Edge-corE

Powered by Accton

ES4626/ES4650 L3 Gigabit Ethernet Switch

www.edge-core.com

Preface

ES4626/ES4650 L3 Gigabit Ethernet Switch is a high performance routing switch released by Edge-Core that can be deployed as an aggregation device for campus networks, enterprise networks, as well as core layer switches for small and medium-sized networks.ES4626/ES4650 L3 Gigabit Ethernet Switch support a variety of network interfaces from 100Mb, 1000Mb to 10 GB Ethernet.

We are providing this manual for your better understanding, use and maintenance of the ES4626/ES4650 L3 Gigabit Ethernet Switch. We strongly recommend you to read through this manual carefully before installation and configuration to avoid possible malfunction or damage to the switch. Furthermore, we sincerely hope our products and services satisfy you.

Content

Chapter 1 Switch Management

1.1 Management Options

After purchasing the switch, the user needs to configure the switch for network management. ES4626/ES4650 Switch provides two management options: in-band management and out-of-band management.

1.1.1 Out-Of-Band Management

Out-of-band management is the management through Console interface. Generally, the user will use out-of-band management for the initial switch configuration, or when in-band management is not available. For instance, the user must assign an IP address to the switch via the Console interface to be able to access the switch through Telnet.

The procedures for managing the switch via Console interface are listed below:

Step 1: setting up the environment:

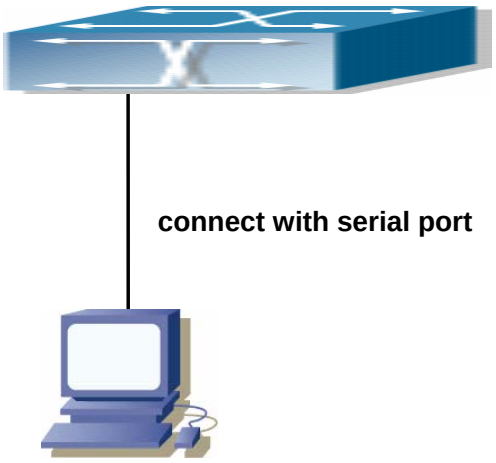


Fig 1-1 Out-of-band Management Configuration Environment

As shown in Fig 1-1, the serial port (RS-232) is connected to the switch with the serial cable provided. The table below lists all the devices used in the connection.

Device Name	Description
PC machine	Has functional keyboard and RS-232, with terminal emulator installed, such as HyperTerminal included in

	Windows 9x/NT/2000/XP.
Serial port cable	One end attach to the RS-232 serial port, the other end to the Console port.
ES4626/ES4650	Functional Console port required.

Step 2 Entering the HyperTerminal

Open the HyperTerminal included in Windows after the connection established. The example below is based on the HyperTerminal included in Windows XP.

1) Click Start menu - All Programs -Accessories -Communication - HyperTerminal.

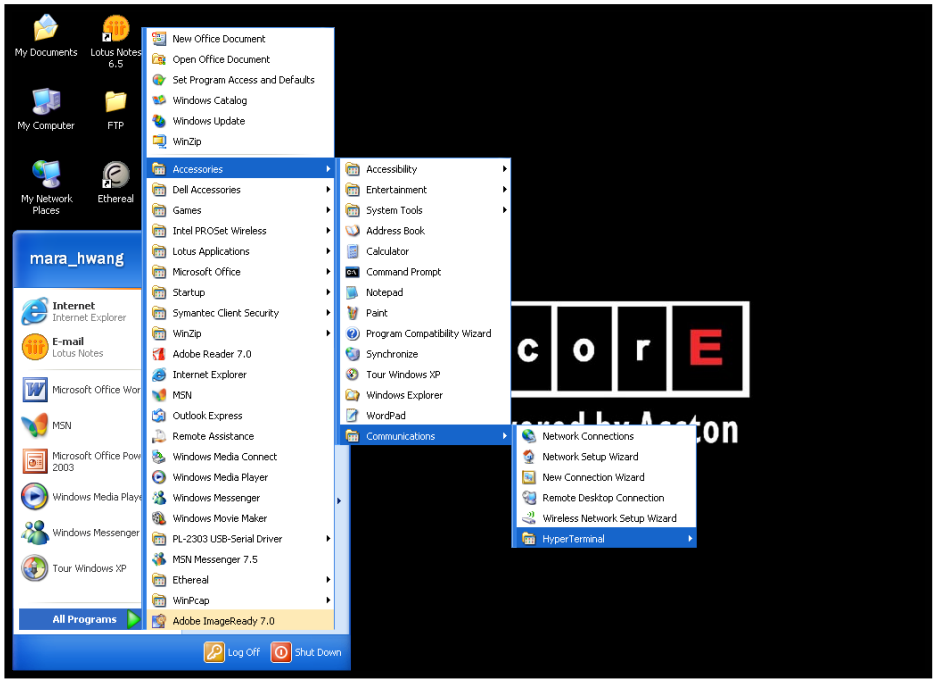


Fig 1-2 Opening HyperTerminal

2) Type a name for opening HyperTerminal, such as “Switch”.

Fig 1-3 Opening HyperTerminal

3) In the “Connecting using” drop-list, select the RS-232 serial port used by the PC, e.g. COM1, and click “OK”.

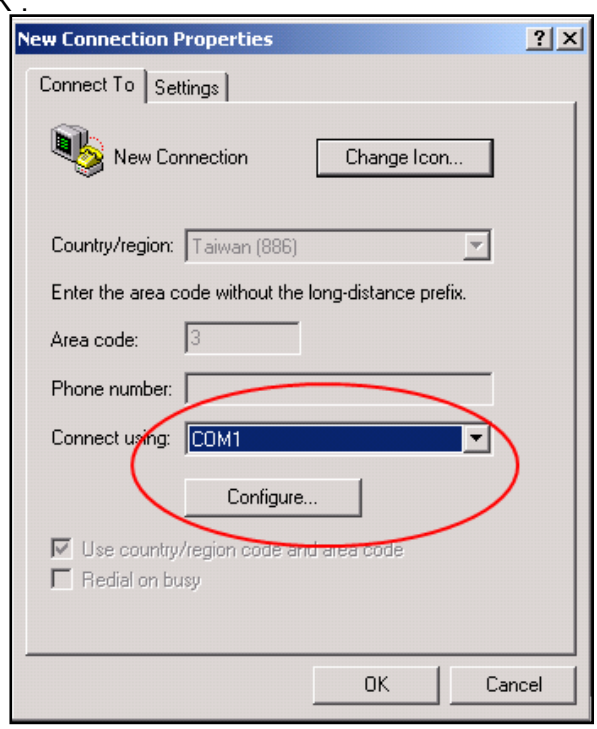


Fig 1-4 Opening HyperTerminal

4) COM1 property appears, select “9600” for “Baud rate”, “8” for “Data bits”, “none” for “Parity checksum”, “1” for stop bit and “none” for traffic control; or, you can also click “Restore default” and click “OK”.

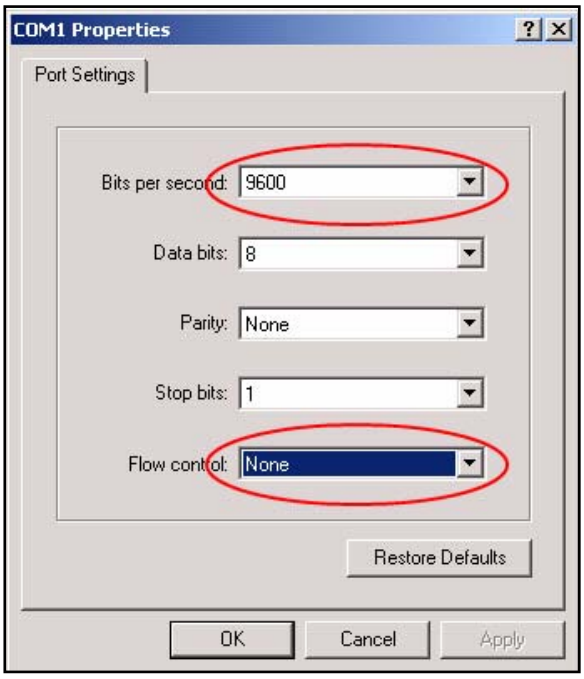


Fig 1-5 Opening HyperTerminal

Step 3 Entering switch CLI interface:

Power on the switch, the following appears in the HyperTerminal windows, that is the CLI configuration mode for ES4626/ES4650 Switch.

ES4650 Management Switch

Copyright (c) 2001-2004 by Accton Technology Corporation.
All rights reserved.

Reset chassis ... done.
Testing RAM...
134,217,728 RAM OK.

Initializing...
Attaching to file system ... done.

Loading nos.img ... done.
Starting at 0x10000...

Current time is WED APR 20 09: 37: 52 2005

ES4650 Switch Operating System, Software Version ES4650 1.1.0.0,
Copyright (C) 2001-2006 by Accton Technology Corporation
http: //www.edge-core. com.

ES4650 Switch
24 Ethernet/IEEE 802.3 interface(s)
Press ENTER to start session

The user can now enter commands to manage the switch. For a detailed description for the commands, please refer to the following chapters.

1.1.2 In-band Management

In-band management refers to the management by login to the switch using Telnet. In-band management enables management of the switch for some devices attached to the switch. In the case when in-band management fails due to switch configuration changes, out-of-band management can be used for configuring and managing the switch.

1.1.3 Management Via Telnet

To manage the switch with Telnet, the following conditions should be met:

1) Switch has an IP address configured
2) The host IP address (Telnet client) and the switch's VLAN interface IP address is in the same network segment.
3) If not 2), Telnet client can connect to an IP address of the switch via other devices, such as a router.

ES4626/ES4650 Switch is a Layer 3 switch that can be configured with several IP addresses. The following example assumes the shipment status of the switch where only VLAN1 exists in the system.

The following describes the steps for a Telnet client to connect to the switch's VLAN1 interface by Telnet.

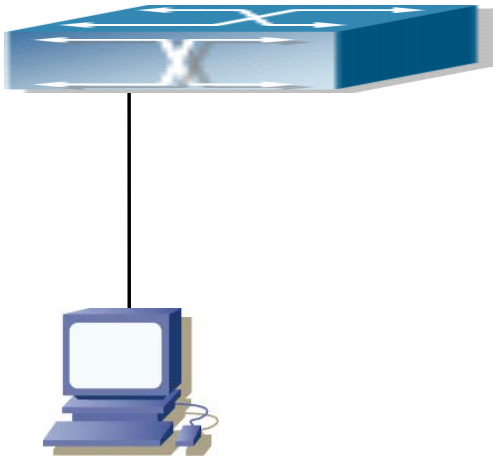


Fig 1-6 Manage the switch by Telnet

Step 1: Configure the IP addresses for the switch

First is the configuration of host IP address. This should be within the same network segment as the switch VLAN1 interface IP address. Suppose the switch VLAN interface IP address 10.1.128.251/24. Then, a possible host IP address is 10.1.128.252/24. Run "ping 10.1.128.251" from the host and verify the result, check for reasons if ping failed.

The IP address configuration commands for VLAN1 interface are listed below. Before in-band management, the switch must be configured with an IP address by out-of-band management (i.e. Console mode), The configuration commands are as follows (All switch configuration prompts are assumed to be "switch" hereafter if not otherwise specified):

Switch>

Switch>en
Switch#config
Switch(Config)#interface vlan 1
Switch(Config-If-Vlan1)#ip address 10.1.128.251 255.255.255.0
Switch(Config-If-Vlan1)#no shutdown

Step 2: Run Telnet Client program.

Run Telnet client program included in Windows with the specified Telnet target.

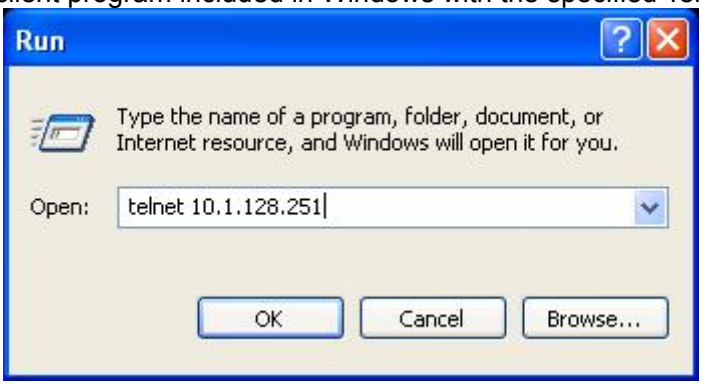


Fig 1-7Run telnet client program included in Windows

Step 3: Login to the switch

Login to the Telnet configuration interface.Valid login name and password are required, otherwise the switch will reject Telnet access. This is a method to protect the switch from unauthorized access. As a result, when Telnet is enabled for configuring and managing the switch, username and password for authorized Telnet users must be configured with the following command:

username <user> password {0|7} <password>.

Assume an authorized user in the switch has a username of “test”, and password of “test”, the configuration procedure should like the following:

Switch>en
Switch#config
Switch(Config)#username test password 0 test

Enter valid login name and password in the Telnet configuration interface, Telnet user will be able to enter the switch’s CLI configuration interface. The commands used in the Telnet CLI interface after login is the same as that in the Console interface.

