completed / NA

```
*****
```

ID	Test Name	Attributes	test interval day hh:mm:ss	Thre- shold
----	-----------	------------	-------------------------------	----------------

```

=====
1) InBandChannelTest-----> **N*F*I**** 0 00:00:30 6
2) OutBandChannelTest-----> **N*F*I**** 0 00:00:30 6
3) OutbandSelfTest-----> **DX***** not config N/A
4) InbandSelfTest-----> **DX***** not config N/A
5) MacSelfTest-----> C*DX***** not config N/A
6) TestCpld-----> C*DX***** not config N/A
7) TestNandFlash-----> **DX***** not config N/A
8) TestNorFlash-----> **DX***** not config N/A
9) TestI2C-----> C*DX***** not config N/A
10) TestPCI-----> C*DX***** not config N/A
11) TestDdr-----> **DX****B** not config N/A
Ruijie#

```

## Example of Command Line Test

### Networking Requirements

NA

### Network Topology

NA

### Test Tips

Command line tests shall be strictly performed as per the following sequence:

1. Before the test, deactivate all background monitoring tests and disable all scheduled tests.
2. First execute non-disruptive tests; execute **show diagnostic content** command to obtain the attributes of all test items related to the management board or line card.
3. Execute port loopback test, channel test and similar tests. These tests are disruptive test items, but will not influence the test results other subsequent tests.
4. Execute PCI/PCIE bus test, CPLD test, MAC self-test and etc.
5. Finally, execute complete storage test.

S57#show diagnostic content

\*\*\*\*\*

\*Diagnostic test suite attributes:

M/C\*/-Minimal bootup level test / Complete bootup level test / NA

P/V\*/-Per port test / Per device test / NA

D/N\*/-Disruptive test / Non-disruptive test / NA

X\*/-Not a health monitoring test / NA

F\*/-Fixed monitoring interval test / NA

E\*/-Always enabled monitoring test / NA

A/I\*/-Monitoring in active / Monitoring in inactive / NA

Y/O\*/-Key test / Non-key test / NA

B\*/-Basic ondemand test / NA

R\*/-Power-down line cards and need reload mainbord / NA

K\*/-Require resetting the line card after the test completed / NA

\*\*\*\*\*

ID	Test Name	Attributes	test interval		Thre-
			day	hh:mm:ss	shold
====	=====	=====	=====	=====	=====
1)	PortLoopbackTest----->	MPDX***** not config		N/A	
2)	MacSelfTest----->	C*DX***** not config		N/A	
3)	TestNandFlash----->	**DX***** not config		N/A	
4)	TestNorFlash----->	**DX***** not config		N/A	
5)	TestI2C----->	C*DX***** not config		N/A	
6)	TestPCI----->	C*DX***** not config		N/A	
7)	TestDdr----->	**DX****B** not config		N/A	

## First execute non-disruptive tests

S57#**diagnostic start test all**

Running test[7] may reload system

Running test(s) [1 2 3 4 5 6] may disrupt normal system operation

Do you want to continue? [no]:y

S57#\*Oct 8 12:53:34: %GRTD-6-TEST\_RUNNING: Running PortLoopbackTest{ID=1}...

\*Oct 8 12:53:35: %GRTD-6-TEST\_OK: PortLoopbackTest{ID=1} completed successfully.

\*Oct 8 12:53:35: %GRTD-6-TEST\_RUNNING: Running MacSelfTest{ID=2}...

\*Oct 8 12:53:35: %GRTD-6-TEST\_OK: MacSelfTest{ID=2} completed successfully.

\*Oct 8 12:53:35: %GRTD-6-TEST\_RUNNING: Running TestNandFlash{ID=3}...

\*Oct 8 12:53:35: %GRTD-6-TEST\_OK: TestNandFlash{ID=3} completed successfully.

\*Oct 8 12:53:35: %GRTD-6-TEST\_RUNNING: Running TestNorFlash{ID=4}...

\*Oct 8 12:53:38: %GRTD-6-TEST\_OK: TestNorFlash{ID=4} completed successfully.

\*Oct 8 12:53:38: %GRTD-6-TEST\_RUNNING: Running TestI2C{ID=5}...

\*Oct 8 12:53:38: %GRTD-3-TEST\_ERR: TestI2C{ID=5} completed error.

\*Oct 8 12:53:38: %GRTD-6-TEST\_RUNNING: Running TestPCI{ID=6}...

\*Oct 8 12:53:38: %GRTD-6-TEST\_OK: TestPCI{ID=6} completed successfully.

\*Oct 8 12:53:38: %GRTD-5-TEST\_ESCAPE: Ddr test should be done alone.

## Verification

S57#**show diagnostic result test all**

Current bootup diagnostic level: complete

Overall Diagnostic Result for Module: FAIL

Test result: (P = Pass, F = Fail, U = Untested)

1) PortLoopbackTest(loop mode: Mac):

slot 0 port 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24

```

P P P P P P P P P P P P P P P P P P P P P P P
slot 0 port 25 26 27 28 29 30 31 32 33 34 35 36 37 38 39 40 41 42 43 44 45 46 47 48
P P P P P P P P P P P P P P P P P P P P P P P
```

- 2) MacSelfTest-----> P
- 3) TestNandFlash-----> P
- 4) TestNorFlash-----> P
- 5) TestI2C-----> F
- 6) TestPCI-----> P
- 7) TestDdr-----> U

Note: For time-consuming tests, execute the **show diagnostic status** command to display the current system diagnosis status, as shown below:

```
ruijie#show diagnostic status
(BU)-Bootup Diagnostics, (HM)-Health Monitoring Diagnostics,
(OD)-OnDemand Diagnostics, (SCH)-Scheduled Diagnostics
=====
Slot  Description                               Current Running Test  Run by
-----
2      M8600-24GT/12SFP                          N/A                  N/A
3      M8600-24GT/12SFP                          N/A                  N/A
M1     M8610-CM II                               TestNandFlash        (HM)
=====
ruijie#
```

  
**Caution**

All the above messages show that the management board M1 is carrying out serial flash test, namely the serial flash test of M1 is not finished yet.

## Example of Scheduled Test Time Configuration

### Networking Requirements

NA

### Network Topology

NA

### Configuration Tips

Once you have configured a test plan to be run at a particular time, you cannot configure other test plans to be run at the same time. Therefore, make sure there is no conflict in the time of test plans. If the test is scheduled to run at a particular time, make sure the year, month and date are valid.

- 1) Run all tests on management board M1 at 12:00 each day.

```
Ruijie(config)#diagnostic schedule module mboard m1 test all daily 12:00
```

Scheduling test(s) [ 1 2 3 6 ] may disrupt normal system operation

Ruijie(config)#

## 2) Run all tests on management board M1 at 3:00 Wednesday every week.

Ruijie(config)#diagnostic schedule module mboard m1 test all weekly Wednesday 3:00

Scheduling test(s) [ 1 2 3 6 ] may disrupt normal system operation

Ruijie(config)#

## 3) Run all tests on management board M1 at 00:00 on August 1, 2010.

Ruijie(config)#diagnostic schedule module mboard m1 test all on 2010 August 1 00:00

Scheduling test(s) [ 1 2 3 6 ] may disrupt normal system operation

Ruijie(config)#

## Verification

Ruijie# **show diagnostic schedule module mboard m1**

Diagnostic for m1:

Schedule #1:

To be run on daily 12:00

Test ID(s) to be executed : 1 2 3 4 5 6

Schedule #2:

To be run on August 1 2010 00:00

Test ID(s) to be executed : 1 2 3 4 5 6

Schedule #3:

To be run on Wednesday 03:00

Test ID(s) to be executed : 1 2 3 4 5 6

Ruijie#

# SEM Configuration

## Introduction to SEM

### Overview

SEM (Smart Embedded Manager) is a network management tool embedded in the device. It can be deployed independently or configured through user commands, and is independent of external network management, making it very easy to deploy.

The conventional external network management is accomplished by accessing the device through the network. Once the network connection fails, the external network management will become meaningless. Since SEM is embedded in the device, it can directly manage the device under any circumstances and is capable of processing or capturing the key information in case of any network and device failure.

SEM can detect the events configured by the user in a real-time manner, and will take the corresponding actions once these events occur. The entire process is highly customizable. By providing user with fault detection/handling and automated management, SEM can well enhance the serviceability of device and network.

There are abundant types of SEM events. They can be critical events such as key alert syslog, key trap and time point, or user inputs & operations such as CLI commands inputted and user's SNMP operations. They can also be the thresholds related to interface statistics count, snmp object value, system resources statistics and etc. SEM also supports multiple actions, all CLI commands, log sending, device reload and etc.

### Basic concepts

#### Event

The event concerned and configured by the user, and is affiliated with the policy. There can be one or multiple events, and each event will be detected by a specific detector. When event conditions are met, the event detector will trigger the event. For example, if the user needs to detect commands containing "shutdown" in the privileged EXEC mode, the user will need to execute "**event tag example cli pattern shutdown mode exec**" to configure an event for the command line event detector.

#### Action

The action to be taken by the user upon occurrence of the event. Action is configured by the user and is affiliated with the policy. There can be one or multiple actions, and each action corresponds with a specific action configuration. Upon the occurrence of policy event, the policy will execute the corresponding action. For example, if the user needs to reload the device upon the occurrence of a specific event, he will need to execute "**action example reload**" command.

#### Policy

Policy is used to sort the relationship between events and between event and action. The policy will be triggered when the policy event meets the preconfigured rule and policy actions will be taken in turn.

### **Event detector**

It is embedded in a specific service and monitor such service according to user configurations. It will also trigger the event when the service meets user configurations and forward the event message to the intelligence management server.

### **Intelligence management server**

It receives the event notice sent by event detector and determines whether or not to trigger the policy according to the actual circumstances. Once the policy is triggered, the intelligence management server will execute such policy.

### **Policy manager**

It manages SEM policy information and execute the actions defined in the policy after the policy has been triggered by the intelligence management server.

### **SEM environment variable**

The variable used by policy action during the process of SEM operation. There are three types of SEM environment variables:

- Global variable
- System local variable
- User local variable

When using variable in the policy, the word and symbol between "\$" and the subsequent first character which is not a letter, number or underline will be substituted as the name of variable. The global variable can be used in all policies, while system local variable and user local variable are both local variables which can only be used in a specific policy. System local variable is read-only and cannot be changed. User local variable is defined by the action in policy during its execution. Therefore, system local variable generally starts with "\_" to avoid conflicting with user local variable.

### **SEM application-specific event**

SEM only supports internal use of application-specific event within SEM system, so as to help the running policy to trigger other policies. To distinguish between different application-specific events, sub-system and type are used to identify such events. SEM application-specific events are detected by application-specific event detector according to the sub-system and type, and will be published by the application-specific event action during policy execution. When a policy action publishes an application-specific event of certain sub-system and type, the event with corresponding sub-system and type being detected will be triggered. For details, please refer to "SEM detection of application-specific event" in "Typical SEM configuration example".

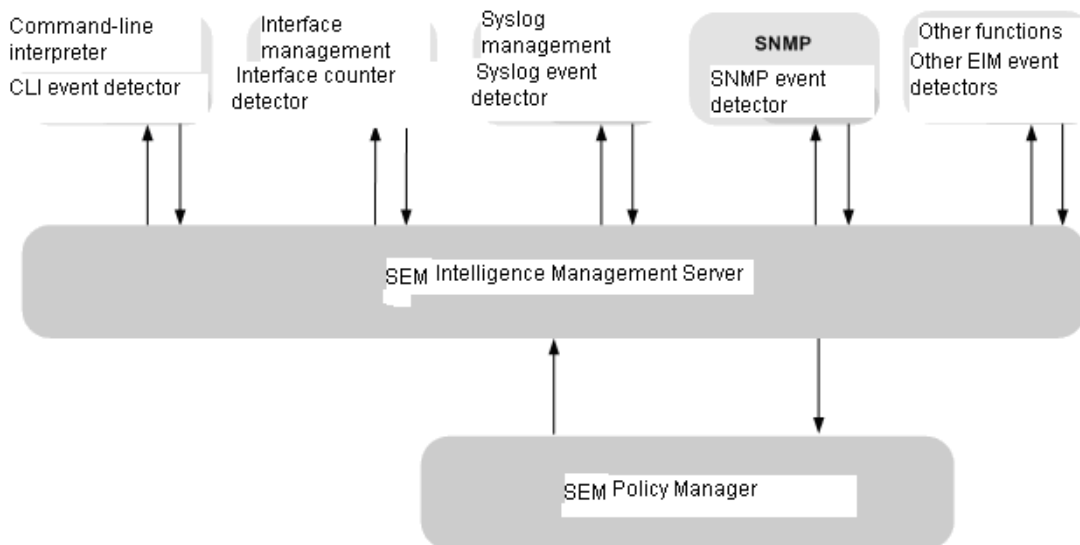
### **SEM named counter**

SEM supports a named counter used inside the SEM system. The SEM counter event detector will detect the variance in SEM named counter, and the value of SEM named counter will be controlled by SEM counter action during policy execution. SEM named counter can be used by the policy to



trigger such actions as summation, numerical value statistics and etc. For details, please refer to "SEM detection of counter" in "Typical SEM configuration example".

## Working principle



**Fig 1 SEM structural diagram**

SEM provides different kinds of event detectors, which are embedded in different services to monitor service operation in a real-time manner. These detectors will compare the conditions generated through user configuration with the service operation events. Once matched, the event detector will notify the intelligence management server of event occurrence.

The intelligence management server will determine whether the event can trigger the policy according to event configurations in the policy. Once the event meets the policy trigger conditions, the intelligence management server will execute the policies in policy manager.

The policies in policy manager will execute the preconfigured actions in turn according to user configurations.

## Protocol specification

NA

## SEM features

The following sections describe the features of SEM:

- Event detectors supported by SEM

- Policy actions supported by SEM

- Environment variables supported by SEM

- SEM intelligence management server management

## Event detectors supported by SEM

SEM supports multiple kinds of event detectors, which have been embedded in respective services. Events are detected during service operation to determine whether they have occurred or not. Currently, the types of detectors supported include:

### CLI event detector

CLI event detector will detect user's command line inputs. The user command lines to be detected must have passed command line format check. The extended form of user inputs will be subject to regulation match. Once matched, the CLI event will be triggered. Two waiting modes are supported when the CLI event is triggered.

- Synchronization mode: Once CLI event is triggered, CLI synchronously waits for the completion of policy execution and then determines whether or not to execute the command inputted by the user according to the result of policy execution.
- Asynchronization mode: Once CLI event is triggered, CLI will not wait for the completion of policy execution. The configuration to ignore command execution is supported under this mode. When so configured, the CLI will ignore this command after the CLI event has been triggered.

### Counter event detector

The counter event detector will detect the named counter within SEM. When the named counter exceeds the specified threshold, the counter event will be triggered, after which the counter event detection will be disabled temporarily until the counter restores to the threshold. The value of named counter will be changed by the counter action being executed. Therefore, other policies may accumulate the value of the counter and when the value reaches the threshold, the counter event will be triggered and the policy will be executed. During policy execution, the counter will be reset, allowing cyclic operation.

### Application-specific event detector

The application-specific event detector will detect the application-specific event within SEM. The internal events of SEM are published by the application-specific event action being executed. When the application-specific event published by SEM has the same sub-system and type with the current application-specific event, the application-specific event will be triggered.

### Interface counter event detector

Interface counter event detector will detect the interface statistical counter of the device. Through periodic acquisition and statistics, the detector will determine whether the interface counter has exceeded the threshold, and the counter event will be triggered when the threshold is exceeded, after which the counter event detection will be disabled temporarily until the interface counter reaches the recovery threshold or the out-of-service time has exceeded its recovery cycle.

### None event detector

None event detector will not carry out actual detection. Instead, it is triggered by executing "smart manager run" command. The parameter of this command is the name of policy containing none event. When this command is successfully executed, the corresponding none event of the policy will be triggered. Two waiting modes are supported when none event is triggered.

- Synchronization mode: Once none event is triggered, CLI synchronously waits for the completion of policy execution before release.
- Asynchronization mode: The null event will be released directly without waiting after being triggered.

### **OIR event detector**

In a modularized device, the OIR event detector will detect the online insertion and removal of modules, which will trigger the OIR event. Two types of events are supported by the OIR event detector.

- Plug-in
- Plug-out

### **SNMP event detector**

SNMP event detector can be classified into the following three types:

- SNMP MIB detector: collect and take statistics of SNMP MIB object values. When any SNMP MIB object value exceeds the threshold configured, SNMP MIB event will be triggered, after which this SNMP MIB event detector will be temporarily disabled until the SNMP MIB object value reaches the recovery threshold or the out-of-service time has exceeded its recovery cycle.
- SNMP Trap detector: By detecting SNMP traps, it will trigger SNMP event when any SNMP Trap complies with event configurations.
- SNMP Object detector: By detecting SNMP operations, it will trigger SNMP event when any SNMP operation complies with event configurations. SNMP Object detector supports synchronization mode and asynchronization mode, and is capable of giving customized SNMP replies with the help of SNMP Object action.

### **Syslog event detector**

Syslog event detector will detect device logs, which will be subject to regulation match. Once matched, the Syslog event will be triggered.

### **Timer event detector**

The timer event detector detects time related events, which can be classified into:

- Absolute-time-of-day timer event: An absolute-time-of-day timer is set to a future time. When this time comes, the timer event will be triggered.
- Countdown timer event: The timer is set to the seconds counting from policy initiation, and the timer event is triggered when the timer counts down to zero.
- Watchdog timer event: The timer is set to the seconds elapsed from policy initiation. Each time when the timer counts down to zero, the timer will reset and trigger a timer event.
- CRON timer event: CRON is derived from the Greek word of chronos, which means "time". It is widely applied in Unix-based operating systems to configure commands to be executed periodically. SEM supports CRON-based time detection. When the time point described in the CRON string comes, the timer event is triggered.

### **Watchdog system event detector**

The watchdog system event detector will detect system resources of the device. When resource usage by the system or task crosses the preconfigured threshold, the watchdog system event will be triggered. Currently, the following system resource detection items are supported:

- CPU usage by the device.
- CPU usage by the task.
- Memory usage by the device.
- Memory usage by the device.
- Memory usage by the task.

### CPP event detector

CPP event detector will detect the statistics of CPP (CPU Protect) function. When CPP statistics crosses the preconfigured threshold, CPP event will be triggered. CPP event detector supports the detection of different kinds of packets: ARP, DHCP, IGMP, PIM, OSPF and etc. Meanwhile, it can also detect packet pps, total packet count and dropped packet count.

### GRTD event detector

GRTD event detector will detect the diagnostic results of Generic Real-Time Diagnostics, so as to detect any fault on hardware components and the communication channels between them. When the fault detected by GRTD matches with the preconfigured event, GRTD event will be triggered.

## Policy actions supported by SEM

SEM supports multiple types of actions, which will be executed after the policy has been triggered by event. They can help collect information and rectify device/network related problems. Currently, SEM supports the following types of actions:

1. Execute a CLI command: execute the command configured by the user.
2. Send Syslog: send a message to Syslog.
3. Operate the named counter: operate the named counter in SEM.
4. Switch to a standby engine: switching between main device and standby device.
5. Reload device: reload the device.
6. Trigger an application-specific event: publish an application-specific event in SEM.
7. Respond to SNMP operation: respond to the operations detected by SNMP Object.
8. Suspend policy execution: suspend policy execution for a while.

## Environment variables supported by SEM

SEM allows environment variables to be used in policies. SEM supports the following environment variables:

1. **Global variable:** When defined by executing "smart manager environment", it can be used in all policies. Only the value of global variable can be read in policy.
2. **Local variable:** The variable generated during policy execution, and can be classified into system local variable and user local variable. The system local variable is created by the

detector to describe the event occurred. It is read only and unchangeable. The user local variable is created by policy action, and can be modified during operation.

In policies, the priority level of local variable is higher than that of global variable. Reading nonexistent local variable and global variable or modifying read-only local variable will result in errors. Setting nonexistent local variable will automatically generate user local variable.

## SEM intelligence management server management

SEM intelligence management server provides user with a management interface through which the user can view SEM operational information and carry out management. The user can view various information of SEM, mainly including:

- Display the types of detectors supported.
- Display the version of intelligence management server and respective event detectors.
- Display the policies configured and submitted by the user.
- Display the policies being executed.
- Display the policies which are not executed.
- Display historic events.
- Display the counter defined currently.
- Display the SEM global variable defined currently.

The user can manage the policies being executed during the operation of SEM intelligence management server:

- Suspend and resume the scheduler of SEM policy.
- Hold and release a specific policy or policies in the specified class.
- Adjust the scheduling priority of a specific class.
- Force to end a specific policy, a specific class or all policies.

## Configure SEM

SEM configuration will be introduced through the following:

Prerequisites

Necessary information

How to configure policy

### Prerequisites

Certain prerequisites are required in order to use SEM. Most prerequisites will be needed to execute policy actions:

1. Syslog must be enabled by executing "logging" command before configuring Syslog actions.

2. Before switching to the standby engine, a normal standby engine must have been configured on the device.

## Necessary information

The configuration of SEM policies may involve the configuration of different kinds of detectors, actions and policies, as well as the environment variables to be used. Please refer to "SEM Command Reference" for detailed configuration steps.

## How to configure policy

The configuration of SEM policy can be divided into the following steps.

- Create policy
- Configure event
- Configure action
- Configure description
- Configure trigger parameters
- Display current policy configurations
- Submit configurations
- Display policy registered
- Roll back configurations
- Configure multiple events
- Configure and use variables
- Suspend/resume scheduler
- Hold/release policy execution
- Force to end policy execution
- Display SEM history events
- Display SEM detector
- Display SEM version

## Create policy

Command	Function
Ruijie> <b>enable</b>	Enter privileged EXEC mode
Ruijie# <b>configure terminal</b>	Enter global configuration mode
Ruijie(config)# <b>smart manager applet</b> <i>applet-name</i> [ <b>class</b> <i>class-options</i> ]	Create policy and enter SEM configuration mode. <i>applet-name</i> is the specified policy name. <b>class</b> parameter specifies the policy class.

To delete the policy, execute "**no smart manager applet** *applet-name*" command in the global configuration mode.

Configuration example:

# Configure a policy named "policy\_A" on the device, and then enter SEM configuration mode.

Ruijie# **configure terminal**

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

Ruijie(config)# **smart manager applet** policy\_a

Ruijie(SEM-applet)#



A newly created policy or a policy being modified will not take effect immediately. It will only come into effect after configuring event and action and executing "commit" command.

Policy configurations which haven't been submitted can be rolled back by executing "rollback" command.

A complete policy includes event and action. If no event is configured for the policy, then the submission of policy will result in an error. If no action is configured for the policy, the submission of policy may be successful but there will be a prompt. Once the policy is triggered, it will do nothing and end directly.

## Configure event

Command	Function
Ruijie> <b>enable</b>	Enter privileged EXEC mode
Ruijie# <b>configure terminal</b>	Enter global configuration mode
Ruijie(config)# <b>smart manager applet</b> <i>applet-name</i> [ <b>class</b> <i>class-options</i> ]	Enter SEM configuration mode. <i>applet-name</i> is the specified policy name. <b>class</b> parameter specifies the policy class.
Ruijie(SEM-applet)# <b>event tag</b> <i>event-name</i> [ <b>correlate</b> { <b>andnot</b>   <b>and</b>   <b>or</b> }] <b>syslog pattern</b> <i>regular-expression</i> [ <b>priority</b> <i>priority-level</i> ] [ <b>occurs</b> <i>num-occurrences</i> ] [ <b>period</b> <i>period-value</i> ] [ <b>skip</b> { <b>yes</b>   <b>no</b> }]	The detection of every event corresponds to an event command. Here we take Syslog event as an example and introduce the steps to configure an event. Please refer to "SEM Command Reference" for information about other commands.

To delete the policy, execute "**no event tag** *event-name*" command in the SEM configuration mode.

Configuration example:

# Configure a syslog event named "event\_a" for a policy named "policy\_a" to detect logs containing "shutdown" content.

Ruijie# **configure terminal**

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

Ruijie(config)# **smart manager applet** policy\_a

Ruijie(SEM-applet)# **event tag** event\_a **syslog pattern** "shutdown"

**Caution**

If policy configurations are submitted without configuring event, the policy will not be registered and remain in editing state

You can configure multiple events for one policy. These events will be sequenced according to the tag parameter of policy.

**Configure action**

Command	Function
Ruijie> <b>enable</b>	Enter privileged EXEC mode
Ruijie# <b>configure terminal</b>	Enter global configuration mode
Ruijie(config)# <b>smart manager applet</b> <i>applet-name</i> [ <b>class</b> <i>class-options</i> ]	Enter SEM configuration mode. <i>applet-name</i> is the specified policy name. <b>class</b> parameter specifies the policy class.
Ruijie(SEM-applet)# <b>action</b> <i>label</i> <b>syslog</b> [ <b>priority</b> <i>priority-level</i> ] <b>msg</b> <i>msg-text</i> <b>facility</b> <i>string</i>	Every action corresponds to an action command. Here we take Syslog action as an example and introduce the steps to configure an action. Please refer to "SEM Command Reference" for information about other commands.

To delete the policy, execute "**no action** *label*" command in the SEM configuration mode.

Configuration example:

# Configure a syslog action named "action\_a" for a policy named "policy\_a" to send the log of "action running", with priority level being 6.

```
Ruijie# configure terminal
```

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

```
Ruijie(config)# smart manager applet policy_a
```

```
Ruijie(SEM-applet)# action label syslog priority 6 msg "action running"
```

**Caution**

If policy configurations are submitted without configuring action, the policy can still be registered but it will do nothing when triggered.

You can configure multiple actions for one policy. When the policy is triggered, the actions will be executed according to the alphabetical order of action's "label" parameter.

**Configure description**

Command	Function
Ruijie> <b>enable</b>	Enter privileged EXEC mode
Ruijie# <b>configure terminal</b>	Enter global configuration mode



Ruijie(config)# <b>smart manager applet</b> <i>applet-name</i> [ <b>class</b> <i>class-options</i> ]	Enter SEM configuration mode. <i>applet-name</i> is the specified policy name. <b>class</b> parameter specifies the policy class.
Ruijie(SEM-applet)# <b>description</b> <i>string</i>	Configure descriptive information

To delete policy description, execute "**no description**" command in the SEM configuration mode.

Configuration example:

# Configure the descriptive information for a policy named "policy\_a", with content being "policy\_for\_test".

Ruijie# **configure terminal**

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

Ruijie(config)# **smart manager applet** policy\_a

Ruijie(SEM-applet)# **description** "policy\_for\_test"



The change to description will take effect immediately without the need to submit.

**Caution**

## Configure trigger parameters

Command	Function
Ruijie> <b>enable</b>	Enter privileged EXEC mode
Ruijie# <b>configure terminal</b>	Enter global configuration mode
Ruijie(config)# <b>smart manager applet</b> <i>applet-name</i> [ <b>class</b> <i>class-options</i> ]	Enter SEM configuration mode. <i>applet-name</i> is the specified policy name. <b>class</b> parameter specifies the policy class.
Ruijie(SEM-applet)# <b>trigger</b> [ <b>occurs-value</b> <i>occurs-value</i> ] [ <b>occurs-period</b> <i>occurs-period-value</i> ] [ <b>correlate-start</b> <i>period-start-value</i> ] [ <b>correlate-period</b> <i>correlate-period-value</i> ] [ <b>delay</b> <i>delay-value</i> ] [ <b>maxrun</b> <i>maxruntime-number</i> ]	Configure policy trigger parameters

To restore policy trigger parameters to default settings, execute "**no trigger**" command in the SEM configuration mode.

Configuration example:

# Configure trigger parameters for a policy named "policy\_a", so that it will be executed 5 seconds after being triggered, and the maximum running time shall be 15 seconds.

Ruijie# **configure terminal**

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

Ruijie(config)# **smart manager applet** policy\_a

Ruijie(SEM-applet)# **trigger delay 5 maxrun 15**

## Configure CLI Action Output Record

Command	Function
Ruijie> <b>enable</b>	Enter privileged EXEC mode
Ruijie# <b>configure terminal</b>	Enter global configuration mode
Ruijie(config)# <b>smart manager applet</b> <i>applet-name</i> [ <b>class</b> <i>class-options</i> ]	Enter SEM configuration mode. <i>applet-name</i> is the specified policy name. <b>class</b> parameter specifies the policy class.
Ruijie(sem-applet)# <b>policy record</b>	Record the CLI action output into the file.

To stop recording the CLI action output, execute "**no policy record**" command in the SEM configuration mode.

Configuration example:

# Configure the CLI action output record for a policy named "policy\_a", the size of the record file generated by running the policy for one time shall not be greater than 500K, and the size of record file generated by the policy\_a shall not be greater than 2M.

Ruijie# **configure terminal**

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

Ruijie(config)# **smart manager applet** *policy\_a*

Ruijie(sem-applet)# **action action\_1 cli command** "enable"

Ruijie(sem-applet)# **action action\_2 cli command** "show arp"

Ruijie(sem-applet)# **policy record per-instance 500 per-policy 2000**

## Display current policy configurations

Command	Function
Ruijie> <b>enable</b>	Enter privileged EXEC mode
Ruijie# <b>configure terminal</b>	Enter global configuration mode
Ruijie(config)# <b>smart manager applet</b> <i>applet-name</i> [ <b>class</b> <i>class-options</i> ]	Enter SEM configuration mode. <i>applet-name</i> is the specified policy name. <b>class</b> parameter specifies the policy class.
Ruijie(SEM-applet)# <b>list-config</b>	Display current policy configurations

Configuration example:

### # Display the configurations of "policy\_a".

Ruijie# **configure terminal**

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

Ruijie(config)# **smart manager applet** policy\_a

Ruijie(SEM-applet)# **list-config**

smart manager applet policy\_a

description "policy\_for\_test"

event tag event\_a syslog pattern "shutdown"

trigger delay 5 maxrun 15

action label syslog priority informational msg "action running"

Ruijie(SEM-applet)#



#### Caution

When the policy is in editing state and not submitted, executing "list-config" will display configurations being edited and not submitted, and no "commit" command will be included in the contents displayed. When the policy has been submitted, configurations of the policy submitted will be displayed, including "commit" command.

### Submit configurations

Command	Function
Ruijie> <b>enable</b>	Enter privileged EXEC mode
Ruijie# <b>configure terminal</b>	Enter global configuration mode
Ruijie(config)# <b>smart manager applet</b> <i>applet-name</i> [ <b>class</b> <i>class-options</i> ]	Enter SEM configuration mode. <i>applet-name</i> is the specified policy name. <b>class</b> parameter specifies the policy class.
Ruijie(SEM-applet)# <b>commit</b>	Submit policy configurations

Configuration example:

### # Submit the configurations of "policy\_a".

Ruijie# **configure terminal**

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

Ruijie(config)# **smart manager applet** policy\_a

Ruijie(SEM-applet)# **commit**

During the process of submission, policy configurations will be subject to validation check. If failed, the policy configurations will not be submitted and the policy will not be registered. They will remain in editing state. For example, if no event is configured for the policy, the check will not pass.



### Caution

There are two kinds of policies that can be submitted: newly created policy and edited & registered policy. Policies of other circumstances (for example: registered policy, but not edited) will not be submitted, and there will be the corresponding prompting messages.

For the aforementioned two types of policies, if the user expects to discard the changes made to policy configurations, the user can execute "rollback" command to roll back policy configurations.

## Display policy registered

Command	Function
Ruijie>enable	Enter privileged EXEC mode
Ruijie# <b>show smart manager policy registered</b> [ <b>policy</b> <i>policy-name</i> ] [ <b>event-type</b> <i>event-name</i> ] [ <b>class</b> <i>class-options</i> ] [ <b>time-ordered</b>   <b>name-ordered</b> ]	Display the information of policy registered

Configuration example:

# Submit the configurations of "policy\_a".

Ruijie# **show smart manager policy registered**

```

No.   Class    Event Type      Time Registered      Secu  Name
1     applet    syslog          Wed Mar 10 10:49:03 2010  none  policy_a
event_a: syslog: pattern {shutdown}
trigger delay 5.000
maxrun 15.000
action label syslog priority informational msg "action running"

```

Ruijie#

## Roll back configurations

Command	Function
Ruijie>enable	Enter privileged EXEC mode
Ruijie# <b>configure terminal</b>	Enter global configuration mode

Ruijie(config)# <b>smart manager applet</b> <i>applet-name</i> [ <b>class</b> <i>class-options</i> ]	Enter SEM configuration mode. <i>applet-name</i> is the specified policy name. <b>class</b> parameter specifies the policy class.
Ruijie(SEM-applet)# <b>rollback</b>	Roll back policy configurations

Configuration example:

# Roll back the configurations of "policy\_a".

Ruijie# **configure terminal**

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

Ruijie(config)# **smart manager applet** policy\_a

Ruijie(SEM-applet)# **rollback**



#### Note

The user can roll back policy configuration under two circumstances: newly configured policy which hasn't been submitted yet; policy has been submitted and registered, but the changes to policy has not been submitted.

In the aforementioned two cases, the user can execute "rollback" command to roll back policy configurations which haven't been submitted yet.

## Configure multiple events

Command	Function
Ruijie> <b>enable</b>	Enter privileged EXEC mode
Ruijie# <b>configure terminal</b>	Enter global configuration mode
Ruijie(config)# <b>smart manager applet</b> <i>applet-name</i> [ <b>class</b> <i>class-options</i> ]	Enter SEM configuration mode. <i>applet-name</i> is the specified policy name. <b>class</b> parameter specifies the policy class.
Ruijie(sem-applet)# <b>event tag</b> <i>event-name</i> [ <b>correlate</b> { <b>andnot</b>   <b>and</b>   <b>or</b> }] <b>syslog pattern</b> <i>regular-expression</i> [ <b>priority</b> <i>priority-level</i> ] [ <b>occurs</b> <i>num-occurrences</i> ] [ <b>period</b> <i>period-value</i> ] [ <b>skip</b> { <b>yes</b>   <b>no</b> }]	Configure first event
Ruijie(sem-applet)# <b>event tag</b> <i>event-name</i> [ <b>correlate</b> { <b>andnot</b>   <b>and</b>   <b>or</b> }] <b>syslog pattern</b> <i>regular-expression</i> [ <b>priority</b> <i>priority-level</i> ] [ <b>occurs</b> <i>num-occurrences</i> ] [ <b>period</b> <i>period-value</i> ] [ <b>skip</b> { <b>yes</b>   <b>no</b> }]	Configure other events

Configuration example:

# Configure a policy named "policy\_a" and configure two events. The first event will detect whether the log contains the content of "need reload", and the other event will detect whether any card is inserted. The interval between both events must be less than 180 seconds.