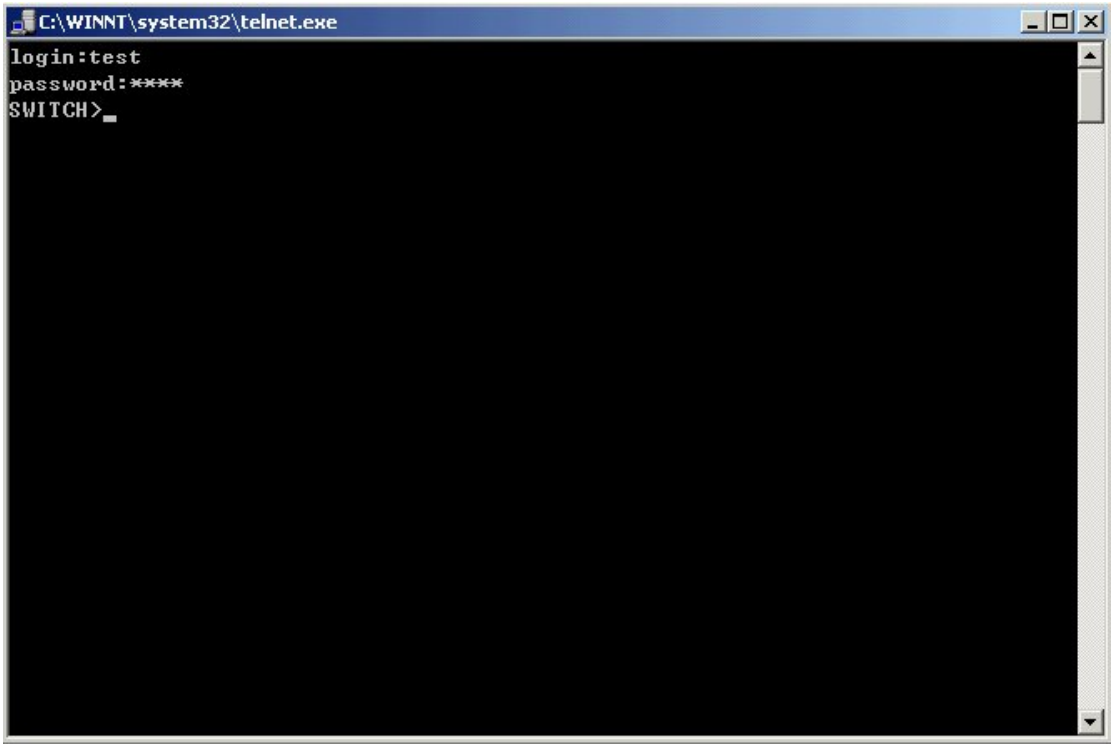


Fig 1-8 Telnet Configuration Interface

1.1.4 Management Via HTTP

To manage the switch via HTTP, the following conditions should be met:

1) Switch has an IP address configured
2) The host IP address (HTTP client) and the switch's VLAN interface IP address are in the same network segment;
3) If 2) is not met, HTTP client should connect to an IP address of the switch via other devices, such as a router.

Similar to management via Telnet, as soon as the host succeeds to ping an IP address of the switch and to type the right login password, it can access the switch via HTTP. The configuration list is as below:

Step 1: Configure the IP addresses for the switch and start the HTTP function on the switch.

For configuring the IP address on the switch through out-of-band management, see the relevant chapter.

To enable the WEB configuration, users should type the CLI command **ip http server** in the global mode as below:

Switch>en
Switch#config

Switch(Config)#ip http server

Step 2: Run HTTP protocol on the host.

Open the Web browser on the host and type the IP address of the switch. Or run directly the HTTP protocol on the Windows. For example, the IP address of the switch is "10.1.128.251".

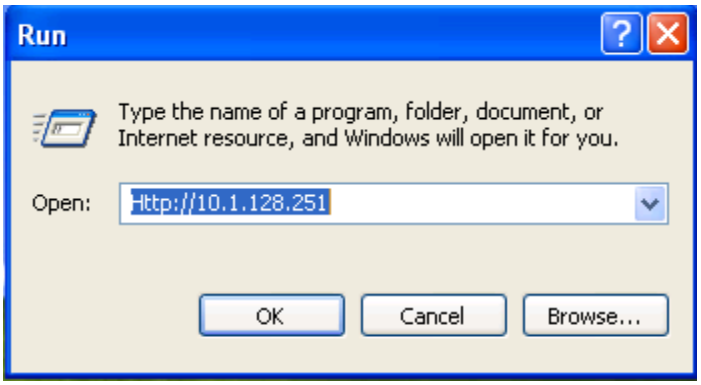


Fig 1-9 Run HTTP Protocol

When accessing a switch with IPv6 address, it is recommended to use the Firefox browser with 1.5 or later version. For example, if the IPv6 address of the switch is "3ffe:506:1:2::3", enter the switch address at the address bar: http://[3ffe:506:1:2::3], where the address should be in the square brackets.

Step 3: Logon to the switch

To logon to the HTTP configuration interface, valid login user name and password are required; otherwise the switch will reject HTTP access. This is a method to protect the switch from the unauthorized access. Consequently, in order to configure the switch via HTTP, username and password for authorized HTTP users must be configured with the following command in the global mode:

username <*username*> password <*show_flag*> <*password*>.

Suppose an authorized user in the switch has a username as "test", and password as "test". The configuration procedure is as below:

Switch>en

Switch#config

Switch(Config)# username test password 0 test

The Web login interface is as below:

Fig 1-10 Web Login Interface

Input the right username and password, and then the main Web configuration interface is shown as below.

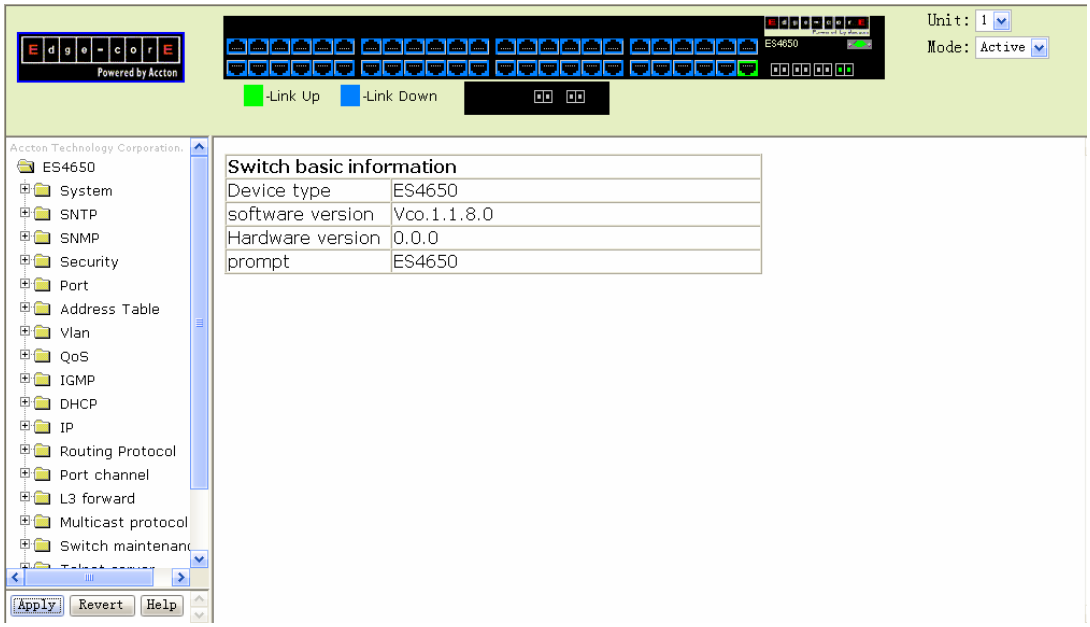


Fig 1-11 Main Web Configuration Interface

1.2 Management Interface

1.2.1 CLI Interface

CLI interface is familiar to most users. As before mentioned, out-of-band management and Telnet login are all performed through CLI interface to manage the switch.

CLI Interface is supported by Shell program, which consists of a set of configuration commands. Those commands are categorized according to their functions in switch configuration and management. Each category represents a different configuration mode. The Shell for the switch is described below:

- Configuration Modes
- Configuration Syntax
- Shortcut keys
- Help function
- Input verification
- Fuzzy match support

1.2.2 Configuration Modes

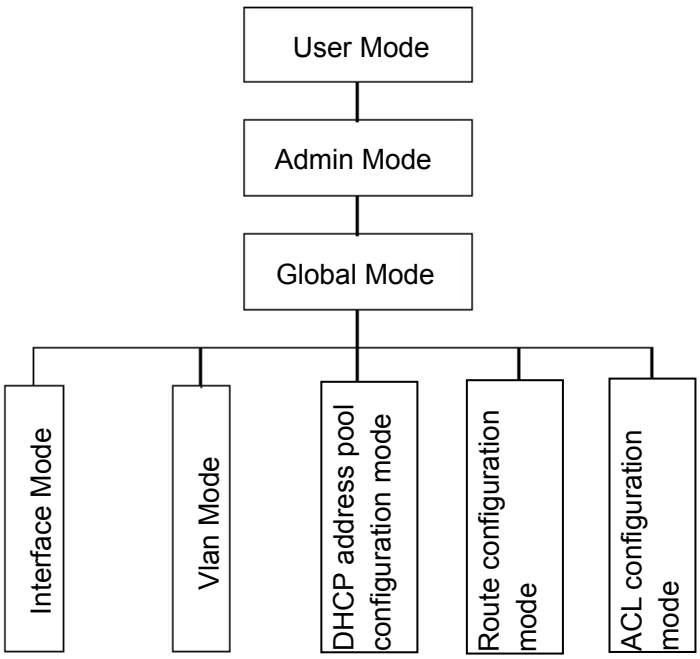


Fig 1-11 Shell Configuration Modes

1.2.2.1 User Mode

On entering the CLI interface, entering user entry system first. If as common user, it is defaulted to User Mode. The prompt shown is “Switch>“, the symbol “>“ is the prompt for User Mode. When **disable** command is run under Admin Mode, it will also return to the User Mode.

Under User Mode, no configuration to the switch is allowed, only clock time and version information of the switch can be queries.

1.2.2.2 Admin Mode

To Admin Mode sees the following: In user entry system, if as Admin user, it is defaulted to Admin Mode. Admin Mode prompt “Switch#” can be entered under the User Mode by running the *enable* command and entering corresponding access levels admin user password, if a password has been set. Or, when *exit* command is run under Global Mode, it will also return to the Admin Mode. ES4626/ES4650 Switch also provides a shortcut key sequence "Ctrl+z”, this allows an easy way to exit to Admin Mode from any configuration mode (except User Mode).

Under Admin Mode, when disable command is run, it will return to User Mode. When exit command is run, it will exit the entry and enter user entry system direct. Next users can reenter the system on entering corresponding user name and password.

Under Admin Mode, the user can query the switch configuration information, connection status and traffic statistics of all ports; and the user can further enter the Global Mode from Admin Mode to modify all configurations of the switch. For this reason, a password must be set for entering Admin mode to prevent unauthorized access and malicious modification to the switch.

1.2.2.3 Global Mode

Type the config command under Admin Mode will enter the Global Mode prompt “Switch(Config)#”. Use the *exit* command under other configuration modes such as Interface Mode, VLAN mode will return to Global Mode.

The user can perform global configuration settings under Global Mode, such as MAC Table, Port Mirroring, VLAN creation, IGMP Snooping start, GVRP and STP, etc. And the user can go further to Interface Mode for configuration of all the interfaces.

1.2.2.4 Interface Mode

Use the *interface* command under Global Mode can enter the interface mode specified. ES4626/ES4650 Switch provides three interface type: VLAN interface, Ethernet port and port-channel, and accordingly the three interface configuration modes.

Interface Type	Entry	Prompt	Operates	Exit
VLAN	Type **interface**	Switch(Config-If-Vl	Configure	Use the *exit*

Interface	**vlan <Vlan-id>** command under Global Mode.	anx)#	switch IPs, etc	command to return to Global Mode.
Ethernet Port	Type **interface ethernet <interface-list>** command under Global Mode.	**Switch(Config-ethernetxx)#**	Configure supported duplex mode, speed, etc. of Ethernet Port.	Use the *exit* command to return to Global Mode.
port-channel	Type **interface port-channel <port-channel-number>** command under Global Mode.	**Switch(Config-if-port-channelx)#**	Configure port-channel related settings such as duplex mode, speed, etc.	Use the *exit* command to return to Global Mode.

1.2.2.5 VLAN Mode

Using the *vlan* <vlan-id> command under Global Mode can enter the corresponding VLAN Mode. Under VLAN Mode the user can configure all member ports of the corresponding VLAN. Run the exit command to exit the VLAN Mode to Global Mode.

1.2.2.6 DHCP Address Pool Mode

Type the **ip dhcp pool <*name*>** command under Global Mode will enter the DHCP Address Pool Mode prompt "**Switch(Config-<name>-dhcp)#**". DHCP address pool properties can be configured under DHCP Address Pool Mode. Run the *exit* command to exit the DHCP Address Pool Mode to Global Mode.

1.2.2.7 Route Mode

Routing Protocol	Entry	Prompt	Operates	Exit
RIP Routing Protocol	Type **router rip** command under Global Mode.	**Switch(Config-Router-Rip)#**	Configure RIP protocol parameters.	Use the "*exit*" command to return to Global Mode.

OSPF Routing Protocol	Type **router ospf** command under Global Mode.	**Switch(Config-Router-Ospf)#**	Configure OSPF protocol parameters.	Use the "*exit*" command to return to Global Mode.

1.2.2.8 ACL Mode

ACL type	Entry	Prompt	Operates	Exit
Standard IP ACL Mode	Type **access-list ip** command under Global Mode.	**Switch(Config-Std-Nacl-a)#**	Configure parameters for Standard IP ACL Mode	Use the "*exit*" command to return to Global Mode.
Extended IP ACL Mode	Type **access-list ip** command under Global Mode.	**Switch(Config-Ext-Nacl-b)#**	Configure parameters for Extended IP ACL Mode	Use the "*exit*" command to return to Global Mode.

1.2.3 Configuration Syntax

ES4626/ES4650 Switch provides various configuration commands. Although all the commands are different, they all abide by the syntax for ES4626/ES4650 Switch configuration commands. The general commands format of ES4626/ES4650 Switch is shown below:

cmdtxt <*variable*> { enum1 | … | enumN } [option]

Conventions: **cmdtxt** in bold font indicates a command keyword; **<*variable*>** indicates a variable parameter; **{enum1 | … | enumN }** indicates a mandatory parameter that should be selected from the parameter set **enum1~enumN**; and the square bracket ([ ]) in **[option]** indicate an optional parameter. There may be combinations of "< >", "{ }" and "[ ]" in the command line, such as **[<*variable*>]**,**{enum1 <*variable*>| enum2}**, **[option1 [option2]]** ,**etc.**

Here are examples for some actual configuration commands:

- **show calendar**, no parameters required. This is a command with only a keyword and no parameter, just type in the command to run.
- **vlan <*vlan-id*>**, parameter values are required after the keyword.
- **duplex {auto|full|half}**, user can enter *duplex half*, *duplex full* or *duplex auto* for this command.
- **snmp-server community <*string*>{ro|rw}**, the followings are possible:

snmp-server community <*string*> ro

snmp-server community <*string*> rw

1.2.4 Shortcut Key Support

ES4626/ES4650 Switch provides several shortcut keys to facilitate user configuration, such as up, down, left, right and Blank Space. If the terminal does not recognize Up and Down keys, ctrl +p and ctrl +n can be used instead.

Key(s)	Function	
Back Space	Delete a character before the cursor, and the cursor moves back.	
Up "↑"	Show previous command entered. Up to ten recently entered commands can be shown.	
Down "↓"	Show next command entered. When use the Up key to get previously entered commands, you can use the Down key to return to the next command	
Left "←"	The cursor moves one character to the left.	You can use the Left and Right key to modify an entered command.
Right "→"	The cursor moves one character to the right.	
Ctrl +p	The same as Up key "↑".	
Ctrl +n	The same as Down key "↓".	
Ctrl +b	The same as Left key "←".	
Ctrl +f	The same as Right key "→".	
Ctrl +z	Return to the Admin Mode directly from the other configuration modes (except User Mode).	
Ctrl +c	Break the ongoing command process, such as ping or other command execution.	
Tab	When a string for a command or keyword is entered, the Tab can be used to complete the command or keyword if there is no conflict.	

1.2.5 Help Function

There are two ways in ES4626/ES4650 Switch for the user to access help information: the “help” command and the “?”.

Access to Help	Usage and function
Help	Under any command line prompt, type in “help” and press Enter will get a brief description of the associated help system.
“?”	1. Under any command line prompt, enter “?” to get a command list of the current mode and related brief description. 2. Enter a “?” after the command keyword with a embedded space. If the position should be a parameter, a description of that parameter type, scope, etc, will be returned; if the position should be a keyword, then a set of keywords with brief description will be returned; if the output is “<cr>“, then the command is complete, press Enter to run the command. 3. A “?” immediately following a string. This will display all the commands that begin with that string.

1.2.6 Input Verification

Returned Information: success

All commands entered through keyboards undergo syntax check by the Shell. Nothing will be returned if the user entered a correct command under corresponding modes and the execution is successful.

Returned Information: error

Output error message	Explanation
Unrecognized command or illegal parameter!	The entered command does not exist, or there is error in parameter scope, type or format.
Ambiguous command	At least two interpretations is possible basing on the current input.
Invalid command or parameter	The command is recognized, but no valid parameter record is found.
This command is not exist in current mode	The command is recognized, but this command can not be used under current mode.
Please configure precursor command "*" at first !	The command is recognized, but the prerequisite command has not been configured.
syntax error : missing "" before the end of command line!	Quotation marks are not used in pairs.

1.2.7 Fuzzy Match Support

ES4626/ES4650 switch shell support fuzzy match in searching command and keyword. Shell will recognize commands or keywords correctly if the entered string causes no conflict.

For example:

1. For command “show interfaces status ethernet 1/1”, typing “sh in status e 1/1” will work
2. However, for command “show running-config”, the system will report a “> Ambiguous command!” error if only “show r” is entered, as Shell is unable to tell whether it is “show run” or “show running-config”. Therefore, Shell will only recognize the command if “sh ru” is entered.

1.3 Web Management

1.3.1 Main Page

ES4626/ES4650 switch routing switch provides HTTP web management function and users can configure and monitor the status of the switch through the web interface.

To manage the switch through web browser use the following steps:

Configure valid IP address, mask and confirm gateway for the switch.

1. Configure web user management and its password
2. Connect to the switch using the web browser. Enter the username and password to proceed to web management.

1.3.2 Module Front Panel

When entering username, password and passing authentication, you will see the following web management main page. On the left of the management page is the main management menu and on the right of the page system information and command parameter are displayed. Click the main menu link to browse other management links and to display configuration and statistic information.

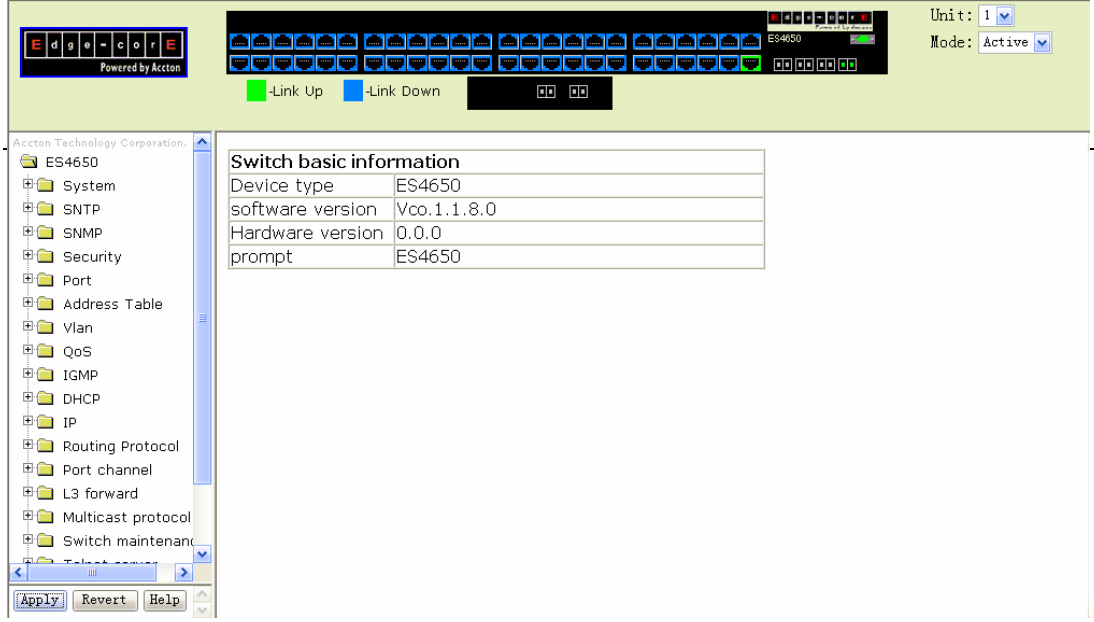


Fig 1-13 Module Front Panel

Chapter 2 Basic Switch Configuration

2.1 Basic Switch Configuration Commands

Basic switch configuration includes commands for entering and exiting the admin mode, commands for entering and exiting interface mode, for configuring and displaying the switch clock, for displaying the version information of the switch system, etc.

Command	Explanation
Normal User Mode/ Admin Mode	
enable **disable**	The User uses **enable** command to step into admin mode from normal user mode. The **disable** command is for exiting admin mode.
Admin Mode	
config [terminal]	Enter global mode from admin mode
Various Modes	
Exit	Exit current mode and enter previous mode, such as using this command in global mode to go back to admin mode, and back to normal user mode from admin mode
Admin Mode	
calendar set *<HH> <MM> <SS> {<DD> <MON> <YYYY> | <MON> <DD> <YYYY>}*	Set system date and time
Show version	Display version information of the switch
set default	Restore to the factory default
Write	Flash Memory Save current configuration parameters to Flash Memory
Reload	Hot reset the switch

2.1.1 Commands For Basic Configuration

2.1.1.1 authentication login

Command: **authentication login {local | radius | local radius | radius local|tacacs }**

no authentication login

Function: Configure the authentication mode and priority on Telnet Server for remote login users; the "**no authentication login**" command restores to the default login authentication mode.

Default: Default login authentication mode is local.

Command mode: Global mode

Usage guide: When using authentication modes combinations, the mode at the first of the queue is with the highest priority which receding accordingly. When a user passes authentication mode with higher priority, the login will be granted without proceeding to other modes with lower priority. It is to be noted that to login in only one authentication mode is required. When using radius authentication, the AAA function must be enabled and radius server be configured.

Example: Configure the remote login authentication mode to radius

Switch(Config)#authentication login radius

2.1.1.2 calendar set

Command: calendar set *<HH> <MM> <SS> {<DD> <MON> <YYYY> | <MON> <DD> <YYYY>}*

Function: Set system date and time.

Parameter: *<HH> <MM> <SS>* is the current time, and the valid scope for ***HH*** is 0 to 23, ***MM*** and ***SS*** 0 to 59; ***<DD> <MON> <YYYY>*** or ***<MON> <DD> <YYYY>*** is the current date, month and year or the current year, month and date, and the valid scope for ***YYYY*** is 1970~2100, ***MON*** meaning month, and ***DD*** between 1 to 31.

Command mode: Admin Mode

Default: upon first time start-up, it is defaulted to 2001.1.1 0: 0: 0.

Usage guide: The switch can not continue timing with power off, hence the current date and time must be first set at environments where exact time is required.

Example: To set the switch current date and time to 2002.8.1 23: 0: 0:

Switch# calendar set 23 0 0 8 1 2002

2.1.1.3 config

Command: config [terminal]

Function: Enter Global Mode from Admin Mode.

Parameter: [terminal] indicates terminal configuration.

Command mode: Admin Mode

Example:

Switch#config

2.1.1.4 debug ssh-server

Command: debug ssh-server

no debug ssh-server

Function: Display SSH server debugging information; the "**no debug ssh-server**" command stops displaying SSH server debugging information.

Default: This function is disabled by default.

Command mode: Admin Mode

Example:

Switch#debug ssh-server

2.1.1.5 dir

Command: dir

Function: Display the files and their sizes in the Flash memory.

Command mode: Admin Mode

Example: Check for files and their sizes in the Flash memory.

Switch#dir

boot.rom	329,828 1900-01-01 00: 00: 00 --SH
boot.conf	94 1900-01-01 00: 00: 00 --SH
nos.img	2,449,496 1980-01-01 00: 01: 06 ----
startup-config	2,064 1980-01-01 00: 30: 12 ----

2.1.1.6 enable

Command: enable

Function: Enter Admin Mode from User Mode.

Command mode: User Mode

Usage Guide: To prevent unauthorized access of non-admin user, user authentication is required (i.e. Admin user password is required) when entering Admin Mode from User Mode. If the correct Admin user password is entered, Admin Mode access is granted; if 3 consecutive entry of Admin user password are all wrong, it remains in the User Mode. Set the Admin user password under Global Mode with "**enable password**" command.

Example:

Switch>enable

password: ***** (admin)

Switch#

2.1.1.7 enable password

Command: enable password [8] <password>

no enable password

Function: Configure the password used for enter Admin Mode from the User Mode,

The "**no enable password**" command deletes this password

Parameter: password is the configured code. Encryption will be performed by entering 8.

Command mode: Global Mode

Default: This password is empty by system default

Usage Guide: Configure this password to prevent unauthorized entering Admin Mode. It is recommended to set the password at the initial switch configuration. Also, it is recommended to exit Admin Mode with "**exit**" command when the administrator needs to leave the terminal for a long time.

Example: Set the Admin user password to "admin".

Switch(Config)#enable password 8 admin

2.1.1.8 exec-timeout

Command: exec-timeout <minutes > [<seconds>]

no exec-timeout

Function: Configure the timeout of exiting admin mode. The "***no*** **exec-timeout**" command restores the default value.

Parameters: < minute > is the time value shown in minute and ranges between 0~35791.**<seconds>** is the time value shown in seconds and ranges between 0~2147483

Command mode: Global mode

Default: Default timeout is 10 minutes.

Usage guide: To secure the switch, as well to prevent malicious actions from unauthorized user, the time will be count from the last configuration the admin had made, and the system will exit the admin mode at due time. It is required to enter admin code and password to enter the admin mode again. The timeout timer will be disabled when the timeout is set to 0.

Example: Set the admin mode timeout value to 6 minutes

Switch(Config)#exec-timeout 6

2.1.1.9 exit

Command: exit

Function: Quit current mode and return to it's previous mode.

Command mode: All Modes

Usage Guide: This command is to quit current mode and return to it's previous mode.

Example: Quit global mode to it's previous mode

Switch(Config)#exit

Switch#

2.1.1.10 help

Command: help

Function: Output brief description of the command interpreter help system.

Command mode: All configuration modes.

Usage Guide: An instant online help provided by the switch. Help command displays information about the whole help system, including complete help and partial help. The user can type in ? any time to get online help.

Example:

```
Switch>help
  enable                    -- Enable Admin mode
  exit                      -- Exit telnet session
  help                      -- help
  show                      -- Show running system information
```

2.1.1.11 hostname

Command: hostname <*hostname*>

Function: Set the prompt in the switch command line interface.

Parameter ***<hostname>*** is the string for the prompt, up to 30 characters are allowed.

Command mode: Global Mode

Default: The default prompt is ES4626/ES4650 switch.

Usage Guide: With this command, the user can set the CLI prompt of the switch according to their own requirements.

Example: Set the prompt to “Test”.

Switch(Config)#hostname Test

2.1.1.12 ip host

Command: ip host <hostname> <ip_addr>

no ip host <*hostname*>

Function: Set the mapping relationship between the host and IP address; the “no ip host” parameter of this command will delete the mapping.