Ruijie# **configure terminal**

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

Ruijie(config)# **smart manager applet** policy\_a

Ruijie(SEM-applet)# **event tag** event\_a **syslog pattern** "need reload"

Ruijie(SEM-applet)# **event tag** event\_b **correlate and oir type plugin**

Ruijie(SEM-applet)# **trigger correlate-period** 180



#### Caution

When configuring multiple events, SEM will automatically sequence events according to the alphabetical order of "tag". It is suggested to use an orderly naming rule, such as: 01\_cli, 02\_timer, 03\_counter ...

Relation between events: combination of current event with all preceding events. SEM will only check whether the policy shall be triggered after the first event is triggered.

All events other than the first event shall be configured with parallel relation ("and" by default). The parallel relation configured for the first event will be neglected.

## Configure and use variables

Command	Function
Ruijie> <b>enable</b>	Enter privileged EXEC mode
Ruijie# <b>configure terminal</b>	Enter global configuration mode
Ruijie# <b>smart manager environment</b> <i>variable-name string</i>	Configure SEM global variable
Ruijie(config)# <b>smart manager applet</b> <i>applet-name [class class-options]</i>	Enter SEM configuration mode. <i>applet-name</i> is the specified policy name. <b>class</b> parameter specifies the policy class.
Ruijie(SEM-applet)# <b>action label set</b> <i>variable-name variable-value</i>	Configure SEM local variable
Ruijie(SEM-applet)# <b>action label</b> <b>syslog</b> [ <b>priority</b> <i>priority-level</i> ] <b>msg</b> <i>msg-text</i> [ <b>facility</b> <i>string</i> ]	Use SEM variable (Variables can be used in multiple actions. Here we take Syslog as the example. Please refer to "SEM Command Reference" for details.)

Configuration example:

# Configure SEM global variable of "var\_g"; configure a policy named "policy\_a"; configure action "set" and set the SEM local variable of "var\_1"; further configure action "Syslog" and use "var\_g" and "var\_1" in the action.

Ruijie# **configure terminal**

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

Ruijie(config)# **smart manager environment** var\_g value\_1

```
Ruijie(config)# smart manager applet policy_a
Ruijie(SEM-applet)# action action_1 set var_l value_2
Ruijie(SEM-applet)# action action_2 syslog msg "var_g = $var_g ; var_l = $var_l ; _event_type_string =
$_event_type_string"
```

**Caution**

In the above example, "var\_g" is the global variable set by "smart manager environment" command. var\_l is the user local variable set by action "set". \_event\_type\_string is the system local variable set by SEM event detector.

System local variable is read-only and unchangeable. When the action tries to change such variable, the policy execution will be terminated due to the error. The priority level of local variable is higher than global variable. When a local variable having the same name as the global variable is configured, the local variable will be used when such name is referred.

**Suspend/resume scheduler**

Command	Function
Ruijie> <b>enable</b>	Enter privileged EXEC mode
Ruijie# <b>configure terminal</b>	Enter global configuration mode
Ruijie(config)# <b>smart manager scheduler suspend</b>	Suspend SEM policy scheduler

To resume the scheduler, execute "**no smart manager scheduler suspend**" command in the global configuration mode.

Configuration example:

# Suspend SEM policy scheduler

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

**Caution**

Suspending SEM scheduler will only suspend the scheduling function. Threads which have been scheduled will not be suspended due to the suspension of scheduler.

**Hold/release policy execution**

Command	Function
Ruijie> <b>enable</b>	Enter privileged EXEC mode
Ruijie# <b>smart manager scheduler hold {all   policy job-id   class class-options}</b>	Hold the policy being executed

Ruijie# <b>smart manager scheduler release</b> {all   <b>policy</b> <i>policy-id</i>   <b>class</b> <i>class-options</i> }	Release the policy being held
--	-------------------------------

Configuration example:

# Hold the execution of policies falling within class A.

Ruijie# **smart manager scheduler hold class** a

# Release policies falling within class A.

Ruijie# **smart manager scheduler release class** a



Only unscheduled threads can be held. Once they have been scheduled, they cannot be held anymore.

Parameter "class" or "all" will hold a specified class or all classes, and the subsequent threads in the class will be held as well. Parameter "policy" will only hold a specified class, and other policies in the class will remain unaffected.

### Force to end policy execution

Command	Function
Ruijie> <b>enable</b>	Enter privileged EXEC mode
Ruijie# <b>smart manager scheduler clear</b> {all   <b>policy</b> <i>job-id</i>   <b>class</b> <i>class-options</i> }	Force to end policy execution

Configuration example:

# Force to end the policy with ID being 150.

Ruijie# **smart manager scheduler clear policy** 150

### Display SEM history events

Command	Function
Ruijie> <b>enable</b>	Enter privileged EXEC mode
Ruijie# <b>show smart manager history events</b>	Display SEM history events

Configuration example:

# Display SEM history events

Ruijie# **show smart manager history events**

No.	Job Id	Proc Status	Time of Event	Event Type	Name
1	1	Actv success	Tue Mar 9 00:00:00 2010	timer cron	applet: policy_a

### Display SEM detector

Command	Function
---------	----------



Ruijie> <b>enable</b>	Enter privileged EXEC mode
Ruijie# <b>show smart manager detector</b> [all   <i>detector-name</i> ] [detailed   statistics]	Display SEM detector

Configuration example:

# Display SEM detector

```
Ruijie# show smart manager detector syslog detailed
```

```
No.  Name          Version
1    syslog         01.00
```

Applet Configuration Syntax:

event tag event-name [correlate {andnot | and | or }] syslog pattern regular-expression [occurs num-occurrences] [period period-value] [priority priority-level]

Applet Built-in Environment Variables:

```
$_event_id
$_event_type
$_event_type_string
$_event_pub_time
$_event_pub_sec
$_event_pub_msec
$_syslog_msg
$_syslog_priority
```

```
Ruijie# show smart manager detector syslog statistics
```

Syslog Detecotr Statistics:

```
Policy    Event    Detect  NoPri PriPass  PriDeny  PatternPass  trigge
policy_a  event_a  1000   100   400       500       10           4
```

## Display SEM version

Command	Function
Ruijie> <b>enable</b>	Enter privileged EXEC mode
Ruijie# <b>show smart manager version</b>	Display SEM version

Configuration example:

# Display SEM version

```
Ruijie# show smart manager version
```

```
Smart Embedded Manager Version 1.0
```

Event Detectors:

```
name          version
application    1.0
syslog         1.0
cli            1.0
```

counter	1.0
cpp	1.0
grtd	1.0
interface	1.0
none	1.0
oir	1.0
snmp	1.0
snmp-object	1.0
snmp-notification	1.0
sysmon	1.0
timer	1.0

## Typical SEM configuration example

### SEM detection of interface counter

#### Networking requirements

Device A is directly connected with Device B. GigabitEthernet1/1 of Device A is connected with GigabitEthernet2/1 of Device B. Due to certain fault on the link or Device B, Device A may suddenly and frequently receive substantial continuous error frames from Device B, and data communication is hence compromised. The problem can be solved by executing "shutdown" on GigabitEthernet1/1 of Device A and the resume the port.

#### Network topology

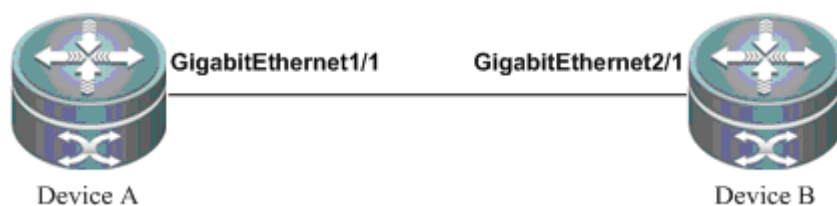


Fig 2 Topology of interface counter detection

#### Configuration tips

- 1) Create policy
- 2) Configure interface event
- 3) Configure CLI action
- 4) Submit policy configurations

#### Configuration steps

- 1) Configure Device A

- a, Name the policy configured for Device A as "policy\_a".
- b, Configure an event named "event\_1" for policy\_a, with type being "interface". Detailed parameters are shown below:

Configure the type of interface counter detection: "parameter input\_errors\_frame", which means to detect the number of input error frames on the interface;

Configure the name of the interface being detected: "name GigabitEthernet 1/1", which is used to specify the interface being detected;

Configure the threshold of detection: "entry-type value entry-op ge entry-val 2000", which means the absolute value of counter detection. When the absolute value is greater than or equal to 2000, the detection is passed.

Configure the frequency of detection: "poll-interval 5", which means that the time interval for detecting interface counter shall be five seconds.

The parameter to restore event detection conditions after counter detection is: "exit-type value exit-op ge exit-val 2000 exit-time 60 exit-comb and". The part of "exit-type value exit-op ge exit-val 2000" is same as the foregoing parameter related to the threshold of detection, namely, after the event is triggered, the value check immediately meets the condition to recover, while "exit-time 60 exit-comb and" means that the recovery time and recovery check are of "and" relationship. Since the condition of recovery check is immediately met after the event is triggered, once the event has been triggered for over 60 seconds and the other condition of recovery time is met as well, event detection will be recovered.

- c, Configure multiple actions for policy\_a, as shown below:
  1. Enter GigabitEthernet1/1 interface configuration mode;
  2. Execute "shutdown";
  3. Execute "no shutdown";
  4. Enter privileged EXEC mode;
  5. Clear the interface statistical counter of GigabitEthernet 1/1.
- d, Submit the policy
- e, End policy editing

Ruijie# **configure terminal**

Ruijie(config)# **smart manager applet policy\_a**

Ruijie(SEM-applet)# **event tag event\_1 interface parameter input\_errors\_frame name GigabitEthernet 1/1 entry-type value entry-op ge entry-val 2000 poll-interval 5 exit-type value exit-op ge exit-val 2000 exit-time 60 exit-comb and**

Ruijie(SEM-applet)# **action action\_1 cli command "enable"**

Ruijie(SEM-applet)# **action action\_2 cli command "configure terminal"**

Ruijie(SEM-applet)# **action action\_3 cli command "interface GigabitEthernet 1/1"**

Ruijie(SEM-applet)# **action action\_4 cli command "shutdown"**

Ruijie(SEM-applet)# **action action\_5 cli command "no shutdown"**

Ruijie(SEM-applet)# **action action\_6 cli command "exit"**

Ruijie(SEM-applet)# **action action\_7 cli command "exit"**

```
Ruijie(SEM-applet)# action action_8 cli command "clear counters GigabitEthernet 1/1" pattern "y"
Ruijie(SEM-applet)# commit
Ruijie(SEM-applet)# exit
Ruijie(config)#
```

## Verification

### 1) Display SEM policy registered

```
Ruijie# show smart manager policy registered
```

No.	Class	Event Type	Time Registered	Secu	Name
1	applet	interface	Mon Mar 8 16:19:15 2010	none	policy_a

event\_1: interface: name GigabitEthernet 1/1 parameter input\_errors\_frame entry\_op ge entry\_val 2000 entry\_type value exit\_comb and exit\_op ge exit\_val 2000 exit\_type value exit\_time 60.000 poll\_interval 5.000 maxrun 20.000

action action\_1 cli command "enable"

action action\_2 cli command "configure terminal"

action action\_3 cli command "interface GigabitEthernet 1/1"

action action\_4 cli command "shutdown"

action action\_5 cli command "no shutdown"

action action\_6 cli command "exit"

action action\_7 cli command "exit"

action action\_8 cli command "clear counters GigabitEthernet 1/1" pattern "y"

### 2) Display CLI action output record after the policy is executed.

```
Ruijie# more /sem_record/policy_a/2010-05-08_16-21-15_1001.txt
```

#### SEM CLI RECORD FILE

SEM policy name: policy\_a

SEM policy trigger id :1

SEM policy cli record time : Mon Mar 8 16:21:15 2010

=====

```
Ruijie#enable
```

```
Ruijie#configure terminal
```

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

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

```
Ruijie(config-GigabitEthernet 1/1)#shutdown
```

```
Ruijie(config-GigabitEthernet 1/1)#no shutdown
```

```
Ruijie(config-GigabitEthernet 1/1)#exit
```

```
Ruijie(config)#exit
```

```
Ruijie#clear counters GigabitEthernet 1/1
```

```
Ruijie#
```

## SEM detection of application-specific events

### Networking requirements

Device A is directly connected with Device B. GigabitEthernet1/1 of Device A is connected with GigabitEthernet2/1 of Device B. Due to certain fault on the link or Device B, Device A may suddenly and frequently receive substantial continuous error frames from Device B, and data communication is hence compromised. The problem can be solved by executing "shutdown" on GigabitEthernet1/1 of Device A and then resume the port. Meanwhile, when the event is triggered five times within one hour on Device A, logs and alerts shall be sent to determine the time distribution of fault.

### Network topology

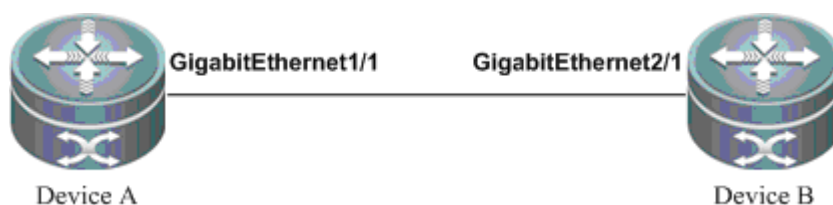


Fig 3 Topology of application-specific event detection

### Configuration tips

- 1) Create interface detection policy; configure interface counter event, CLI action and application-specific action.
- 2) Create application-specific event detection policy and configure application-specific event and Syslog action.

### Configuration steps

- 1) Configure Device A
  - a. Name the policy configured for Device A as "policy\_a".
  - b. Configure an event named "event\_1" for policy\_a, with type being "interface". Detailed parameters are shown below:

Configure the type of interface counter detection: "parameter input\_errors\_frame", which means to detect the number of input error frames on the interface;

Configure the name of the interface being detected: "name GigabitEthernet 1/1", which is used to specify the interface being detected;

Configure the threshold of detection: "entry-type value entry-op ge entry-val 2000", which means the absolute value of counter detection. When the absolute value is greater than or equal to 2000, the detection is passed.

Configure the frequency of detection: "poll-interval 5", which means that the time interval for detecting interface counter shall be five seconds.

The parameter to restore event detection conditions after counter detection is: "exit-type value exit-op ge exit-val 2000 exit-time 60 exit-comb and". The part of "exit-type value

exit-op ge exit-val 2000" is same as the foregoing parameter related to the threshold of detection, namely, after the event is triggered, the value check immediately meets the condition to recover, while "exit-time 60 exit-comb and" means that the recovery time and recovery check are of "and" relationship. Since the condition of recovery check is immediately met after the event is triggered, once the event has been triggered for over 60 seconds and the other condition of recovery time is met as well, event detection will be recovered.

- c, Configure multiple actions for policy\_a, as shown below:

Enter GigabitEthernet1/1 interface configuration mode;

Execute "shutdown";

Execute "no shutdown";

Enter privileged EXEC mode;

Clear the interface statistical counter of GigabitEthernet 1/1.

Publish SEM application-specific event, with sub-system being 100 and type being 50.

- d, Submit the policy

- e, End policy editing

Ruijie# **configure terminal**

Ruijie(config)# **smart manager applet policy\_a**

Ruijie(SEM-applet)# **event tag event\_1 interface parameter input\_errors\_frame name GigabitEthernet 1/1 entry-type value entry-op ge entry-val 2000 poll-interval 5 exit-type value exit-op ge exit-val 2000 exit-time 60 exit-comb and**

Ruijie(SEM-applet)# **action action\_1 cli command "enable"**

Ruijie(SEM-applet)# **action action\_2 cli command "configure terminal"**

Ruijie(SEM-applet)# **action action\_3 cli command "interface GigabitEthernet 1/1"**

Ruijie(SEM-applet)# **action action\_4 cli command "shutdown"**

Ruijie(SEM-applet)# **action action\_5 cli command "no shutdown"**

Ruijie(SEM-applet)# **action action\_6 cli command "exit"**

Ruijie(SEM-applet)# **action action\_7 cli command "exit"**

Ruijie(SEM-applet)# **action action\_8 cli command "clear counters GigabitEthernet 1/1" pattern "y"**

Ruijie(SEM-applet)# **action action\_9 publish-event sub-system 100 type 50**

Ruijie(SEM-applet)# **commit**

Ruijie(SEM-applet)# **exit**

Ruijie(config)#

## 2) Configure Device A

- a, Name the policy configured for Device A as "policy\_b".

b, Configure an application-specific event named "event\_1" for Device A (events of different policies can have the same name), with sub-system and type being same as that of action\_9 in the foregoing policy\_a. Detect the events published by action\_9 of policy\_a, and event\_1 will be triggered after action publishes an event with sub-system being 100 and type being 50.

- c, Configure an action for policy\_b to log a message.
- d, Submit the policy
- e, End policy editing

```
Ruijie# configure terminal
Ruijie(config)# smart manager applet policy_b
Ruijie(SEM-applet)# event tag event_1 application sub-system 100 type 50
Ruijie(SEM-applet)# action action_1 syslog msg "shutdown and no shutdown 5 times" priority 5
Ruijie(SEM-applet)# trigger occurs 5 occurs-period 3600
Ruijie(SEM-applet)# commit
Ruijie(SEM-applet)# exit
Ruijie(config)#
```

## Verification

Ruijie# show smart manager policy registered

No.	Class	Event Type	Time Registered	Name
1	applet	interface	Mon Mar 8 21:07:21 2010	policy_a
event_1: interface: name GigabitEthernet 1/1 parameter input_errors_frame entry_op ge entry_val 2000 entry_type value exit_comb and exit_op ge exit_val 2000 exit_type value exit_time 60.000 poll_interval 5.000 maxrun 20.000 action action_1 cli command "enable" action action_2 cli command "configure terminal" action action_3 cli command "interface GigabitEthernet 1/1" action action_4 cli command "shutdown" action action_5 cli command "no shutdown" action action_6 cli command "exit" action action_7 cli command "exit" action action_8 cli command "clear counters GigabitEthernet 1/1" pattern "y" action action_9 publish-event sub-system 100 type 50 arg1 "tmp"				
2	applet	user application	Mon Mar 8 21:08:11 2010	policy_b
event_1: application: sub_system 100 type 50 trigger occurs 5 period 3600.000 maxrun 20.000 action action_1 syslog priority notifications msg "shutdown and no shutdown 5 times"				

## SEM detection of counter

### Networking requirements

Device A is directly connected with Device B. GigabitEthernet1/1 of Device A is connected with GigabitEthernet2/1 of Device B. There is also a low-bandwidth backup link between Ethernet3/1 of Device A and Ethernet4/1 of Device B. Due to certain fault on the link or Device B, Device A may suddenly and frequently receive substantial continuous error frames from Device B on

GigabitEthernet1/1, and data communication is hence compromised. When such event has been triggered for over 50 times, shut down GigabitEthernet1/1 and use the back link.

## Network topology

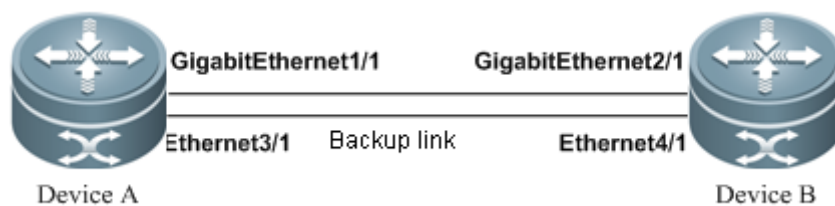


Fig 4 Topology of counter event detection

## Configuration tips

- 1) Create interface detection policy; configure interface counter event, CLI action and counter action.
- 2) Create application-specific event detection policy and configure counter event and CLI action.

## Configuration steps

### 1) Configure Device A

- a. Name the policy configured for Device A as "policy\_a".
- b. Configure an event named "event\_1" for policy\_a, with type being "interface".

Detailed parameters are shown below:

Configure the type of interface counter detection: "parameter input\_errors\_frame", which means to detect the number of input error frames on the interface;

Configure the name of the interface being detected: "name GigabitEthernet 1/1", which is used to specify the interface being detected;

Configure the threshold of detection: "entry-type value entry-op ge entry-val 2000", which means the absolute value of counter detection. When the absolute value is greater than or equal to 2000, the detection is passed.

Configure the frequency of detection: "poll-interval 5", which means that the time interval for detecting interface counter shall be five seconds.

The parameter to restore event detection conditions after counter detection is: "exit-type value exit-op ge exit-val 2000 exit-time 60 exit-comb and". The part of "exit-type value exit-op ge exit-val 2000" is same as the foregoing parameter related to the threshold of detection, namely, after the event is triggered, the value check immediately meets the condition to recover, while "exit-time 60 exit-comb and" means that the recovery time and recovery check are of "and" relationship. Since the condition of recovery check is immediately met after the event is triggered, once the event has been triggered for over 60 seconds and the other condition of recovery time is met as well, event detection will be recovered.



- c, Configure multiple actions for policy\_a, as shown below:  
 Enter GigabitEthernet1/1 interface configuration mode;  
 Execute "shutdown";  
 Execute "no shutdown";  
 Enter privileged EXEC mode;  
 Clear the interface statistical counter of GigabitEthernet 1/1.  
 Counter action to increase the value of counter\_a by 1.
- d, Submit the policy
- e, End policy editing

```
Ruijie# configure terminal
Ruijie(config)# smart manager applet policy_a
Ruijie(SEM-applet)# event tag event_1 interface parameter input_errors_frame name GigabitEthernet 1/1 entry-type
value entry-op ge entry-val 2000 poll-interval 5 exit-type value exit-op ge exit-val 2000 exit-time 60 exit-comb and
Ruijie(SEM-applet)# action action_1 cli command "enable"
Ruijie(SEM-applet)# action action_2 cli command "configure terminal"
Ruijie(SEM-applet)# action action_3 cli command "interface GigabitEthernet 1/1 "
Ruijie(SEM-applet)# action action_4 cli command "shutdown"
Ruijie(SEM-applet)# action action_5 cli command "no shutdown"
Ruijie(SEM-applet)# action action_6 cli command "exit"
Ruijie(SEM-applet)# action action_7 cli command "exit"
Ruijie(SEM-applet)# action action_8 cli command "clear counters GigabitEthernet 1/1 " pattern "y"
Ruijie(SEM-applet)# action action_9 counter name counter_a op inc value 1
Ruijie(SEM-applet)# commit
Ruijie(SEM-applet)# exit
Ruijie(config)#
```

## 2) Configure Device A

- a, Name the policy configured for Device A as "policy\_b".
- b, Configure an EMI counter event named "event\_1" for Device A (events of different policies can have the same name), with parameters shown below:

The name of the SEM counter detected shall be "counter\_a", which is the same as the name of counter operated by action\_9 in policy\_a.

The detection parameters of counter shall be "entry-op ge entry-val 50", which means that the event will be triggered when the value of SEM counter is greater than or equal to 50.

The counter recovery parameter is "exit-op ge exit-val 50", with the type and value configured being the same as the detection parameter, which means that event detection will resume immediately after counter event is passed.

- c, Configure actions for policy\_b, as shown below:  
 Enter GigabitEthernet1/1 interface configuration mode;

Execute "shutdown" to shut down interface permanently.

- d, Submit the policy
- e, End policy editing

Ruijie# **configure terminal**

Ruijie(config)# **smart manager applet policy\_b**

Ruijie(SEM-applet)# **event tag event\_1 counter name counter\_a entry-op ge entry-val 50 exit-op ge exit-val 50**

Ruijie(SEM-applet)# **action action\_1 cli command "enable"**

Ruijie(SEM-applet)# **action action\_2 cli command "configure terminal"**

Ruijie(SEM-applet)# **action action\_3 cli command "interface GigabitEthernet 1/1"**

Ruijie(SEM-applet)# **action action\_4 cli command "shutdown"**

Ruijie(SEM-applet)# **action action\_5 cli command "exit"**

Ruijie(SEM-applet)# **commit**

Ruijie(SEM-applet)# **exit**

Ruijie(config)#

## Verification

Ruijie# **show smart manager policy registered**

No.	Class	Event Type	Time Registered	Name
1	applet	interface	Mon Mar 8 22:21:26 2010	policy_a

```

event_1: interface: name GigabitEthernet 0/1 parameter input_errors_frame entry_op ge entry_val 2000 entry_type value
exit_comb and exit_op ge exit_val 2000 exit_type value exit_time 60.000 poll_interval 5.000
maxrun 20.000
action action_1 cli command "enable"
action action_2 cli command "configure terminal"
action action_3 cli command "interface GigabitEthernet 1/1"
action action_4 cli command "shutdown"
action action_5 cli command "no shutdown"
action action_6 cli command "exit"
action action_7 cli command "exit"
action action_8 cli command "clear counters GigabitEthernet 1/1" pattern "y"
action action_9 counter name counter_a value 1 op inc

```

2	applet	user counter	Mon Mar 8 22:23:26 2010	policy_b
---	--------	--------------	-------------------------	----------

```

event_1: counter: name {counter_a} entry_val 50 entry_op ge exit_val 50 exit_op ge
maxrun 20.000
action action_1 cli command "enable"
action action_2 cli command "configure terminal"
action action_3 cli command "interface GigabitEthernet 1/1"
action action_4 cli command "shutdown"
action action_5 cli command "exit"

```

## SEM detection of OIR

### Networking requirements

After only insertion of new line card into Device A, due to software defect, the newly inserted line card is incomplete in routing information, which will result in abnormal forwarding. The problem can be solved by executing "clear ip route \*" and refresh the routing table.

### Network topology

<NA>

### Configuration tips

- 1) Create policy
- 2) Configure OIR event
- 3) Configure action
- 4) Submit policy configurations

### Configuration steps

- 1) Configure Device A
  - a, Name the policy configured for Device A as "policy\_a".
  - b, Configure an OIR event named "event\_1" for policy\_a, with type being "plugin".
  - c, Configure multiple actions for policy\_a, as shown below:
 

Enter privileged EXEC mode;

Execute "clear ip route \*" to refresh the routing table.
  - d, Submit the policy
  - e, End policy editing

```
Ruijie# configure terminal
Ruijie(config)# smart manager applet policy_a
Ruijie(SEM-applet)# event tag event_1 oir type plugin
Ruijie(SEM-applet)# action action_1 cli command "enable"
Ruijie(SEM-applet)# action action_2 cli command "clear ip route *"
Ruijie(SEM-applet)# delay 60
Ruijie(SEM-applet)# commit
Ruijie(SEM-applet)# exit
Ruijie(config)#
```

### Verification

```
Ruijie# show smart manager policy registered
```

No.	Class	Event Type	Time Registered	Secu	Name
1	applet	oir	Mon Mar 8 16:45:17 2010	none	policy_a

```
event_1: oir: type{plugin}  
maxrun 20.000  
delay 60.000  
action action_1 cli command "enable"  
action action_2 cli command "clear ip route *"
```

## SEM timer event

### Networking requirements

Device A is connected with Tftp Server. Device A will automatically send log file to Tftp Server at 0:00 everyday and delete the original log file.

### Network topology



Fig 5 Topology of timer detection

### Configuration tips

- 1) Create policy
- 2) Configure timer event
- 3) Configure action
- 4) Submit policy configurations

### Configuration steps

- 1) Configure Device A
  - a, Name the policy configured for Device A as "policy\_a".
  - b, Configure an CRON timer event named "event\_1" for policy\_a, with time being 0:00 everyday.
  - c, Configure multiple actions for policy\_a, as shown below:  
Enter privileged EXEC mode;  
Execute "copy" command to send the log file.
  - d, Submit the policy
  - e, End policy editing

Ruijie# **configure terminal**

```

Ruijie(config)# smart manager applet policy_a
Ruijie(SEM-applet)# event tag event_1 timer cron cron-entry "0 0 * * *"
Ruijie(SEM-applet)# action action_1 cli command "enable"
Ruijie(SEM-applet)# action action_2 cli command "copy flash:logfile.txt tftp://172.16.0.2/device_a/log_${event}_pub_time"
Ruijie(SEM-applet)# action action_3 cli command "delete flash:logfile.txt"
Ruijie(SEM-applet)# commit
Ruijie(SEM-applet)# exit
Ruijie(config)#exit

```

## Verification

Ruijie# show smart manager policy registered

No.	Class	Event Type	Time Registered	Secu	Name
1	applet	timer cron	Mon Mar 8 17:25:47 2010	none	policy_a

event\_1: timer cron: cron entry "0 0 \* \* \*"

maxrun 20.000

action action\_1 cli command "enable"

action action\_2 cli command "copy flash:logfile.txt tftp://172.16.0.2/device\_a/log\_\${event}\_pub\_time"

action action\_3 cli command "delete flash:logfile.txt"

## SEM Detection of CPP Counter

### Networking requirements

Device A is connected with user, and sometimes unknown attacks from network may result in high CPU utilization of the device. If such attacks can be detected and the priority level of attack packets can be lowered, the impacts caused by such attacks can be eased.

### Network topology

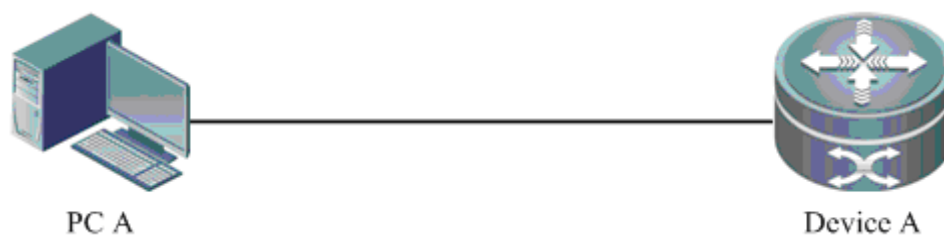


Fig 6 Topology of CPP counter detection

### Configuration tips

- 1) Preparation
- 2) Create policy
- 3) Configure CPP counter event
- 4) Configure action
- 5) Submit policy configurations

## Configuration steps

### 1) Configure Device A

a, Adjust the packet priority lower than 1 to 1 in order to detect attack packets, and then set their priority level to 0 (smaller than the priority level of normal packets) in order to guarantee normal operations of the device.

b, Name the policy configured for Device A as "policy\_a".

c, Configure an event named "event\_1" for policy\_a, with type being "cpp". Detailed parameters are shown below:

Use "parameter any" to detect all types of CPP packets;

Detect the drop rate of CPP packets: "type drop op ge value 1000", which means that the event will be triggered when the drop rate of a specific type of CPP packet is greater than or equal to 1000.

Configure the detection interval: "poll-interval 15", which means that the detection interval is 15 seconds.

d, Configure multiple actions for policy\_a, as shown below:

Enter global configuration mode;

Execute "cpu-protect type \$\_type pri 0" to detect the lowered priority level of attack CCP packets; "\$\_type" is environment variable set by CPP event detector. It will be replaced by the type of specific CPP packets during operation.

e, Submit the policy

f, End policy editing

Ruijie# **configure terminal**

Ruijie(config)# **cpu-protect type tp-guard pri 1**

Ruijie(config)# **cpu-protect type arp pri 1**

Ruijie(config)# **cpu-protect type dhcps pri 1**

Ruijie(config)# **cpu-protect type dot1x pri 1**

Ruijie(config)# **cpu-protect type gvrp pri 1**

Ruijie(config)# **cpu-protect type ipv6-mc pri 1**

Ruijie(config)# **cpu-protect type rip pri 1**

Ruijie(config)# **cpu-protect type unknow-ipmc pri 1**

Ruijie(config)# **cpu-protect type err-ttl pri 1**

Ruijie(config)# **cpu-protect type dhcp\_relay\_client pri 1**

Ruijie(config)# **cpu-protect type dhcp\_realy\_server pri 1**

Ruijie(config)# **cpu-protect type dhcp\_option82 pri 1**

Ruijie(config)# **smart manager applet policy\_a**

Ruijie(SEM-applet)# **event tag event\_1 cpp parameter any type drop op ge value 1000 poll-interval 15**

Ruijie(SEM-applet)# **action action\_1 cli command "enable"**

Ruijie(SEM-applet)# **action action\_2 cli command "configure terminal"**

Ruijie(SEM-applet)# **action action\_3 cli command "cpu-protect type \$\_type pri 0"**

```
Ruijie(SEM-applet)# commit
Ruijie(SEM-applet)# exit
Ruijie(config)#
```

## Verification

```
Ruijie# show smart manager policy registered
```

No.	Class	Event Type	Time Registered	Name
1	applet	cli	Mon Mar 8 19:30:00 2010	policy_a

```
event_1: cpp: parameter any type drop op ge value {1000} poll-interval 15
maxrun 20.000

action action_1 cli command "enable"

action action_2 cli command " configure terminal "

action action_3 cli command " cpu-protect type $_type pri 0"
```

## SEM detection of CLI

### Networking requirements

Device A is connected with Tftp Server. Before executing "copy running-config startup-config", Device A will backup the old configurations to the Tftp Server.