Parameter: <*hostname*> is the host name, up to 15 characters are allowed; ***<ip_addr>*** is the corresponding IP address for the host name, takes a dot decimal format.

Command mode: Global Mode

Usage Guide: Set the association between host and IP address, which can be used in commands like **“ping <host>**“.

Example: Set IP address of a host with the hostname of “beijing” to 200.121.1.1.

Switch(Config)#ip host beijing 200.121.1.1

2.1.1.13 ipv6 host

Command: ipv6 host <*hostname*> <*ipv6_addr*>

no ipv6 host <*hostname*>

Function: Configure the mapping relationship between the IPv6 address and the host; the "**no ipv6 host <*hostname*>**" command deletes this mapping relationship

Parameter：**<*hostname*>** is the name of the host,containing max 15 characters;**<*ipv6_addr*>** is the IPv6 address corresponding to the host name.

Command Mode: Global Mode

Usage Guide: Configure a fixed corresponding relationship between the host and the IPv6 address, applicable in commands such as "**traceroute6 <host>**", etc.

Example: Set the IPv6 address of the host named beijing to 2001:1:2:3::1

Switch(Config)#ipv6 host beijing 2001:1:2:3::1

2.1.1.14 ip http server

Command: ip http server

no ip http server

Function: Enable Web configuration; the "**no ip http server**" command disables Web configuration

Command mode: Global mode

Usage guide: Web configuation is for supplying a interface configured with HTTP for the user, which is straight and visual, esay to understand. This command functions equal to selection [2] of the main menu in Setup mode to configure the Web Server.

Example: Enable Web Server function and enable Web configurations.

Switch(Config)#ip http server

2.1.1.15 login

Command: login

no login

Function: login enable password authentication ,no login command cancels the login configuration

Command mode: Global mode

Default: no login by default

Usage guide: By using this command, users have to enter the password set by password command to enter normal user mode with console; no login cancels this restriction

Example: Enable password

Switch(Config)#login

2.1.1.16 language

Command: language {chinese|english}

Function: Set the language for displaying the help information.

Parameter: Chinese for Chinese display; **English** for English display.

Command mode: Admin Mode

Default: The default setting is English display.

Usage Guide: ES4626/ES4650 switch provides help information in two languages, the user can select the language according to their preference. After the system restart, the help information display will revert to English.

2.1.1.17 login local

Command：login local

no login

Function： Login enables local user name and password identification, no login cancels login local configuration.

Command Mode： Global Mode

Default： System Default is no login.

Usage Guide： The command enable the user access in common mode of shell, types in user name and password configured by username command, and then can access in common user mode through level configured by the command. No login cancels login local configuration.

Notice： Executing the command, it insures that priority of one user is 15, if it uses username command configuration to login. Only this can ensure that the user accesses from common mode to admin mode and modify system configuration after the user pass the shell login identification. If there is no user of priority 15, the user can not access in admin and global mode.

Example： Enable local use password identification

Switch(Config)#login local

2.1.1.18 password

Command: password <password>

no password

Function: Configure the password used for enter normal user mode on the console. The "**no password**" command deletes this password

Parameter: password is the configured code. Encryption will be performed by entering 8

Command mode: Global mode

Default: This password is empty by system default

Usage guide: When both this password and login command are configured, users have to enter the password set by password command to enter normal user mode on console

Example:

Switch(Config)#password 8 test

Switch(Config)#login

2.1.1.19 ping

Command: ping [<*ip-addr*> | <host>|vrf|]

Function: The switch send ICMP packet to remote devices to verify the connectivity between the switch and remote devices.

Parameter: <*ip-addr*> is the target host IP address for ping, in dot decimal format.

<host> is the target host name for ping.

<vrf>VPN Routing/Forwarding instance.it is useful only when VR is configured.

Default: Send 5 ICMP packets of 56 bytes each, timeout in 2 seconds.

Command mode: Admin Mode

Usage Guide: When the user types in the ping command and press Enter, the system will provide an interactive mode for configuration, and the user can choose all the parameters for ping.

Example:

Example 1: Default parameter for ping.

Switch#ping 10.1.128.160

Type ^c to abort.

Sending 5 56-byte ICMP Echoes to 10.1.128.160, timeout is 2 seconds.

...!!

Success rate is 40 percent (2/5), round-trip min/avg/max = 0/0/0 ms

As shown in the above example, the switch pings a device with an IP address of 10.1.128.160, three ICMP request packets sent without receiving corresponding reply packets (i.e. ping failed), the last two packets are replied successfully, the successful rate is 40%. The switch represent ping failure with a “.”, for unreachable target; and ping success with “!” , for reachable target.

Switch#ping

VRF name:

Target IP address: 10.1.128.160

Repeat count [5]: 100

Datagram size in byte [56]: 1000

Timeout in milli-seconds [2000]: 500

Extended commands [n]: n

Displayed information	Explanation
VRF name:	VPN Routing/Forwarding instance
Target IP address:	Target IP address
Repeat count [5]	Packet number, the default is 5
Datagram size in byte [56]	ICMP packet size the default is 56 bytes
Timeout in milli-seconds [2000]:	Timeout (in milliseconds,) the default is 2 seconds.
Extended commands [n]:	Whether to change the other options or not

2.1.1.20 ping6

Command: ping6 [<*dst-ipv6-address*> | host <*hostname*> | src < *src-ipv6-address* > {<*dst- ipv6-address* > | host <*hostname*>}]

Function: Verify the accessibility of the network

Parameter：*<dst- ipv6-address >* is the destination IPv6 address,**< *src-ipv6-address* >** is the source IPv6 address,***<hostname>*** is the host name of the remote host,containing no more than 30 characters.

Default: None

Command Mode: User Mode

Usage Guide: Ping6 followed by IPv6 address is the default configuration. Ping6 function can configure the parameters of the ping packets on users' demands. When the ipv6-address is the local link address, a vlan interface name is needed to be specified. When specifying source IPv6 address, the sent icmp query packets will use specified source IPv6 address as the source address of the ping packets.

Example:

(1) Default parameters of the ping6 program

Switch>ping6 2001:1:2::4

Type ^c to abort.

Sending 5 56-byte ICMP Echoes to 2001:1:2::4, timeout is 2 seconds.

!!!!!

Success rate is 100 percent (5/5), round-trip min/avg/max = 1/320/1600 ms

(2) Specify source IPv6 address when using ping6

switch>ping6 src 2001:1:2::3 2001:1:2::4

Type ^c to abort.

Sending 5 56-byte ICMP Echoes to 2001:1:2::4, using src address 2001:1:2::3, timeout is 2 seconds.

!!!!!

Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms

(3) Modify ping6 parameter with the help of the ping6 program

switch>ping6
Target IPv6 address:fe80::2d0:59ff:feb8:3b27
Output Interface: vlan1
Use source address option[n]:y
Source IPv6 address: fe80::203:fff:fe0b:16e3
Repeat count [5]:
Datagram size in byte [56]:
Timeout in milli-seconds [2000]:
Extended commands [n]:
Type ^c to abort.
Sending 5 56-byte ICMP Echoes to fe80::2d0:59ff:feb8:3b27, using src address fe80::203:fff:fe0b:16e3, timeout is 2 seconds.
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/4/16 ms

Displayed Information	Explanation
ping6	Run ping6 function
Target IPv6 address	Destination IPv6 address
Output Interface	Name of Vlan interface,required to be specified when destination address is a local link address
Use source IPv6 address [n]:	Use source IPv6 address, not used by default
Source IPv6 address	Source IPv6 IP address
Repeat count[5]	Number of ping packets to be sent,5 by default
Datagram size in byte[56]	Size of Ping packet,56 by default
Timeout in milli-seconds[2000]	Permitted delay time, 2 seconds by default
Extended commands[n]	Configuration of extended parameter, not applied by default
!	Indicate the network is accessible
.	Indicate the network is inaccessible
Success rate is 100 percent (8/8), round-trip min/avg/max = 1/1/1 ms	Statistic information,indicating that ping packets has succeeded in arriving in 100% without any packet lost

2.1.1.21 reload

Command: reload

Function: Warm reset the switch.

Command mode: Admin Mode

Usage Guide: The user can use this command to restart the switch without power off.

2.1.1.22 service password-encryption

Command: service password-encryption

no service password-encryption

Function: Encrypt system password. The "**no service password-encryption**" command cancels the encryption

Command mode: Global mode

Default: no service password-encryption by system default

Usage guide: The current unencrypted passwords as well as the coming passwords configured by password, enable password and username command will be encrypted by executed this command. no service password-encryption cancels this function however encrypted passwords remain unchanged.

Example: Encrypt system passwords

Switch(Config)#service password-encryption

2.1.1.23 service terminal-length

Command: service terminal-length <0-512>

no service terminal-length

Function: Configure the columns of characters displayed in each screen on terminal (vty). The "**no service terminal-length**" command cancels the screen shifting operation.

Parameter: Columns of characters displayed on each screen of vty, ranging between 0-512.

Command mode: Global mode

Usage guide: Configure the columns of characters displayed on each screen of the terminal. The columns of characters displayed on each screen on the telent.ssh client and the Console will be following this configuration.

Example: Set the number of vty threads to 20.

Switch(Config)#service terminal-length 20

2.1.1.24 set default

Command: set default

Function: Reset the switch to factory settings.

Command mode: Admin Mode

Usage Guide: Reset the switch to factory settings. That is to say, all configurations made by the user to the switch will disappear. When the switch is restarted, the prompt will be the same as when the switch was powered on for the first time.

Note: After the command, "**write**" command must be executed to save the operation. The switch will reset to factory settings after restart.

Example:

Switch#set default

Are you sure? [Y/N] = y

Switch#write

Switch#reload

2.1.1.25 setup

Command: setup

Function: Enter the Setup Mode of the switch.

Command mode: Admin Mode

Usage Guide: ES4626/ES4650 switch provides a Setup Mode, in which the user can configure IP addresses, etc.

2.1.1.26 terminal length

Command: terminal length <0-512>

terminal no length

Function: Set columns of characters displayed in each screen on terminal; the "**terminal no length**" cancels the screen switching operation and display content once in all.

Parameter: Columns of characters displayed in each screen, ranging between 0-512 (0 refers to non-stop display)

Command mode: Admin mode

Default: Default columns is 25

Usage guide: Set columns of characters displayed in each screen on terminal, so that the-More-message will be shown when displayed information exceeds the screen. Press any key to show information in next screen. 25 columns by default

Example: Configure treads in each display to 20

Switch#terminal length 20

2.1.1.27 terminal monitor

Command: terminal monitor

terminal no monitor

Function: Copy debugging messages to current display terminal; the "**terminal no monitor**" command restores to the default value

Command mode: Admin mode

Usage guide: Configures whether the current debugging messages is displayed on this terminal. If this command is configured on telnet or ssh clients, debug messages will be sent to that client. The debug message is displayed on console by default

Example: Switch#terminal monitor

2.1.1.28 traceroute

Command: traceroute {<*ip-addr*> | host <*hostname*> }[hops <*hops*>] [timeout <*timeout*>]

Function: This command is tests the gateway passed in the route of a packet from the source device to the target device. This can be used to test connectivity and locate a failed sector.

Parameter: <*ip-addr*> is the target host IP address in dot decimal format. **<*hostname*>** is the hostname for the remote host. **<*hops*>** is the maximum gateway number allowed by Traceroute command. **<*timeout*>** Is the timeout value for test packets in milliseconds, between 100 -10000.

Default: The default maximum gateway number is 16, timeout in 2000 ms.

Command mode: Admin Mode

Usage Guide: Traceroute is usually used to locate the problem for unreachable network nodes.

2.1.1.29 cli username

Command：cli username <username> [privilege < privilege >] [password (0|7) <password>]

no cli username <username>

Function： Configure shell user and priority shell by logging in user name and password.

Parameter： Username is the user name, privilege is the highest level executed by the user, level is 1 to 15, default is 1, and password is user password, if input option 7 on password setting, the password is encrypted; if input option 0, the password is not processed.

Command Mode： Global Mode

Usage Guide： Currently there are two priorities 1 and 15 of registered commands in system. The command of priority 1 often registers in common user mode and admin mode. The command of priority 15 registers in other modes, except for common user mode. The command configures user, priority and password. After executing login local command, it can control that users must use configured user name and password to access common user mode of shell. Only the user of priority 15 can access admin mode by enable command. If the priority of identified user by login local is less than 15, the

user can not access in admin mode, other than common user mode.

Notice： The user can log in use name and priority after the command configures, before login local command is executed (Enable username and password), it insures that priority of one user is maximum 15, so that users could log in by this username and access in admin mode and global mode to modify system configuration, otherwise, users only access in common mode, not admin mode to take the users effect.

Example： Configure an administrator user admin, priority is 15, configure two common users, priority is 1, and enable local user name and password identification.

Switch(Config)#cli username admin privilege 15 password 0 admin

Switch(Config)#cli username user1 privilege 1 password 7 user1

Switch(Config)#cli username user2 password 0 user2

Switch(Config)#login local

2.1.1.30 username password

Command: username <*user_name*> password <*show_flag*> <*pass_word*>

no uername <*user_name*>

Function: Configure username and password for logging on the switch; the "**no username <*user_name*>**" command deletes the user.

Parameter: <*user_name*> is the username. It can't exceed 16 characters; **<*show_flag*>** can be either 0 or 7. 0 is used to display unencrypted username and password, whereas 7 is used to display encrypted username and password; **<*pass_word*>** is password. It can't exceed 16 characters;

Command mode: Global Mode

Default: The username and password are null by default.

Usage Guide: This command can be used to set the username for logging on the switch and set the password as null.

Example: Set username as "admin" and set password as "admin"

Switch(Config)#username admin password 0 admin

Switch(Config)#

2.1.1.31 username nopassword

Command: username <*user_name*> nopassword

Function: Set the username for logging on the switch and set the password as null.

Parameter: <*user_name*> is the username. It can't exceed 16 characters.

Command mode: Global Mode

Usage Guide: This command is used to set the username for logging on the switch and set the password as null.

Example: Set username as "admin" and set password as null.

Switch(Config)#username admin nopassword

2.1.1.32 write

Command: write
Function: Save the currently configured parameters to the Flash memory.
Command mode: Admin Mode
Usage Guide: After a set of configuration with desired functions, the setting should be saved to the Flash memory, so that the system can revert to the saved configuration automatically in the case of accidentally powered off or power failure. This is the equivalent to the **copy running-config startup-config** command.

2.2 Monitor and Debug Command

When the users configures the switch, they will need to verify whether the configurations are correct and the switch is operating as expected, and in network failure, the users will also need to diagnostic the problem. ES4626/ES4650 switch provides various debug commands including ping, telnet, show and debug, etc. to help the users to check system configuration, operating status and locate problem causes.

2.2.1 Ping

Ping command is mainly used for sending ICMP query packet from the switches to remote devices, also for check the accessibility between the switch and the remote device. Refer to the Ping command chapter in the Command Manual for explanations of various parameters and options of the Ping command.

2.2.2 Ping6

Ping6 command is mainly used by the switch to send ICMPv6 query packet to the remote equipment, verifying the accessibility between the switch and the remote equipment. Options and explanations of the parameters of the Ping6 command please refer to Ping6 command chapter in the command manual.

2.2.3 Telnet

2.2.3.1 Introduction To Telnet

Telnet is a simple remote terminal protocol for remote login. Using Telnet, the user can login to a remote host with its IP address of hostname from his own workstation. Telnet can send the user's keystrokes to the remote host and send the remote host output to the user's screen through TCP connection. This is a transparent service, as to the user, the keyboard and monitor seems to be connected to the remote host directly.

Telnet employs the Client-Server mode, the local system is the Telnet client and the remote host is the Telnet server. ES4626/ES4650 switch can be either the Telnet Server or the Telnet client.

When ES4626/ES4650 switch is used as the Telnet server, the user can use the Telnet client program included in Windows or the other operation systems to login to ES4626/ES4650 switch, as described earlier in the In-band management section. As a Telnet server, ES4626/ES4650 switch allows up to 5 telnet client TCP connections.

And as Telnet client, using **telnet** command under Admin Mode allows the user to login to the other remote hosts. ES4626/ES4650 switch can only establish TCP connection to one remote host. If a connection to another remote host is desired, the current TCP connection must be dropped.

2.2.3.2 Telnet Configuration Task List

1. Configuring Telnet Server
2. Telnet to a remote host from the switch.

1. Configuration of Telnet Server

Command	Explanation
Global Mode	
ip telnet server **no ip telnet server**	Enable the Telnet server function in the switch: the "no **ip telnet server"** command disables the Telnet function.
telnet-server securityip <*ip-addr*> **no telnet-server securityip <*ip-addr*>**	Configure the secure IP address to login to the switch through Telnet: the "**no telnet-server securityip <*ip-addr*>" command deletes the authorized Telnet secure address.**
Admin Mode	
monitor **no monitor**	Display debug information for Telnet client login to the switch; the "**no monitor" command disables the** debug information.

2. Telnet to a remote host from the switch

Command	Explanation
Admin Mode	
telnet [<*ip-addr*>] [<*port*>]	Login to a remote host with the Telnet client included in the switch.

2.2.3.3 Commands for Telnet

2.2.3.3.1 telnet

Command: telnet {<*ip-addr*> | <*ipv6-addr*> | host <*hostname*>} [<*port*>]

Function: Log on the remote host by Telnet

Parameter：<*ip-addr*> is the IP address of the remote host,shown in dotted decimal notation;**<*ipv6-addr*>** is the IPv6 address of the remote host;**<*hostname*>** is the name of the remote host,containing max 30 characters;**<*port*>** is the port number,ranging between 0~65535.

Command Mode: Admin Mode

Usage Guide: This command is used when the switch is applied as Telnet client, for logging on remote host to configure. When a switch is applied as a Telnet client, it can only establish one TCP connection with the remote host. To connect to another remote host, the current TCP connection must be disconnected with a hotkey “CTRL+ |”. To telnet a host name, mapping relationship between the host name and the IP/IPv6 address should be previously configured. For required commands please refer to ip host and ipv6 host. In case a host corresponds to both an IPv4 and an IPv6 addresses, the IPv6 should be preferred when telneting this host name.

Example:

(1) The switch Telnets to a remote host whose IP address is 20.1.1.1
Switch#telnet 20.1.1.1 23

(2) The switch Telnets to a remote host whose IPv6 address is 3ffe:506:1:2::3
Switch#telnet 3ffe:506:1:2::3

(3) Configure the mapping relationship between the host name ipv6host and the IPv6 address 3ffe:506:1:2::3, and then telnet to host ipv6host
Switch#config
Switch(Config)# ipv6 host ipv6host 3ffe:506:1:2::3
Switch#telnet host ipv6host

2.2.3.3.2 ip telnet server

Command: ip telnet server

no ip telnet server

Function: Enable the Telnet server function in the switch: the “**no ip telnet server”** command disables the Telnet function in the switch.

Default: Telnet server function is enabled by default.

Command mode: Global Mode

Usage Guide: This command is available in Console only. The administrator can use this command to enable or disable the Telnet client to login to the switch.

Example: Disable the Telnet server function in the switch.

Switch(Config)#no ip telnet server

2.2.3.3.3 telnet-server securityip

Command: **telnet-server securityip <*ip-addr*>**

no telnet-server securityip <*ip-addr*>

Function: Configure the secure IP address of Telnet client allowed to login to the switch; the "**no telnet-server securityip <*ip-addr*>"** command deletes the authorized Telnet secure address.

Parameter: <*ip-addr*> is the secure IP address allowed to access the switch, in dot decimal format.

Default: no secure IP address is set by default.

Command mode: Global Mode

Usage Guide: When no secure IP is configured, the IP addresses of Telnet clients connecting to the switch will not be limited; if a secure IP address is configured, only hosts with the secure IP address is allowed to connect to the switch through Telnet for configuration. The switch allows multiple secure IP addresses.

Example: Set 192.168.1.21 as a secure IP address.

Switch(Config)#telnet-server securityip 192.168.1.21

2.2.4 SSH

2.2.4.1 Introduction to SSH

SSH (Secure Shell) is a protocol which ensures a secure remote access connection to network devices. It is based on the reliable TCP/IP protocol. By conducting the mechanism such as key distribution, authentication and encryption between SSH server and SSH client, a secure connection is established. The information transferred on this connection is protected from being intercepted and decrypted. The switch meets the requirements of SSH2.0. It supports SSH2.0 client software such as SSH Secure Client and putty. Users can run the above software to manage the switch remotely.

The switch presently supports RSA authentication, 3DES cryptography protocol and SSH user password authentication etc.

2.2.4.2 SSH Server Configuration Task List

1. SSH Server Configuration

Command	Explanation
Global Mode	
ssh-server enable **no ssh-server enable**	Enable SSH function on the switch; the "**no ssh-server enable**" command disables SSH function.
ssh-user <*user-name*> password {0|7} <*password*> **no ssh-user <*user-name*>**	Configure the username and password of SSH client software for logging on the switch; the "**no ssh-user <user-name>**" command deletes the username.
ssh-server timeout <*timeout*> **no ssh-server timeout**	Configure timeout value for SSH authentication; the "**no ssh-server timeout**" command restores the default timeout value for SSH authentication.
ssh-server authentication-retires < *authentication-retires*> **no ssh-server authentication-retries**	Configure the number of times for retrying SSH authentication; the "**no ssh-server authentication-retries**" command restores the default number of times for retrying SSH authentication.
ssh-server host-key create rsa modulus <*moduls*>	Generate the new RSA host key on the SSH server.
Admin Mode	
monitor **no monitor**	Display SSH debug information on the SSH client side; the "**no monitor**" command stops displaying SSH debug information on the SSH client side.

2.2.4.3 Commands for SSH

2.2.4.3.1 ssh-server authentication-retries

Command: ssh-server authentication-retries < authentication-retries >

no ssh-server authentication-retries

Function: Configure the number of times for retrying SSH authentication; the "**no ssh-server authentication-retries**" command restores the default number of times for retrying SSH authentication.

Parameter: < authentication-retries > is the number of times for retrying authentication; valid range is 1 to 10.

Command mode: Global Mode

Default: The number of times for retrying SSH authentication is 3 by default.

Example: Set the number of times for retrying SSH authentication to 5.

Switch(Config)#ssh-server authentication-retries 5

2.2.4.3.2 ssh-server enable

Command: ssh-server enable

no ssh-server enable

Function: Enable SSH function on the switch; the "**no ssh-server enable**" command disables SSH function.

Command mode: Global Mode

Default: SSH function is disabled by default.

Usage Guide: In order that the SSH client can log on the switch, the users need to configure the SSH user and enable SSH function on the switch.

Example: Enable SSH function on the switch.

Switch(Config)#ssh-server enable

2.2.4.3.3 ssh-server host-key create rsa

Command: ssh-server host-key create rsa [modulus < modulus >]

Function: Generate new RSA host key

Parameter: modulus is the modulus which is used to compute the host key; valid range is 768 to 2048. The default value is 1024.

Command mode: Global Mode

Default: The system uses the key generated when the ssh-server is started at the first time.

Usage Guide: This command is used to generate the new host key. When SSH client logs on the server, the new host key is used for authentication. After the new host key is generated and "write" command is used to save the configuration, the system uses this key for authentication all the time. Because it takes quite a long time to compute the new key and some clients are not compatible with the key generated by the modulus 2048, it is recommended to use the key which is generated by the default modulus 1024.

Example: Generate new host key.

Switch(Config)#ssh-server host-key create rsa

2.2.4.3.4 ssh-server timeout

Command: ssh-server timeout <*timeout*>

no ssh-server timeout

Function: Configure timeout value for SSH authentication; the "**no ssh-server timeout**" command restores the default timeout value for SSH authentication.

Parameter: <*timeout*> is timeout value; valid range is 10 to 600 seconds.

Command mode: Global Mode

Default: SSH authentication timeout is 180 seconds by default.

Example: Set SSH authentication timeout to 240 seconds.

Switch(Config)#ssh-server timeout 240

2.2.4.3.5 ssh-user

Command: ssh-user <*username*> password {0|7} <*password*>

no ssh-user <*username*>

Function: Configure the username and password of SSH client software for logging on the switch; the "**no ssh-user <user-name>**" command deletes the username.

Parameter: <*username*> is SSH client username. It can't exceed 16 characters; **<*password*>** is SSH client password. It can't exceed 8 characters; **0|7** stand for unencrypted password and encrypted password.

Command mode: Global Mode

Default: There are no SSH username and password by default.

Usage Guide: This command is used to configure the authorized SSH client. Any unauthorized SSH clients can't log on and configure the switch. When the switch is a SSH server, it can have maximum three users and it allows maximum three users to connect to it at the same time.

Example: Set a SSH client which has "switch" as username and "switch" as password.

Switch(Config)#ssh-user switch password 0 switch

2.2.4.4 Typical SSH Server Configuration

Example :

Requirement: Enable SSH server on the switch, and run SSH2.0 client software such as Secure shell client and putty on the terminal. Log on the switch by using the username and password from the client.

Configure the IP address, add SSH user and enable SSH service on the switch. SSH2.0 client can log on the switch by using the username and password to configure the switch.

Switch(Config)#interface vlan 1

Switch(Config-Vlan-1)#ip address 100.100.100.200 255.255.255.0

Switch(Config-Vlan-1)#exit

Switch(Config)#ssh-user test password 0 test

Switch(Config)#ssh-server enable

2.2.5 Traceroute

Trace route command is for testing the gateways through which the data packets travels from the source device to the destination device, so to check the network accessibility and locate the network failure.

Execution procedure of the Trace route command consists of: first a data packet with TTL at 1 is sent to the destination address, if the first hop returns an ICMP error message to inform this packet can not be sent (due to TTL timeout), a data packet with TTL at 2 will be sent. Also the send hop may be a TTL timeout return, but the procedure will carries on till the data packet is sent to its destination. These procedures is for recording every source address which returned ICMP TTL timeout message, so to describe a path the IP data packets traveled to reach the destination

2.2.6 Traceroute6

The Traceroute6 function is used on testing the gateways passed through by the data packets from the source equipment to the destination equipment, to verify the accessibility and locate the network failure. The principle of the Traceroute6 under IPv6 is the same as that under IPv4, which adopts the hop limit field of the ICMPv6 and IPv6 header. First, Traceroute6 sends an IPv6 datagram (including source address, destination address and packet sent time) whose HOPLIMIT is set to 1. When first route on the path receives this datagram, it minus the HOPLIMIT by 1 and the HOPLIMIT is now 0. So the router will discard this datagram and returns with a 「ICMPv6 time exceeded」 message (including the source address of the IPv6 packet, all content in the IPv6 packet and the IPv6 address of the router). Upon receiving this message, the Traceroute6 sends another datagram of which the HOPLIMIT is increased to 2 so to discover the second router. Plus 1 to the HOPLIMIT every time to discover another router, the Traceroute6 repeat this action till certain datagram reaches the destination.

Traceroute6 Options and explanations of the parameters of the Traceroute6 command please refer to traceroute6 command chapter in the command manual.

2.2.7 Show

show command is used to display information about the system , port and protocol operation. This part introduces the **show** command that displays system information, other **show** commands will be discussed in other chapters.