### Network topology

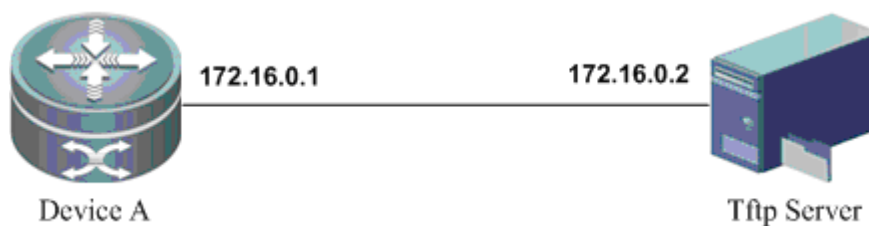


Fig 7 Topology of CLI detection

### Configuration tips

- 1) Create policy
- 2) Configure CLI event
- 3) Configure action
- 4) Submit policy configurations

### Configuration steps

- 1) Configure Device A

- a) Name the policy configured for Device A as "policy\_a".
- b) Configure a CLI event named "event\_1" for policy\_a to detect commands containing the content of "copy running-config startup-config"; execute the policy to use synchronization mode by using parameter "sync yes".
- c) Configure multiple actions for policy\_a, as shown below:  
 Enter privileged EXEC mode;  
 Execute "copy" command to backup configuration file.
- d) Submit the policy
- e) End policy editing

```
Ruijie# configure terminal
Ruijie(config)# smart manager applet policy_a
Ruijie(SEM-applet)# event tag event_1 cli pattern "copy running-config startup-config" sync yes
Ruijie(SEM-applet)# action action_1 cli command "enable"
Ruijie(SEM-applet)# action action_2 cli command "copy startup-config tftp://172.16.0.2/device_a/conf_${event_pub_time}"
Ruijie(SEM-applet)# action action_3 exit 1
Ruijie(SEM-applet)# commit
Ruijie(SEM-applet)# exit
Ruijie(config)#
```

## Verification

```
Ruijie# show smart manager policy registered
```

No.	Class	Event Type	Time Registered	Name
1	applet	cli	Mon Mar 8 19:30:00 2010	policy_a

```

event_1: cli: pattern "copy running-config startup-config" sync yes

maxrun 20.000

action action_1 cli command "enable"

action action_2 cli command "copy startup-config tftp://172.16.0.2/device_a/conf_${event_pub_time}"

action action_3 exit 1
```

## SEM detection of SNMP event

### Networking requirements

NetManager is connected with Device A over Ethernet. SNMP service is enabled on Device A so that NetManager can manage Device A through network. The SNMP operation of value of "get OID 1.3.6.1.2.1.2.1" must be stopped for purpose of compatibility.



## Network topology

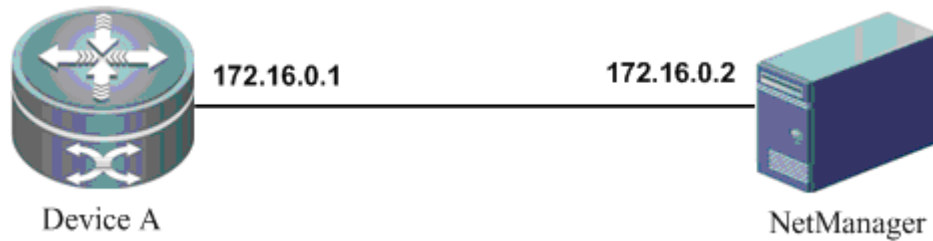


Fig 8 Topology of SNMP event detection

## Configuration tips

- 1) Create policy
- 2) Configure SNMP event and SNMP Object event
- 3) Configure action
- 4) Submit policy configurations

## Configuration steps

- 1) Configure Device A
  - a) Name the policy configured for Device A as "policy\_a".
  - b) Configure an event named "event\_1" for policy\_a, with type being "SNMP Object". Detailed parameters are shown below:

Detect OID of SNMP operations: "oid 1.3.6.1.2.1.2.1";

OID must not be of table type: "istable no";

OID type must be int: "type int";

The asynchronization mode must be used to execute the policy, skip SNMP Object operations, and use the parameter "skip yes".
  - c) Configure actions for policy\_a: the snmp operation of record is cancelled.
  - d) Submit the policy
  - e) End policy editing

```
Ruijie# configure terminal
Ruijie(config)# smart manager applet policy_a
Ruijie(sem-applet)# event tag event_1 snmp-object oid 1.3.6.1.2.1.2.1 istable no type int skip yes
Ruijie(sem-applet)# action action_1 syslog msg "cancel snmp operate" priority 5
Ruijie(sem-applet)# commit
Ruijie(sem-applet)# exit
Ruijie(config)#
```

## Verification

```
Ruijie# show smart manager policy registered
```

No.	Class	Event Type	Time Registered	Secu	Name
1	applet	snmp-object	Tue Mar 9 17:46:01 2010	none	policy_a
event_1: snmp-object: oid 1.3.6.1.2.1.2.1 type int skip yes istable no					
maxrun 20.000					
action action_1 syslog msg "cancel snmp operate"					

## SEM detection of none event

### Networking requirements

During the installation and troubleshooting of Device A, the routing table, ARP table and IPv6 routing table must be cleared repeatedly. A simple method is needed to realize batch operations.

### Network topology

<NA>

### Configuration tips

- 1) Create policy
- 2) Configure none event
- 3) Configure action
- 4) Submit policy configurations

### Configuration steps

- 1) Configure Device A
  - a) Name the policy configured for Device A as "policy\_a".
  - b) Configure an event named "event\_1" for policy\_a, with type being "none". This event will be triggered manually by CLI.
  - c) Configure multiple actions for policy\_a, as shown below:
 

Enter privileged EXEC mode;

Execute "clear arp-cache" to clear ARP cache;

Execute "clear ip route \*" to refresh IPv4 routing table;

Execute "clear ipv6 route \*" to refresh IPv6 routing table;
  - d) Submit the policy
  - e) End policy editing

Ruijie# **configure terminal**

Ruijie(config)# **smart manager applet policy\_a**

Ruijie(SEM-applet)# **event tag event\_1 none**

Ruijie(SEM-applet)# **action action\_1 cli command "enable"**

Ruijie(SEM-applet)# **action action\_2 cli command "clear arp-cache"**

```
Ruijie(SEM-applet)# action action_3 cli command "clear ip route *"  
Ruijie(SEM-applet)# action action_4 cli command "clear ipv6 route *"  
Ruijie(SEM-applet)# commit  
Ruijie(SEM-applet)# exit  
Ruijie(config)#
```

## Verification

```
Ruijie# show smart manager policy registered  
  
No.   Class   Event Type           Time Registered           Name  
-----  
1    applet   none                 Mon Mar 8 21:43:07 2010   policy_a  
  
event_1: none: policyname policy_a sync yes  
  
maxrun 20.000  
  
action action_1 cli command "enable"  
  
action action_2 cli command "clear arp-cache"  
  
action action_3 cli command "clear ip route *"  
  
action action_4 cli command "clear ipv6 route *"
```

## SEM detection of Syslog event

### Networking requirements

Device A will send the logs in condition of insufficient memory. Main/standby switchover must be carried out when the logs are received.

### Network topology

<NA>

### Configuration tips

- 1) Create policy
- 2) Configure Syslog event
- 3) Configure action
- 4) Configure policy trigger parameters
- 5) Submit policy configurations

### Configuration steps

- 1) Configure Device A
  - a) Name the policy configured for Device A as "policy\_a".

- b) Configure a Syslog event named "event\_1" for policy\_a to detect logs of level 2 containing "No-memory" content.
- c) Configure a switchover action for policy\_a.
- d) Submit the policy
- e) End policy editing

```
Ruijie# configure terminal
Ruijie(config)# smart manager applet policy_a
Ruijie(sem-applet)# event tag event_1 syslog pattern "No-memory" priority critical
Ruijie(sem-applet)# action action_1 reload
Ruijie(sem-applet)# commit
Ruijie(sem-applet)# exit
Ruijie(config)#
```

## Verification

```
Ruijie# show smart manager policy registered
```

No.	Class	Event Type	Time Registered	Secu	Name
1	applet	syslog	Tue Mar 9 18:38:23 2010	none	policy_a

```
event_1: syslog: pattern "No-memory" priority critical
maxrun 20.000
action action_1 switchover
```

## SEM detection of watchdog system event

### Networking requirements

Device A may result in insufficient memory or memory leak due to the burst traffic, and device failure may incur when memory is exhausted. To avoid that services are compromised due to memory problem, main/standby switchover must be carried out when memory usage reaches 95%.

### Network topology

<NA>

### Configuration tips

- 1) Create policy
- 2) Configure watchdog system event
- 3) Configure action
- 4) Configure policy trigger parameters
- 5) Submit policy configurations

### Configuration steps

- 1) Configure Device A

- a) Name the policy configured for Device A as "policy\_a".
- b) Configure a watchdog system event named "event\_1" for policy\_a, with parameter being "type memory scope system-use percent" to detect the percentage of system memory usage. The detection threshold is "entry-op ge entry-val 95", which means the event will be triggered when the percentage exceeds 95%.
- c) Configure main/standby switchover action for policy\_a.
- d) Submit the policy
- e) End policy editing

Ruijie# **configure terminal**

Ruijie(config)# **smart manager applet** *policy\_a*

Ruijie(SEM-applet)# **event tag** *event\_1* **sysmon type memory system-use percent entry-op ge entry-val 95**

Ruijie(SEM-applet)# **action** *action\_1* **force-switchover**

Ruijie(SEM-applet)# **commit**

Ruijie(SEM-applet)# **exit**

Ruijie(config)#

## Verification

Ruijie# **show smart manager policy registered**

No.	Class	Event Type	Time Registered	Secu	Name
1	applet	sysmon	Tue Mar 9 18:38:23 2010	none	policy_a

event\_1: sysmon: type memory scope system-use percent entry-op ge entry-val 95  
 maxrun 20.000  
 action action\_1 switchover

## SEM detection of GRTD event

### Networking requirements

When GRTD monitoring on Device A diagnoses a severe problem, main/standby switchover will be performed to avoid that normal services affected by the problem diagnosed.

### Network topology

<NA>

### Configuration tips

- 1) Create policy
- 2) Configure GRTD event
- 3) Configure action
- 4) Configure policy trigger parameters
- 5) Submit policy configurations

## Configuration steps

- 1) Configure Device A
  - a) Name the policy configured for Device A as "policy\_a".
  - b) Configure a GRTD event named "event\_1" for policy\_a to detect the severe problems monitored on all slots, with parameter being "slot all testing-type monitoring severity-major".
  - c) Configure main/standby switchover action for policy\_a.
  - d) Submit the policy
  - e) End policy editing

Ruijie# **configure terminal**

Ruijie(config)# **smart manager applet** *policy\_a*

Ruijie(SEM-applet)# **event tag** *event\_1* **grtd slot all testing-type monitoring severity-major**

Ruijie(SEM-applet)# **action** *action\_1* **force-switchover**

Ruijie(SEM-applet)# **commit**

Ruijie(SEM-applet)# **exit**

Ruijie(config)#

## Verification

Ruijie# **show smart manager policy registered**

No.	Class	Event Type	Time Registered	Secu	Name
1	applet	grtd	Tue Mar 9 18:38:23 2010	none	policy_a

event\_1: grtd: slot all testing-type monitoring level severity-major

maxrun 20.000

action action\_1 force-switchover

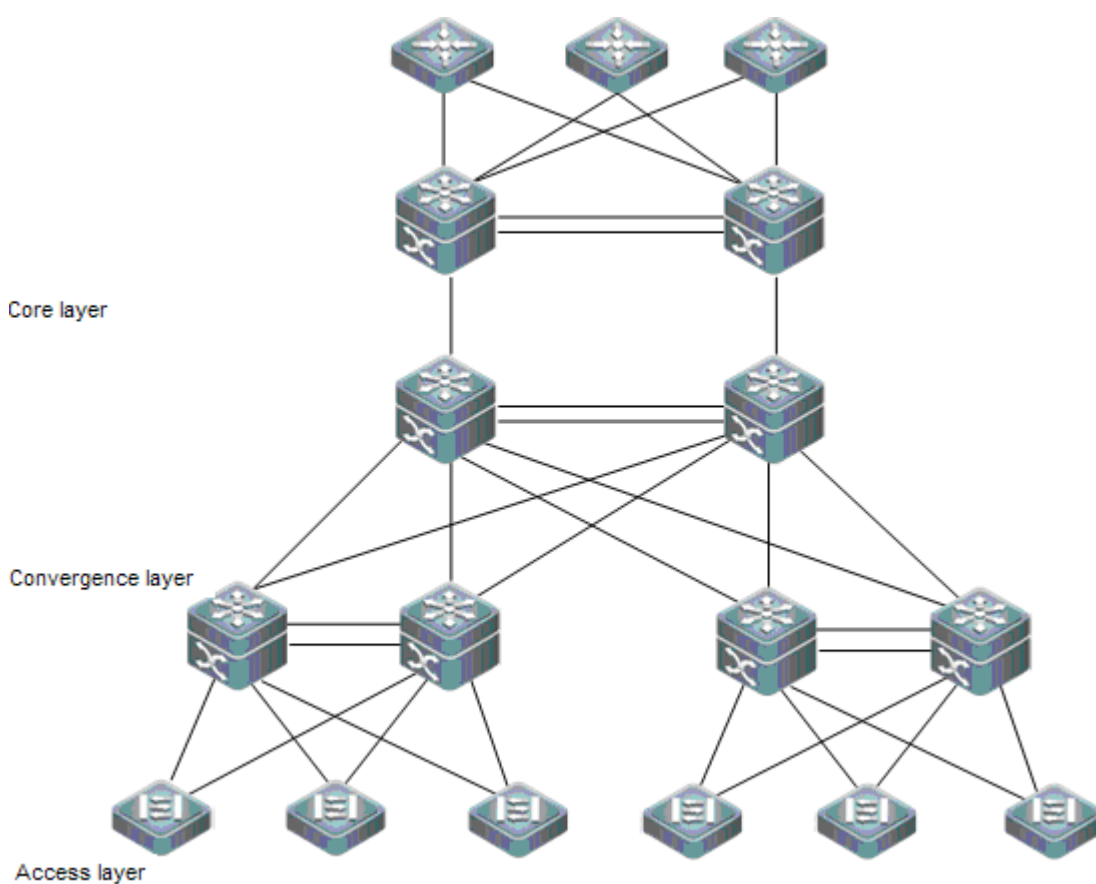
# VSU Configuration

## Overview

### Introduction

In order to improve the reliability of networks, the two devices at core layer and convergence layer of traditional networks are configured with two cores to provide redundancy. Access and convergence devices are respectively connected to the cores through two links. The following figure shows a typical traditional network architecture. Redundant network architecture increases the complexity of network design and operation. At the same time, a large number of redundant links reduce the utilization of network resources and return on investment.

Figure 1-1 Traditional network architecture



Virtual Switching Unit (VSU) is a kind of network system virtualization technology that supports combining multiple devices into a single virtualized device. As shown in Figure 1-2, access, convergence and core layer devices can respectively form VSUs, and then these VSUs connect to one another to form an end-to-end VSU network. Compared with traditional network, this networking can:

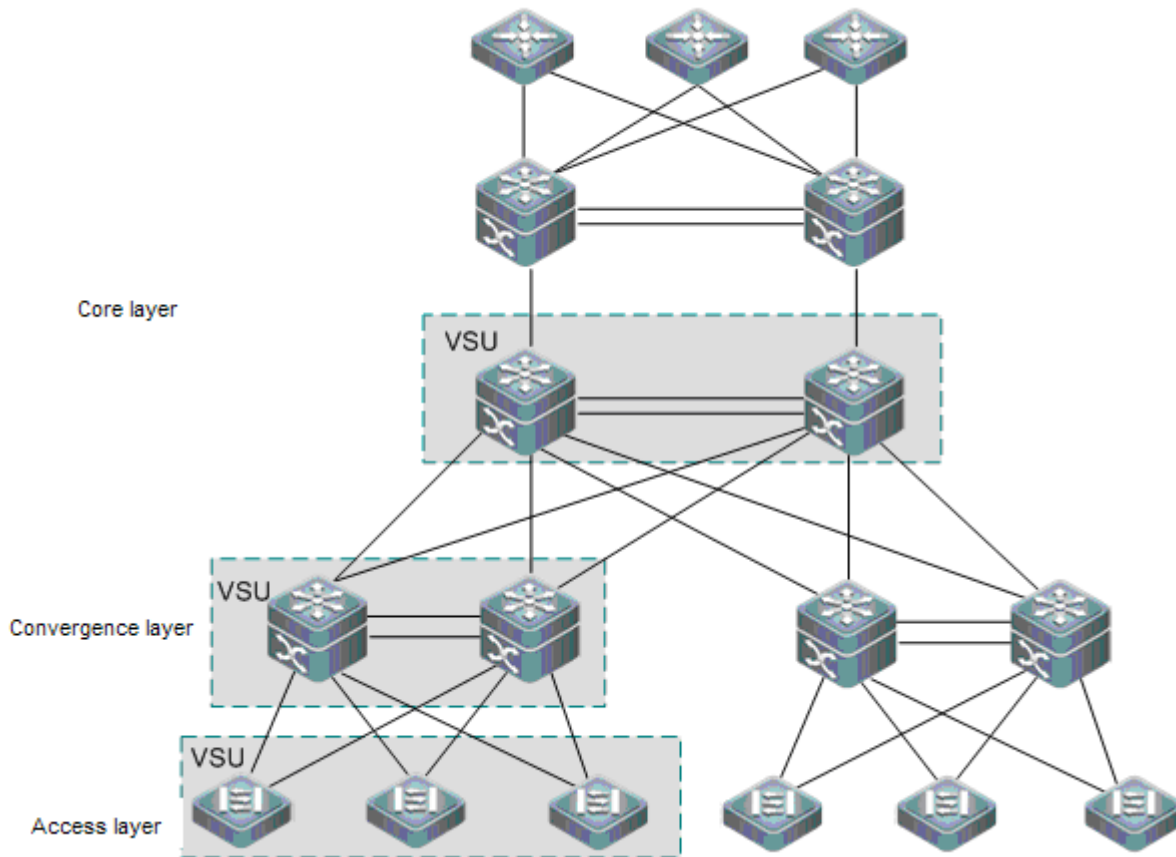
Simplify the network topology.

Reduce the costs of network management and maintenance.

Shorten application recovery time and service interruption time.

Enhance the utilization of network resources.

Figure 1-2 End-to-end VSU networking solution

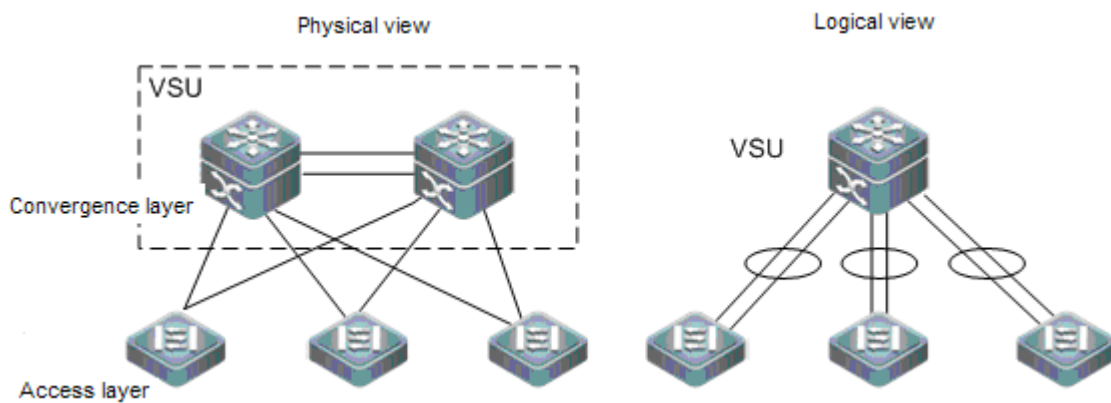


## Basic Concepts

### VSU system

VSU system is a single logical entity consisting of two or multiple devices in traditional network architecture. For example, the convergence layer VSU system as shown in the following figure can be seen as a single device that interacts with the core layer and access layer.

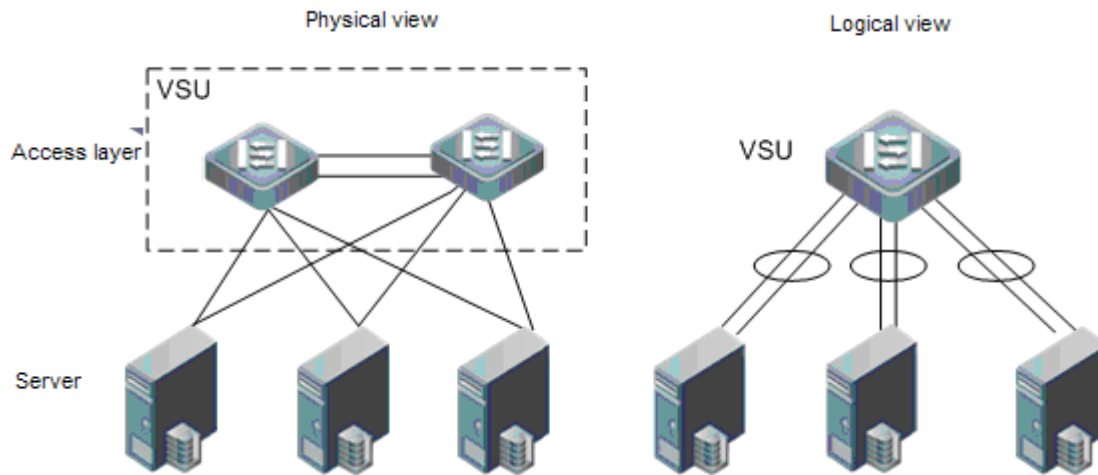
Figure 1-3 Convergence layer VSU





In the above VSU network structure, the member devices form a logical entity through internal links and the access layer devices are connected to the VSU through aggregated links. In this way, there is no layer 2 loop between the access and convergence layers. Additionally, VSU reduces the number of routers and simplifies layer 3 network topology.

Figure 1-4 Access layer VSU



Except the core and convergence layer devices, the access layer devices can also form a VSU system. A server that requires high availability can adopt multiple network cards to form an Aggregate Port (AP) to connect access layer devices. Since AP can only connect to the same access device, the risk of single device fault increases. In this case, VSU can be used to solve the problem. In the VSU mode, a server adopts multiple network cards and binds them into an AP to connect different member devices in the same VSU group. This way can prevent single point failure and network interruption caused by single link failure.

---

In comparison with traditional cassette device cooling stack, VSU has the following advantages:

1. VSU supports hot swap, namely, allowing inserting, removing and replacing member devices while the system operates.
  2. If a VSU system adopts ring topology, any device fault or VSL link disconnection does not affect the VSU system operation, that is, the VSU system does not restart or cut off the data flow.
- 

## VSU domain ID

A VSU domain has only one ID. Only the devices with the same domain ID can form a VSU system.

## Member device ID

Every member device in a VSU system has a unique ID, namely, Switch ID. Switch IDs can be used in device management or configuring interfaces on member devices. You need to configure an ID for a device when adding the device to a VSU system and ensure that the ID is unique in the same VSU system. If an ID conflict occurs, the VSU system will automatically assign IDs to the devices.

## Member device role

A VSU system consists of several devices. When establishing a VSU system, you need to select a global master device and a global slave device. All other devices are global candidate devices.

The global master device is responsible for controlling the entire VSU system, running control plane protocols and participating in data forwarding. Other devices, including the global slave devices and candidate devices, participate in data forwarding but do not run control plane protocols. All received control plane data flows are forwarded to the global master device for processing.

The global slave device also receive the statuses of the global master device in real-time and provide 1:1 redundancy with the global master device. If the global master device becomes faulty, the global slave device will take over services from the master device and manage the entire VSU system.

---

The following is the method for selecting the master device of a VSU system:

1. Rules for selecting the master device of a VSU system include (Continue with the next rule if the previous rule does not help in selecting the master device): a) Select the host as the master device (All devices are not master devices during startup). b) Select the device with the highest priority as the master device. c) Select the device with the smallest MAC address as the master device.
  2. Select the device that has the most familiar configurations with the master device as the slave device to prevent dual active devices. The selection order is: the nearest/the highest priority/the smallest MAC address.
  3. VSU system supports hot adding a support device. Even the hot added device has a higher priority than the master device has, the VSU system does not perform active/standby switch.
  4. The startup order of member device may affect the election of master device. A member device may not join in the VSU system because it starts up too slowly. In this case, the device will be hot added to the VSU system. Even the device has a higher priority than the master device, the VSU system does not perform active/standby switchover.
- 

## Hardware Requirements

There are two solutions for cassette device VSU system. Some products support both solutions and some products support only either of them.

Stacked module solution: Special stacked modules can provide high-bandwidth and low-cost connections. This solution requires special stacked modules and stacked cables. The distance between member devices is limited by the length of stacked cable.

Common port solution: Common ports can provide low-cost and long-distance connections. This solution does not require special stacked cables but provides relatively low bandwidth.

---

☒ The following table lists products supported on IS2700G series:

Product Name	Stacked Module	Common Port	Linear Topology	Ring Topology	Maximum Number of Member Devices
IS2700G series	Not support	Support	Support	Support	8

---

If stacked modules or stacked cables are used to establish a stacked system, refer to specific hardware instructions for the installation method.

VSU2.0 only supports the same series products forming VSU systems.

---

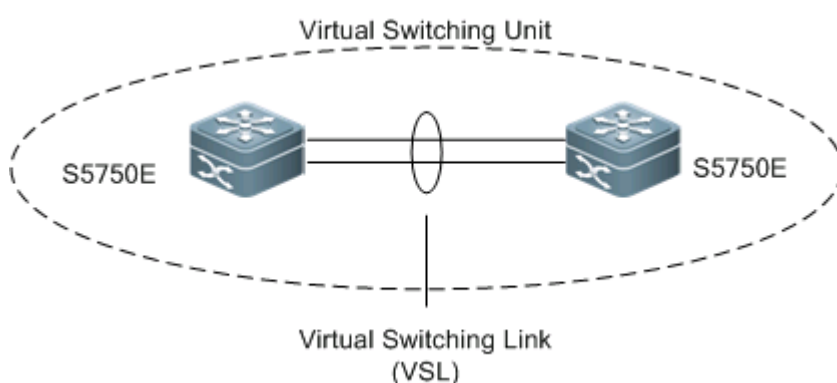
## Working Principles

### Virtual Switching Link (VSL)

#### VSL

The VSU system is a network entity that consists of multiple devices. These devices need to share control information and part of data streams. The VSL is a special link used for transmission of control information and data streams among devices of the VSU system. For example, the VSL can be established between two devices through 10 Gigabit Ethernet interfaces. Figure 1-5 shows the position of the VSL in the VSU system.

Figure 1-5 VSL



The VSL exists in the form of AP groups. The data streams transmitted through the VSL balance load among the aggregation port members according to the traffic balancing algorithm.

#### VSL traffic

The control streams transmitted through the VSL between devices include:

- 1) The protocol packets received by the member devices: These protocol packets need to be forwarded through the VSL to the global master device for processing.
- 2) The protocol packets processed by the global master device: These protocol packets need to be forwarded through the VSL to the interfaces of other member devices and then sent to the peer devices by these interfaces.

The data streams transmitted through the VSL between devices include:

- 1) The data stream flooded on the VLAN
- 2) The data streams that need to be forwarded across devices and transmitted through the VSL

Furthermore, the internal management packets of the VSU system are also transmitted through the VSL. The management packets include the protocol information switched by the hot backup and configuration information delivered by the host to other member devices.

---

In terms of the switched port analyzer (SPAN) function, the interface associated with the VSL cannot be regarded as the source port or destination port of the SPAN.

---

#### VSL failure

If a certain member link connected to the VSL AP group fails to work, the VSU will adjust the configurations of the VSL aggregation port automatically to prevent the traffic from being transmitted through the faulty member link.

If all member links are disconnected to the VSL AP group, the VSU topology will change. If the original VSU topology is a ring topology, the ring will convert into a line. For details, see topology ring and line conversion in the section of *Topology Changes*.

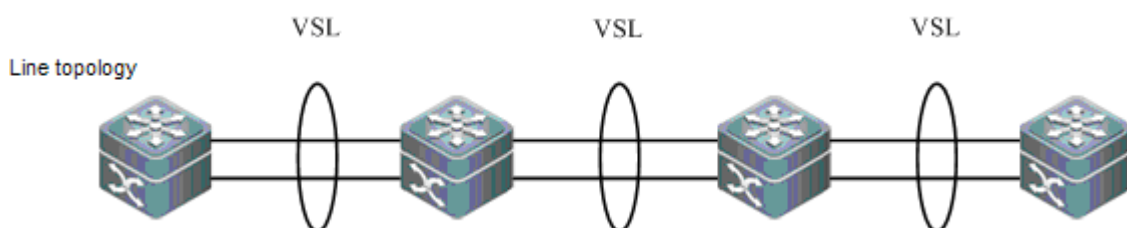
All member ports of a VSL-AP must be connected to the member ports of the same VSL-AP rather than the member ports of multiple VSL-APs. For example, the VSL-AP1 of Switch1 has two member ports a and b; the VSL-AP1 of Switch2 has two member ports c and d; the VSL-AP2 of Switch2 also has a member port e. If port a is connected to the port c, then port b must be connected to port d. You cannot connect port b to port e, or the system will disable ports b and e automatically.

If a member port of a VSL-AP is disabled, you can reconnect the disabled member port to a correct VSL-AP member to enable the disabled member port.

## Topology

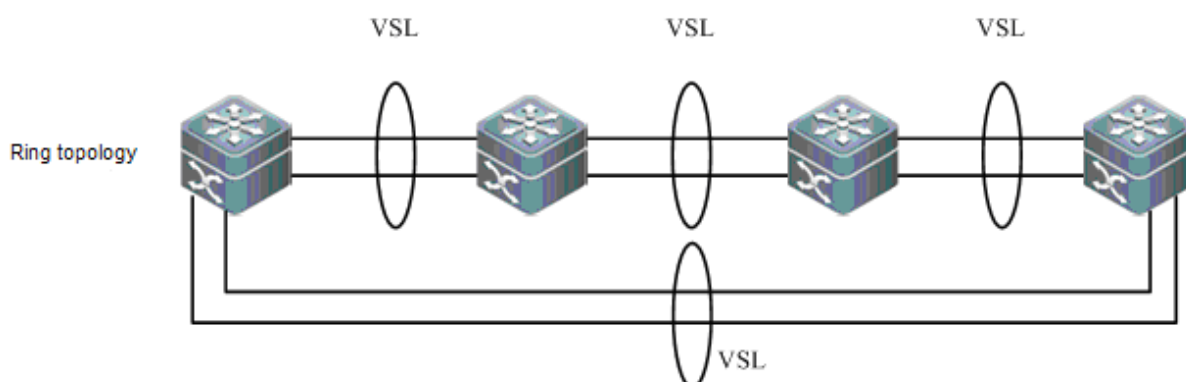
The VSU system supports line topology and ring topology. Devices are connected through a VSL to form a line that is called the line topology, as shown in Figure 1-6. The line topology is simple. It uses a very few ports and cables. Two devices are connected with a communication link only. Therefore, the VSL has low reliability.

Figure 1-6 Line topology



Except for the line topology, devices can also form a ring topology, as shown in Figure 1-7. In the ring topology, the two communication links between devices can back up for each other and perform link redundancy to improve the reliability of the VSU system.

Figure 1-7 Ring topology



You are advised to select the ring topology for the VSU system, thus the normal operation of the whole VSU system will not be affected by any single faulty device or VSL.

Expect for selecting the ring topology networking, you are advised to configure multiple VSLs for every VSL-AP to improve the reliability of a single VSL-AP.

## Topology Convergence

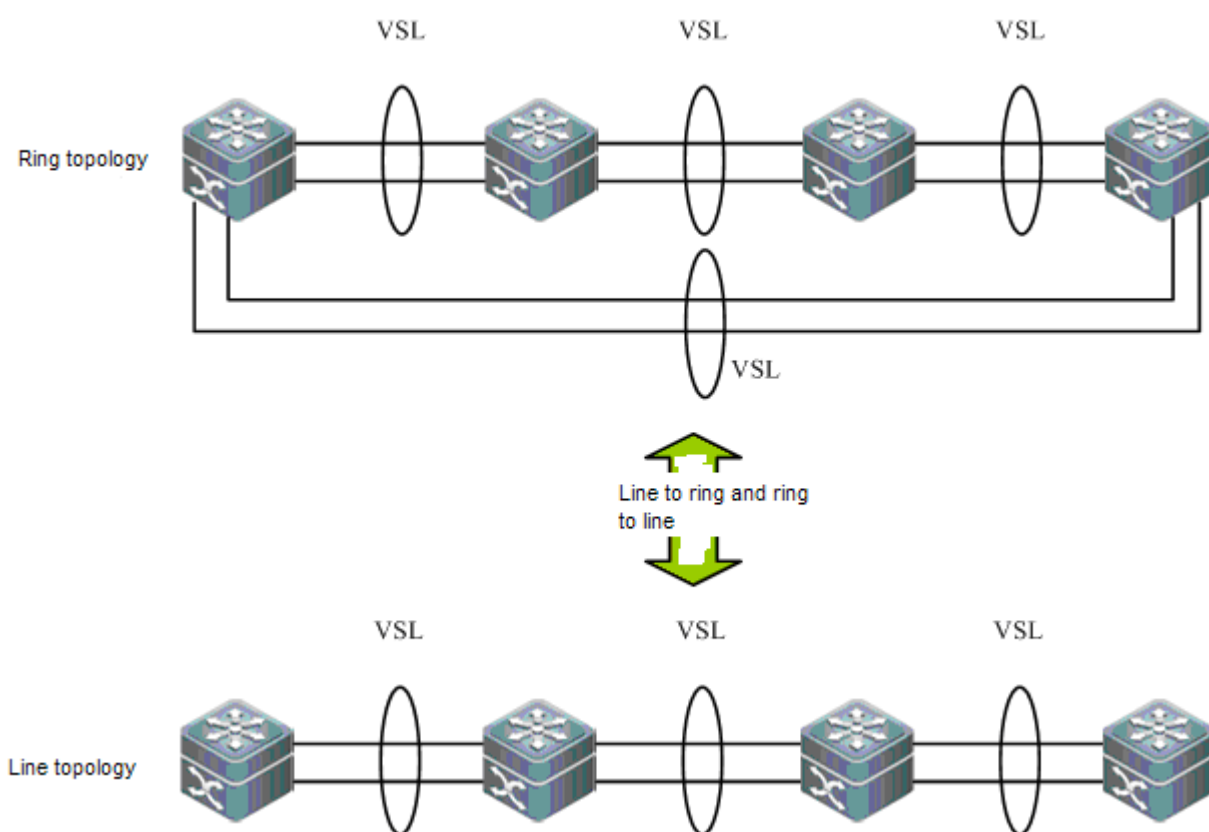
Before the establishment of the VSU, the member devices need to discover neighbors through topology discovery protocols and check devices in the VSU system to confirm the range of the management domain. Then a global master device is selected to manage the whole VSU system and a global slave device is selected for backup of the master device. Then the whole VSU topology is converged. As the start up time differs for different devices, the first convergence time of the topology is also different.

## Topology Changes

### Topology ring and line conversion

In a ring topology, if a VSL-AP link is disconnected, the ring topology will convert into a line topology. The whole VSU system will still run normally without network disconnection. To prevent other VSL-AP links and nodes from being faulty, you are advised to locate the VSL failures and recover the availability of the VSL. After the VSL-AP link is recovered, the line topology will convert into the ring topology.

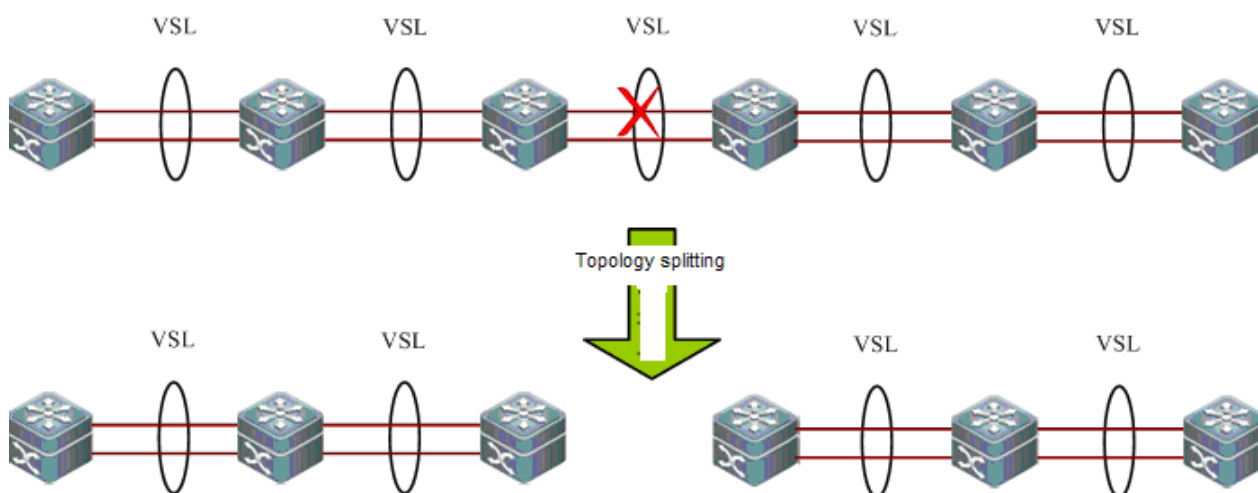
Figure 1-8 Ring-to-line and line-to-ring



### Topology splitting

In the line topology, if the VSL-AP link is disconnected, the line topology will be split, as shown in Figure 1-9. A VSU group is split into two groups. In this condition, two devices with the absolutely same configurations may exist on the network, which will cause abnormal operation of the network. Therefore, the multi-active detection (MAD) function (for details, see 1.1.4.6 Multi-Active Detection) needs to be deployed to solve the problem of topology splitting.

Figure 1-9 Topology splitting



### Topology combining

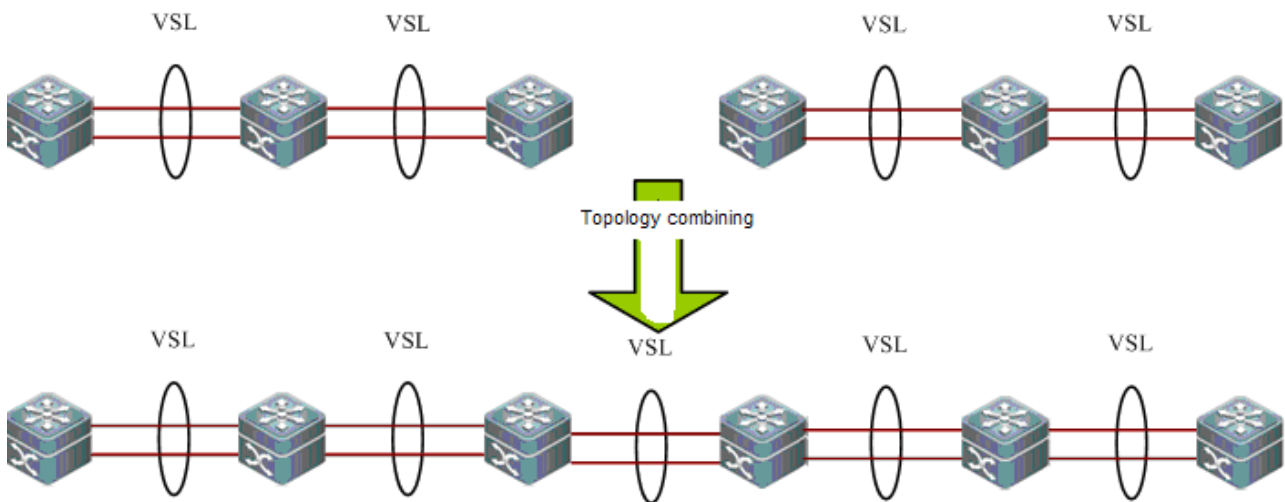
If the two VSU groups are connected through the VSL-AP link, the line topology will be combined. During the topology combining, restart one VSU group and then hot add the other VSU group.

The principle of topology combining: Minimizing influences on the services during topology combining. The rules are as follows (*Judge from the first item. If you cannot select the optimal topology, continue to judge the next item*):

- 1) Prioritize the VSU system with the highest priority of the GM members.
- 2) Prioritize the VSU system with the highest bandwidth of the up ports (VSL port excluded). For example, if the highest bandwidth of the up port of a VSU system is 40 G and that of the other VSU system is 10 G, the former VSU system is prioritized.
- 3) Prioritize the VSU system with the largest quantity of the up ports (VSL port excluded) that have the highest bandwidth. For example, two VSU systems both have the highest bandwidth of the up ports of 40 G. The VSU system with the most up ports is prioritized.
- 4) Prioritize the VSU system with the most up ports (VSL port excluded).
- 5) Prioritize the VSU system with the smallest MAC address of the GM.

Figure 1-10

Topology combining




---

During topology combining of two VSU groups, the two VSU groups need to be elected. The VSU group that fails the election will restart automatically and hot add to the other VSU group.

---

## Hot Backup

### Hot backup principle

According to the description above, the VSU system devices include the global master device, global slave device, and global candidate device. The global master device manages the whole VSU group and performs 1:1 hot backup with the global slave device. The global candidate device does not participate in the hot backup. If the global master device is faulty, the global slave device will upgrade to the master device to manage the whole VSU system. To implement the global hot backup, the master and slave devices must perform synchronization as follows:

- Status synchronization: The running status of the master device needs to be synchronized with that of the slave device to facilitate slave device's management instead of the master device at any time.
- Configuration synchronization: The running-config needs to be synchronized with the startup-config.

---

Although the global candidate device does not participate in the hot backup, the global configuration file `config.text` on the master device will be synchronized to all other member devices. In this way, even if the master and slave devices are both faulty, you can restart all remaining devices to recover the configurations.

---

### Member device fault recovery

The member device faults of the VSU system include:

- 1) If the global master device is faulty, the VSU system will perform hot backup master-slave switching. The original global slave device upgrades to the master device to manage the whole VSU group. The faulty device is restarted and hot added to the VSU system.
- 2) If the global slave device is faulty, the VSU system will not perform hot backup master-slave switching but elect a new global slave device from the remaining global candidate devices. The faulty device is restarted and hot added to the VSU system.
- 3) If the global candidate device is faulty, the VSU system will not perform hot backup master-slave switching. The faulty device is restarted and hot added to the VSU system.

The member device faults of the VSU system also have influences on the topology.

- 1) In terms of the line topology, a single faulty device may split a topology into two topologies. For details, see topology splitting in the section of *Topology Changes*.
- 2) In terms of the ring topology, a single faulty device may convert the ring topology into the line topology. For details, see topology ring and line conversion in the section of *Topology Changes*.

## Manual hot backup switching or restarting

You can perform hot backup switching and reset through the master device console interface.

- 1) Reset the whole VSU system by running the **reload** command to.
- 2) Restart a member device by running the **reload switch** [switchid] command or the **redundancy reload shelf** [switchid] command.
- 3) Clear the configurations of a device by running the **remove configuration switch** [switchid] command. Then this device will restart automatically.
- 4) Reset the global slave device by running the **redundancy reload peer** command. In terms of the shelves with double management modules, if you reset the global management module only, the overall device will not restart.
- 5) Perform hot backup master-slave switching for the VSU system by running the **redundancy forceswitch** command.

---

If the current VSU system has a line topology, when a certain device is restarted, the other devices may also be restarted simultaneously. For example, a topology is shaped as 1-2-3-4. When device 3 is restarted, device 4 will also be restarted. In this condition, the system will display a prompt for you to confirm whether to restart the devices or not.

---

## Dual-Active Detection

When the VSL is disconnected, the slave device switches to the master device. If the original master device is still running, a series of problems including IP address conflict on the LAN will be caused due to there are two master devices and their configurations are the same completely. In this condition, the VSU system must detect the two devices and take recovery measures. The VSU system provides two methods to perform MAD as follows:

- Bidirectional forwarding detection (BFD)
- AP-based detection

### BFD

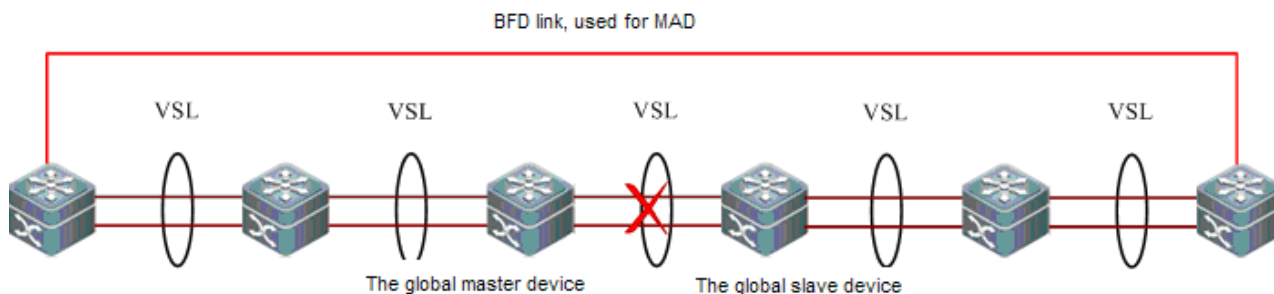
The VSU system supports the BFD to detect multiple master devices. Figure 1-11 shows the topology. A link is added for the two devices on the edges for MAD specially. When the VSL link is disconnected between the global master and slave devices, two master devices exist concurrently. If the BFD function is set, the two master devices will send the BFD packets to each other through the BFD link. Thereby the same devices are detected on the current system. Finally shut down the VSU system of a master device according to some rules (for details, see the topology combining rules in the section 1.1.4.4 *Topology Changes*) and enter the recovery state to avoid network abnormality.

The BFD-based detection provides especially dual-active rapid detection for the VSU dual-active networking scenario: When adopting VSU dual-active networking and configuring BFD-based detection, if a topology split occurs, the original master device is kept and the slave device enters the recovery state. Actually, when the dual-active rapid detection is using and a topology split occurs, there is only one device in the new topology where the original slave device resides.



This also applies to the scenario that one or multiple devices exist in the new topology where the original master device resides. In scenarios complying with the dual-active rapid detection, the dual-active rapid detection function takes effect in priority. If this function loses effect, the MAD takes effect.

Figure 1-11 BFD



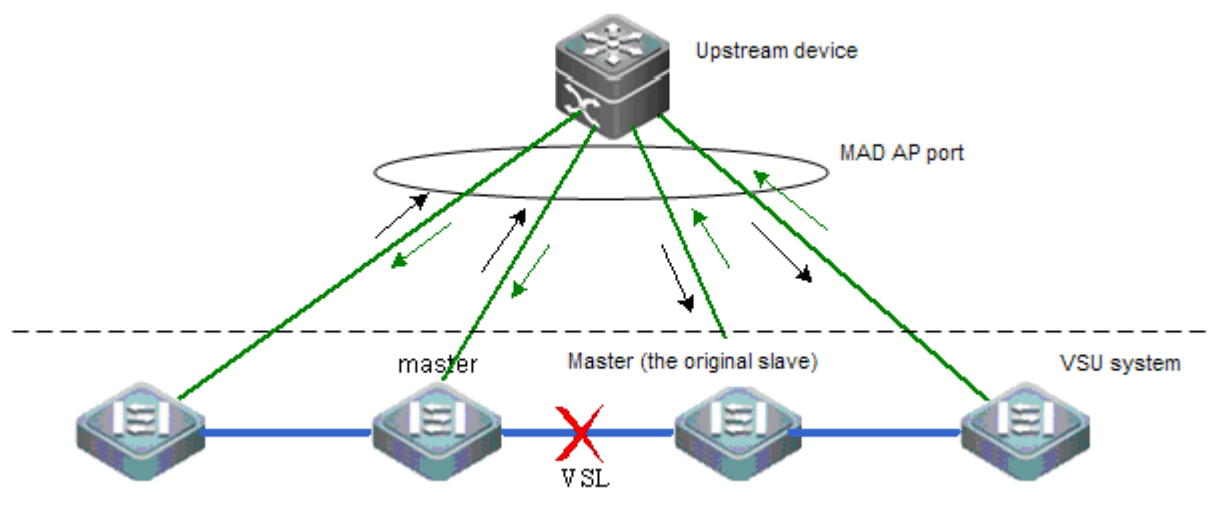
When there is a pair of BFD links, you are advised to deploy the detection links at the two ends of the topology.

You need to adopt the extension BFD and you cannot configure the dual-active detection port by using the existing BFD configurations and commands.

## MAD

The VSU system also supports the MAD dual-active detection mechanism. Figure 1-12 shows the topology. The VSU system and the upstream device both need to support the MAD function. When the VSL link is disconnected, two master devices exist concurrently. The two master devices respectively send the MAD packets to the member ports of the MAD-APs and then the MAD packets are forwarded to each other through the upstream device. As shown in Figure 1-12, the MAD-AP has four member ports. Each member port is connected to a different device of the VSU system. When the topology splitting occurs, the four member ports all send and receive the MAD packets. Thereby the same devices are detected on the current system. Finally shut down the VSU system of a master device according to some rules (for details, see the topology combining rules in the section 1.1.4.4 *Topology Changes*) and enter the recovery state to avoid network abnormality.

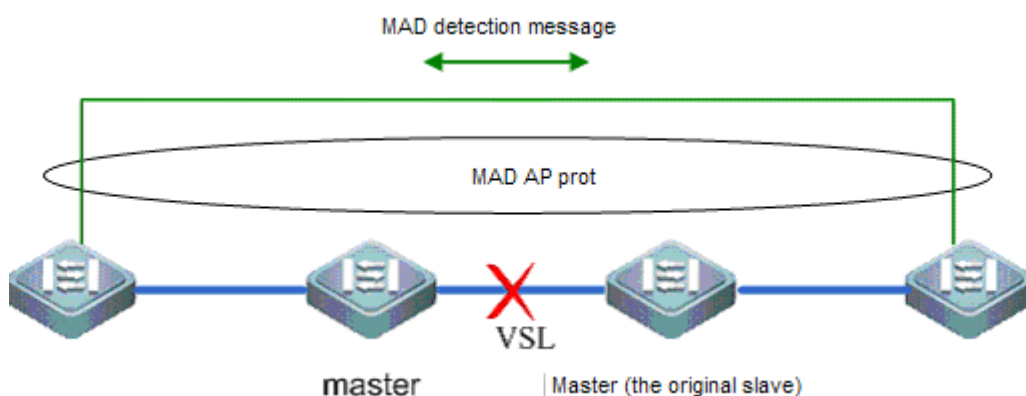
Figure 1-12 MAD based on upstream and downstream devices



☒ In the topology above, the upstream device must be Ruijie device and support the MAD packet forwarding function.

The MAD can also be deployed similar to the BFD. Figure 1-13 shows the connection topology. Add the physical detection ports of the two devices at the edges to a same MAD-AP. When the VSL link is disconnected between the global master and slave devices, the members of the MAD-AP start to detect multiple devices. After multiple devices are detected, shut down the VSU system of a master device according to the topology combining rules and then enter the recovery state to avoid network abnormality

Figure 1-13 MAD based on directly-connected devices



The MAD based on directly-connected devices is the same to the BFD in terms of the detection effect. The MAD is applied to all layer 3 devices and layer 2 devices. The BFD can be applied to layer 3 devices only.

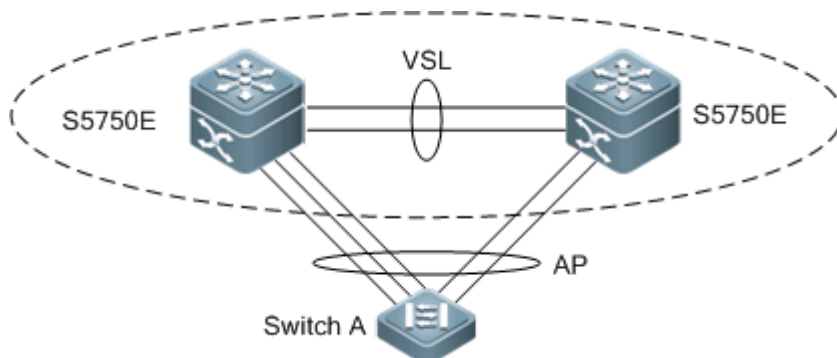
## External Connection of VSU Devices

### Cross-device AP group

An AP binds multiple physical links together to form a logical link. The VSU system supports the AP across the member devices.

As shown in Figure 1-14, two devices form a VSU group. The external access device Switch A is connected to the VSU in the form of the AP. In terms of Switch A, there is no difference between the AP in Figure 1-14 and the common AP group.

Figure 1-14 Cross-device aggregation port



## Troubleshooting

You are advised to configure the cross-device AP with the physical link between the peripheral device and each VSU device. On the one hand, the VSL bandwidth can be reserved (prioritize the AP member of the same chassis as the egress to transmitted the cross-chassis AP traffic and prevent unnecessary traffic from being transmitted through the VSL link). On the other hand, the network reliability can be improved (if a certain chassis is faulty, the member ports of normal devices can work normally).

The follows sections describe the possible faults of the cross-device AP and the consequences

#### ■ Single link failure

If a single link of the cross-device AP is faulty but other links still work normally, the cross-device AP will reallocate the traffic for the remaining normal links.

#### ■ Link failure of all cross-device AP member ports on the global master device

If the links of all cross-device AP member ports on the global master device fail to work, only the member ports of other member devices continue working normally. In terms of the data stream transmitted through the AP to the VSU system, if the data stream forwarding egress is on the global master device, the system will forward the data stream to the corresponding egress on the global master device through the VSL link.

The control plane protocols are still running on the global master device. Therefore, the protocol packets that enter the VSU system need to be forwarded to the global master device through the VSL link for protocol computing.

#### ■ Failure of all links of other member devices

If all links of the cross-device AP and a single device A fail to work, only the member ports of other member devices continue working normally. In terms of the data stream transmitted through the AP to the VSU system, if the data stream forwarding egress is on the member device A, the system will forward the data stream to the corresponding egress on the member device A through the VSL.

#### ■ All link failure

If all links of the cross-device AP fail to work, the AP state shifts into the Link-Down, as processing for the common AP.

#### ■ Global master device fault

If the global master device is faulty, the hot backup switching is performed to switch the original slave device to the master device. Meanwhile, the member ports on other member devices continue working. The link failure is detected on the peer device connected to the VSU through this AP. Therefore, the traffic balancing algorithm needs to be adjusted to allocate the data stream to normal links.

#### ■ Member device fault

If a member device is faulty, the AP member link connected to this member device is disconnected. However, other member links still work normally. The link failure is detected on the peer device connected to the VSU through this AP. Therefore, the traffic balancing algorithm needs to be adjusted to allocate the data stream forwarding paths to normal links.

## System Management

### Access to the console

The master device console of VSU system manages multiple devices on the system simultaneously. The consoles of the slave and candidate devices do not support command line input. However, you can configure the VSU system on the

master device for a specified member device and log in to the master device console through the serial port of the slave device.

### Cable clip naming

In terms of the chassis device, in the VSU mode, the cable clip is named with the device number (Switch ID). Therefore, the cable clip number turns from one-dimensional into two-dimensional. For example, cable clip 1/1 indicates the cable clip numbered 1 of the slot 1 on a member device.

### Interface naming

In the VSU working mode, a slot number may occur in multiple devices. Therefore, the interface is named with the device number (Switch ID).

For example, interface gigabitEthernet 1/0/1 indicates the Gigabit port 1 on the slot 0 of the device whose ID is 1; interface gigabitEthernet 2/0/2 indicates the Gigabit port 2 on the slot 0 of the device whose ID is 2.

### Access to the file system

In the VSU working mode, you can access to the file system on other member devices from the master device. The detailed access method is the same to that of the local file system. The unique difference is that different URL prefixes are used.

### System upgrade

Generally the VSU system requires version consistency of the main program version numbers of the member devices. However, there are so many member devices that it takes too much time and energy to perform upgrade one by one in the standalone mode and it is also easy to make mistakes. Ruijie switches provide consummate system upgrade solution to help you with system upgrade by adopting the two methods as follows:

- When the VSU system is being established: the system will automatically align the main program version numbers of all member devices. Once the main program versions are discovered inconsistency, the main program of the master device will be selected to be synchronized to all member devices.
- After the VSU system is established: the main program version will be synchronized to all member devices automatically by using the file that is downloaded by the TFTP.

### SYSLOG

All member devices of the VSU system can display the SYSLOG. The SYSLOG generated by the master device is displayed on the master device console with the same format to that in the standalone mode. The SYSLOG generated by other member devices is also displayed on the master device console, but the message format is different from that in the standalone mode because the device number information is added.

For example, the SYSLOG information generated in the standalone state is "%VSU-5-DTM\_TOPO\_CVG:Node discovery done. Topology converged." The SYSLOG information generated by the member device numbered 3 is "%VSU-5-DTM\_TOPO\_CVG:(3) Node discovery done. Topology converged."

### Typical Cases

For details, see part of the descriptions of the VSU system in section 1.1 1 *Introduction*.

## VSU Configuration

### Default configuration

Configuration	Default Value
Switch working mode	Standalone
Switch ID in the VSU mode	1
Switch priority in the VSU mode	100
VSL member port in the VSU mode	None
Spare configurations of the chassis	None

### Configuration steps

Step	Task	Description
1	Set VSU parameters in the standalone mode.	Mandatory
2	Set VSU parameters in the VSU mode.	Optional
3	Reconfigure the member devices.	Optional
4	Perform manual hot backup switching.	Optional
5	Reset the device.	Optional

### Setting VSU Parameters in the Standalone Mode

The switch works in the standalone mode by default. Therefore, before establishing the VSU system, you can start up the switch in the standalone mode to set relevant VSU parameters. The follows sections describe how to set VSU parameters in the standalone mode.

### Configuring VSU Attributes

You need to set the same domain ID on the two chassis of the established VSU system. The domain ID must be unique on the local area network (LAN). Furthermore, you need to set the ID of each chassis in the virtual device. The switch starts up in the standalone mode by default. You can configure the switch by using the following command.

Command	Function
Ruijie(config)# <b>switch virtual domain</b> <i>domain_id</i>	Set the domain ID whose range is 1-255.
Ruijie(config-vs-domain)# <b>switch</b> <i>sw_id</i>	Set the switch ID in the virtual device. The range of the switch ID is 1-16.
Ruijie(config-vs-domain)# <b>switch</b> <i>sw_id</i> <b>priority</b> <i>priority_num</i>	The priority range of the <i>priority_num</i> is 1-255, 100 by default. The more the value is, the higher the priority is.
Ruijie(config-vs-domain)# <b>switch</b> <i>sw_id</i> <b>description</b> <i>switch1</i>	Set an alias for the switch with a maximum of 32 characters (optional).
Ruijie(config-vs-domain)# <b>exit</b>	Exit the virtual switch configuration mode.

Configuration precautions:

1. The command used for configuring a priority can modify the priority only rather than modify a switch ID. Therefore, you must enter the current switch ID correctly for the configuration. For example, you have set the switch ID to 1. If you enter **switch 2 priority 100**, the priority configuration cannot take effect.
2. The syntax of the command used for alias configuration is similar to that of the priority configuration.

## Configuring the VSL

To establish the VSU system, you need to decide which ports are configured as the VSL member ports. Configure the VSL member ports of the switch by running the commands as follows:

Command	Function
Ruijie(config)# <b>vsl-aggregateport</b> <i>ap-num</i>	VSLs exist in the form of aggregation ports. Enter the configuration mode of the VSL-AP aggregation ports first. <b>ap_num</b> indicates the VSL-AP aggregation port number. A switch can be configured with two VSL-APs whose number can be 1 or 2 only.
Ruijie(config-vsl-ap-1)#[no] <b>port-member interface</b> <i>interface-name</i> [ <b>copper</b>   <b>fiber</b> ]	Add or delete a member port of the VSL-AP link. <b>interface-name</b> indicates the two-dimensional port name in the standalone mode. The two-dimensional port can be the 10 Gigabit interface or Gigabit interface. (The Gigabit interface can be an optoelectrical interface. If the media type is not specified, the Gigabit electrical interface is adopted by default.)
Ruijie(config-vsl-ap-1)# <b>exit</b>	Exit the VSL-AP configuration mode.

Configuration precautions:

1. In the standalone mode, the VSL-AP configurations cannot take effect immediately unless the device shifts into the VSU mode and restart.
2. The attributes of the member ports that belong to the same VSL-AP must be the same. For example, the VSL-AP can consist of two 10 Gigabit electrical interfaces rather than a 10 Gigabit electrical interface and a Gigabit electrical interface or a 10 Gigabit electrical interface and a 10 Gigabit optical interface.
3. In terms of the optoelectrical interface, the optical or electrical attributes must be displayed before it is added to the VSL-AP.

## Viewing VSU Parameters

In the standalone mode, view the current VSU configurations by running the command as follows:

Command	Function
Ruijie# <b>show switch virtual config</b>	View VSU configurations of the current switch in the standalone mode.

Configuration notes:

1. The relevant VSU configurations are set for a single physical switch and the configuration information is stored in the special configuration file config\_vsu.dat. Therefore, you can view the current relevant VSU configurations by running the **show switch virtual config** command rather than the **show running config** command
2. In the standalone mode, the VSU running information is null. When you enter commands such as the **show switch virtual** command, the system will prompt you that the switch is in the standalone mode and there is no VSU running information.

The follows example displays how to set and view VSU parameters in the standalone mode.

```

Ruijie(config)#switch virtual domain 1
Ruijie(config-vs-domain)#switch 1
Ruijie(config-vs-domain)# switch 1 priority 200
Ruijie(config-vs-domain)# switch 1 description buildingA
Ruijie(config-vs-domain)#exit
Ruijie(config)#vsl-aggregateport 1
Ruijie(config-vsl-ap)# port-member interface GigabitEthernet 0/1
Ruijie(config-vsl-ap)# port-member interface GigabitEthernet 0/2
Ruijie(config-vsl-ap)# exit
Ruijie(config)# exit
Ruijie# show switch virtual config
sw_id: 1 (mac: 00d0.f810.3323)
!
switch virtual domain 1
!
switch 1
switch 1 priority 200
switch 1 description buildingA
!
vsl-aggregateport 1
port-member interface GigabitEthernet 0/1
port-member interface GigabitEthernet 0/2
!
Switch convert mode standalone
!
Ruijie#show switch virtual
Current system is running in "STANDALONE" mode.

```

## Shifting from the Standalone Mode to the VSU Mode

In the standalone mode, the software will take the following actions after you run the **switch convert mode virtual** command.

- 1) Back up the global configuration file config.text in the standalone mode as standalone.text for subsequent use.
- 2) Clear the contents of the configuration file config.text.
- 3) Write the relevant VSU configurations to the special configuration file config\_vsu.dat.

If there is a virtual\_switch.text file on the switch, the system will prompt you whether to overwrite the contents of the file virtual\_switch.text to the file config.text (the file virtual\_switch.text is a backup file for the file config.text when the switch shifts from the VSU mode to the standalone mode). Then you can click **Yes** or **No**. Finally the switch restarts in the VSU mode and reads VSU parameters in the file config\_vsu.dat. Shift the switch from the standalone mode into the VSU mode by running the command as follows:

Command	Function
Ruijie# <b>switch convert mode virtual</b>	Shift the switch from the standalone mode into the virtual switching mode, that is, VSU mode.

If the current switch has been in the VSU mode, you are not allowed to shift the switch into the VSU mode again. In other words, the command above is invalid.

The following examples show how to shift the switch from the standalone mode into the VSU mode.

Example 1:

```
Ruijie# switch convert mode virtual
Do you want to convert switch to virtual mode[yes/no]: yes
Do you want to recover "config.text" from "virtual_switch.text" [yes/no]: yes
```

Example 2:

```
Ruijie# switch convert mode virtual
System is running in virtual mode, can't convert to virtual mode again.
```

## Setting VSU Parameters in the VSU Mode

If the switch has been working in the VSU mode, the VSU configurations differ from those in the standalone mode. The following sections describe how to set VSU parameters in the VSU mode.

- Configure VSU attributes (optional).
- Configure the VSL (optional).
- Configure the dual-active detection (optional).
- Configure the flow load balancing (optional).
- Shift from the standalone mode into the VSU mode (optional).

## Configuring VSU Attributes

During the VSU system running, you can modify the domain ID, switch ID, and priority of the master device or the slave device. However, you can only log in to the VSU master device console to modify these parameters. You are not allowed to enter the global configuration mode on the slave device console. The following commands show how to modify VSU parameters of the master device or the slave device in the VSU mode.

Command	Function
Ruijie (config)# <b>switch virtual domain</b> <i>domain_id</i>	Enter the domain configuration mode. Currently the VSU domain ID is <i>domain_id</i> .
Ruijie(config-vs-domain)# <b>switch</b> <i>sw_id</i> <b>domain</b> <i>new_domain_id</i>	Modify the domain ID of the current switch numbered <i>sw_id</i> to <i>new_domain_id</i> .
Ruijie(config-vs-domain)# <b>switch</b> <i>sw_id</i> <b>renumber</b> <i>new_sw_id</i>	Modify the ID of the current switch numbered <i>sw_id</i> to <i>new_sw_id</i> .
Ruijie(config-vs-domain)# <b>switch</b> <i>sw_id</i> <b>priority</b> <i>new_priority_num</i>	Modify the priority of the current switch numbered <i>sw_id</i> to <i>new_priority_num</i> .
Ruijie(config-vs-domain)# <b>switch</b> <i>sw_id</i> <b>description</b> <i>switch1</i>	Set an alias for the switch with a maximum of 32 characters (optional).
Ruijie(config-vs-domain)# <b>exit</b>	Exit the virtual switch configuration mode.
Ruijie# <b>write</b>	Save the configurations to the file.



Command	Function
Ruijie# <b>show switch virtual [topology   config]</b>	Display the current VSU running information, topology, or configuration parameters.

Command descriptions:

1. Among the commands above, the all configuration commands take effect only after the switch restarts except the **switch sw\_id description switch1** command that can take effect immediately.
2. You can view the VSU running information or configuration parameters only by running the **show switch virtual [config]** command rather than the **show running config** command.

The following examples describe how to configure or display the relevant VSU status and parameters in the VSU mode.

#1 Display the original running information and configuration parameters in the VSU mode as follows:

```
Ruijie#show switch virtual
Sw_id      Domain_id    Priority    Status    Role
-----
1 (1)      1 (1)          100 (100)   OK        ACTIVE
2 (2)      1 (1)          100 (100)   OK        CANDIDATE
3 (3)      1 (1)          100 (100)   OK        STANDBY
```

Descriptions of the preceding lines:

1. The numerical values outside the parentheses indicate the current running parameters. The numerical values inside the parentheses indicate the configuration parameters in the config\_vsu.dat file. For example, 200(200) indicates that the current running priority and the set priority are both 200.
2. The member devices have two status values including OK and recovery.

# View the topology information of the VSU group.

```
Ruijie # show switch virtual topology
Chain Topology:
[1]---[2]---[3]---[4]
switch[1] (mac: 001a.a97e.1111, description: switch1):
    vsu-ap[1] <--> vsu-ap[1] of switch[2]
switch[2] (mac: 001a.a97e.2222, description: switch2):
    vsu-ap[1] <--> vsu-ap[1] of switch[1]
    vsu-ap[2] <--> vsu-ap[1] of switch[3]
switch[3] (mac: 001a.a97e.3333, description: switch3):
    vsu-ap[1] <--> vsu-ap[2] of switch[2]
    vsu-ap[2] <--> vsu-ap[1] of switch[4]
switch[4] (mac: 001a.a97e.4444, description: switch4):
    vsu-ap[1] <--> vsu-ap[2] of switch[3]
```

The preceding lines indicate that the VSU-AP1 of the switch 1 is connected to the VSU-AP1 of the switch 2; the VSU-AP2 is connected to the VSU-AP1 of the switch 2; the rest may be deduced by analogy.

# View the VSU configuration information.

```
Ruijie#show switch virtual config
switch id: 1 (mac: 00d0.f810.1111) → The factory MAC address of each switch is changeless.
!
switch virtual domain 1
!
switch 1
switch 1 priority 100
switch 1 description switch1
!
vsl-aggregateport 1
port-member interface GigabitEthernet 0/1
port-member interface GigabitEthernet 0/2
!
Switch convert mode virtual
!

sw_id: 2 (mac: 00d0.f810.2222)
!
switch virtual domain 1
!
switch 2
switch 2 priority 100
switch 2 description switch2
!
vsl-aggregateport 1
port-member interface GigabitEthernet 0/1
port-member interface GigabitEthernet 0/2
!
Switch convert mode virtual
!

sw_id: 3 (mac: 00d0.f810.3333)
!
switch virtual domain 1
!
switch 3
switch 3 priority 100
switch 3 description switch3
!
vsl-aggregateport 1
port-member interface GigabitEthernet 0/1
port-member interface GigabitEthernet 0/2
!
Switch convert mode virtual
!

sw_id: 4 (mac: 00d0.f810.4444)
!
```

```

switch virtual domain 1
!
switch 4
switch 4 priority 100
switch 4 description switch4
!
vsl-aggregateport 1
port-member interface GigabitEthernet 0/1
port-member interface GigabitEthernet 0/2
!
Switch convert mode virtual
!