Admin Mode	
show calendar	Display current system clock
show debugging	Display the debugging state

dir	Display the files and the sizes saved in the flash
show history	Display the recent user input history command
show memory	Display content in specified memory area
show running-config	Display the switch parameter configuration validating at current operation state.
show startup-config	Display the switch parameter configuration written in the Flash Memory at current operation state, which is normally the configuration file applied in next time the switch starts up
show switchport interface [ethernet <interface-list>]	Display the VLAN port mode and the belonging VLAN number of the switch as well as the Trunk port information
show tcp	Display the TCP connection status established currently on the switch
show udp	Display the UDP connection status established currently on the switch
show telnet login	Display the information of the Telnet client which currently establishes a Telnet connection with the switch
show telnet user	Display the information of all the Telnet clients which are authorized to access the switch through Telnet.
Show tech-support	Display the operation information and the state of each task running on the switch. It is used by the technicians to diagnose whether the switch operates properly.
show version	Display the version of the switch

2.2.7.1 Commands for Show

2.2.7.1.1 show calendar

Command: show calendar

Function: Display the system clock.

Command mode: Admin Mode

Usage Guide: The user can use this command to check system date and time so that

the system clock can be adjusted in time if inaccuracy occurs.

Example:

Switch#show calendar

Current time is TUE AUG 22 11: 00: 01 2002

2.2.7.1.2 show debugging

Command: show debugging

Function: Display the debug switch status.

Usage Guide: If the user need to check what debug switches have been enabled, **show debugging** command can be executed.

Command mode: Admin Mode

Example: Check for currently enabled debug switch.

Switch#show debugging

STP:

Stp input packet debugging is on

Stp output packet debugging is on

Stp basic debugging is on

2.2.7.1.3 show history

Command: show history

Function: Display the recent user command history,.

Command mode: Admin Mode

Usage Guide: The system holds up to 10 commands the user entered, the user can use the UP/DOWN key or their equivalent (ctrl+p and ctrl+n) to access the command history.

Example:

Switch#show history

enable

config

interface ethernet 1/3

enable

dir

show ftp

2.2.7.1.4 show memory

Command: show memory

Function: Display the contents in the memory.

Command mode: Admin Mode

Usage Guide: This command is used for switch debug purposes. The command will interactively prompt the user to enter start address of the desired information in the memory and output word number. The displayed information consists of three parts:

address, Hex view of the information and character view.

Example:

Switch#show memory

start address : 0x2100

number of words[64]:

002100: 0000 0000 0000 0000 0000 0000 0000 0000 *.....*

002110: 0000 0000 0000 0000 0000 0000 0000 0000 *.....*

002120: 0000 0000 0000 0000 0000 0000 0000 0000 *.....*

002130: 0000 0000 0000 0000 0000 0000 0000 0000 *.....*

002140: 0000 0000 0000 0000 0000 0000 0000 0000 *.....*

002150: 0000 0000 0000 0000 0000 0000 0000 0000 *.....*

002160: 0000 0000 0000 0000 0000 0000 0000 0000 *.....*

002170: 0000 0000 0000 0000 0000 0000 0000 0000 *.....*

2.2.7.1.5 show running-config

Command: show running-config

Function: Display the current active configuration parameters for the switch.

Default: If the active configuration parameters are the same as the default operating parameters, nothing will be displayed.

Command mode: Admin Mode

Usage Guide: When the user finishes a set of configuration and needs to verify the configuration, show running-config command can be used to display the current active parameters.

Example:

Switch#show running-config

2.2.7.1.6 show ssh-server

Command: show ssh-server

Function: Display SSH state and users which log on currently.

Command mode: Admin Mode

Example:

Switch#show ssh-server

ssh-server is enabled

connection	version	state	user name
1	2.0	session started	test

2.2.7.1.7 show ssh-user

Command: show ssh-user

Function: Display the configured SSH usernames.

Parameter: Admin Mode

Example:

Switch#show ssh-user

test

2.2.7.1.8 show startup-config

Command: show startup-config

Function: Display the switch parameter configurations written into the Flash memory at the current operation; those are usually also the configuration files used for the next power-up.

Default: If the configuration parameters read from the Flash are the same as the default operating parameter, nothing will be displayed.

Command mode: Admin Mode

Usage Guide: The **show running-config** command differs from **show startup-config** in that when the user finishes a set of configurations, **show running-config** displays the added-on configurations whilst **show startup-config** won't display any configurations. However, if **write** command is executed to save the active configuration to the Flash memory, the displays of **show running-config** and **show startup-config** will be the same.

2.2.7.1.9 show interface switchport

Command: show interface switchport [ethernet <interface-list>]

Function: Show the VLAN port mode, VLAN number and Trunk port messages of the VLAN port mode on the switch.

Parameter: ***<interface-list>*** is the port number or port list, which could be any port information existing in the switch

Command mode: Admin mode

Example: Show VLAN messages of port ethernet 1/1.

Switch#show interface switchport ethernet 1/1
Ethernet1/1
Type :Universal
Mac addr num :-1
Mode :Access
Port VID :1
Trunk allowed Vlan :ALL

Displayed Information	Description
Ethernet1/1	Corresponding interface number of the Ethernet
Type	Current interface type
Mac addr num	Number of interfaces with MAC address learning ability
Mode :Access	Current interface VLAN mode

Port VID :1	Current VLAN number the interface belongs
Trunk allowed Vlan :ALL	VLAN permitted by Trunk.

2.2.7.1.10 show users

Command: show users

Function: Display all user information that can login the switch .

Usage Guide: This command can be used to check for all user information that can login the switch.

Example:

Switch#show users

User level havePasword

admin 0 1

Online user info: user ip login time(second) usertype

2.2.7.1.11 show tcp

Command: show tcp

Function: Display the current TCP connection status established to the switch.

Command mode: Admin Mode

Example:

Switch#show tcp

LocalAddress LocalPort ForeignAddress ForeignPort State

0.0.0.0 23 0.0.0.0 0 LISTEN

0.0.0.0 80 0.0.0.0 0 LISTEN

Displayed information	Description
LocalAddress	Local address of the TCP connection.
LocalPort	Local pot number of the TCP connection.
ForeignAddress	Remote address of the TCP connection.
ForeignPort	Remote port number of the TCP connection.
State	Current status of the TCP connection.

2.2.7.1.12 show udp

Command: show udp

Function: Display the current UDP connection status established to the switch.

Command mode: Admin Mode

Example:

Switch#show udp

LocalAddress LocalPort ForeignAddress ForeignPort State

0.0.0.0 161 0.0.0.0 0 CLOSED

0.0.0.0 123 0.0.0.0 0 CLOSED

0.0.0.0 1985 0.0.0.0 0 CLOSED

Displayed information	Description
LocalAddress	Local address of the udp connection.
LocalPort	Local pot number of the udp connection.
ForeignAddress	Remote address of the udp connection.
ForeignPort	Remote port number of the udp connection.
State	Current status of the udp connection.

2.2.7.1.13 show version

Command: show version<unit>

Parameter: where the range of unit is 1

Function: Display the switch version.

Default: The default value for <unit> is 1

Command mode: Admin Mode

Usage Guide: Use this command to view the version information for the switch, including hardware version and software version.

Example:

Switch#show ver 1

ES4650 Device, Apr 14 2005 11: 19: 29

Hardware version is 2.0, SoftWare version packet is ES4650 _1.1.0.0, BootRom version is ES4650 _1.0.4

Copyright (C) 2001-2006 by Accton Technology Corporation..

All rights reserved.

Last reboot is cold reset

Uptime is 0 weeks, 0 days, 0 hours, 28 minutes

2.2.8 Debug

All the protocols ES4626/ES4650 switch supports have their corresponding debug commands. The users can use the information from debug commands for troubleshooting. Debug commands for their corresponding protocols will be introduced in the later chapters.

2.2.9 System log

2.2.9.1 System Log Introduction

The system log takes all information output under it control, while making detailed catalogue, so to select the information effectively. Combining with Debug programs, it will

provide a powerful support to the network administrator and developer in monitoring the network operation state and locating the network failures.

The switch system log has following characteristics

- Log output from four directions (or log channels) of the Console, Telnet terminal and monitor, log buffer zone, and log host.
- The log information is classified to four level of severities by which the information will be filtered
- According to the severity level the log information can be auto outputted to corresponding log channel.

2.2.9.1.1 Log Output Channel

So far the system log can be outputted the log information through four channels

- Through Console port to the local console
- Output the log information to remote Telnet terminal or monitor, this function is good for remote maintenance.
- Assign a proper log buffer zone inside the switch, for record the log information permanently or temporarily
- Configure the log host, the log system will directly send the log information to the log host, and save it in files to be viewed at any time

Among above log channels, users rarely use the console monitor, but will commonly choose the Telnet terminal to monitor the system operation status. However information outputted from these channels are of low traffic capacity and can not be recorded for later view. The other two channels---the log buffer zone and log host channel are two important channels

SDRAM (Synchronous Dynamic Random Access Memory) and NVRAM (Non Vulnerable Random Access Memory) is provided inside the switch as two part of the log buffer zone, The two buffer zone record the log information in a circuit working pattern, namely when log information need to be recorded exceeds the buffer size, the oldest log information will be erased and replaced by the new log information, information saved in NVRAM will stay permanently while those in SDRAM will lost when the system restarts or encounter an power failure. Information in the log buffer zone is critical for monitoring the system operation and detecting abnormal states.

Note: the NVRAM log buffer may not exist on some switches, which only have the SDRAM log buffer zone

It is recommended to use the system log server. By configuring the log host on the switch, the log can be sent to the log server for future examination

2.2.9.1.2 Format And Severity Of The Log Information

The log information format is compatible with the BSD syslog protocol, so we can

record and analyze the log by the syslog (system log protect session) on the UNIX/LINUX, as well as syslog similar applications on PC.

The log information is classified into eight classes by severity or emergency procedure. One level per value and the higher the emergency level the log information has, the smaller its value will be. For example, the level of critical is 2, and warning is 4, debugging is leveled at 7, so the critical is higher than warnings which no doubt is high than debugging. The rule applied in filtering the log information by severity level is that: only the log information with level equal to or higher than the threshold will be outputted. So when the severity threshold is set to debugging, all information will be outputted and if set to critical, only critical, alerts and emergencies will be outputted.

Follow table summarized the log information severity level and brief description. **Note: these severity levels are in accordance with the standard UNIX/LINUX syslog**

Table 1-1 Severity of the log information

Severity	Value	Description
emergencies	0	System is unusable
alerts	1	Action must be taken immediately
critical	2	Critical conditions
errors	3	Error conditions
warnings	4	Warning conditions
notifications	5	Normal but significant condition
informational	6	Informational messages
debugging	7	Debug-level messages

Right now the switch can generate information of following four levels

- Restart the switch, mission abnormal, hot plug on the CHASSIS switch chips are classified critical
- Up/down switch, topology change, aggregate port state change of the interface are classified warnings
- Outputted information from the CLI command is classified informational
- Information from the debugging of CLI command is classified debugging

Log information can be automatically sent to corresponding channels with regard to respective severity levels. Amongst the debugging information can only be sent to the monitor. Those with the Informational level can only be sent to current monitor terminal, such as the information from the Telnet terminal configuration command can only be transmitted to the Telnet terminal. Warnings information can be sent to all terminal with also saved in the SDRAM log buffer zone. And the critical information can be save both in

SDRAM and the NVRAM (if exists) besides sent to all terminals. To check the log save in SDRAM and the NVRAM, we can use the show logging buffered command. To clear the log save in NVRAM and SDRAM log buffer zone, we can use the clear logging command

2.2.9.2 System Log Configuration

2.2.9.2.1 System Log Configuration Task Sequence

1. Display and clear log buffer zone
2. Configure the log host output channel

1. Display and clear log buffer zone

Command	Description
Admin Mode	
show logging buffered|level{*critical* | *warnings*} |range <*begin-index*> <*end-index*>]	Show detailed log information in the log buffer channel
clear logging { *sdram* | *nvram* }	Clear log buffer zone information

2. Configure the log host output channel

Command	Description
Global Mode	
logging {<*ipv4-addr*> | <*ipv6-addr*>} [facility <*local-number*>] [level <*severity*>] **no logging {<*ipv4-addr*> | <*ipv6-addr*>}[facility <*local-number*>]**	Enable the output channel of the log host. The “no” form of this command will disable the output at the output channel of the log host.

2.2.9.2.2 System Log Configuration Command

2.2.9.2.2.1 show logging buffered

Command: show logging buffered [level { *critical* | *warnings*} | range <*begin-index*> <*end-index*>]

Function: This command displays the detailed information in the log buffer channel. This command is not supported on low end switches

Parameter: <***begin-index***> is the index start value of the log message, the valid range is 1-65535,**<*end-index*>** is the index end value of the log message, the valid range is 1-65535.

Command Mode: Admin Mode

Default: No parameter specified indicates all the critical log information will be displayed.

Usage Guide: Warning and critical log information is saved in the buffer zone. When displayed to the terminal, their display format should be: index ID time <level> module ID [mission name] log information.

2.2.9.2.2.2 clear logging

Command: clear logging { *sdram* | *nvram* }

Function: This command is used to clear all the information in the log buffer zone.

Command Mode: Admin Mode

Usage Guide: When the old information in the log buffer zone is no longer concerned, we can use this command to clear all the information

example：Clear all information in the log buffer zone sdram

Switch# clear logging sdram

2.2.9.2.2.3 logging host

Command: logging {<*ipv4-addr*> | <*ipv6-addr*>} [facility <*local-number*>] [level <*severity*>]

no logging {<*ipv4-addr*> | <*ipv6-addr*>}[facility <*local-number*>]

Function: The command is used to configure the output channel of the log host. The "no" form of this command will disable the output at the log host output channel

Parameter: <*ipv4-addr*> is the IPv4 address of the host,**<*ipv6-addr*>** is the IPv6 address of the host;**<*local-number*>** is the recording equipment of the host with a valid range of local0 ～ local7,which is in accordance with the facility defined in the RFC3164;**<*severity*>** is the severity threshold of the log information severity level,The rule of the log information output is explained as follows：only those with a level equal to or higher than the threshold will be outputted. For detailed description on the severity please refer to the operation manual.