```

#2 Modify the relevant configurations and display the configurations again.

```

Ruijie(config)#switch virtual domain 1
Ruijie(config-vs-domain)#switch 1 domain 5
Ruijie(config-vs-domain)#switch 1 renumber 2
Ruijie(config-vs-domain)#switch 1 priority 150
Ruijie(config-vs-domain)#switch 2 domain 6
Ruijie(config-vs-domain)#switch 2 renumber 1
Ruijie(config-vs-domain)#switch 2 priority 250
Ruijie(config-vs-domain)#exit
Ruijie#show switch virtual

```

Sw_id	Domain_id	Priority	Status	Role
1(2)	1(5)	100(150)	OK	ACTIVE
2(1)	1(6)	100(250)	OK	CANDIDATE
3(3)	1(1)	100(100)	OK	STANDBY

```

Ruijie#show switch virtual config
sw_id: 1 (mac: 00d0.f810.1111) → Change the ID of the switch whose MAC address is 1111 to 2.
!
switch virtual domain 5 → Change the domain ID to 5.
!
switch 2
switch 2 priority 150 → Change the priority to 150.
switch 2 description switch1
!
vsl-aggregateport 1
port-member interface GigabitEthernet 0/1
port-member interface GigabitEthernet 0/2
!
Switch convert mode virtual
!

sw_id: 2 (mac: 00d0.f810.2222) → Change the ID of the switch whose MAC address is 2222 to 1.

```

```
!  
switch virtual domain 6 → Change the domain ID to 6.  
!  
switch 1  
switch 1 priority 250 → Change the priority to 250.  
switch 1 description switch2  
!  
vsl-aggregateport 1  
port-member interface GigabitEthernet 0/1  
port-member interface GigabitEthernet 0/2  
!  
Switch convert mode virtual  
!  
sw_id: 3 (mac: 00d0.f810.3333)  
!  
switch virtual domain 1  
!  
switch 3  
switch 3 priority 100  
switch 3 description switch3  
!  
vsl-aggregateport 1  
port-member interface GigabitEthernet 0/1  
port-member interface GigabitEthernet 0/2  
!  
Switch convert mode virtual  
!  
sw_id: 4 (mac: 00d0.f810.4444)  
!  
switch virtual domain 1  
!  
switch 4  
switch 4 priority 100  
switch 4 description switch4  
!  
vsl-aggregateport 1  
port-member interface GigabitEthernet 0/1  
port-member interface GigabitEthernet 0/2  
!  
Switch convert mode virtual  
!
```

The switch restarts after the configurations are modified. Only the domain\_ids of switch 3 and switch 4 are both 1. Switch 1 and switch 2 cannot add to the VSU system with the domain\_id of 1.

## Configuring the VSL

The relevant commands are as follows:

Command	Function
Ruijie(config)# <b>vsl-aggregateport</b> <i>sw_id/vsl_ap_num</i>	sw_id indicates the switch ID to set. vsl_ap_num indicates the number of the VSL-AP aggregation port with a range of 1-2.
Ruijie(config-vsl-ap-1/1)# <b>[no]port-member interface</b> <i>interface-name</i> <b>[copper   fiber ]</b>	Add or delete a member port of the VSL-AP link. Configure the VSL-AP1 link of the switch numbered 1. interface-name indicates the name of the two-dimensional port.
Ruijie(config-vsl-ap-1/1)# <b>end</b>	Exit the VSL-AP configuration mode.
Ruijie# <b>show switch virtual link [port]</b>	View the current VSL-AP running information.

Configuration precautions:

1. The attributes of all member ports that belong to a same VSL-AP must be the same.
2. During the VSU running, the real-time configured VSL member links take effect in three minutes after the configuration and any command operated on these VSL member links does not take effect.
3. Add a member port number that must be a two-dimensional port number. For example, enter the VSL-AP-1/1 configuration mode and run the **port-member interface** *GigabitEthernet 0/1* command to add the global 3D port 1/0/1 to the VSL-AP1 of the switch numbered 1.

Configuration examples:

#1 Display the current VSL-AP status as follows:

```
Ruijie#show switch virtual link
```

VSL-AP	State	Peer-VSL	Rx	Tx	Uptime
-----					
1/1	UP	3/2	25398921	25398921	0d, 0h, 25m
1/2	UP	2/1	50797842	50797842	0d, 0h, 25m
3/1	UP	2/2	50031614	50031614	0d, 0h, 25m
3/2	UP	1/1	25015807	25015807	0d, 0h, 25m
2/1	UP	1/2	50071394	50071394	0d, 0h, 25m
2/2	UP	3/1	50071394	50071394	0d, 0h, 25m

#2 Display the state of each VSL-AP member port as follows:

```
Ruijie# show switch virtual link port
```

VSL-AP-1/1:

Port	State	Peer-port	Rx	Tx	Uptime
-----					
GigabitEthernet 1/0/21	OK	GigabitEthernet 2/0/22	171753	171753	0d, 0h, 25m

VSL-AP-1/2:

Port	State	Peer-port	Rx	Tx	Uptime
-----					
GigabitEthernet 1/0/22	OK	GigabitEthernet 2/0/21	171753	171753	0d, 0h, 25m

VSL-AP-2/1:

Port	State	Peer-port	Rx	Tx	Uptime
-----					
GigabitEthernet 2/0/21	OK	GigabitEthernet 1/0/22	170501	170501	0d, 0h, 25m

VSL-AP-2/2:

Port	State	Peer-port	Rx	Tx	Uptime
-----					
GigabitEthernet 2/0/22	OK	GigabitEthernet 1/0/21	170501	170501	0d, 0h, 25m

Descriptions of the preceding lines:

1. Peer-port indicates the member port of the peer VSL-AP. The VSL-AP state has two values including: **DOWN** and **UP**.
2. **Rx/Tx** indicates the statistical value (number of the packets) of the packets received and sent by this member port.
3. The member port has four state values including **DOWN**, **DISABLE**, **UP**, and **OK**. **DOWN** indicates the current port is in the LINK DOWN state physically. **DISABLE** indicates the current port is misconnected physically and the receiving and sending functions are disabled. **UP** indicates the current port is in the LINK UP state physically, but the peer port has not been detected an effective VSL-AP member port. **OK** indicates the current port is in the LINK UP state physically, and the peer port has been detected an effective VSL-AP member port.

## Configuring the Dual-Active Detection

To prevent the dual-active is being generated, you need to configure the relevant detection mechanism. The dual-active detection can be configured in the VSU mode only. You are not allowed to configure the dual-active detection mechanism in the standalone mode.

### Configuring the BFD dual-active detection

The BFD dual-active detection requires establishing a directly connected link between two switches. The ports on the two ends must be physical routing ports. Configure the BFD dual-active detection by running the commands as follows:

Command	Function
Ruijie(config)# <b>interface</b> <i>interface-name1</i>	Enter the interface configuration mode of the detection interface 1.
Ruijie(config-if)# <b>no switchport</b>	Set the detection interface 1 to a routing interface.

Ruijie (config-if)# <b>end</b>	Exit the interface configuration mode of the detection interface 1.
Ruijie(config)# <b>interface</b> <i>interface-name2</i>	Enter the interface configuration mode of the detection interface 2.
Ruijie(config-if)# <b>no switchport</b>	Set the detection interface 2 to the routing interface.
Ruijie(config-if)# <b>end</b>	Exit the interface configuration mode of the detection interface 2.
Ruijie(config)# <b>switch virtual domain</b> <i>number</i>	Enter the virtual switch configuration mode.
Ruijie(config-vs-domain)# <b>dual-active detection bfd</b>	Enable the BFD dual-device detection switch that is disabled by default.
Ruijie(config-vs-domain)# <b>dual-active pair interface</b> <i>interface-name1</i> <b>interface</b> <i>interface-name2</i> [ <b>bfd</b> ]	Configure a pair of BFD dual-device detection interfaces.
Ruijie (config-vs-domain)# <b>exit</b>	Exit the virtual switch configuration mode.

Configuration notes:

1. The BFD detection interfaces must be directly connected physical routing ports. The two ports must be on different devices.
2. You can configure pairs of BFD detection interfaces.
3. The interface type is not limited. The dual-active detection link is only used to transmit BFD packets with a small amount of traffic. Therefore, you are advised to adopt the Gigabit interface or 100 M interface as the dual-active detection interface.
4. After the layer 3 routing interface that is configured with two master devices is converted into a layer 2 switch interface (run the **switchport** command under this interface), the BFD dual-active detection will be cleared automatically.
5. The BFD-detected configuration information can be displayed only by running the dual-active detection display command rather than the BFD display command.

## Configuring the AP-based dual-active detection

To configure the AP-based detection mechanism, you must configure an AP aggregation port first and then specify the AP aggregation port as the MAD detection interface.

Command	Function
Ruijie(config-if)# <b>port-group</b> <i>ap-num</i>	Add the physical member port to the AP aggregation port.
Ruijie(config)# <b>switch virtual domain</b> <i>domain_id</i>	Enter the domain configuration mode.
Ruijie(config-vs-domain)# <b>dual-active detection aggregateport</b>	Enable the AP-based detection switch that is disabled by default.
Ruijie(config-vs-domain)# <b>dual-active interface</b> <i>interface-name</i>	Configure the aggregation port as the interface of the dual-active detection.
Ruijie(config-vs-domain)# <b>exit</b>	Exit the virtual switch configuration mode.

Enable the MAD forwarding function on the upstream and downstream devices by running the command as follows:

Command	Function
---------	----------

Ruijie(config-if)# <b>dad relay enable</b>	Enable the dual-active detection packets relay function of the interface on upstream and downstream devices. This function is disabled by default.
--	--

Configuration note: You are advised to distribute the physical interfaces that are added to the detection aggregation ports to different devices.

## Configuring the excluded port list in the recovery mode

When two master devices are detected, one of them must enter the recovery mode. In the recovery mode, you need to disable all service ports. For some special usages (for example, configuring a management switch from which you can log in to a remote port), you can set some ports to excluded ports that are not disabled in the recovery mode. The configuration commands are as follows:

Command	Function
Ruijie(config)# <b>switch virtual domain</b> <i>domain_id</i>	Enter the virtual switch configuration mode.
Ruijie(config-vs-domain)# <b>dual-active exclude interface</b> <i>interface-name</i>	Specify an excluded port that is not disabled in the recovery mode.
Ruijie(config-vs-domain)# <b>exit</b>	Exit the virtual switch configuration mode.

Configuration notes:

1. The excluded port must be a routing port rather than a VSL port.
2. After the excluded port is converted from a routing port into a switch port (run the **switchport** command under this interface), the configurations of the excluded port that is associated with this interface will be cleared automatically.

## Displaying the dual-active configurations and status

Display the current dual-active configurations and status by running the command as follows:

Command	Function
Ruijie# <b>show switch virtual dual-active { aggregateport   bfd   summary }</b>	View the current dual-active configuration information.

The following examples display the dual-active detection information.

# The current dual-active detection status:

```
Ruijie# show switch virtual dual-active summary
BFD dual-active detection enabled: Yes
Aggregateport dual-active detection enabled: NO
Interfaces excluded from shutdown in recovery mode:
GigabitEthernet 1/0/3
GigabitEthernet 1/0/4
In dual-active recovery mode: NO
```

# The current BFD dual-active detection status:

```
Ruijie# show switch virtual dual-active bfd
BFD dual-active detection enabled: Yes
BFD dual-active interface pairs configured:
```



```
Pair interface gigabitEthernet 1/0/1 and interface gigabitEthernet 2/0/1: UP
Pair interface gigabitEthernet 1/0/2 and interface gigabitEthernet 2/0/2: UP
```

# The current AP-based dual-active detection status:

```
Ruijie# show switch virtual dual-active aggregateport
Aggregateport dual-active detection enabled: Yes
Aggregateport dual-active interface AggregatePort configured:
    AggregatePort 1: UP
        GigabitEthernet 1/0/1: UP
        GigabitEthernet 2/0/1: UP
        GigabitEthernet 1/0/2: UP
        GigabitEthernet 2/0/2: UP
DAD relay enable AP list:
    AggregatePort 1
```

All dual-active detection configurations will take effect after being configured on the master or slave devices. These configurations are global configurations that can be viewed by running the **show running-config** command.

## Configuring Traffic Balancing

### Configure the AP LFF mode

The member ports of AP can be distributed on two chassis of the VSU system. You can configure whether the AP egress traffic is forwarded through local member ports first based on actual traffic conditions by running the following commands:

Command	Function
Ruijie(config)# <b>switch virtual domain</b> <i>domain_id</i>	Enter the virtual switch configuration mode.
Ruijie(config-vs-domain)# <b>[no] switch virtual aggregateport lff enable</b>	Enable or disable the AP Local Forward First (LFF) mode. To recover the cross-chassis traffic balancing mode, run the <b>no</b> command.
Ruijie(config-vs-domain)# <b>exit</b>	Exit the virtual switch configuration mode.

### Configure the ECMP LFF mode

The Equal-Cost MultiPath (ECMP) routing egress can be distributed on two chassis of the VSU system. You can configure whether the ECMP egress traffic is forwarded through local member ports first based on actual traffic conditions by running the following commands:

Command	Function
Ruijie(config)# <b>switch virtual domain</b> <i>domain_id</i>	Enter the virtual switch configuration mode.
Ruijie(config-vs-domain)# <b>[no] switch virtual ecmp lff enable</b>	Enable or disable the ECMP LFF mode.
Ruijie(config-vs-domain)# <b>exit</b>	Exit the virtual switch configuration mode.

### Display the current traffic balancing configuration mode

Display the current AP or ECMP configuration mode of the VSU system by running the following command:

Command	Function
---------	----------

Ruijie# <b>show switch virtual balance</b>	View the current traffic balancing mode of the VSU system.
--	--

The following example displays the current traffic balancing configuration mode.

```
Ruijie#show switch virtual balance
Aggregate port LFF: enable
```

Configuration notes:

1. The cross-chassis EMCP LFF mode is disabled by default in the VSU mode.
2. The cross-chassis AP LFF mode is disabled by default in the VSU mode.

## Shifting from the VSU Mode into the Standalone Mode

To change the VSU system into a device that can operate in the standalone mode, run the following command:

Command	Function
Ruijie# <b>switch convert mode standalone</b> [ <i>sw_id</i> ]	<b>sw_id</b> indicates the ID of the switch that is about to shift into standalone mode, and is an optional parameter. If this parameter is not added, the host server will shift into the standalone mode.

After you run the switching command, the system will prompt you as follows:

Whether to restore the configuration file to **standalone text**? If **yes**, the configuration file will be restored; if **no**, the configuration of virtual device mode will be cleared.

After the device shifts into the standalone mode, if you select **no** while recovering the configuration file, the standalone mode configuration information in the flash can be recovered after the standalone mode is enabled by running the following commands:

Command	Function
Ruijie# <b>copy flash:standalone.text flash:config.text</b>	Recover the saved <b>standalone.text</b> to the configuration file.
Ruijie# <b>reload</b>	Restart the switch and reapply the parameter file.

## Clearing the Member Device Configuration

You can clear the configuration of a device by running the **remove configuration switch** [*sw\_id*] command. This command will incur the device reboot.

Command	Function
Ruijie(config)# <b>remove configuration switch</b> <i>sw_id</i>	<ol style="list-style-type: none"> <li>1. If a specified device is added to the VSU system, the device configuration will be cleared and the device will be automatically restarted.</li> <li>2. Delete relevant configuration of a specified device.</li> </ol>

## Switching Manual Hot Backup

You can reset a slave device or the overall VSU group by running the following command:

Command	Function
Ruijie# <b>redundancy forceswitch</b>	Perform hot backup master-slave switching. Restart the master device and upgrade the slave device into master device.

## Resetting Device

You can reset a specified member device by running the following commands:

Command	Function
Ruijie# reload switch <i>sw_id</i>	Reset the member device with an ID of <i>sw_id</i> .
Ruijie# reload	Reset the overall VSU group.

You can reset a slave device or a VSU member device by running the following command:

Command	Function
Ruijie# <b>redundancy reload</b> { <b>peer</b>   <b>shelf</b> <i>sw_id</i> }	<p><b>Peer</b> indicates reset the slave device only.</p> <p><b>Shelf</b> indicates resetting and restarting the device with an ID of <i>sw_id</i>.</p> <p>Note: <b>sw_id</b> only exists in the VSU mode.</p>

In the VSU system, resetting a specified device will result in topology splitting and greatly impact the system. To avoid this risk, the VSU will prompt you when you reset a specified device.

1. If the current topology is a ring topology, you can reset any device freely without causing topology splitting, only the ring topology will become linear topology.
2. If the current topology is a linear topology, you can reset the devices at the edge of the topology, which will not result in topology splitting. If you reset devices in the middle of the topology, for example, the current connection mode of a linear topology is: device 1 (master)-device 2 (standby)-device 3 (slave)-device 4 (standby), you can reset device 1 or device 4 only. The reset of device 2 or device 3 will result in the inaccessible devices of master device 1 become unavailable and the system prompts you to confirm before reset.

The commands that will lead to reset of a device are as follows:

1. **Redundancy forceswitch**: Perform manual hot backup switching.
2. **Redundancy reload peer**: Perform hot backup and reset the peer slave device.
3. **Redundancy reload shelf** <*switch\_id*>: Perform hot backup and reset a specified device.
4. **Reload switch** <*switch\_id*>: Restart a device.
5. **Remove configuration switch** <*switch\_id*>: Clear the configuration of a device.

## Shifting from the VSU System into the Stack System

You can shift forcibly from the VSU system to the stack system by performing the following command:

Command	Function
Ruijie# <b>vsu convert-to stack</b>	Shift the VSU system to the stack system.

This command supports shifting from the VSU system in release of 10.4 (3b16) to the stack system in release of 10.4 (3b2). Before the shift, it is required to download the destination RGOS program image to a device and synchronize the image to all devices using the **upgrade system** command. At last, shift from the VSU to stack by running the **vsu conver-to stack** command.

During the shifting from VSU to stack, the system will forcibly transfer the VSU configuration to the stack configuration and restart the VSU system. Since there are differences between the VSU configuration and the stack configuration, during the forcible shifting, the VSU configuration that is not compatible with stack will be dropped. The system only keeps the configuration related to the stack. Therefore, when you shift from stack to VSU after you shift from VSU to stack, you need to re-configure the VSU configuration that is not compatible with the stack.

## Monitoring and Maintenance

Command	Function
Ruijie# <b>show switch virtual [ topology   config ]</b>	Display the current VSU running information, topology or configuration parameters.
Ruijie# <b>show switch virtual dual-active { aggregateport   bfd   summary }</b>	View the current dual-active configuration information.
Ruijie# <b>show switch virtual link [port]</b>	View the current VSL-AP running information in the VSU mode.

## Configuration Example

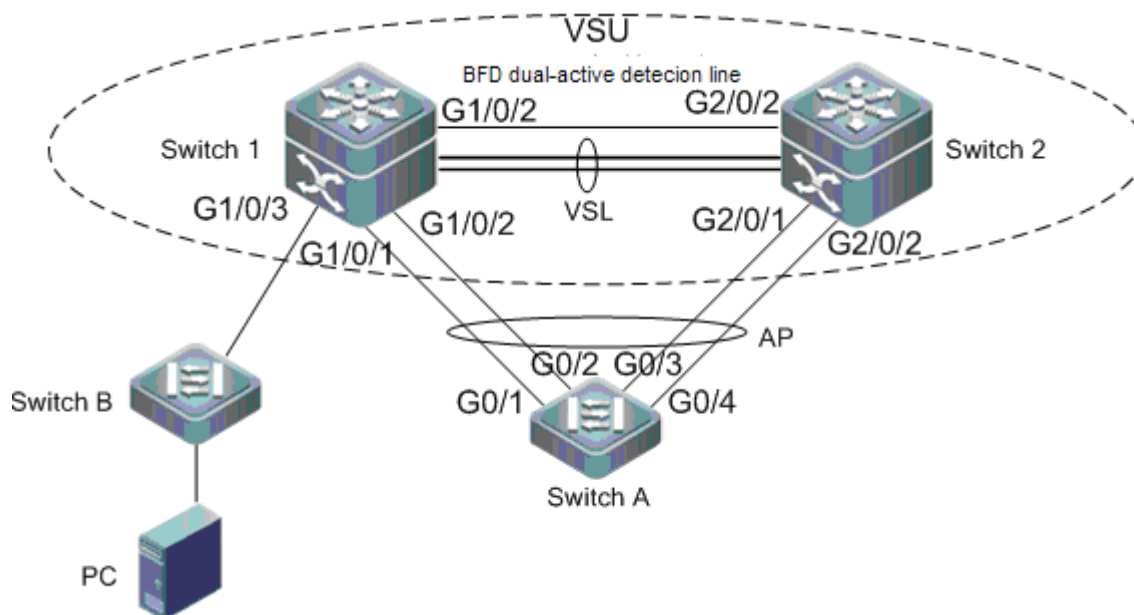
### Typical VSU Configuration

#### Networking requirements

- 1) Switch 1 and Switch 2 form a VSU (The domain ID is 1). The priority of Switch 1 and Switch 2 respectively are 200 and 150. The link between Te1/3/1 and Te1/3/2 of Switch 1 with Te2/3/1 and Te2/3/2 of Switch 2 are respectively set up and form a VSL between Switch 1 with Switch 2.
- 2) The G0/1, G0/2, G0/3 and G0/4 interfaces of Switch A, the G1/0/1 and G1/0/2 of Switch 1, and the G2/0/1 and G2/0/2 of Switch 2 are respectively connected and form an AP group including four member links. The ID of the AP group is 1.
- 3) The VSU is configured with a layer-3 interface VLAN1. The IP address is 1.1.1.1/24.
- 4) The Switch A is configured with a layer-3 interface VLAN2. The IP address is 1.1.1.2/24.
- 5) Adopt BFD or AP ports to detect the dual servers.
- 6) G1/0/2 and G2/0/2 is a pair of heartbeat interface. The respective IP addresses are 2.1.1.1/32 and 2.1.2.1/32.

#### Networking topology

Figure 1-14 VSU networking topology



### Configuration key points

- 1) All members of the AP group 1 are Gigabit optical ports.
- 2) G1/0/2 and G2/0/2 are routing ports.

### Configuration steps

- a) Configure Switch 1

#Configure the VSU domain ID, switch ID and priority on Switch 1.

```
Switch1# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch1(config)# switch virtual domain 1
Switch1(config-vs-domain)# switch 1
Switch1(config-vs-domain)# switch 1 priority 200
Switch1(config-vs-domain)# switch 1 description switch1
Switch1(config-vs-domain)# exit
Switch1(config)# vsl-aggregateport 1
Switch1(config-vsl-ap-1)# port-member interface 0/1
Switch1(config-vsl-ap-1)# port-member interface 0/2
Switch1(config-vsl-ap-1)# exit
Switch1(config)# exit
```

- b) Configure Switch 2

#Configure the VSU domain ID, switch ID and priority on Switch 2.

```
Switch2# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch2(config)# switch virtual domain 1
Switch2(config-vs-domain)# switch 2
```

```
Switch2(config-vs-domain)# switch 2 priority 150
Switch1(config-vs-domain)# switch 2 description switch2
Switch2(config-vs-domain)# exit
Switch1(config)# vsl-aggregateport 1
Switch1(config-vsl-ap-1)# port-member GigabitEthernet interface 1/1
Switch1(config-vsl-ap-1)# port-member GigabitEthernet interface 1/2
Switch1(config-vsl-ap-1)# exit
Switch2(config)# exit
```

c) **Shift Switch 1 and Switch 2 into the VSU mode**

```
Switch1# switch convert mode virtual
Switch2# switch convert mode virtual
```

d) **Configure VSU**

#Configure the AP group 1 on VSU.

```
Switch1# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch1(config)# interface aggregateport 1
Switch1(config-if)# interface GigabitEthernet 1/0/1
Switch1(config-if)# port-group 1
Switch1(config-if)# interface GigabitEthernet 1/0/2
Switch1(config-if)# port-group 1
Switch1(config-if)# interface GigabitEthernet 2/0/1
Switch1(config-if)# port-group 1
Switch1(config-if)# interface GigabitEthernet 2/0/2
Switch1(config-if)# port-group 1
```

e) **Configure Switch A**

```
SwitchA# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
SwitchA(config)# interface aggregateport 1
SwitchA(config-if)# interface range GigabitEthernet 0/1-4
SwitchA(config-if)# port-group 1
```

f) **Configure SVI**

#Configure SVI 1 on VSU.

```
Switch1(config)# interface vlan 1
Switch1(config-if)# ip address 1.1.1.1 255.255.255.0
```

#Configure SVI 1 on Switch A.

```
SwitchA (config)# interface vlan 1
SwitchA (config-if)# ip address 1.1.1.2 255.255.255.0
```

g) **Configure BFD dual-active interface**

```
Switch1(config)# interface GigabitEthernet 1/1/2
```

```
Switch1(config-if)# no switchport
Switch1(config)# interface GigabitEthernet 2/1/2
Switch1(config-if)# no switchport
Switch1(config-if)# switch virtual domain 1
Switch1(config-if)# dual-active detection bfd
Switch1(config-vs-domain)# dual-active pair interface GigabitEthernet 1/1/2 interface
GigabitEthernet 2/1/2
```

#### h) Configure AP-based dual-active detection

#Configure MAD on VSU system 1.

```
Switch1(config)# switch virtual domain 1
Switch1(config-vs-domain)# dual-active detection aggregateport
Switch1(config-vs-domain)# dual-active interface aggregate-port 1 mad
Switch1(config-vs-domain)# exit
```

#Configure MAD on Switch A.

```
Ruijie(config)#interface aggregateport 1
Ruijie(config-if-AggregatePort 1)# dad relay enable
Switch1(config-if-AggregatePort 1)# exit
```

### Display verification

#View basic VSU information.

```
Ruijie#show switch virtual
Switch_id      Domain_id      Priority      Status      Role      Description
-----
1(1)           1(1)          200(200)     OK          ACTIVE    switch1
2(2)           1(1)          150(150)     OK          STANDBY   switch2

Ruijie#show switch virtual config
switch_id: 1 (mac: 00d0.f810.1111)
!
switch virtual domain 1
!
switch 1
switch 1 priority 200
!
vsl-aggregateport 1
port-member interface TenGigabitEthernet 0/1
port-member interface TenGigabitEthernet 0/2
!
Switch convert mode virtual
!

switch_id: 2 (mac: 00d0.f810.2222)
!
```

```

switch virtual domain 1
!
switch 2
switch 2 priority 150
!
vsl-aggregateport 1
port-member interface TenGigabitEthernet 0/1
port-member interface TenGigabitEthernet 0/2
!
Switch convert mode virtual
!

```

#View the VSL status and configuration information.

```
Ruijie#show switch virtual link
```

VSL-AP	State	Peer-VSL	Rx	Tx	Uptime
1/1	UP	2/1	25398921	25398922	0d,0h,25m
2/1	UP	1/1	25398922	25398921	0d,0h,25m

```
Ruijie# show switch virtual link port
```

```
VSL-AP-1/1:
```

Port	State	Peer-port	Rx	Tx	Uptime
GigabitEthernet 1/0/21	OK	GigabitEthernet 2/0/22	171753	171753	0d,0h,25m

```
VSL-AP-1/2:
```

Port	State	Peer-port	Rx	Tx	Uptime
GigabitEthernet 1/0/22	OK	GigabitEthernet 2/0/21	171753	171753	0d,0h,25m

```
VSL-AP-2/1:
```

Port	State	Peer-port	Rx	Tx	Uptime
GigabitEthernet 2/0/21	OK	GigabitEthernet 1/0/22	170501	170501	0d,0h,25m

```
VSL-AP-2/2:
```

Port	State	Peer-port	Rx	Tx	Uptime
------	-------	-----------	----	----	--------



GigabitEthernet 2/0/22	OK	GigabitEthernet 1/0/21	170501	170501
0d,0h,25m				

#### #View the dual-active configuration status.

```
Ruijie# show switch virtual dual-active summary
BFD dual-active detection enabled: Yes
Aggregateport dual-active detection enabled: Yes
Interfaces excluded from shutdown in recovery mode:
GigabitEthernet 1/0/3
In dual-active recovery mode: NO
```

#### # View the BFD dual-active chassis detection configuration.

```
Ruijie# show switch virtual dual-active bfd
BFD dual-active detection enabled: Yes
BFD dual-active interface configured:
    GigabitEthernet 1/0/12: UP
    GigabitEthernet 1/0/12: UP
```

#### #View the AP dual-active detection configuration.

```
Ruijie# show switch virtual dual-active aggregateport
Aggregateport dual-active detection enabled: Yes
Aggregateport dual-active interface AggregatePort configured:
    AggregatePort 1: UP
        GigabitEthernet 1/0/1: UP
        GigabitEthernet 1/0/2: UP
        GigabitEthernet 2/0/1: UP
        GigabitEthernet 2/0/2: UP
```

#### #View the traffic balancing mode.

```
Ruijie#show switch virtual balance
Aggregate port LFF: enable
ECMP LFF: disable
```

#### #View the topology information of the VSU group.

```
Ruijie# show switch virtual topology
Chain Topology:
[1]---[2]

switch[1] (mac: 00d0.f810.1111, description: switch1):
    vsl-ap[1] <--> vsl-ap[1] of switch[2]

switch[2] (mac: 00d0.f810.2222, description: switch2):
    vsl-ap[1] <--> vsl-ap[1] of switch[1]
```

## Network Management and Monitoring Configuration

---

1. SNMP Configuration
2. RMON Configuration
3. NTP Configuration
4. SNTP Configuration
5. SPAN Configuration
6. RSPAN Configuration

# SNMP Configuration

## SNMP Overview

### Introduction

As the abbreviation of Simple Network Management Protocol, SNMP has been a network management standard (RFC1157) since the August, 1988. So far, the SNMP becomes the actual network management standard for the support from many manufacturers. It is applicable to the situation of interconnecting multiple systems from different manufacturers. Administrators can use the SNMP protocol to query information, configure network, locate failure and plan capacity for the nodes on the network. Network supervision and administration are the basic function of the SNMP protocol.

As a protocol in the application layer, the SNMP protocol works in the client/server mode, including three parts as follows:

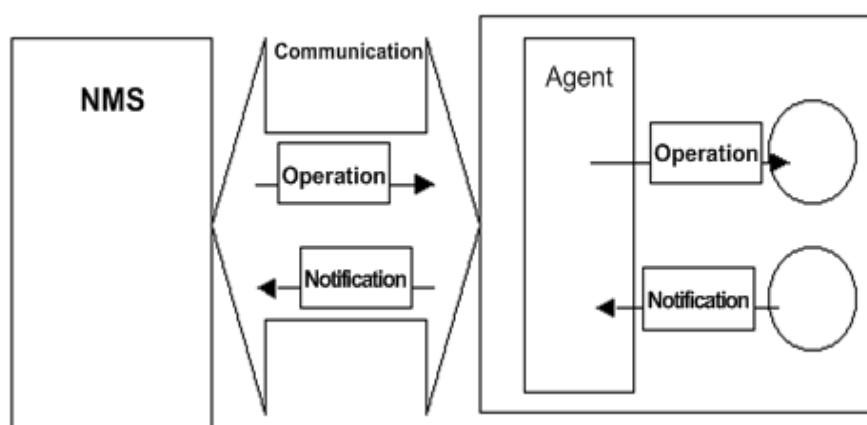
- SNMP network manager
- SNMP agent
- MIB (management information base)

The SNMP network manager, also referred to as NMS (Network Management System), is a system to control and monitor the network using the SNMP protocol. HP OpenView, CiscoView and CiscoWorks 2000 are the typical network management platforms running on the NMS. Ruijie has developed a suit of software (Star View) for network management against its own network devices. These typical network management softwares are convenient to monitor and manage network devices.

The SNMP Agent is the software running on the managed devices. It receives processes and responds the monitoring and controlling messages from the NMS, and also sends some messages to the NMS.

The relationship between the NMS and the SNMP Agent can be indicated as follows:

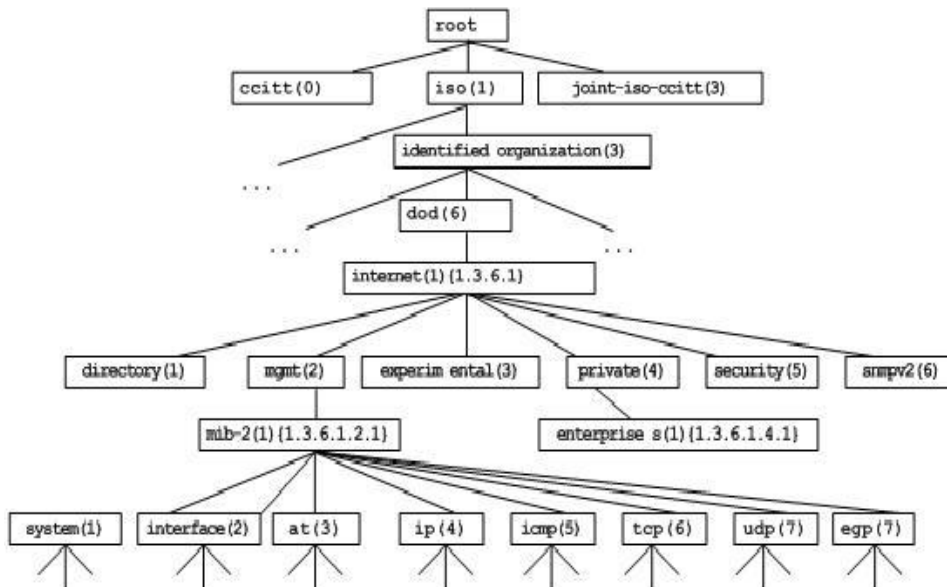
### Relationship between the NMS and the SNMP Agent



The MIB (Management Information Base) is a virtual information base for network management. There are large volumes of information for the managed network equipment. In order to uniquely identify a specific management unit in the SNMP message, the tree-type hierarchy is used to by the MIB to describe the management units in the network management equipment. The node in the tree indicates a specific management unit. Take the following figure of MIB as an example to

name the objectives in the tree. To identify a specific management unit system in the network equipment uniquely, a series of numbers can be used. For instance, the number string {1.3.6.1.2.1.1} is the object identifier of management unit, so the MIB is the set of object identifiers in the network equipment.

Tree-type MIB hierarchy



## SNMP Versions

This software supports these SNMP versions:

- SNMPv1: The first formal version of the Simple Network Management Protocol, which is defined in RFC1157.
- SNMPv2C: Community-based Administrative Framework for SNMPv2, an experimental Internet protocol defined in RFC1901.
- SNMPv3: Offers the following security features by authenticating and encrypting packets:
  1. Ensure that the data are not tampered during transmission.
  2. Ensure that the data come from a valid data source.
  3. Encrypt packets to ensure the data confidentiality.