Command Mode: Global Mode

Default: No log information output to the log host by default. The default recorder of the log host is the local0, the default severity level is warnings

Usage Guide: Only when the log host is configured by the logging command, this command will be available. We can configure many IPv4 and IPv6 log hosts.

Example 1：Send the log information with a severity level equal to or higher than warning to the log server with an IPv4 address of 100.100.100.5, and save to the log recording equipment local1

Switch(Config)# logging 100.100.100.5 facility local1 level warnings

Example 2：Send the log information with a severity level equal to or higher than informational to the log server with an IPv6 address of 3ffe:506:1:2::3, and save to the log recording equipment local1

Switch(Config)# logging 3ffe:506:1:2::3 facility local5 level informational

2.2.9.3 System Log Configuration Example

Example 1：When managing VLAN the IPv4 address of the switch is 100.100.100.1, and

the IPv4 address of the remote log server is 100.100.100.5. It is required to send the log information with a severity equal to or higher than warnings to this log server and save in the log record equipment local1

Configuration procedure:

```
Switch(Config)#interface Ethernet 0
Switch(Config-Ethernet0)#ip address 100.100.100.1 255.255.255.0
Switch(Config-Ethernet0)#exit
Switch(Config)#logging 100.100.100.5 facility local1 level warnings
```

Example 2：When managing VLAN the IPv6 address of the switch is 3ffe:506::1, and the IPv4 address of the remote log server is 3ffe:506::4. It is required to send the log information with a severity equal to or higher than critical to this log server and save the log in the record equipment local7.

Configuration procedure

```
Switch(Config)#interface Ethernet 0
Switch(Config-Ethernet0)#ipv6 address 3ffe:506::1/64
Switch(Config-Ethernet0)#exit
Switch(Config)#logging 3ffe:506::4 facility local7 level warnings
```

2.3 Configurate Switch IP Addresses

All Ethernet ports of ES4626/ES4650 switch is default to Data Link layer ports and perform layer 2 forwarding. VLAN interface represent a Layer 3 interface function which can be assigned an IP address, which is also the IP address of the switch. All VLAN interface related configuration commands can be configured under VLAN Mode. ES4626/ES4650 switch provides three IP address configuration methods:

- Manual
- BootP
- DHCP

Manual configuration of IP address is assign an IP address manually for the switch.

In BootP/DHCP mode, the switch operates as a BootP/DHCP client, send broadcast packets of BootPRequest to the BootP/DHCP servers, and the BootP/DHCP servers assign the address on receiving the request. In addition, ES4626/ES4650 switch can act as a DHCP server, and dynamically assign network parameters such as IP addresses, gateway addresses and DNS server addresses to DHCP clients DHCP Server configuration is detailed in later chapters.

2.3.1 Switch IP Addresses Configuration Task List

1. Manual configuration
2. BootP configuration
3. DHCP configuration

1. Manual configuration

Command	Explanation
ip address <*ip_address*> <*mask*> [secondary] **no ip address <*ip_address*> <*mask*> [secondary]**	Configure the VLAN interface IP address; the "**no ip address <*ip_address*> <*mask*> [secondary]"** command deletes VLAN interface IP address.

2. BootP configuration

Command	Explanation
ip address bootp-client **no ip address bootp-client**	Enable the switch to be a BootP client and obtain IP address and gateway address through BootP negotiation; the "**no ip address bootp-client**" command disables the BootP client function.

3.DHCP configuration

Command	Explanation
ip address dhcp-client **no ip address dhcp-client**	Enable the switch to be a DHCP client and obtain IP address and gateway address through DHCP negotiation; the "**no ip address dhcp-client** " command disables the DHCP client function.

2.3.2 Commands For Configuring Switch IP

2.3.2.1 ip address

Command: ip address <*ip-address*> <*mask*> [secondary]

no ip address [<ip-address> <mask>**] [secondary]**

Function: Set the IP address and mask for the specified VLAN interface; the "**no ip address <*ip address*> <*mask*> [secondary]"** command deletes the specified IP address setting.

Parameter: <*ip-address*> is the IP address in dot decimal format; **<*mask*>** is the subnet mask in dot decimal format; **[secondary]** indicates the IP configured is a secondary IP address.

Default: No IP address is configured upon switch shipment.

Command mode: Interface Mode

Usage Guide: A VLAN interface must be created first before the user can assign an IP address to the switch.

Example: Set 10.1.128.1/24 as the IP address of VLAN1 interface.

Switch(Config)#interface vlan 1

Switch(Config-If-Vlan1)#ip address 10.1.128.1 255.255.255.0

Switch(Config-If-Vlan1)#exit

2.3.2.2 ip address bootp-client

Command: **ip address bootp-client**

no address ip bootp-client

Function: Enable the switch to be a BootP client and obtain IP address and gateway address through BootP negotiation; the "**no ip address bootp-client**" command disables the BootP client function and releases the IP address obtained in BootP .

Default: BootP client function is disabled by default.

Command mode: Interface Mode

Usage Guide: Obtaining IP address through BootP, Manual configuration and DHCP are mutually exclusive, enabling any 2 methods for obtaining IP address is not allowed. Note: To obtain IP address via DHCP, a DHCP server or a BootP server is required in the network.

Example: Get IP address through BootP.

Switch(Config)#interface vlan 1

Switch(Config-If-Vlan1)#ip address bootp-client

Switch (Config-If-Vlan1)#exit

2.3.2.3 ip address dhcp-client

Command: ip address dhcp-client

no address ip dhcp-client

Function: Enables the switch to be a DHCP client and obtain IP address and gateway address through DHCP negotiation; the "**no ip dhcp -client enable**" command disables the DHCP client function and releases the IP address obtained in DHCP. Note: To obtain IP address via DHCP, a DHCP server is required in the network.

Default: the DHCP client function is disabled by default.

Command mode: Interface Mode

Usage Guide: Obtaining IP address by DHCP, Manual configuration and BootP are mutually exclusive, enabling any 2 methods for obtaining an IP address is not allowed.

Example: Getting an IP address through DHCP.

Switch (Config)#interface vlan 1

Switch (Config-If-Vlan1)#ip address dhcp-client
Switch (Config-If-Vlan1)#exit

2.4 SNMP Configuration

2.4.1 Introduction To SNMP

SNMP (Simple Network Management Protocol) is a standard network management protocol widely used in computer network management. SNMP is an evolving protocol. SNMP v1 [RFC1157] is the first version of SNMP which is adapted by vast numbers of manufacturers for its simplicity and easy implementation; SNMP v2c is an enhanced version of SNMP v1, which supports layered network management; SNMP v3 strengthens the security by adding USM (User-based Security Mode) and VACM (View-based Access Control Model).

SNMP protocol provides a simple way of exchange network management information between two points in the network. SNMP employs a polling mechanism of message query, and transmits messages through UDP (a connectionless transport layer protocol). Therefore it is well supported by the existing computer networks.

SNMP protocol employs a station-agent mode. There are two parts in this structure: NMS (Network Management Station) and Agent. NMS is the workstation on which SNMP client program is running. It is the core on the SNMP network management. Agent is the server software runs on the devices which need to be managed. NMS manages all the managed objects through Agents. The switch supports Agent function.

The communication between NMS and Agent functions in Client/Server mode by exchanging standard messages. NMS sends request and the Agent responds. There are seven types of SNMP message:

- Get-Request
- Get-Response
- Get-Next-Request
- Get-Bulk-Request
- Set-Request
- Trap
- Inform-Request

NMS sends queries to the Agent with Get-Request, Get-Next-Request, Get-Bulk-Request and Set-Request messages; and the Agent, upon receiving the requests, replies with Get-Response message. On some special situations, like network device ports are on Up/Down status or the network topology changes, Agents can send

Trap messages to NMS to inform the abnormal events. Besides, NMS can also be set to alert to some abnormal events by enabling RMON function. When alert events are triggered, Agents will send Trap messages or log the event according to the settings. Inform-Request is mainly used for inter-NMS communication in the layered network management.

USM ensures the transfer security by well-designed encryption and authentication. USM encrypts the messages according to the user typed password. This mechanism ensures that the messages can't be viewed on transmission. And USM authentication ensures that the messages can't be changed on transmission. USM employs DES-CBC cryptography. And HMAC-MD5 and HMAC-SHA are used for authentication.

VACM is used to classify the users' access permission. It puts the users with the same access permission in the same group. Users can't conduct the operation which is not authorized.

Introduction to MIB

The network management information accessed by NMS is well defined and organized in a Management Information Base (MIB). MIB is pre-defined information which can be accessed by network management protocols. It is in layered and structured form. The pre-defined management information can be obtained from monitored network devices. ISO ASN.1 defines a tree structure for MID. Each MIB organizes all the available information with this tree structure. And each node on this tree contains an OID (Object Identifier) and a brief description about the node. OID is a set of integers divided by periods. It identifies the node and can be used to locate the node in a MID tree structure, shown in the figure below:

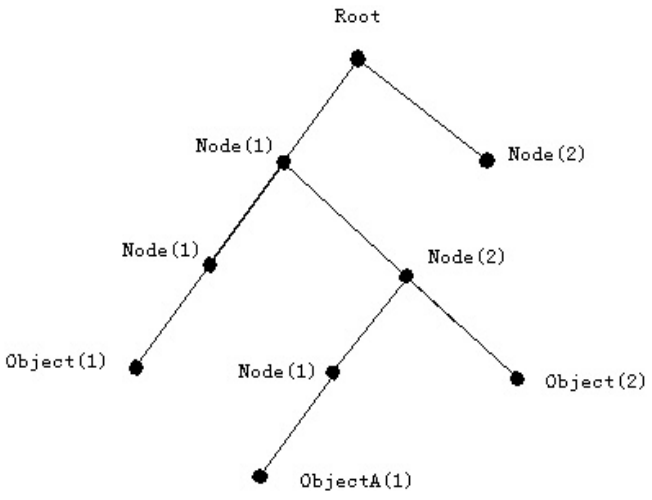


Fig 2-1 ASN.1 Tree Instance

In this figure, the OID of the object A is 1.2.1.1. NMS can locate this object through this unique OID and gets the standard variables of the object. MIB defines a set of standard variables for monitored network devices by following this structure.

If the variable information of Agent MIB needs to be browsed, the MIB browse software needs to be run on the NMS. MIB in the Agent usually consists of public MIB and private MIB. The public MIB contains public network management information that can be accessed by all NMS; private MIB contains specific information which can be viewed and controlled by the support of the manufacturers

MIB-I [RFC1156] is the first implemented public MIB of SNMP, and is replaced by MIB-II [RFC1213]. MIB-II expands MIB-I and keeps the OID of MIB tree in MIB-I. MIB-II contains sub-trees which are called groups. Objects in those groups cover all the functional domains in network management. NMS obtains the network management information by visiting the MIB of SNMP Agent.

The switch can operate as a SNMP Agent, and supports both SNMP v1/v2c and SNMP v3. The switch supports basic MIB-II, RMON public MIB and other public MID such as BRIDGE MIB. Besides, the switch supports self-defined private MIB.

Introduction to RMON

RMON is the most important expansion of the standard SNMP. RMON is a set of MIB definitions, used to define standard network monitor functions and interfaces, enabling the communication between SNMP management terminals and remote monitors. RMON provides a highly efficient method to monitor actions inside the subnets.

MID of RMON consists of 10 groups. The switch supports the most frequently used group 1, 2, 3 and 9:

Statistics: Maintain basic usage and error statistics for each subnet monitored by the Agent.

History: Record periodical statistic samples available from Statistics.

Alarm: Allow management console users to set any count or integer for sample intervals and alert thresholds for RMON Agent records.

Event: A list of all events generated by RMON Agent.

Alarm depends on the implementation of Event. Statistics and History display some current or history subnet statistics. Alarm and Event provide a method to monitor any integer data change in the network, and provide some alerts upon abnormal events (sending Trap or record in logs).

2.4.2 SNMP Configuration Task List

1. Enable or disable SNMP Agent server function
2. Configure SNMP community string
3. Configure IP address of SNMP management base
4. Configure engine ID
5. Configure user

6. Configure group
7. Configure view
8. Configuring TRAP
9. Enable/Disable RMON

1. Enable or disable SNMP Agent server function

Command	Explanation
snmp-server **no snmp-server**	Enable the SNMP Agent function on the switch; the "**no snmp-server**" command disables the SNMP Agent function on the switch.

2. Configure SNMP community string

Command	Explanation
snmp-server community <*string*> {ro|rw} **no snmp-server community <*string*>**	Configure the community string for the switch; the "**no snmp-server community <*string*>**" command deletes the configured community string.

3. Configure IP address of SNMP management base

Command	Explanation
snmp-server securityip {<*ipv4-address*>| <*ipv6-address*>} **no snmp-server securityip {<*ipv4-address*>| <*ipv6-address*>}**	Configure the secure IPv4/IPv6 address which is allowed to access the switch on the NMS; the "**no snmp-server securityip {<*ipv4-address*>| <*ipv6-address*>}**" command deletes configured secure address.
snmp-server SecurityIP enable **snmp-server SecurityIP disable**	Enable or disable secure IP address check function on the NMS.

4. Configure engine ID

Command	Explanation
snmp-server engineid < *engine-string* > **no snmp-server engineid < *engine-string* >**	Configure the local engine ID on the switch. This command is used for SNMP v3.