Both the SNMPv1 and SNMPv2C use a community-based security framework. They restrict administrator's operations on the MIB by defining the host IP addresses and community string.

With the GetBulk retrieval mechanism, SNMPv2C sends more detailed error information type to the management station. GetBulk allows you to obtain all the information or a great volume of data from the table at a time, and thus reducing the times of request and response. Moreover, SNMPv2C improves the capability of handling errors, including expanding error codes to distinguish different kinds of errors, which are represented by one error code in SNMPv1. Now, error types can be distinguished by error codes. Since there may be the management workstations supporting SNMPv1 and SNMPv2C in a network, the SNMP agent must be able to recognize both SNMPv1 and SNMPv2C messages, and return the corresponding version of messages.

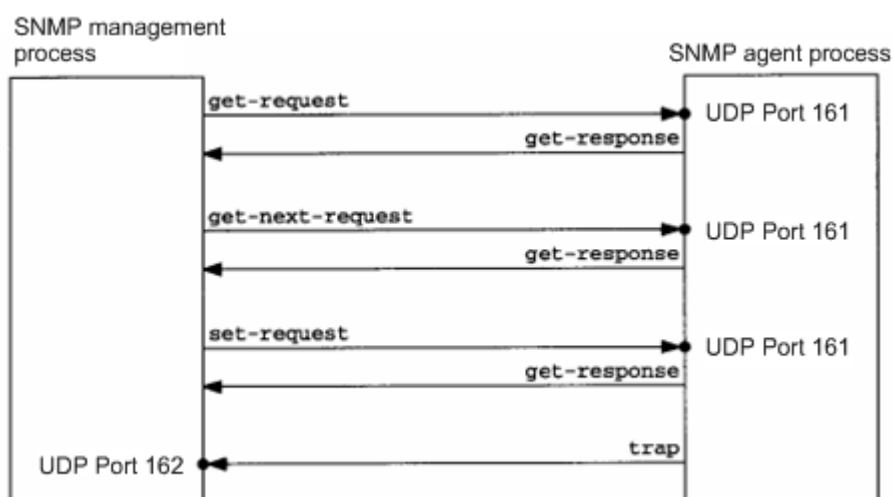
## SNMP Management Operations

For the information exchange between the NMS and the SNMP Agent, six types of operations are defined:

- Get-request: The NMS gets one or more parameter values from the SNMP Agent.
- Get-next-request: The NMS gets the next parameter value of one or more parameters from the SNMP Agent.
- Get-bulk: The NMS gets a bulk of parameter values from the SNMP Agent.
- Set-request: The NMS sets one or more parameter values for the SNMP Agent.
- Get-response: The SNMP Agent returns one or more parameter values, the response of the SNMP Agent to any of the above 3 operations of the NMS.
- Trap: The SNMP Agent proactively sends messages to notify the NMS that some event will occur.

The first four messages are sent from the NMS to the SNMP Agent, and the last two messages are sent from the SNMP Agent to the NMS (Note: SNMPv1 does not support the Get-bulk operation). These operations are described in the following figure:

Message types in SNMP



NMS sends messages to the SNMP Agent in the first three operations and the SNMP Agent responds a message through the UDP port 161. However, the SNMP Agent sends a message in the Trap operation through the UDP port 162.

## SNMP Security

Both SNMPv1 and SNMPv2 use the community string to check whether the management workstation is entitled to use MIB objects. In order to manage devices, the community string of NMS must be identical to a community string defined in the devices.

A community string Features:

- Read-only: Authorized management workstations are entitled to read all the variables in the MIB.
- Read-write: Authorized management workstations are entitled to read and write all the variables in the MIB.

Based on SNMPv2, SNMPv3 can determine a security mechanism for processing data by security model and security level. There are three types of security models: SNMPv1, SNMPv2C and SNMPv3.

The table below describes the supported security models and security levels.

Model	Level	Authentication	Encryption	Description
SNMPv1	noAuthNoPriv	Community string	None	Ensures the data validity through community string.
SNMPv2c	noAuthNoPriv	Community string	None	Ensures the data validity through community string.
SNMPv3	noAuthNoPriv	User name	None	Ensures the data validity through user name.
SNMPv3	authNoPriv	MD5 or SHA	None	Provides HMAC-MD5 or HMAC-SHA-based authentication mechanism.
SNMPv3	authPriv	MD5 or SHA	DES	Provides HMAC-MD5 or HMAC-SHA-based authentication mechanism and CBC-DES-based encryption mechanism.

## SNMP Engine ID

The engine ID is designed to identify a SNMP engine uniquely. Every SNMP entity contains a SNMP engine; a SNMP engine ID identifies a SNMP entity in a management domain. So every SNMPV3 entity has a unique identifier named SNMP Engine ID.

The SNMP Engine ID is an octet string of 5 to 32 bytes, which is defined in RFC3411:

- The first four bytes indicate the private enterprise number of an enterprise (assigned by IANA) in hex system.
- The fifth byte indicates how to identify the rest bytes.

0: Reserved

1: The following 4 bytes indicate an IPv4 address.

2: The following 16 bytes indicate an IPv6 address.

3: The following 6 bytes indicate an MAC address

4: Texts of up to 27 bytes defined by manufacturers

5: A hexadecimal value of up to 27 bytes defined by manufacturers

6-127: Reserved

128-255: In the format specified by manufacturers.

## SNMP Configuration

To configure SNMP, enter the global configuration mode.

### Setting the Community String and Access Authority

SNMPv1 and SNMPv2C adopt community string-based security scheme. The SNMP Agent supports only the management operations from the management workstations of the same community string. The SNMP messages without matching the community string will be discarded. The community string serves as the password between the NMS and the SNMP Agent.

- Configure an ACL rule to allow the NMS of the specified IP address to manage devices.
- Set the community's operation right: ReadOnly or ReadWrite.
- Specify a view for view-based management. By default, no view is configured. That is, the management workstation is allowed to access to all MIB objects
- Indicate the IP address of the NMS who can use this community string. If it is not indicated, any NMS can use this community string. By default, any NMS can use this community string.

To configure the SNMP community string, run the following command in the global configuration mode:

Command	Function
Ruijie(config)# <b>snmp-server community</b> <i>string</i> [ <b>view</b> <i>view-name</i> ] [ <b>ro</b>   <b>rw</b> ] [ <b>host</b> <i>host-ip</i> ] [ <b>ipv6</b> <i>ipv6-aclname</i> ][ <i>aclnum</i>   <i>aclname</i> ]	Set the community string and its right.

One or more community strings can be specified for the NMS of different rights. To remove the community name and its right, run the **no snmp-server community** *string* command in the global configuration mode.

Keywords 0 and 7 represent the encryption types of community strings. The community string with the keyword 0 in the front indicates the community name is in plain text; with the keyword 7, the community name is in encrypted text. If the encryption type is absent, the community name is in plain text, by default. With the command **service password-encryption** configured, community strings are displayed and saved in the encrypted form. In this case, if the configuration with **service password-encryption** is removed, the community strings are still displayed and saved in the encrypted form rather than in the plain text.

## Configuring the SNMP-Enabled Port

By the SNMP protocol, the 161 UDP port is used for receiving SNMP packets by default. In consideration of security, you can customize the UDP port used.

Execute the following command in the global configuration mode to configure the SNMP-enabled port number:

Command	Function
Ruijie(config)# <b>snmp-server udp-port</b> <i>port-num</i>	Set the number of a UDP port receiving packets in the SNMP protocol.

Use the **no snmp-server udp-port** command to restore the use of the default port.

## Configuring MIB Views and Groups

With view-based access control model, you can determine whether the object of a management operation is in a view or not. For access control, generally some users are associated with a group and then the group is associated with a view. The users in a group have the same access right.

- Set an inclusion view and an exclusion view.
- Set a Read-only view and a Read-write view for a group.
- Set security levels, whether to authenticate, and whether to encrypt for SNMPv3 users.

To configure the MIB views and groups, run the following commands in the global configuration mode:

Command	Function
Ruijie(config)# <b>snmp-server view</b> <i>view-name oid-tree {include   exclude}</i>	Create a MIB view to include or exclude associated MIB objects.
Ruijie(config)# <b>snmp-server group</b> <i>groupname {v1   v2c   v3 {auth   noauth   priv}}</i> [ <i>read readview</i> ] [ <i>write writeview</i> ] [ <i>access {[ipv6 ipv6_aclname] [aclnum   aclname] }</i> ]	Create a group and associate it with the view.

You can delete a view by using the **no snmp-server view** *view-name* command, or delete a tree from the view by using the **no snmp-server view** *view-name oid-tree* command. You can also delete a group by using the **no snmp-server group** *groupname {v1 | v2c | v3}* command.

## Configuring SNMP Users

User-based security model can be used for security management. In this mode, you should configure user information first. The NMS can communicate with the SMP Agent by using a valid user account.

For SNMPv3 users, you can specify security level, authentication algorithm (MD5 or SHA), authentication password, encryption algorithm (only DES now) and encryption password.

To configure a SNMP user, run the following commands in the global configuration mode:



Command	Function
Ruijie(config)# <b>snmp-server user</b> <i>username groupname {v1   v2c   v3</i> <b>[encrypted] [auth { md5 sha }</b> <i>auth-password ] [priv des56</i> <i>priv-password] } [access {[ipv6</i> <i>ipv6_aclname] [aclnum   aclname] }}</i>	Configure the user information.

To remove the specified user, execute the **no snmp-server user username groupname {v1 | v2c | v3}** command in the global configuration mode.

## Configuring Host Address

In special cases, the SNMP Agent may also proactively send messages to the NMS.

To configure the NMS host address that the SNMP Agent proactively sends messages to, execute the following commands in the global configuration mode:

Command	Function
Ruijie(config)# <b>snmp-server host</b> <i>{ host-addr   ipv6 ipv6-addr } [ vrf</i> <i>vrfname ] [ traps ] [ version { 1   2c   3</i> <i>{ auth   noauth   priv } ]</i> <i>community-string [ udp-port port-num ]</i> <i>[ notification-type ]</i>	Set the SNMP host address, vrf, community string, message type (or security level in SNMPv3).

## Configuring SNMP Agent Parameters

You can configure the basic parameters of the SNMP Agent, including contact, device network element code, device location and sequence number. With these parameters, the NMS knows the contact, location and other information of the device.

To configure the SNMP agent parameters, run the following commands in the global configuration mode:

Command	Function
Ruijie(config)# <b>snmp-server contact</b> <i>text</i>	Configure the contact.
Ruijie(config)# <b>snmp-server location</b> <i>text</i>	Configure the location.
Ruijie(config)# <b>snmp-server net-id</b> <i>text</i>	Configure the network element code.
Ruijie(config)# <b>snmp-server</b> <b>chassis-id</b> <i>number</i>	Configure the sequence number.

## Defining the Maximum Message Size of the SNMP Agent

In order to enhance network performance, you can configure the maximum packet size of the SNMP Agent. To configure the maximum packet size of the SNMP Agent, run the following command in the global configuration mode:

Command	Function
Ruijie(config)# <b>snmp-server</b> <i>packetsize</i> <i>byte-count</i>	Set the maximum packet size of the SNMP Agent.

## Shielding the SNMP Agent

The SNMP Agent service is a service provided by Ruijie product and enabled by default. When you do not need it, you can shield the SNMP agent service and related configuration by executing the following command in the global configuration mode:

Command	Function
Ruijie(config)# <b>no snmp-server</b>	Shield the SNMP agent service.

## Disabling the SNMP Agent

Ruijie products provide a different command from the shield command to disable the SNMP Agent. This command will act on all of the SNMP services instead of shielding the configuration information of the SNMP Agent. To disable the SNMP agent service, run the following command in the global configuration mode:

Command	Function
Ruijie(config)# <b>no enable service snmp-agent</b>	Disable the SNMP agent service.

## Configuring the SNMP Agent to Send the Trap Message to the NMS Initiatively

The TRAP message is a message automatically sent by the SNMP Agent to the NMS unsolicitedly, and is used to report some critical and important events. By default the SNMP Agent is not allowed to send the TRAP message. To enable it, run the following command in the global configuration mode:

Command	Function
Ruijie(config)# <b>snmp-server enable traps</b> [ <i>type</i> ] [ <i>option</i> ]	Allow the SNMP Agent to send the TRAP message proactively.
Ruijie(config)# <b>no snmp-server enable traps</b> [ <i>type</i> ] [ <i>option</i> ]	Forbid the SNMP Agent to send the TRAP message proactively.

## Configuring LinkTrap Policy

You can configure whether to send the LinkTrap message of an interface. When this function is enabled and the link status of the interface changes, the SNMP will send the LinkTrap message. Otherwise, it will not. By default, this function is enabled.

Command	Function
Ruijie(config)# <b>interface</b> <i>interface-id</i>	Enter the interface configuration mode.
Ruijie(config-if)# <b>[no] snmp trap link-status</b>	Enable or disable sending the LinkTrap message of the interface.

The following configures not to send LinkTrap message on the interface:

```
Ruijie(config)# interface gigabitEthernet 1/1
Ruijie(config-if)#no snmp trap link-status
```

## Configuring the Parameters for Sending the Trap Message

To set the parameters for the SNMP Agent to send the Trap message, execute the following commands:

Command	Function
Ruijie(config)# <b>snmp-server trap-source</b> <i>interface</i>	Specify the source port sending the Trap message.
Ruijie(config)# <b>snmp-server queue-length</b> <i>length</i>	Specify the queue length of each Trap message.
Ruijie(config)# <b>snmp-server trap-timeout</b> <i>seconds</i>	Specify the interval of sending Trap message.

## Configuring the TRAP Message to Carry a Private Field

You can specify an agent to send trap messages carrying a private format field. The private field contains the following information:

- Alarm number
- Element identifier
- Original alarm level: the level contained in the alarm information reported by the device: 1. severe; 2. major; 3. minor; 4. average; 5. uncertain
- Original alarm type: the alarm type contained in the alarm information reported by the device, including communication, environment, device, processing error and service quality alarms.
- Alarm cause number: the internal alarm number identifying the alarm cause
- Alarm cause: description of the alarm cause
- Alarming time
- Alarm status: shows whether an alarm is removed or still active
- Alarm title
- Alarm content

Refer to the description of the file RUIJIE-TRAP-FORMAT-MIB.mib for the detailed data types and ranges of the above fields.

The configuration commands are set out below:

Command	Function
Ruijie(config)# <b>snmp-server trap-format private</b>	Configure the TRAP Message to Carry a Private Field
Ruijie(config)# <b>no snmp-server trap-format private</b>	Remove the configuration of the TRAP Message to Carry a Private Field



This configuration will not take effect when the version SNMP v1 is applied for sending TRAP messages.

## SNMP Monitoring and Maintenance

### Checking the Current SNMP Status

To monitor the SNMP status and troubleshoot SNMP configurations, Ruijie product provides monitoring commands for SNMP, with which it is possible to easily check the SNMP status of the current network device. In the privileged EXEC mode, execute **show snmp** to check the current SNMP status.

```
Ruijie# show snmp
Chassis: 1234567890 0987654321
Contact: wugb@i-net.com.cn
Location: fuzhou
2381 SNMP packets input
  5 Bad SNMP version errors
  6 Unknown community name
  0 Illegal operation for community name supplied
  0 Encoding errors
  9325 Number of requested variables
  0 Number of altered variables
  31 Get-request PDUs
  2339 Get-next PDUs
  0 Set-request PDUs
2406 SNMP packets output
  0 Too big errors (Maximum packet size 1500)
  4 No such name errors
  0 Bad values errors
  0 General errors
  2370 Get-response PDUs
  36 SNMP trap PDUs
SNMP global trap: disabled
SNMP logging: enabled
SNMP agent: enabled
```

The above statistics is explained as follows:

Showing Information	Description
Bad SNMP version errors	SNMP version is incorrect.
Unknown community name	The community name is not known.
Illegal operation for community name supplied	Illegal operation
Encoding errors	Code error
Get-request PDUs	Get-request message
Get-next PDUs	Get-next message
Set-request PDUs	Set-request message
Too big errors (Maximum packet size 1500)	Too large response message
No such name errors	Not in the specified management unit

Showing Information	Description
Bad values errors	Specified value type error
General errors	General error
Get-response PDUs	Get-response message
SNMP trap PDUs	SNMP trap message

## Checking the MIB Objects Supported by the Current SNMP Agent

To check the MIB objects supported by the current SNMP Agent, run the **show snmp mib** command in the privileged EXEC mode:

```
Ruijie# show snmp mib
sysDescr
sysObjectID
sysUpTime
sysContact
sysName
sysLocation
sysServices
sysORLastChange
snmpInPkts
snmpOutPkts
snmpInBadVersions
snmpInBadCommunityNames
snmpInBadCommunityUses
snmpInASNParseErrs
snmpInTooBig
snmpInNoSuchNames
snmpInBadValues
snmpInReadOnly
snmpInGenErrs
snmpInTotalReqVars
snmpInTotalSetVars
snmpInGetRequests
snmpInGetNexts
snmpInSetRequests
snmpInGetResponses
snmpInTraps
snmpOutTooBig
snmpOutNoSuchNames
snmpOutBadValues
snmpOutGenErrs
snmpOutGetRequests
snmpOutGetNexts
snmpOutSetRequests
snmpOutGetResponses
snmpOutTraps
snmpEnableAuthenTraps
snmpSilentDrops
snmpProxyDrops
entPhysicalEntry
entPhysicalEntry.entPhysicalIndex
entPhysicalEntry.entPhysicalDescr
```

```
entPhysicalEntry.entPhysicalVendorType
entPhysicalEntry.entPhysicalContainedIn
entPhysicalEntry.entPhysicalClass
entPhysicalEntry.entPhysicalParentRelPos
entPhysicalEntry.entPhysicalName
entPhysicalEntry.entPhysicalHardwareRev
entPhysicalEntry.entPhysicalFirmwareRev
entPhysicalEntry.entPhysicalSoftwareRev
entPhysicalEntry.entPhysicalSerialNum
entPhysicalEntry.entPhysicalMfgName
entPhysicalEntry.entPhysicalModelName
entPhysicalEntry.entPhysicalAlias
entPhysicalEntry.entPhysicalAssetID
entPhysicalEntry.entPhysicalIsFRU
entPhysicalContainsEntry
entPhysicalContainsEntry.entPhysicalChildIndex
entLastChangeTime
```

## Viewing SNMP Users

To view the SNMP users configured on the current SNMP agent, run the **show snmp user** command in the privileged EXEC mode:

```
Ruijie# show snmp user
User name: test
Engine ID: 8000131103000000000000
storage-type: permanent    active
Security level: auth priv
Auth protocol: SHA
Priv protocol: DES
Group-name: g1
```

## Viewing SNMP Views and Groups

To view the group configured on the current SNMP agent, run the **show snmp group** command in the privileged EXEC mode:

```
Ruijie# show snmp group
groupname: g1
securityModel: v3
securityLevel:authPriv
readview: default
writeview: default
notifyview:

groupname: public
securityModel: v1
securityLevel:noAuthNoPriv
readview: default
writeview: default
notifyview:

groupname: public
securityModel: v2c
```

```
securityLevel:noAuthNoPriv
readview: default
writeview: default
notifyview:
```

To view the view configured on the current SNMP agent, run the **show snmp view** command in the privileged EXEC mode:

```
Ruijie# show snmp view
default(include) 1.3.6.1
test-view(include) 1.3.6.1.2.1
```

## Viewing Host Information

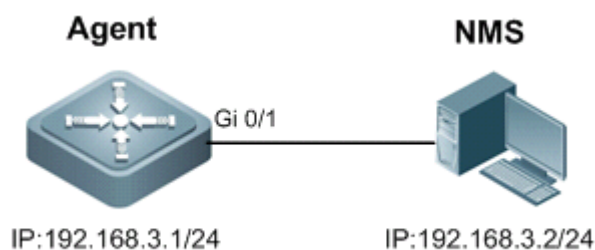
To view the host information configured on the SNMP agent, run the **show snmp host** command in the privileged EXEC mode:

```
Ruijie# show snmp host
Notification host: 192.168.64.221
udp-port: 162   type: trap
user: public   security model: v1
Notification host: 2000:1234::64
udp-port: 162   type: trap
user: public   security model: v1
```

## Typical SNMP Configuration Example

### SNMP v1/v2 Configuration Example

#### Topological Diagram



Topology for SNMP v1/2 application

#### Application Requirements

- The Network Management Station (NMS) manages the network device (Agent) by applying the community-based authentication model, and the network device can control the operation permission (read or write) of the community to access the specified MIB objects. For example, community "user1" can only read and write objects under System (1.3.6.1.2.1.1) node.
- The network device can only be managed by NMS with a specific IP (i.e., 192.168.3.2/24).
- The network device can actively send messages to NMS.

- The NMS can acquire the basic system information of the device, such as contact, location, ID and etc.

## Configuration Tips

- By creating MIB view and associating authentication name (Community) and access permission (Read or Write), the first application need can be met.
- While configuring the authentication name and access permission, associate ACL or specify the IP of administrator using this authentication name to meet the second application need (this example associates the ACL).
- Configure the address of SNMP host and enable the Agent to actively send Traps.
- Configure the parameters of SNMP proxy.

## Configuration Steps

Step 1: Configure MIB view and ACL.

! Create a MID view named "v1", which contains the associated MIB object (1.3.6.1.2.1.1).

```
Ruijie(config)#snmp-server view v1 1.3.6.1.2.1.1 include
```

! Create an ACL named "a1" to permit the IP address of 192.168.3.2/24.

```
Ruijie(config)#ip access-list standard a1
Ruijie(config-std-nacl)#permit host 192.168.3.2
Ruijie(config-std-nacl)#exit
```

Step 2: Configure authentication name and access permission.

! Configure Community of "user1", associate read and write permission for MIB view of "v1", and associate the ACL of "a1".

```
Ruijie(config)#snmp-server community user1 view v1 rw a1
```

Step 3: Configure the Agent to actively send messages to NMS.

! Configure the address of SNMP host to 192.168.3.2, message format to Version 2c and authentication name to "user1".

```
Ruijie(config)#snmp-server host 192.168.3.2 traps version 2c user1
```

! Enable the Agent to actively send traps.

```
Ruijie(config)#snmp-server enable traps
```

Step 4: Configure parameters of SNMP proxy.

! Configure system location.

```
Ruijie(config)#snmp-server location fuzhou
```

! Configure system contact.

```
Ruijie(config)#snmp-server contact ruijie.com.cn
```

! Configure system ID.

```
Ruijie(config)#snmp-server chassis-id 1234567890
```



Step 5: Configure the IP address of Agent.

! Configure the IP address of Gi 0/1 as 192.168.3.1/24.

```
Ruijie(config)#interface GigabitEthernet 0/1
Ruijie(config-if-GigabitEthernet 0/1)#ip address 192.168.3.1 255.255.255.0
Ruijie(config-if-GigabitEthernet 0/1)#exit
```

## Verification

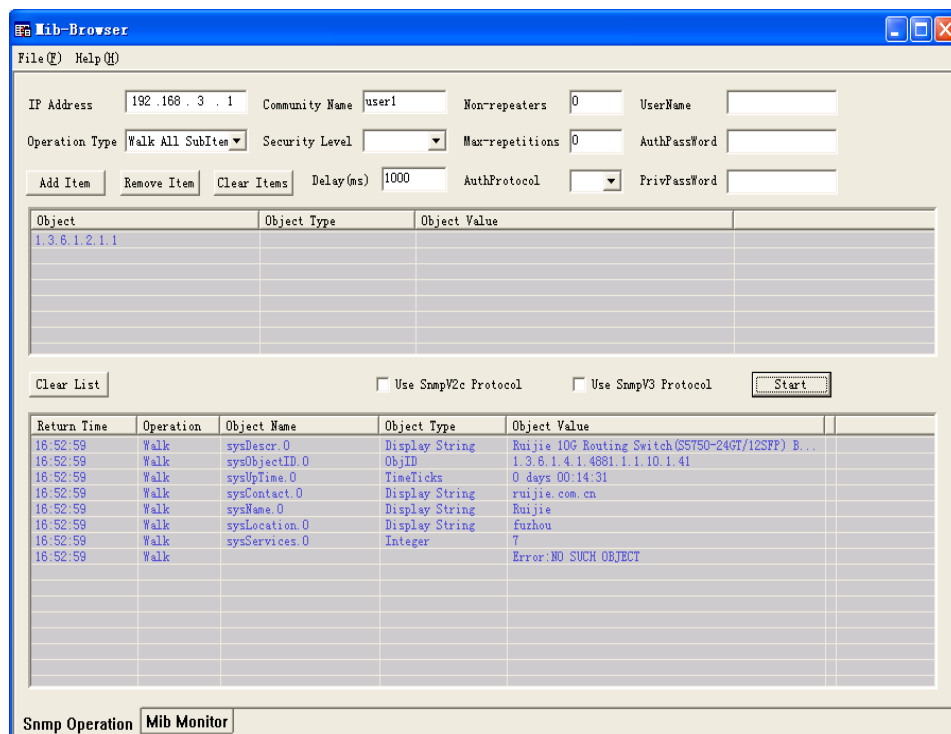
Step 1: Display configurations of the device.

```
Ruijie#show running-config
!
ip access-list standard a1
 10 permit host 192.168.3.2
!
interface GigabitEthernet 0/1
 no ip proxy-arp
 ip address 192.168.3.1 255.255.255.0
!
snmp-server view v1 1.3.6.1.2.1.1 include
snmp-server location fuzhou
snmp-server host 192.168.3.2 traps version 2c user1
snmp-server enable traps
snmp-server contact ruijie.com.cn
snmp-server community user1 view v1 rw a1
snmp-server chassis-id 1234567890
```

Step 2: Display information about SNMP view and group.

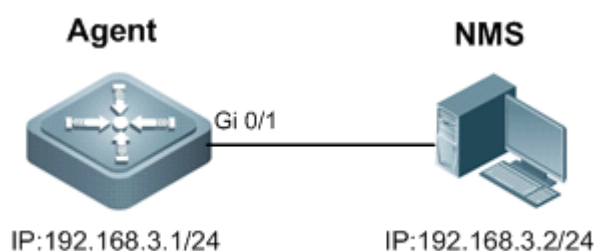
```
Ruijie#show snmp view
v1(include) 1.3.6.1.2.1.1 //define MIB object of "v1"
default(include) 1.3.6.1 //default MIB object
Ruijie#show snmp group
groupname: user1 //Configure Community as SNMP group
securityModel: v1
securityLevel:noAuthNoPriv
readview: v1
writeview: v1
notifyview:
groupname: user1
securityModel: v2c
securityLevel:noAuthNoPriv
readview: v1
writeview: v1
notifyview:
```

Step 3: Install MIB-Browser. Type in device IP of "192.168.3.1" in the field of IP Address; type in "user1" in the field of Community Name; click "Add Item" button and select the specific management unit for querying MIB, such as the System shown below. Click Start button to implement MIB query of network device. The query result is shown in the bottommost box:



## SNMP v3 Configuration Example

### Topological Diagram



### SNMPv3 application topology

### Application Requirements

- Network Management Station manages the network device (Agent) by applying user-based security model. For example: the user name is "user1", authentication mode is MD5, authentication key is "123", encryption algorithm is DES56, and the encryption key is "321".
- The network device can control user's permission to access MIB objects. For example: "User1" can read the MIB objects under System (1.3.6.1.2.1.1) node, and can only write MIB objects under SysContact (1.3.6.1.2.1.1.4.0) node.
- The network device can actively send authentication and encryption messages to the network management station.

## Configuration Tips

- Create MIB view and specify the included or excluded MIB objects.
- Create SNMP group and configure the version to "v3"; specify the security level of this group, and configure the read-write permission of the view corresponding to this group.
- Create user name and associate the corresponding SNMP group name in order to further configure the user's permission to access MIB objects; meanwhile, configure the version number to "v3" and the corresponding authentication mode, authentication key, encryption algorithm and encryption key.
- Configure the address of SNMP host, configure the version number to "3" and configure the security level to be adopted.

## Configuration Steps

Step 1: Configure MIB view and group.

! Create a MIB view of "view1" and include the MIB object of 1.3.6.1.2.1.1; further create a MIB view of "view2" and include the MIB object of 1.3.6.1.2.1.1.4.0.

```
Ruijie(config)#snmp-server view view1 1.3.6.1.2.1.1 include
Ruijie(config)#snmp-server view view2 1.3.6.1.2.1.1.4.0 include
```

! Create a group named "g1" and select the version number of "v3"; configure security level to "priv" to read "view1" and write "view2".

```
Ruijie(config)#snmp-server group g1 v3 priv read view1 write view2
```

Step 2: Configure SNMP user.

! Create a user named "user1", which belongs to group "g1"; select version number of "v3" and configure authentication mode to "md5", authentication key to "123", encryption mode to "DES56" and encryption key to "321".

```
Ruijie(config)#snmp-server user user1 g1 v3 auth md5 123 priv des56 321
```

Step 3: Configure the address of SNMP host.

! Configure the host address as 192.168.3.2 and select version number of "3"; configure security level to "priv" and associate the corresponding user name of "user1".

```
Ruijie(config)#snmp-server host 192.168.3.2 traps version 3 priv user1
```

! Enable the Agent to actively send traps to NMS.

```
Ruijie(config)#snmp-server enable traps
```

Step 4: Configure the IP address of Agent.

! Configure the IP address of Gi 0/1 as 192.168.3.1/24.

```
Ruijie(config)#interface GigabitEthernet 0/1
Ruijie(config-if-GigabitEthernet 0/1)#ip address 192.168.3.1 255.255.255.0
Ruijie(config-if-GigabitEthernet 0/1)#exit
```

## Verification

Step 1: Display configurations of device.

```
Ruijie#show running-config
!
interface GigabitEthernet 0/1
 no ip proxy-arp
 ip address 192.168.3.1 255.255.255.0
!
snmp-server view view1 1.3.6.1.2.1.1 include
snmp-server view view2 1.3.6.1.2.1.1.4.0 include
snmp-server user user1 g1 v3 encrypted auth md5 7EBD6A1287D3548E4E52CF8349CBC93D priv des56
D5CEC4884360373ABBF30AB170E42D03
snmp-server group g1 v3 priv read view1 write view2
snmp-server host 192.168.3.2 traps version 3 priv user1
snmp-server enable traps
```

Step 2: Display SNMP user.

```
Ruijie#show snmp user
User name: user1
Engine ID: 800013110300d0f8221120
storage-type: permanent      active
Security level: auth priv
Auth protocol: MD5
Priv protocol: DES
Group-name: g1
```

Step 3: Display SNMP view.

```
Ruijie#show snmp view
view1(include) 1.3.6.1.2.1.1
view2(include) 1.3.6.1.2.1.1.4.0
default(include) 1.3.6.1
```

Step 4: Display SNMP group.

```
Ruijie#show snmp group
groupname: g1
securityModel: v3
securityLevel:authPriv
readview: view1
writeview: view2
notifyview:
```

Step 5: Display host information configured by the user.

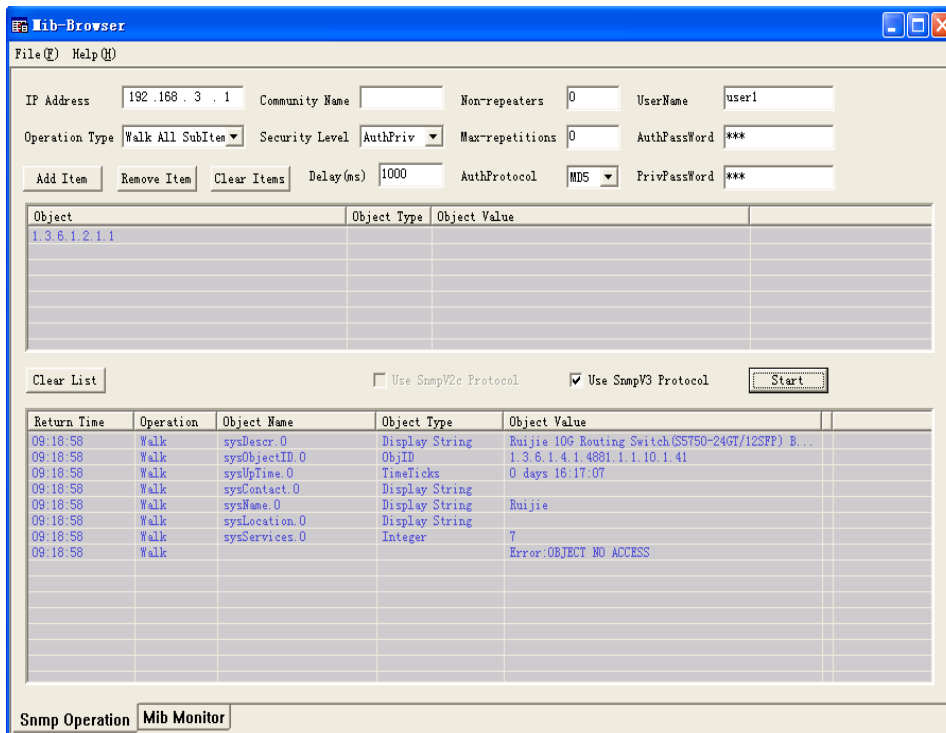
```
Ruijie#show snmp host
Notification host: 192.168.3.2
udp-port: 162
```

```

type: trap
user: user1
security model: v3 authPriv

```

Step 6: Install MIB-Browser. Type in device IP of "192.168.3.1" in the field of IP Address; type in "user1" in the field of UserName; select "AuthPriv" from Security Level; type in "123" in the field of AuthPassWord; select "MD5" from AuthProtocol; type in "321" in the field of PrivPassWord. Click "Add Item" button and select the specific management unit for querying MIB, such as the System shown below. Click Start button to implement MIB query of network device. The query result is shown in the bottommost box:



# RMON Configuration

## Overview

RMON (Remote Monitoring) is a standard monitoring specification of IETF (Internet Engineering Task Force). It can be used to exchange the network monitoring data among various network monitors and console systems. In the RMON, detectors can be placed on the network nodes, and the NMS determines which information is reported by these detectors, for example, the monitored statistics and the time buckets for collecting history. The network device such as the switch or router acts as a node on the network. The information of current node can be monitored by means of the RMON.

There are three stages in the development of RMON. The first stage is the remote monitoring of Ethernet. The second stage introduces the token ring which is referred to as the token ring remote monitoring module. The third stage is known as RMON2, which develops the RMON to a high level of protocol monitor.

The first stage of RMON (known as RMON1) contains nine groups. All of them are optional (not mandatory), but some groups should be supported by the other groups.

The switch implements the contents of Group 1, 2, 3 and 9: the statistics, history, alarm and event.

## Statistics

Statistics is the first group in RMON. It measures the basic statistics information of each monitored subnet. At present, only the Ethernet interfaces of network devices can be monitored and measured. This group contains a statistics of Ethernet, including the discarded packets, broadcast packets, CRC errors, size block, conflicts and etc.

## History

History is the second group in RMON. It collects the network statistics information regularly and keeps them for processing later. This group contains two subgroups:

- The subgroup History Control is used to set such control information as sampling interval and sampling data source.
- The subgroup Ethernet History provides history data about the network section traffic, error messages, broadcast packets, utilization, number of collision and other statistics for the administrator.

## Alarm

Alarm is the third group in RMON. It monitors a specific management information base (MIB) object at the specified interval. When the value of this MIB object is higher than the predefined upper limit or lower than the predefined lower limit, an alarm will be triggered. The alarm is handled as an event by means of recording the log or sending the SNMP Trap message.

## Event

Event is the ninth group in RMON. It determines to generate a log entry or a SNMP Trap message when an event is generated due to alarms.

## RMON Configuration Task List

### Configuring Statistics

One of these commands can be used to add a statistic entry.

Command	Function
Ruijie(config-if)# <b>rmon collection stats</b> <i>index</i> [ <b>owner</b> <i>ownername</i> ]	Add a statistic entry.
Ruijie(config-if)# <b>no rmon collection stats</b> <i>index</i>	Remove a statistic entry.

**Caution**

The current version of Ruijie product supports only the statistics of Ethernet interface. The index value should be an integer between 1 and 65535. At present, at most 100 statistic entries can be configured at the same time.

### Configuring History

One of these commands can be used to add a history entry.

Command	Function
Ruijie(config-if)# <b>rmon collection history</b> <i>index</i> [ <b>owner</b> <i>ownername</i> ] [ <b>buckets</b> <i>bucket-number</i> ] [ <b>interval</b> <i>seconds</i> ]	Add a history entry.
Ruijie(config-if)# <b>no rmon collection history</b> <i>index</i>	Remove a history entry.

**Caution**

The current version of Ruijie product supports only the records of Ethernet. The index value should be within 1 to 65535. At most 10 history entries can be configured.

*Bucket-number*: Specifies the used data source and time interval. Each sampling interval should be sampled once. The sampling results are saved. The Bucket-number specifies the maximum number of sampling. When the maximum is reached for the sampling records, the new one will overwrite the earliest one. The value range of Bucket-number is 1 to 65535. Its default value is 10.

Interval: Sampling interval in the range of 1 to 3600 seconds, 1800 seconds by default.

### Configuring Alarm and Event

One of these commands can be used to configure the alarm:

Command	Function
---------	----------

Command	Function
Ruijie(config)# <b>rmon alarm</b> <i>number</i> <i>variable interval {absolute   delta}</i> <b>rising-threshold</b> <i>value [event-number]</i> <b>falling-threshold</b> <i>value [event-number]</i> <b>[owner</b> <i>ownername</i> ]	Add an alarm entry.
Ruijie(config)# <b>rmon event</b> <i>number [log]</i> <b>[trap</b> <i>community</i> <b>[description</b> <i>description-string] [owner</i> <i>ownername</i> ]	Add an event entry.
Ruijie(config)# <b>no rmon alarm</b> <i>number</i>	Remove an alarm.
Ruijie(config)# <b>no rmon event</b> <i>number</i>	Remove an event.

*number*: Alarm index in the range of 1 to 65535.

*variable*: Variable to be monitored by the alarm(in integer).

*interval*: Sampling interval in the range of 1 to 4294967295.

Absolute: each sampling value compared with the upper and lower limits.

Delta: the difference with previous sampling value compared with the upper and lower limits.

*value*: Upper and lower limits.

*Event-number*: when the value exceeds the upper or lower limit, the event with the index of Event-number will be triggered.

Log: Record the event.

Trap: Send the Trap message to the NMS when the event is triggered.

*Community*: Community string used for sending the SNMP Trap message.

*Description-string*: Description of the event.

*Ownername*: Owner of the alarm or the event.

## Showing RMON status

Command	Function
Ruijie(config)# <b>show rmon alarms</b>	Show alarms.
Ruijie(config)# <b>show rmon events</b>	Show events.
Ruijie(config)# <b>show rmon history</b>	Show history.
Ruijie(config)# <b>show rmon statistics</b>	Show statistics.



## RMON Configuration Examples

### Example of Configuring Statistics

If you want to get the statistics of Ethernet Port 3 , use the following commands:

```
Ruijie(config)# interface gigabitEthernet 0/3
Ruijie(config-if)# rmon collection stats 1 owner aaa1
```

### Example of Configuring History

Use the following commands if you want to get the statistics of Ethernet Port 3 every 10 minutes:

```
Ruijie(config)# interface gigabitEthernet 0/3
Ruijie(config-if)# rmon collection history 1 owner aaa1 interval 600
```

### Example of Configuring Alarm and Event

If you want to configure the alarm function for a statistical MIB variable, the following example shows you how to set the alarm function to the instance ifInNUcastPkts.6 (number of non-unicast frames received on port 6; the ID of the instance is 1.3.6.1.2.1.2.2.1.12.6) in *IfEntry* table of MIB-II. The specific function is as follows: the switch checks the changes to the number of non-unicast frames received on port 6 every 30 seconds. If 20 or more than 20 non-unicast frames are added after last check (30 seconds earlier), or only 10 or less than 10 are added, the alarm will be triggered, and event 1 is triggered to do corresponding operations (record it into the log and send the Trap with “community” name as “rmon”). The “description” of the event is “ifInNUcastPkts is too much”. The “owner” of the alarm and the event entry is “aaa1”.

```
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 aaa1
Ruijie(config)#rmon event 1 log trap rmon description "ifInNUcastPkts is too much " owner
aaa1
```

### Example of Showing RMON Status

#### show rmon alarm

```
Ruijie# show rmon alarms
rmon alarm table:
      index: 10,
      interval: 30,
      oid = 1.3.6.1.2.1.2.2.1.12.6
      sampleType: 2,
      alarmValue: 0,
      startupAlarm: 3,
      risingThreshold: 20,
      fallingThreshold: 10,
      risingEventIndex: 1,
      fallingEventIndex: 1,
      owner: zhangesan,
      stats: 1,
```

## show rmon event

```
Ruijie# show rmon events
rmon event table:
    index = 1
    description = ifInNUcastPkts
    type = 4
    community = rmon
    lastTimeSent = 0 d:0 h:0 m:0 s
    owner = zhangsan
    status = 1
```

## show rmon history

```
Ruijie# show rmon history
rmon history control table:
    index = 1
    interface = FastEthernet 0/1
    bucketsRequested = 10
    bucketsGranted = 10
    interval = 1800
    owner = zhangsan
    stats = 1

rmon history table:
    index = 1
    sampleIndex = 198
    intervalStart = 0d:14h:0m:47s
    dropEvents = 0
    octets = 67988
    pkts = 726
    broadcastPkts = 502
    multiPkts = 189
    crcAlignErrors = 0
    underSizePkts = 0
    overSizePkts = 0
    fragments = 0
    jabbers = 0
    collisions = 0
    utilization = 0
```

## show rmon statistics

```
Ruijie# show rmon statistics
ether statistic table:
    index = 1
    interface = FastEthernet 0/1
    owner = zhangsan
    status = 0
    dropEvents = 0
    octets = 1884085
    pkts = 3096
    broadcastPkts = 161
    multiPkts = 97
    crcAlignErrors = 0
```

```
underSizePkts = 0
overSizePkts = 1200
fragments = 0
jabbers = 0
collisions = 0
packets64Octets = 128
packets65To127Octets = 336
packets128To255Octets = 229
packets256To511Octets = 3
packets512To1023Octets = 0
packets1024To1518Octets = 1200
```

# NTP Configuration

## Understanding NTP

Network Time Protocol (NTP) is designed for time synchronization on network devices. A device can synchronize its clock source and the server. Moreover, the NTP protocol can provide precise time correction (less than one millisecond on the LAN and dozens of milliseconds on the WAN, compared with the standard time) and prevent from attacks by means of encryption and confirmation.

To provide precise time, NTP needs precise time source, the Coordinated Universal Time (UTC). The NTP may obtain UTC from the atom clock, observatory, satellite or Internet. Thus, accurate and reliable time source is available.

To prevent the time server from malicious destroying, an authentication mechanism is used by the NTP to check whether the request of time correction really comes from the declared server, and check the path of returning data. This mechanism provides protection of anti-interference.

Ruijie switches support the NTP client and server. That is, the switch can not only synchronize the time of server, but also be the time server to synchronize the time of other switches. But when the switch works as the time server, it only support the unicast server mode.

## Configuring NTP

### Configuring the Global NTP Authentication Mechanism

The NTP client of Ruijie supports encrypted communication with the NTP server by means of key encryption.

There are two steps to configure the NTP client to communicate with the NTP server by means of encryption:

Step 1, Authenticate the NTP client and configure the key globally;

Step 2, Configure the trusted key for the NTP server.

To initiate the encrypted communication with the NTP server, you need to set authentication key for the NTP server in addition to performing Step 1.

By default, the NTP client does not use the global security authentication mechanism. Without this mechanism, the communication will not be encrypted. However, enabling the global security authentication does not mean that the encryption is used to implement the communication between the NTP server and the NTP client. You need to configure other keys globally and an encryption key for the NTP server.

To configure the global security authentication mechanism, run the following commands in the global configuration mode:

Command	Function
<b>ntp authenticate</b>	Configure the global NTP security authentication mechanism.
<b>no ntp authenticate</b>	Disable the global NTP security authentication mechanism.

The message is verified by the trusted key specified by the **ntp authentication-key** or **ntp trusted-key** command.

## Configuring the Global NTP Authentication Key

The next step to configure the global security authentication for the NTP is to set the global authentication key.

Each key is identified by a unique key-id globally. The customer can use the command **ntp trusted-key** to set the key corresponding to the key-id as a global trusted key.

To specify a global authentication key, run the following commands in the global configuration mode:

Command	Function
<b>ntp authentication-key</b> <i>key-id</i> <b>md5</b> <i>key-string</i> [ <b>enc-type</b> ]	Specify a global authentication key. key-id: in the range of 1 to 4294967295 key-string: Any enc-type: Two types: 0 and 7
<b>no ntp authentication-key</b> <i>key-id</i>	Remove a global authentication key.

The configuration of global authentication key does not mean the key is effective; therefore, the key must be configured as a global trusted key before using it.



### Caution

The current NTP version can support up to 1024 authentication keys and only one key can be set for each server for secure communication.

## Configure the Global NTP Trusted key ID

The last step is to set a global authentication key as a global trusted key. Only by this trusted key the user can send encrypted data and check the validity of the message.

To specify a global trusted key, run the following commands in the global configuration mode:

Command	Function
<b>ntp trusted-key</b> <i>key-id</i>	Specify a global trusted key ID.
<b>no ntp trusted-key</b> <i>key-id</i>	Remove a global trusted key ID.

The above-mentioned three steps of settings are the first procedure to implement security authentication mechanism. To initiate real encrypted communication between the NTP client and the NTP server, a trusted key must be set for the corresponding server.



### Caution

When a global authentication key is removed, its all trusted information is removed.

## Configuring the NTP Server

No NTP server is configured by default. Ruijie's client system supports simultaneous interaction with up to 20 NTP servers, and one authentication key can be set for each server to initiate encrypted communication with the NTP server after relevant settings of global authentication and key are completed.

NTP version 3 is the default version of communication with the NTP server. Meanwhile, the source interface can be configured to send the NTP message, and the NTP message from the relevant server can only be received on the sending interface.

To configure the NTP server, run the following commands in the global configuration mode:

Command	Function
<b>ntp server</b> <i>ip-addr</i> [ <b>version</b> <i>version</i> ][ <b>source</b> <i>if-name number</i> ][ <b>key</b> <i>keyid</i> ][ <b>prefer</b> ]	Configure the NTP server. version (NTP version number): 1 to 3 if-name (interface type): AggregatePort, Dialer, GigabitEthernet, Loopback, Multilink, Null, Tunnel, Virtual-ppp, Virtual-template and VLAN keyid: 1 to 4294967295
<b>no ntp server</b> <i>ip-addr</i>	Remove the NTP server.

Only when the global security authentication and key setting mechanisms are completed, and the trusted key for communicating with server is set, can the NTP client initiate the encrypted communication with the NTP server. To this end, the NTP server should have the same trusted key configured.

## Disabling the Interface to Receiving the NTP Message

The function of this command is to disable the interface to receive the NTP message.

By default, the NTP messages received on any interface are available to the NTP client for clock synchronization. This function can shield the NTP messages received on the relevant interface.



### Caution

This command takes effect only for the interface whose IP address can be configured to receive and send packets.

To disable the interface to receive the NTP message, run the following commands in the interface configuration model:

Command	Function
<b>interface</b> <i>interface-type number</i>	Enter the interface configuration mode.
<b>ntp disable</b>	Disable the function of receiving NTP messages on the interface.

To enable the function of receiving NTP messages on the interface, use the command **no ntp disable** in the interface configuration mode.

## Enabling or Disabling NTP

The **no ntp** command is to disable the NTP synchronization service, stop the time synchronization, and clear relevant information of NTP configuration.

The NTP function is disabled by default, but may be enabled as long as the NTP server is configured.

To disable the NTP, run the following commands in the global configuration mode:

Command	Function
<b>no ntp</b>	Disable the NTP function.
<b>ntp authenticate or</b> <b>ntp server</b> <i>ip-addr</i> [ <b>version</b> <i>version</i> ] [ <b>source</b> <i>if-name number</i> ] [ <b>key</b> <i>keyed</i> ] [ <b>prefer</b> ]	Enable the NTP function.

## Configuring the NTP Real-time Synchronization

To configure the NTP real-time synchronization, run the following commands in the global configuration mode:

Command	Function
<b>ntp synchronization</b>	Enable the NTP real-time synchronization.
<b>no ntp synchronization</b>	Disable the NTP real-time synchronization.

During the synchronization, the **no ntp** command and the **no ntp synchronization** command can stop or disable the time synchronization. The difference of those two commands is that the **no ntp** command not only disables the NTP function, but also clears the related NTP settings.

NTP real-time synchronization is supported on some products only. For the unsupported products, the **ntp synchronize** command cannot be run.

## Configuring the NTP Update-Calendar

The function of this command is to disable the interface to receive the NTP message.

To configure the NTP update-calendar, run the following commands in the global configuration model:

Command	Function
<b>ntp update-calendar</b>	Configure the update calendar.
<b>no ntp update-calendar</b>	Disable the function of NTP update calendar.

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.

## Configuring the NTP Master

The function of this command is to set the local time as the NTP master (the reference source of the local time is reliable), providing the synchronized time for other devices.

In general, the local system synchronizes the time from the external time source directly or indirectly. However, if the time synchronization of local system fails for the network connection trouble, ect, use the command to set the reliable reference source of the local time, providing the synchronized time for other devices.

Once set, the system time can not be synchronized to the time source with higher stratum.



#### Note

The stratum indicates the level of current clock, reference indicates the address of the server used for synchronization, freq indicates the clock frequency of current system, precision indicates the precision of current system clock, reference time indicates the UTC time of reference clock on the synchronization server, clock offset indicates the offset of current clock, root delay indicates the delay of current clock, root dispersion indicates the precision of top server, peer dispersion indicates the precision of synchronization server.

To configure the NTP master, run the following commands in the global configuration mode:

Command	Function
<b>ntp master</b> [ <i>stratum</i> ]	Set the local time as the NTP master and specify the corresponding stratum. The time stratum ranges from 1-15, 8 by default.
<b>no ntp master</b>	Cancel the NTP master settings.

The following example shows how to set the reliable reference source of the local time and set the time stratum as 12:

```
Ruijie(config)# ntp master 12
```



#### Caution

Using this command to set the local time as the master (in particular, specify a lower stratum value), is likely to be covered by the effective clock source. If multiple devices in the same network use this command, the time synchronization instability may occur due to the time difference between the devices.

In addition, before using this command, if the system has never been synchronized with an external clock source, it is necessary to manually calibrate the system clock to prevent too much bias. (For how to how to manually calibrate the system clock, please refer to the section of system time configuration of "Basic switch management Configuration Guide")

This command is not restricted by ntp access control (even if the NTP access control function has corresponding matching limit, this command is still in force).

## Configuring the Access Control Privilege of NTP Service

NTP services access control function provides a minimal security measures (more secure way is to use the NTP authentication mechanism). By default, no NTP access control rules are configured in the system.

To set the NTP services access control privilege, run the following command in the global configuration mode.

Command	Function
---------	----------



Command	Function
<b>ntp access-group { peer   serve   serve-only   query-only } access-list-number   access-list-name</b>	Set the access control privilege of the local service.
<b>no ntp access-group { peer   serve   serve-only   query-only } access-list-number   access-list-name</b>	Cancel the settings of access control privilege of the local service.

**peer:** not only allow the time requests and control queries for the local NTP service, but also allow the time synchronization between the local device and the remote system (full access privilege).

**serve:** only allow the time requests and control queries for the local NTP service, not allow the time synchronization between the local device and the remote system.

**serve-only:** only allow the time requests for the local NTP service.

**query-only:** only allow the control queries for the local NTP service.

**access-list-number:** IP access control list label; the range of 1 ~ 99 and 1300 ~ 1999. On how to create IP access control list, refer to the relevant description in "Access Control List Configuration Guide".

**access-list-name:** IP access control list name. On how to create IP access control list, refer to the relevant description in "Access Control List Configuration Guide".

When an access request arrives, NTP service matches the rules in accordance with the sequence from the smallest to the largest to access restriction, and the first matched rule shall prevail. The matching order is peer, serve, serve-only, query-only.



#### Caution

Control query function (the network management device controls the NTP server, such as setting the leap second mark or monitor the working state, etc) 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.

If you do not configure any access control rules, then all accesses are allowed. However, once the access control rules are configured, only the rule that allows access can be carried out.

The following example shows how to allow the peer device in acl1 to control the query, request for and synchronize the time with the local device; and limit the peer device in acl2 to request the time for the local device:

```
Ruijie(config)# ntp access-group peer 1
Ruijie(config)# ntp access-group serve-only 2
```

## Showing NTP Information

### NTP Debugging

If you want to debug the NTP function, this command may be used to output necessary debugging information for troubleshooting.

To debug the NTP function, run the following commands in the privilege mode:

Command	Function
<b>debug ntp</b>	Enable the debugging function.
<b>no debug ntp</b>	Disable the debugging function.

## Showing NTP Information

Execute the **show ntp status** command in the privileged EXEC mode to show the current NTP information.

To display the NTP function, run the following command in the privileged EXEC mode:

Command	Function
<b>show ntp status</b>	Show the current NTP information.

Only when the relevant communication server is configured can this command be used to print the display information.

```
Ruijie# show ntp status
Clock is synchronized, stratum 9, reference is 192.168.217.100
nominal freq is 250.0000 Hz, actual freq is 250.0000 Hz, precision is 2**18
reference time is AF3CF6AE.3BF8CB56 (20:55:10.000 UTC Mon Mar 1 1993)
clock offset is 32.97540 sec, root delay is 0.00000 sec
root dispersion is 0.00003 msec, peer dispersion is 0.00003 msec
```



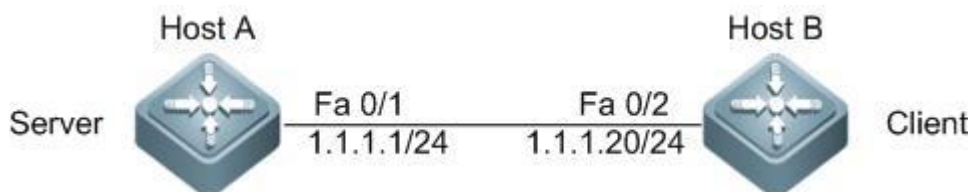
### Note

The stratum indicates the level of current clock, reference indicates the address of the server used for synchronization, freq indicates the clock frequency of current system, precision indicates the precision of current system clock, reference time indicates the UTC time of reference clock on the synchronization server, clock offset indicates the offset of current clock, root delay indicates the delay of current clock, root dispersion indicates the precision of top server, peer dispersion indicates the precision of synchronization server.

## Typical NTP Configuration Examples

### Configuring NTP client/server Mode

#### Topological Diagram



NTP client/server model

## Application Requirements

- On Host A, configure local clock as the NTP master clock, with clock stratum being 12;
- Configure the Host B as the NTP client and specify the Host A as the NTP server;
- The hardware clock of Host B shall be synchronized as well.

## Configuration Tips

### NTP server

- Generally, the local system will directly or indirectly synchronize with the external clock sources. However, the local system may not be able to synchronize with the external clock sources due to the failure of network connections. In such a case, you can execute "ntp master" command to configure the local clock as NPT master clock to synchronize time to other devices.

### NTP client

- Configure the NTP server
- By configuring NTP hardware clock update, NTP client can use the clock value synchronized from external clock sources to update its hardware clock, so that the hardware clock can also maintain precise.

## Configuration Steps

- Configuration of NTP server

! Configure NTP master clock. Configure local clock as the trusted reference clock source, with clock stratum being 12;

```
HostA(config)#ntp master 12
```

- Configuration of NTP client

! Configure Host A as the NTP server

```
HostB(config)#ntp server 1.1.1.1
```

! Configure NTP hardware clock update

```
HostB(config)# ntp update-calendar
```

## Verify Configurations

- Check the time before configuring NTP synchronization

! Check the time of reference clock source

```
HostA#show clock
```

```
17:12:48 UTC Tue, Sep 8, 2009
```

! Check the time of client before synchronization

```
HostB#show clock
```

```
12:01:10 UTC Sat, Jan 1, 2000
```

! Check the NTP status of client before synchronization

```
HostB(config)#show ntp status
```

```
Clock is unsynchronized, stratum 16, no reference clock  
nominal freq is 250.0000 Hz, actual freq is 250.0000 Hz, precision is 2**0  
  
reference time is 0.0 (00:00:00.000 UTC Thu, Jan 1, 1970)  
clock offset is 0.00000 sec, root delay is 0.00000 sec  
  
root dispersion is 0.00000 msec, peer dispersion is 0.00000 msec
```

The above information shows that the time hasn't been synchronized yet;

- After configuring NTP synchronization, display NTP configurations. Key points: NTP server address and stratum.

The following log will be printed on CLI interface:

```
*Sep  8 18:10:37: %SYS-6-CLOCKUPDATE: System clock has been updated to 18:10:37 UTC Tue  
Sep  8 2009.
```

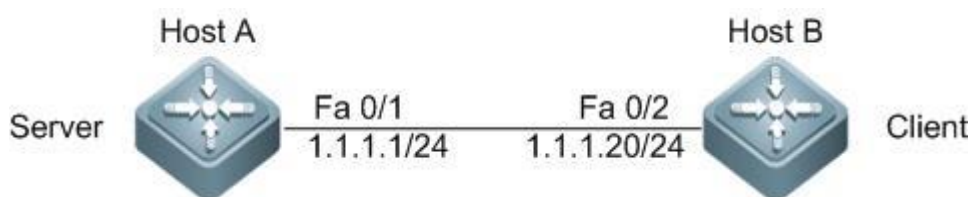
```
HostB#show ntp status
```

```
Clock is synchronized, stratum 13, reference is 1.1.1.1  
nominal freq is 250.0000 Hz, actual freq is 250.0000 Hz, precision is 2**24  
  
reference time is CE511CC9.37EB5B2D (18:11:21.000 UTC Tue, Sep 8, 2009)  
clock offset is -0.00107 sec, root delay is 0.00000 sec  
  
root dispersion is 0.00002 msec, peer dispersion is 0.00002 msec
```

The above information shows that the NTP client has connected to the server and the time of Host B has been synchronized with the time of Host A, with stratum level being higher than that of Host A by 1 level (i.e., 13).

## Configure NTP client/server Mode with authentication

### Topological Diagram



### NTP client/server model

### Application Requirements

- On Host A, configure local clock as the NTP master clock, with clock stratum being 12;
- Configure Host B as the NTP client and specify Host A as the NTP server;
- Enable the authentication mechanism to prevent illegal users from maliciously attacking the clock server.

## Configuration Tips

Configuring NTP server/client authentication will involve the following steps:

- Enable NTP global authentication
- Configure the key for NTP global authentication and the corresponding key ID
- Specify NTP global trusted key ID
- The authentication key used by NTP client to communicate with NTP server shall be identical with the corresponding Key ID.

## Configuration Steps

Configuration of NTP server

Step 1: Configure NTP master clock. Configure local clock as the trusted reference clock source, with clock stratum being 12;

```
HostA(config)#ntp master 12
```

Step 2: Configure NTP authentication;

! Enable NTP global authentication

```
HostA(config)# ntp authenticate
```

! Configure NTP global authentication key as "helloworld" and the corresponding key ID as "6"

```
HostA(config)# ntp authentication-key 6 md5 helloworld
```

! Specify "6" as the NTP global trusted key ID

```
HostA(config)# ntp trusted-key 6
```

### ■ Configuration of NTP client

Step 1: Configure NTP authentication;

! Enable NTP global authentication

```
HostB(config)# ntp authenticate
```

! Configure NTP global authentication key as "helloworld" and the corresponding key ID as "6"

```
HostB(config)# ntp authentication-key 6 md5 helloworld
```

! Specify "6" as the NTP global trusted key ID

```
HostB(config)# ntp trusted-key 6
```

! Configure Host A as the NTP server and set the key ID for communicating with this server as "6"

```
HostB(config)# ntp server 1.1.1.1 key 6
```

## Verify Configurations

- Display the configurations of NTP server. Key points: NTP master clock configuration, NTP server's IP address, and authentication related configurations.

```
HostA#show run

!

interface fastEthernet 0/1

ip address 1.1.1.1 255.255.255.0

!

ntp authentication-key 6 md5 07360623191d300a004609 7

ntp authenticate

ntp trusted-key 6

ntp master 12

!
```

- Display the configurations of NTP client. Key points: IP address and key ID of NTP server, and authentication related configurations.

```
HostB #show run

!

interface fastEthernet 0/2

ip address 1.1.1.20 255.255.255.0

!

ntp authentication-key 6 md5 141a4f012d1d3c23174905 7

ntp authenticate

ntp trusted-key 6

ntp server 1.1.1.1 key 6

!
```

After proper configuration, the following log will be printed on the CLI interface:

```
*Sep  9 11:31:29: %SYS-6-CLOCKUPDATE: System clock has been updated to 11:31:29 UTC Wed
Sep  9 2009.
```

The above log indicates that the clock of HostB (NTP client) has been updated.

- Display NTP status of NTP server

```
HostA #show ntp status

Clock is synchronized, stratum 12, 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 CE521261.E52DECA2 (11:39:13.000 UTC Wed, Sep 9, 2009)  
clock offset is 0.00000 sec, root delay is 0.00000 sec  
root dispersion is 0.00002 msec, peer dispersion is 0.00002 msec
```

- Display NTP status of NTP client. Key points: NTP server address and stratum.

```
HostB#show ntp status  
  
Clock is synchronized, stratum 13, reference is 1.1.1.1  
  
nominal freq is 250.0000 Hz, actual freq is 250.0000 Hz, precision is 2**24  
reference time is CE5212A1.E5D712A0 (11:40:17.000 UTC Wed, Sep 9, 2009)  
clock offset is -0.00005 sec, root delay is 0.00000 sec  
root dispersion is 0.00002 msec, peer dispersion is 0.00002 msec
```

The above information shows that the NTP client has successfully connected to the server and the time of Host B has been synchronized with the time of Host A, with stratum level being higher than that of Host A by 1 level (i.e., 13).

# SNTP Configuration

## Overview

Network Time Protocol (NTP) is designed for time synchronization on network devices. Another protocol, Simple Network Time Protocol (SNMP) can be used to synchronize the network time, too.

NTP protocol can be used across various platforms and operating systems, and provide precise time calculation (1-50ms precision) and prevent from latency and jitter in the network. NTP also provides the authentication mechanism with high security level. However, NTP algorithm is complicated and demands better system.

As a simplified version of NTP, SNTP simplifies the algorithm of time calculation but also has great performance, with precision of about 1s.

SNTP Client is totally compatible with the NTP Server due to the consistency of the SNTP and NTP messages.

## Understanding SNTP

SNTP works in the way of Client/Server. The standard Server system time is set by receiving the GPS signal or the atomic clock. The Client obtains its accurate time from the service time accessing the server regularly, and adjusts its system clock to synchronize the time.

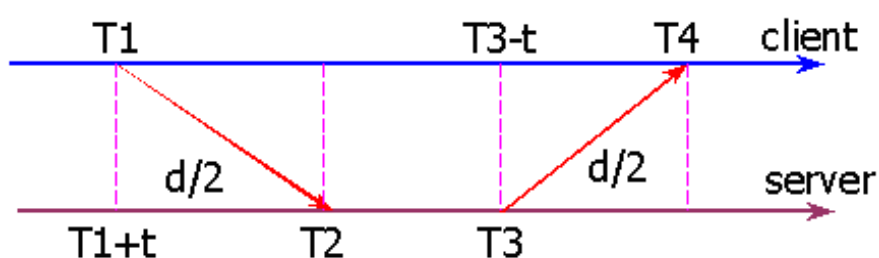


Figure-1

Originate Timestamp	T1	time request sent by client
Receive Timestamp	T2	time request received at server
Transmit Timestamp	T3	time reply sent by server
Destination Timestamp	T4	time reply received at client

T1: time request sent by client (refer to the client time) with the mark "Originate Timestamp";

T2: time request received at server (refer to the server time) with the mark "Receive Timestamp";

T3: time reply by server (refer to the server time) with the mark "Transmit Timestamp";

T4: time reply received at client (refer to the client time) with the mark "Destination Timestamp".

T: time deviation between the Server and the Client

d: time between the Server and the Client



The following formula calculates the time:

$$\therefore T2 = T1 + t + d / 2;$$

$$\therefore T2 - T1 = t + d / 2;$$

$$\therefore T4 = T3 - t + d / 2;$$

$$\therefore T3 - T4 = t - d / 2;$$

$$\therefore d = (T4 - T1) - (T3 - T2);$$

$$t = ((T2 - T1) + (T3 - T4)) / 2;$$

Then, according to the value of  $t$  and  $d$ , SNTP Client gets the current time:  $T4+t$ .

## Configuring SNTP

### Default Configuration

By default, the SNTP configurations are as follows:

Function	Default
SNTP state	Disabled.
IP address for the NTP server	0.
SNTP Sync Interval	1800s
Local Time-zone	GMT+8

### Enabling SNTP

To enable the SNTP, run the following commands in the global configuration mode:

Command	Function
Ruijie(config)# <b>sntp enable</b>	Enable the SNTP and synchronize the time once immediately. (in order to prevent frequent time synchronization, the sync-interval must not be less than 5s.)

To disable the SNTP, use the **no sntp enable** command.

### Configuring the IP address for the NTP server

The SNTP Client is totally compatible with the NTP Server due to the inconsistency of SNTP and NTP messages. There are many NTP servers in the network; you can choose one switch with less latency as the NTP server.

For the detailed NTP server ip addresses, please logon to <http://www.time.edu.cn/> or <http://www.ntp.org/>. For example, 192.43.244.18 (time.nist.gov).

To set the IP address for the SNTP server, run the following commands in the global configuration mode:

Command	Function
Ruijie(config)# <b>sntp server</b> <i>ip-address</i>	Specify the IP address for the SNTP server.

## Configuring the SNTP Sync Interval

To adjust the time regularly, you need to set the sync interval for SNTP Client to access the NTP server SNTP Client regularly.

To configure the SNTP sync interval, run the following commands in the global configuration mode:

Command	Function
Ruijie(config)# <b>sntp interval</b> <i>seconds</i>	Configure the SNTP sync interval, in second. Interval range: 60-65535s; Default value: 1800s.



### Caution

The sync interval configuration cannot take effect immediately. You shall execute the **sntp enable** command immediately after configuring the SNTP sync interval.

## Configuring the Local Time-zone

The time obtained through the SNTP communication is Greenwich Mean Time(GMT). In order to obtain the exact local time, you need to set the local time to adjust the mean time.

To configure the local time-zone, run the following commands in the interface configuration model:

Command	Function
Ruijie(config)# <b>clock time-zone</b> <i>time-zone</i>	Configure the time-zone, ranging from GMT-23 to GMT+23, wherein “-” indicates western area, “+” indicates eastern area and “0” indicates Greenwich mean time. The default time-zone is GMT+8, Beijing time.

To restore the local time-zone to the default, use the command **no clock time-zone**.

## Showing SNTP Information

Execute the **show sntp** command in the privileged EXEC mode to show the current SNTP information.

```
Ruijie# show sntp
SNTP state           : ENABLE           //to view whether SNTP is enabled or not
SNTP server          : 192.168.4.12     //NTP Server
SNTP sync interval   : 60              //SNTP sync interval
Time zone            : +8               //Local Time-zone
```

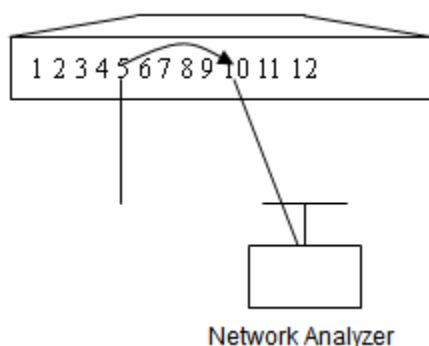
# SPAN Configuration

## Overview

With SPAN, you can analyze the communications between ports by copying a frame from one port to another port connected with a network analysis device or RMON analyzer. The SPAN mirrors all the packets sent/received at a port to a physical port for analysis.

For example, all the frames on the GigabitEthernet port 5 are mirrored to the GigabitEthernet port 10, as shown in Figure 18-1. Although the network analyzer connected to port 10 is not directly connected to port 5, it can receive all the frames from port 5.

Figure 1-1 SPAN Configuration Example



The SPAN allows you to monitor all the frames incoming/outgoing the source port, including the route input frames.

The SPAN does not affect the normal packet switching of the switch. Instead, it copies the frames incoming/outgoing the source port to the destination port. However, the frames may be discarded on an overflowed destination port, for example, when an 100Mbps port monitors an 1000Mbps port.

## SPAN Concepts and Terms

### SPAN Session

One SPAN session is the combination of one destination port and source port. You can monitor the received, transmitted, and bi-directional frames of one or multiple interfaces.

You can set up one or multiple SPAN sessions. Switched port and routed port can be configured with only one SPAN session. However, switched port, routed port, and AP can be configured as source port and destination port. The SPAN session does not affect the normal operation of the switch.

You can configure the SPAN session on one disabled port, but the SPAN does not take effect until you enable the destination and source ports. The **show monitor session session number** command allows you to show the operation status of the SPAN session. One SPAN session does not take effect immediately after the switch is powered on until the destination port is active.

## Frame Type

### Frame Direction

The SPAN session includes the following frame types:

- Received frames

Received frames include all known unicast frames and routing frames, and each received frame is copied to the destination port. In one SPAN session, you can monitor the frames inputted from one or multiple source ports. Although a frame inputted from the source port is dropped due to some reasons, for example, port security, it is still sent to the destination port. This does not affect the function of the SPAN.

- Transmitted frames

All the frames sent from the source port are copied to the destination port. In one SPAN session, you can monitor the frames input from one or multiple source ports. If a frame from a port to the source port is dropped due to some reasons, the frame will not be sent to the destination port as well. Moreover, the format of the frames destined to the source port may change, for example, routed frames, source MAC address, destination MAC address, VLAN ID and TTL. Similarly, the format of the frames copied to the destination port will change.

- Bi-directional frames

Bi-directional frames include the above mentioned two frames. In one SPAN session, you can monitor the frames received and transmitted from/to one or multiple source ports.

### SPAN Traffic

You can use the SPAN to monitor all network communications, including multicast frames and BPDU frames.

### Source Port

A source port (also known as monitored interface) is a switched port or routed port monitored for network analysis. In one SPAN session, you can monitor received, transmitted and bi-directional frames. There is no limit on the maximum number of the source ports.

A source port has the following features:

- It can be a switched port, routed port or AP.
- It cannot be a destination port at the same time.
- It can specify the inbound or outbound direction of the monitored frames.
- The source port and the destination port can reside in the same VLAN or different VLANs.

### Destination Port

The SPAN session has a destination port (also known as the monitoring port) used to receive the frames copied from the source port.

The destination port has the following features:

- It can be a Switched Port , Routed Port or AP.

- The destination port cannot be the source port at the same time.

## Interaction between the SPAN and Other Functions

The SPAN interacts with the following functions.

- Spanning Tree Protocol (STP) — the destination port of SPAN participates in the STP.

## Configuring SPAN

### Default SPAN Configuration

Function	Default Configuration
SPAN status	Disabled

### Creating a SPAN Session and Specifying the Monitoring Port and Monitored Port

To set up a SPAN session and specify the destination port and the source port, execute the following commands.

Command	Function
Ruijie(config)# <b>monitor session</b> <i>session_number</i> <b>source interface</b> <i>interface-id</i> [,] [-] { <b>both</b>   <b>rx</b>   <b>tx</b> }	Specify the source port. <i>interface-id</i> : Specify corresponding interface id.
Ruijie(config)# <b>monitor session</b> <i>session_number</i> <b>destination interface</b> <i>interface-id</i> [ <b>switch</b> ]	Specify the destination port. <i>interface-id</i> : Specify corresponding interface id. The <b>switch</b> parameter supports exchange on the mirrored destination port.

To delete a SPAN session, use the **no monitor session** *session\_number* command in the global configuration mode. To delete all the SPAN sessions, use the **no monitor session all** command in the global configuration mode. You can use the **no monitor session** *session\_number* **source interface** *interface-id* command or the **no monitor session** *session\_number* **destination interface** *interface-id* command to delete the source port or destination port in the global configuration mode.

The following example shows how to create session 1. First, clear the configuration of session 1, and then mirror the frames from port 1 to port 8. The **Show monitor session** command allows you to verify your configuration.

```
Ruijie(config)# no monitor session 1
Ruijie(config)# monitor session 1 source interface gigabitEthernet 3/1 both
Ruijie(config)# monitor session 1 destination interface gigabitEthernet 3/8
Ruijie(config)# end
Ruijie# show monitor session 1
sess-num: 1
src-intf:
GigabitEthernet 3/1 frame-type Both
dest-intf:
GigabitEthernet 3/8
```

**Caution**

Session 1 is used to support the global cross-linecard port mirror.

## Deleting a Port from the SPAN Session

To delete a port from a SPAN session, execute the following commands:

Command	Function
Ruijie(config)# <b>no monitor session</b> <i>session_number</i> <b>source interface</b> <i>interface-id</i> [,] [-] [ <b>both</b>   <b>rx</b>   <b>tx</b> ]	Specify the source port to delete. <i>interface-id</i> : Specify corresponding interface id.

You can use the **no monitor session** *session\_number* **source interface** *interface-id* command to delete the source port from a SPAN session in the global configuration mode. The following example shows how to delete port 1 from session 1 and verify your configuration.

```
Ruijie(config)# no monitor session 1 source interface gigabitethernet 1/1 both
Ruijie(config)# end
Ruijie# show monitor session 1
sess-num: 1
dest-intf:
GigabitEthernet 3/8
```

## Configuring the Flow-based Mirror

To configure the flow-based mirror, execute the following commands:

Command	Function
Ruijie(config)# [ <b>no</b> ] <b>monitor session</b> <i>session_number</i> <b>source interface</b> <i>interface-id</i> <b>rx acl</b> <i>name</i>	Specify the matched acl name for the mirrored flow and the mirrored source and destination ports.

**Product Support**

Only the incoming port mirror is supported.

## Other Precautions

- Connect the network analyzer to the monitoring port.
- When the SPAN is enabled, the configuration change has the following result.
  1. If you change the VLAN configuration of the source port, the configuration takes effect immediately.
  2. If you change the VLAN configuration of the destination port, the configuration takes effect immediately.
  3. If you have disabled the source port or destination port, the SPAN does not take effect.

4. If you add the source or destination port to an AP, this will remove the source port or destination port from the SPAN.

## Showing the SPAN Status

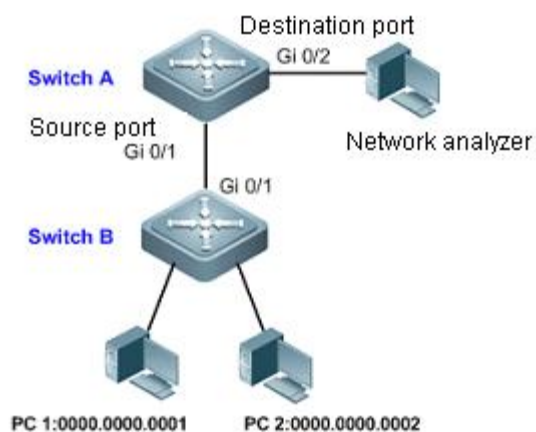
The **show monitor** command shows the current SPAN status. The following example illustrates how to show the current status of SPAN session 1.

```
Ruijie# show monitor session 1
sess-num: 1
src-intf:
GigabitEthernet 3/1 frame-type Both
dest-intf:
GigabitEthernet 3/8
```

## Typical SPAN Configuration Examples

### Example of Flow-based Mirror Configuration

#### Topology Diagram



#### Topology for simple SPAN application

### Application Requirements

The network analyzer shall be able to monitor all dataflow forwarded by Switch A to Switch B and monitor specific dataflow from Switch B (such as the traffic from PC1 and PC2).

### Configuration tips

- Configure SPAN on the device (Switch A) connecting with network analyzer; configure the port (Gi 0/1) connected with Switch B as SPAN source port, and configure the port (Gi 0/2) connected with network analyzer as SPAN destination port.
- Configure flow-based mirror (traffic from PC1 and PC2) on SPAN source port (Gi 0/1).

## Configuration Steps

Step 1: Configure interconnection ports.

! Configure port Gi 0/1 of Switch A as Trunk Port.

```
SwitchA#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
SwitchA(config)#interface gigabitEthernet 0/1
SwitchA(config-if-GigabitEthernet 0/1)#switchport mode trunk
SwitchA(config-if-GigabitEthernet 0/1)#exit
```

Step 2: Configure ACL.

! Create MAC extended ACL of "ruijie" on Switch A to permit source MACs of 0000.0000.0001 and 0000.0000.0002.

```
SwitchA(config)#mac access-list extended ruijie
SwitchA(config-mac-nacl)#permit host 0000.0000.0001 any
SwitchA(config-mac-nacl)#permit host 0000.0000.0002 any
SwitchA(config-mac-nacl)#exit
```

Step 3: Create SPAN session and specify the source port and destination port.

! On Switch A, create Session 1 and configure Gi 0/1 as the source port for mirroring bidirectional dataflow, and configure flow-based ingress mirror.

```
SwitchA(config)#monitor session 1 source interface gigabitEthernet 0/1 tx
SwitchA(config)#monitor session 1 source interface gigabitEthernet 0/1 rx acl ruijie
```

! On Switch A, configure Gi 0/2 as the destination port of Session 1

```
SwitchA(config)#monitor session 1 destination interface gigabitEthernet 0/2
```

## Verification

Step 1: Display configurations of respective devices.

```
SwitchA#show running-config
!
mac access-list extended ruijie
  10 permit host 0000.0000.0001 any etype-any
  20 permit host 0000.0000.0002 any etype-any
!
interface GigabitEthernet 0/1
  switchport mode trunk
!
monitor session 1 destination interface GigabitEthernet 0/2
monitor session 1 source interface GigabitEthernet 0/1 tx
monitor session 1 source interface GigabitEthernet 0/1 rx acl ruijie
!
```

Step 2: Display SPAN state of the device.



```
SwitchA#show monitor session 1
sess-num: 1 //SPAN Session
span-type: LOCAL_SPAN //Local SPAN
src-intf: //information about SPAN source port
GigabitEthernet 0/1 frame-type Both
rx acl id 2900 //Traffic-based SPAN
acl name ruijie
dest-intf: //Information about SPAN destination port
GigabitEthernet 0/2
```

# RSPAN Configuration

## Overview

RSPAN is the expansion of SPAN. Remote mirroring breaks the restriction that mirrored port and mirroring port must be on the same device. Multiple network devices are deployed between them and administrators can observe the data packets on the remotely mirroring port by analyzer in the central machine room.

All the mirrored packets are transmitted to the remote mirroring port via a special RSPAN Vlan (also known as Remote VLAN). Typical application topology is shown as below.

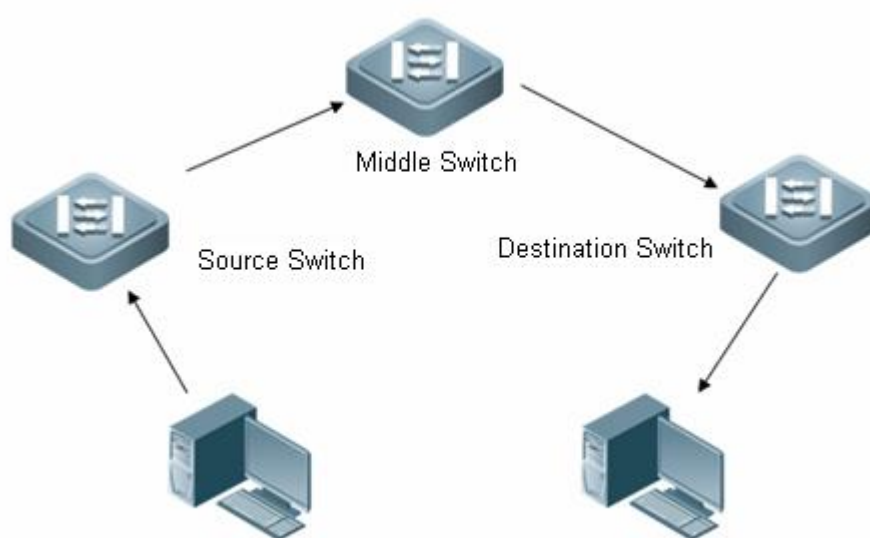


Figure 1 Typical RSPAN application topology

Figure 1 illustrates three roles:


- Source switch: Where the mirrored port is. The source switch copies the packets of source port and forwards them through the Remote VLAN to the middle switch or the destination switch.
- Middle switch: The one between the source switch and the destination switch. It transmits the mirrored packets to the next middle switch or the destination switch via Remote VLAN. If the source switch is directly connected with the destination switch, then there is no middle switch.
- Destination switch: Where the mirroring destination port is. It forwards the mirrored packets received from Remote VLAN to the monitoring device via the mirroring destination port.

The table below presents ports that participate mirroring on the switch:

Switch	Mirrored Port	Function
--------	---------------	----------

Source switch	Source Port	Monitored user port that copies UDP to the designated output port or the reflector port via local port mirroring. There are many source ports.
	Reflector port	Used for one-to-many mirroring. The packets from the mirrored source port are reflected through the reflector port and then outputted through the output port. The reflector port cannot forward traffic. It is recommended to set the port in down state to be reflector port and disable any configuration on it.
	Output port	Send mirrored packets to the middle switch or the destination switch.
Middle switch	Common port	Send mirrored packets to the destination switch. It is recommended to configure two Trunk ports on the middle switch to connect the devices on both sides.
Destination switch	Source port	Receive remote mirrored packets.
	Destination port	Monitoring port of remote mirrored packets.

A special VLAN, Remote VLAN is defined for remote port mirroring. The Remote VLAN transmits only mirrored packet rather than bearing normal services. All mirrored packets are transmitted from the source switch through the Remote VLAN to the designated port of the destination switch. Hence, you can monitor the packets of the source switch on the destination switch.

 <b>Note</b>	<ul style="list-style-type: none"> <li>■ RSPAN and local SPAN can be enabled simultaneously on the source switch, the middle switch and the destination switch.</li> <li>■ The packets of Remote VLAN bring no influence on the CPU utilization.</li> <li>■ You can enable or disable communications on the mirroring destination port. Communications is disabled by default.</li> <li>■ It is recommended to set the mirrored source port and reflector port in different VLANs.</li> <li>■ AP cannot be set as the Reflector Port.</li> <li>■ Remote VLAN can neither be VLAN 1 nor Private VLAN.</li> <li>■ Remote VLAN does not join GVRP.</li> </ul>
--	--

# Configuring RSPAN

## Configuration Preparation

- Determine the source switch, the middle switch and the destination switch.
- Determine the mirrored source port, the reflector port, the mirrored destination port and Remote VLAN.
- Guarantee L2 interoperability between the source switch and the destination switch in Remote VLAN.
- Determine the direction of monitored packets.
- Enable Remote VLAN

## Configuring the Source Switch

### Configuring RSPAN Session

RSPAN session has the same features as local SPAN session. For details, refer to SPAN Configuration Guide.

### Configuring Source Port

Source port is also known as monitored port. In a RSPAN session, data streams of source port are monitored for analysis or troubleshooting. Users can monitor incoming, outgoing or both data streams. The number of source ports is also not limited.

The source port comes with the following features:

- Source port can be switched port, routed port or AP.
- Multiple source ports on the source switch can be mirrored to the designated output port.
- Source port and output port cannot be set to the same one.
- When the mirrored source port is a Layer 3 port, Layer 2 and Layer 3 packets can be monitored.
- In case of bidirectional monitoring of multiple ports, you only need to monitor one flow direction of packets.
- You can monitor the incoming and outgoing packets on the STP-enabled port in block state.
- The source port and the destination port can belong to the same VLAN or different VLANs.

### Configuring Output Port

The RSPAN mirrored streams are broadcasted from the output port of the source switch to the middle switch. The output port features:


- The output port can be switched port, routed port or AP.
- The output port belongs to only one RSPAN session.

## Configuring Remote VLAN

RSPAN mirrored streams are broadcasted via the Remote VLAN. The Remote VLAN transmits only mirrored packets rather than bearing normal services. All mirrored packets are transmitted from the source switch through the Remote VLAN to the designated port of the destination switch. Hence, you can monitor the packets of the source switch on the destination switch.

Remote VLAN features:

- Remote VLAN can neither be VLAN 1 nor private VLAN.
- One Remote VLAN corresponds to one RSPAN session.

 <b>Note</b>	<p>The reflector port needs to join the Remote VLAN.</p> <p>The reflector port cannot forward traffic as normal port. It is recommended to set the port in down state as reflector port and disable other configurations on it.</p>
--	---

## Configure VSPAN

VSPAN, the abbreviation of VLAN SPAN, refers to mirroring the data streams of some VLANs as source to the destination port of the destination device.

VSPAN features:

- A VLAN other than Remote VLAN can be set as the source of mirrored packets by the monitor session session-num source vlan vlan-id [rx | tx | both] command.
- Some VLANs other than Remote VLAN can be set as the source of mirrored packets by the monitor session session-num filter vlan vlan-id-list command.

## Configuring One-to-many Mirroring

RSPAN session supports more than one destination device, each device supports one destination port. To enable one-to-many mirroring, run the following command to configure the reflector port on the source switch:

Command	Function
<pre>Ruijie(config)#      monitor      session session_num  destination remote vlan remote_vlan-id [reflector-port] interface interface-name [switch]</pre>	<p>Configure Remote VLAN and reflector port.</p> <p>The reflector port should join the Remote VLAN.</p> <p>The Switch keyword indicates the destination port joins switching.</p>

 <b>Note</b>	<p>The reflector port needs to join the Remote VLAN.</p> <p>The reflector port cannot forward traffic as normal port. It is recommended to set the port in down state as reflector port and disable other configurations on it.</p>
--	---

## Configuration Steps

Configure the source switch by the following steps:

Command	Function
Ruijie# <b>configure terminal</b>	Enter the global configuration mode.
Ruijie(config)# <b>vlan</b> <i>vlan-id</i>	Enter the VLAN configuration mode.
Ruijie(config-Vlan)# <b>remote-span</b>	Set the VLAN as the remote SPAN VLAN.
Ruijie(config-Vlan)# <b>exit</b>	Return to the global configuration mode.
Ruijie(config)# <b>monitor session</b> <i>session_num</i> <b>remote-source</b>	Configure the remote mirroring source.
Ruijie(config)# <b>monitor session-num source interface</b> <i>interface-name</i> [ <b>rx</b>   <b>tx</b>   <b>both</b> ]	Configure the remote mirrored source port (rx and tx of the source port can be set to the same or different destination port; but each of them can be configured with one destination port only. )
Ruijie(config)# <b>monitor session-num destination remote vlan</b> <i>remote_vlan-id</i> [ <i>reflector-port</i> ] <b>interface</b> <i>interface-name</i> [ <b>switch</b> ]	Configure Remote VLAN and reflector port. The reflector port should join the remote VLAN. The output destination port is mandatory. <b>switch</b> indicates the destination port joins switching.
Ruijie(config)# <b>monitor session-number source interface</b> <i>interface-id</i> <b>rx acl name</b>	Set the ACL for the streams to be mirrored.



- It is not recommended to add common ports to Remote VLAN.
- Do not set the port that is connected to the middle switch or the destination switch to be the mirrored source port, or otherwise it may cause flow confusion in the network.
- In a RSPAN session, if the middle switch uses the port of non-E series line cards as forwarding port, only RX or TX mirroring can be configured on the source switch. And if alternative configuration of TX mirroring and RX mirroring is executed on the source switch, you should clear the MAC address of Remote VLAN on the middle switch.

## Configuring the Middle Switch

In a RSPAN session, the middle switch ensures transparent transmission of mirrored packets in a VLAN.

Command	Function
Ruijie# <b>configure terminal</b>	Enter the global configuration mode.
Ruijie(config)# <b>vlan</b> <i>vlan-id</i>	Enter the VLAN configuration mode.
Ruijie(config-Vlan)# <b>remote-span</b>	Set the VLAN as the remote-span VLAN.
Ruijie(config-Vlan)# <b>exit</b>	Return to the global configuration mode.

## Configuring the Destination Switch

### Destination Port

The remote RSPAN device forwards the mirrored packets received from the Remote VLAN to the monitoring device through the destination port.

Destination port features:

- The destination port can be switched port, routed port or AP.
- The destination port can be set to enable or disable communications. Communications is disabled by default. Under default configuration, neither the packets from other ports nor the packets from CPU are forwarded.

### Configuration Steps

Command	Function
Ruijie# <b>configure terminal</b>	Enter the global configuration mode.
Ruijie(config)# <b>vlan</b> <i>vlan-id</i>	Enter the VLAN configuration mode.
Ruijie(config-Vlan)# <b>remote-span</b>	Set the VLAN as remote-span Vlan.
Ruijie(config-Vlan)# <b>exit</b>	Return to the global configuration mode.
Ruijie(config)# <b>monitor session</b> <i>session_num</i> <b>remote-destination</b>	Configure the remote mirroring destination.
Ruijie(config)# <b>monitor session</b> <i>session-num</i> <b>destination remote vlan</b> <i>vlan-id</i> <b>interface</b> <i>interface-name</i> [ <b>switch</b> ]	Configure Remote VLAN and the remote mirroring destination port. <b>switch</b> indicates the destination port joins switching.
Ruijie(config)# <b>interface</b> <i>interface-name</i>	Enter the remote mirroring destination port.
Ruijie(config-if)# { <b>switchport access vlan</b> <i>vid</i>   <b>switchport trunk native vlan</b> <i>vid</i> }	<i>Vid</i> : VID for remote-span vlan. If the destination port is access port, join the destination port to remote-span vlan; If the destination port is trunk port, join the destination port to remote-span vlan and set the remote-span vlan as the native vlan for the destination port.

## Configuring Flow-based RSPAN

As the expansion of local SPAN, RSPAN supports flow-based mirroring as well. For details, refer to *Mirroring Configuration Guide*.



### Note

- Flow-based RSPAN brings no influence on communications.
- Users can set ACL at the inbound direction of the source port of the source RSPAN switch. Standard ACL, extended ACL, MAC ACL and user-defined ACL are supported.
- Users can set port ACL at the inbound direction of the source port of the source RSPAN switch, and set port ACL at the outbound direction of the destination port of the destination RSPAN switch.
- Users can apply ACL at the outbound direction of Remote VLAN on the source RSPAN switch, and apply ACL at the inbound direction of Remote VLAN on the destination RSPAN switch.

## Showing RSPAN Session

Command	Function
Ruijie# <b>show monitor</b>	Show the mirroring configuration.

For example:

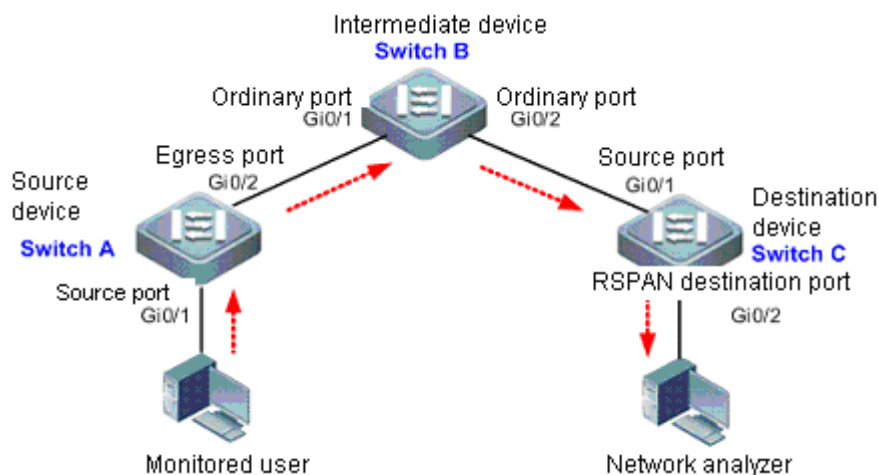
```
Ruijie# show monitor
sess-num: 1
src-intf:
GigabitEthernet 0/4 frame-type Both
dest-intf:
GigabitEthernet 0/6
remote vlan 3
```



## Typical RSPAN Configuration Examples

### Example of configuring RSPAN without supporting reflector port

#### Topological Diagram



Application topology for RSPAN without supporting reflector port

#### Application Requirements

- The network analyzer can monitor the user through remote span.
- Data can be exchanged normally between devices.

#### Configuration Tips

- Configure Remote VLAN on the source device (Switch A), intermediate device (Switch B) and destination device (Switch C).
- On the source device, configure the port (Gi 0/1) directly connected with user as the source port, and configure the port (Gi 0/2) connected with intermediate device as the egress port; enable traffic exchange on the egress port.
- On the intermediate device, ports (Gi 0/1 and Gi 0/2) connected with source device and destination device are configured to ordinary ports.
- On the destination device, the port (Gi 0/1) connected with the intermediate device acts as the source port (configured to ordinary port), and the port (Gi 0/2) connected with network analyzer shall be configured to RSPAN destination port, on which traffic exchange shall be enabled.



- 1. This example applies to devices which doesn't support the reflector port.
- 2. The RSPAN traffic forwarded through the egress port of source device can be broadcasted in Remote VLAN, so that any port other than the source device can monitor the source port after joining Remote VLAN, allowing one-to-many remote mirroring. If a RSPAN destination port is specified on the destination device, then the RSPAN traffic will only be forwarded to this destination port.

## Configuration Steps

Step 1: Configure the Remote VLAN.

! Create VLAN 7 on Switch A and set it as Remote VLAN.

```
SwitchA#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
SwitchA(config)#vlan 7
SwitchA(config-vlan)#remote-span
SwitchA(config-vlan)#exit
```

! Configurations of Switch B and Switch C are the same as above.

Step 2: Configure the RSPAN source device.

! On Switch A, configure port Gi 0/2 as the Trunk Port for connecting Switch B.

```
SwitchA(config)#interface gigabitEthernet 0/2
SwitchA(config-if-GigabitEthernet 0/2)#switchport mode trunk
SwitchA(config-if-GigabitEthernet 0/2)#exit
```

! On Switch A, create RSPAN Session 1; configure this device as the source device and configure Gi 0/1 as the source port and Gi 0/2 as the egress port.

```
SwitchA(config)#monitor session 1 remote-source
SwitchA(config)#monitor session 1 source interface gigabitEthernet 0/1 both
SwitchA(config)#monitor session 1 destination remote vlan 7 interface gigabitEthernet 0/2
switch
```

Step 3: Configure RSPAN intermediate device

! On Switch B, configure ports Gi 0/1 and Gi 0/2 as the Trunk Port.

```
SwitchB(config)#interface range gigabitEthernet 0/1-2
SwitchB(config-if-range)#switchport mode trunk
```

Step 4: Configure RSPAN destination device

! On Switch C, configure port Gi 0/1 as the Trunk Port, which is used as the source port to connect Switch B

```
SwitchC(config)#interface gigabitEthernet 0/1
SwitchC(config-if-GigabitEthernet 0/1)#switchport mode trunk
```

! On Switch C, create RSPAN Session; configure this device as the destination device and configure Gi 0/2 as RSPAN destination port.

```
SwitchC(config)#monitor session 1 remote-destination
SwitchC(config)#monitor session 1 destination remote vlan 7 interface gigabitEthernet 0/2
switch
```

## Verification

Step 1: Display configurations of the device.

! Configurations of Switch A

```
SwitchA#show running-config
!
vlan 7
    remote-span
!
interface GigabitEthernet 0/2
    switchport mode trunk
!
monitor session 1 remote-source
monitor session 1 destination remote vlan 7 interface GigabitEthernet 0/2 switch
monitor session 1 source interface GigabitEthernet 0/1 both
!
```

! Configurations of Switch B

```
SwitchB#show running-config
!
vlan 7
    remote-span
!
interface GigabitEthernet 0/1
    switchport mode trunk
!
interface GigabitEthernet 0/2
    switchport mode trunk
```

! Configurations of Switch C

```
SwitchC#show running-config
!
vlan 7
    remote-span
!
interface GigabitEthernet 0/1
```

```

switchport mode trunk
!
monitor session 1 remote-destination
monitor session 1 destination remote vlan 7 interface GigabitEthernet 0/2 switch

```

Step 2: Display RSPAN information of the device

! Switch A

```

SwitchA#show monitor
sess-num: 1                               //RSPAN Session
span-type: SOURCE_SPAN                   //RSPAN source device
src-intf:                               //information about RSPAN source port
GigabitEthernet 0/1                      frame-type Both
dest-intf:                               //information about RSPAN egress port
GigabitEthernet 0/2
remote vlan 7
mtp_switch on                            //Allow the egress port to exchange normal traffic

```

! Switch C

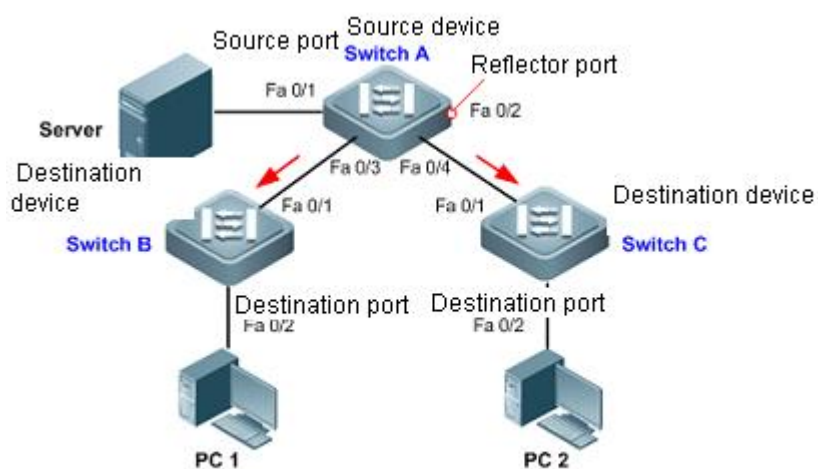
```

SwitchC#show monitor
sess-num: 1                               //RSPAN Session
span-type: DEST_SPAN                     //RSPAN destination device
dest-intf:                               //information about RSPAN destination port
GigabitEthernet 0/2
remote vlan 7
mtp_switch on                            //Allow the destination port to exchange data

```

## Example of configuring RSPAN supporting reflector port

### Topological Diagram



Application topology for RSPAN supporting reflector port

## Application Requirements

Achieve one-to-many remote SPAN, namely both PC1 and PC2 can monitor the traffic sent and received on the service through remote SPAN.

## Configuration Tips

- Create Remote VLAN on all associated devices (Switch A, B and C).
- Configure the server-connecting device (Switch A) as RSPAN source device and configure the server-connecting port (Fa 0/1) as RSPAN source port; configure one port (Fa 0/2) in Down state as the reflector port.
- Configure the PC-connecting devices (Switch B and Switch C) as RSPAN destination device and configure the PC-connecting ports (Fa 0/2) as RSPAN destination port.
- The ports interconnecting devices are only needed to be configured as Trunk port, which by default can forward the RSPAN traffic in Remote VLAN.



### Caution

- This example applies to devices which support the reflector port.
- The RSPAN traffic forwarded through the reflector port can be broadcasted in Remote VLAN, so that any port joining the Remote VLAN can monitor the source port, allowing one-to-many mirroring. If a RSPAN destination port is specified on the destination device, then the RSPAN traffic will only be forwarded to this destination port.
- If multiple intermediate devices exist between source device and destination device, we only need to configure Remote VLAN on the intermediate devices and configure interconnecting ports as Trunk Port to realize cross-device remote SPAN.

## Configuration Steps

Step 1: Create Remote VLAN on the device.

! Create Remote VLAN 7 on Switch A.

```
SwitchA#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
SwitchA(config)#vlan 7
SwitchA(config-vlan)#remote-span
SwitchA(config-vlan)#exit
```

! Configurations of Switch B and Switch C are the same as above.

Step 2: Configure RSPAN source device.

! On Switch A, create RSPAN Session 1; configure this device as the source device and configure Fa 0/1 as RSPAN source port and Fa 0/2 as the reflector port. We can find out that the port state changes from Down to Up.

```
SwitchA(config)#monitor session 1 remote-source
SwitchA(config)#monitor session 1 source interface fastEthernet 0/1 both
SwitchA(config)#monitor session 1 destination remote vlan 7 reflector-port interface
fastEthernet 0/2 switch
```

Step 3: Configure RSPAN destination device.

! On Switch B, create RSPAN Session 1; configure this device as the destination device and configure Fa 0/2 as RSPAN destination port.

```
SwitchB(config)#monitor session 1 remote-destination
SwitchB(config)#monitor session 1 destination remote vlan 7 interface fastEthernet 0/2
switch
```

! Configurations of Switch C are the same as above.

Step 4: Configure ports interconnecting devices as Trunk port.

! Configure ports Fa 0/3 and Fa 0/4 of Switch A as Trunk Port.

```
SwitchA(config)#interface range fastEthernet 0/3-4
SwitchA(config-if-range)#switchport mode trunk
```

! Configure port Gi 0/1 of Switch B as Trunk Port.

```
SwitchB(config)#interface fastEthernet 0/1
SwitchB(config-if-FastEthernet 0/1)#switchport mode trunk
```

! Configurations of Switch C are the same as those of Switch B.

## Verification

Step 1: Display configurations of respective devices.

! Configurations of Switch A

```
SwitchA#show running-config
!
vlan 7
  remote-span
!
interface FastEthernet 0/3
  switchport mode trunk
!
interface FastEthernet 0/4
  switchport mode trunk
!
monitor session 1 remote-source
monitor session 1 destination remote vlan 7 reflector-port interface FastEthernet 0/2 switch
monitor session 1 source interface FastEthernet 0/1 both
```

! Configurations of Switch B

```
SwitchB#show running-config
!
vlan 7
    remote-span
!
interface FastEthernet 0/1
    switchport mode trunk
!
monitor session 1 remote-destination
monitor session 1 destination remote vlan 7 interface FastEthernet 0/2 switch
```

! Configurations of Switch C won't be introduced herein.

## Step 2: Display RSPAN status

! Configurations of Switch A

```
SwitchA#show monitor
sess-num: 1                                //RSPAN Session
span-type: SOURCE_SPAN                   //RSPAN source device
src-intf:                                  //information about RSPAN source port
FastEthernet 0/1          frame-type Both
dest-intf:                                //information about RSPAN destination port
FastEthernet 0/2
remote vlan 7
mtp_switch on                          //Allow the destination port to exchange traffic
```

! Configurations of Switch B

```
SwitchB#show monitor
sess-num: 1
span-type: DEST_SPAN
dest-intf:
FastEthernet 0/2
remote vlan 7
mtp_switch on
```

! Configurations of Switch C won't be introduced herein.