5. Configure user

Command	Explanation
snmp-server user <*user-string*> <*group-string*> [[encrypted] {auth {md5|sha} <*password-string*>}] **no snmp-server user <*user-string*> <*group-string*>**	Add a user to a SNMP group. This command is used to configure USM for SNMP v3.

6. Configure group

Command	Explanation
snmp-server group <*group-string*> {NoauthNopriv|AuthNopriv|AuthPriv} [[read <*read-string*>] [write <*write-string*>] [notify <*notify-string*>]] **no snmp-server group <*group-string*> {NoauthNopriv|AuthNopriv|AuthPriv}**	Set the group information on the switch. This command is used to configure VACM for SNMP v3.

7. Configure view

Command	Explanation
snmp-server view <*view-string*> <*oid-string*> {include|exclude} **no snmp-server view <*view-string*>**	Configure view on the switch. This command is used for SNMP v3.

8. Configuring TRAP

Command	Explanation
snmp-server enable traps **no snmp-server enable traps**	Enable the switch to send Trap message. This command is used for SNMP v1/v2/v3.
Command: snmp-server host {<*ipv4-addr*>|<*ipv6-addr*>} {v1|v2c|{v3 {NoauthNopriv|AuthNopriv|AuthPriv}}} <*user-string*> **no snmp-server host {<*ipv4-addr*>|<*ipv6-addr*>} {v1|v2c|{v3 {NoauthNopriv|AuthNopriv |AuthPriv}}} <*user-string*>**	Set the host IPv4/IPv6 address which is used to receive SNMP Trap information. For SNMP v1/v2, this command also configures Trap community string; for SNMP v3, this command also configures Trap user name and security level.

9. Enable/Disable RMON

Command	Explanation
rmon enable **no rmon enable**	Enable/disable RMON.

2.4.3 Commands For SNMP

2.4.3.1 rmon

Command: rmon enable

no rmon enable

Function: Enable RMON; the "**no rmon enable**" command disables RMON.

Command mode: Global Mode

Default: RMON is disabled by default.

Example 1: Enable RMON

Switch(config)#rmon enable

Example 2: Disable RMON

Switch(config)#no rmon enable

2.4.3.2 show snmp

Command: show snmp

Function: Display all SNMP counter information.

Command mode: Admin Mode

Example:

Switch#show snmp

0 SNMP packets input

0 Bad SNMP version errors

0 Unknown community name

0 Illegal operation for community name supplied

0 Encoding errors

0 Number of requested variables

0 Number of altered variables

0 Get-request PDUs

0 Get-next PDUs

0 Set-request PDUs

0 SNMP packets output

0 Too big errors (Max packet size 1500)

0 No such name errors

0 Bad values errors

0 General errors

0 Get-response PDUs

0 SNMP trap PDUs

Displayed information	Explanation
snmp packets input	Total number of SNMP packet inputs.
bad snmp version errors	Number of version information error packets.
unknown community name	Number of community name error packets.
illegal operation for community name	Number of permission for community

supplied	name error packets.
encoding errors	Number of encoding error packets.
number of requested variables	Number of variables requested by NMS.
number of altered variables	Number of variables set by NMS.
get-request PDUs	Number of packets received by “get” requests.
get-next PDUs	Number of packets received by “getnext” requests.
set-request PDUs	Number of packets received by “set” requests.
snmp packets output	Total number of SNMP packet outputs.
too big errors	Number of “Too_ big” error SNMP packets.
maximum packet size	Maximum length of SNMP packets.
no such name errors	Number of packets requesting for non-existent MIB objects.
bad values errors	Number of “Bad_values” error SNMP packets.
general errors	Number of “General_errors” error SNMP packets.
response PDUs	Number of response packets sent.
trap PDUs	Number of Trap packets sent.

2.4.3.3 show snmp status

Command: show snmp status

Function: Display SNMP configuration information.

Command mode: Admin Mode

Example:

Switch#show snmp status

Trap enable

RMON enable

Community Information:

V1/V2c Trap Host Information:

V3 Trap Host Information:

Security IP Information:

Displayed information	Description
Community string	Community string

Community access	Community access permission
Trap-rec-address	IP address which is used to receive Trap.
Trap enable	Enable or disable to send Trap.
SecurityIP	IP address of the NMS which is allowed to access Agent

2.4.3.4 snmp-server community

Command: snmp-server community <*string*> {ro|rw}

snmp-server community <*string*>

Function: Configure the community string for the switch; the "**no snmp-server community <*string*>**" command deletes the configured community string.

Parameter: <*string*> is the community string set; **ro|rw** is the specified access mode to MIB, **ro** for read-only and **rw** for read-write.

Command mode: Global Mode

Usage Guide: The switch supports up to 4 community strings.

Example 1: Add a community string named "private" with read-write permission.

Switch(config)#snmp-server community private rw

Example 2: Add a community string named "public" with read-only permission.

Switch(config)#snmp-server community public ro

Example 3: Modify the read-write community string named "private" to read-only.

Switch(config)#snmp-server community private ro

Example 4: Delete community string "private".

Switch(config)#no snmp-server community private

2.4.3.5 snmp-server

Command: snmp-server

no snmp-server

Function: Enable the SNMP proxy server function on the switch. The "**no snmp-server**" command disables the SNMP proxy server function

Command mode: Global mode

Default: SNMP proxy server function is disabled by system default.

Usage guide: To perform configuration management on the switch with network manage software, the SNMP proxy server function has to be enabled with this command.

Example: Enable the SNMP proxy server function on the switch.

Switch(Config)#snmp-server

2.4.3.6 snmp-server enable traps

Command: snmp-server enable traps

no snmp-server enable traps

Function: Enable the switch to send Trap message; the "**no snmp-server enable traps**" command disables the switch to send Trap message.

Command mode: Global Mode

Default: Trap message is disabled by default.

Usage Guide: When Trap message is enabled, if Down/Up in device ports or of system occurs, the device will send Trap messages to NMS that receives Trap messages.

Example 1: Enable to send Trap messages.

Switch(config)#snmp-server enable traps

Example 2: Disable to send Trap messages.

Switch(config)#no snmp-server enable trap

2.4.3.7 snmp-server host

Command: snmp-server host {*<ipv4-addr>*|*<ipv6-addr>}* {v1|v2c|{v3 {NoauthNopriv|AuthNopriv|AuthPriv}}} *<user-string>*

no snmp-server host {*<ipv4-addr>*|*<ipv6-addr>}* {v1|v2c|{v3 {NoauthNopriv|AuthNopriv |AuthPriv}}} *<user-string>*

Function: As for the v1/v2c versions this command configures the IP address and trap community character string of the network manage station receiving the SNMP Trap message. And for v3 version, this command is used for receiving the network manage station IP address and the Trap user name and safety level; the "no" form of this command cancels this IP address.

Command Mode: Global Mode

Parameter: *<ipv4-addr>*|*<ipv6-addr>* is the IP address of the NMS managing station which receives Trap message.

v1|v2c|v3 is the version number when sending the trap

NoauthNopriv|AuthNopriv|AuthPriv is the safety level v3 trap is applied, which may be non encrypted and non authentication, non encrypted and authentication, encrypted and authentication.

<user-*string*> is the community character string applied when sending the Trap message at v1/v2, and will be the user name at v3

Usage Guide: The Community character string configured in this command is the default community string of the RMON event group. If the RMON event group has no community character string configured, the community character string configured in this command will be applied when sending the Trap of RMON, and if the community character string is configured, its configuration will be applied when sending the RMON trap.

Example:

Configure an IP address to receive Trap

Switch(config)#snmp-server host 1.1.1.5 v1 usertrap

Delete a Trap receiving IP address

Switch(config)#no snmp-server host 1.1.1.5 v1 usertrap

Configure a Trap receiving IPv6 address

Switch(config)#snmp-server host 2001:1:2:3::1 v1 usertrap

Delete a Trap receiving IPv6 address

Switch(config)#no snmp-server host 2001:1:2:3::1 v1 usertrap

2.4.3.8 debug snmp mib

Command: debug snmp mib

no debug snmp mib

Function: Enable the SNMP mib debugging; the " **no debug snmp mib**" command disables the debugging

Command Mode: Admin Mode

Usage Guide: When user encounters problems in applying SNMP, the SNMP debugging is available to locate the problem causes.

Example:

Switch#debug snmp mib

2.4.3.9 debug snmp keneral

Command: debug snmp keneral

no debug snmp keneral

Function: Enable the SNMP keneral debugging; the "**no debug snmp keneral**" command disables the debugging function

Command Mode: Admin Mode

Usage Guide: When user encounters problems in applying SNMP, the SNMP debugging is available to locate the problem causes.

Example:

Switch#debug snmp keneral

2.4.3.10 show snmp engineid

Command: show snmp engineid

Function: Display the engine ID commands

Command Mode: Admin Mode

Example:

Switch#show snmp engineid

SNMP engineID:3138633303f1276c Engine Boots is:1

Displayed Information	Explanation
SNMP engineID	Engine number
Engine Boots	Engine boot counts

2.4.3.11 show snmp group

Command: show snmp group

Function: Display the group information commands

Command Mode: Admin Mode

Example:

Switch#show snmp group

Group Name:initial Security Level:noAuthnoPriv

Read View:one

Write View:<no writeview specified>

Notify View:one

Displayed Information	Explanation
Group Name	Group name
Security level	Security level
Read View	Read view name
Write View	Write view name
Notify View	Notify view name
<no writeview specified>	No view name specified by the user

2.4.3.12 show snmp mib

Command: show snmp mib

Function: Display all MIB supported by the switch

Command Mode: Admin Mode

2.4.3.13 show snmp user

Command: show snmp user

Function: Display the user information commands

Command Mode: Admin Mode

Example:

Switch#show snmp user

User name: initialsha

Engine ID: 1234567890

Auth Protocol:MD5 Priv Protocol:DES-CBC

Row status:active

Displayed Information	Explanation
User name	User name
Engine ID	Engine ID
Priv Protocol	Employed encryption algorithm
Auth Protocol	Employed identification algorithm
Row status	User state

2.4.3.14 show snmp view

Command: show snmp view

Function: Display the view information commands.

Command Mode: Admin Mode

Example:

Switch#show snmp view

View Name:readview 1. -Included active

1.3. - Excluded active

Displayed Information	Explanation
View Name	View name
1.and1.3.	OID number
Included	The view includes sub trees rooted by this OID
Excluded	The view does not include sub trees rooted by this OID
active	State

2.4.3.15 snmp-server engineid

Command: snmp-server engineid < *engine-string* >

no snmp-server engineid < *engine-string* >

Function: Configure the engine ID; the “no" form of this command restores to the default engine ID

Command Mode: Global mode

Parameter：<engine-string> is the engine ID shown in 1-32 digit hex characters

Default： Default value is the company ID plus local MAC address

Usage Guide:

Example: Set current engine ID to A66688999F

Switch(config)#snmp-server engineid A66688999F

Restore the default engine ID

Switch(config)#no snmp-server engineid A66688999F

2.4.3.16 snmp-server group

Command: snmp-server group <*group-string*>
{NoauthNopriv|AuthNopriv|AuthPriv} [[read <*read-string*>] [write <*write-string*>] [notify <*notify-string*>]]
no snmp-server group <*group-string*> {NoauthNopriv|AuthNopriv|AuthPriv}

Function: This command is used to configure a new group; the "no" form of this command deletes this group.

Command Mode: Global Mode

Parameter：<group-string > group name which includes 1-32 characters

NoauthNopriv Applies the non recognizing and non encrypting safety level

AuthNopriv Applies the recognizing but non encrypting safety level

AuthPriv Applies the recognizing and encrypting safety level

Name of readable view which includes 1-32 characters

Name of writable view which includes 1-32 characters

Name of trappable view which includes 1-32 characters

Usage Guide: There is a default view "v1defaultviewname" in the system. It is recommended to use this view as the view name of the notification. If the read or write view name is empty, corresponding operation will be disabled.

Example: Create a group CompanyGroup, with the safety level of recognizing and encrypting, the read viewname is readview, and the writing is disabled.

Switch (Config)#snmp-server group CompanyGroup AuthPriv read readview

deletet group

Switch (Config)#no snmp-server group CompanyGroup AuthPriv

2.4.3.17 snmp-server SecurityIP enable

Command: snmp-server SecurityIP enable

snmp-server SecurityIP disable

Function: Enable/disable the safety IP address authentication on NMS manage station

Command Mode: Global Mode

Default： Enable the safety IP address authentication function

Example:

Disable the safety IP address authentication function

Switch(config)#snmp-server securityip disable

2.4.3.18 snmp-server view

Command: snmp-server view <*view-string*> <*oid-string*> {include|exclude}

no snmp-server view <*view-string*>

Function: This command is used to create or renew the view information; the “no" form of this command deletes the view information

Command Mode: Global Mode

Parameter: <view-string> view name, containing 1-32 characters;

<oid-string>is OID number or corresponding node name, containing 1-255 characters.

include|exclude , include/exclude this OID

Usage Guide: The command supports not only the input using the character string of the variable OID as parameter. But also supports the input using the node name of the parameter

Example:

Create a view, the name is readview, including iso node but not including the iso.3 node

Switch (Config)#snmp-server view readview iso include

Switch (Config)#snmp-server view readview iso.3 exclude

Delete the view

Switch (Config)#no snmp-server view readview

2.4.3.19 snmp-server user

Command:snmp-server user <*user-string*> <*group-string*> [[encrypted] {auth {md5|sha} <*password-string*>}]

no snmp-server user <*user-string*> <*group-string*>

Function: Add a new user to an SNMP group; the "no” form of this command deletes this user

Command Mode: Global Mode

Parameter: <user-string> is the user name containing 1-32 characters

<group-string> is the name of the group the user belongs to, containing 1-32 characters

encrypted use DES for the packet encryption

auth perform packet authentication

md5 packet authentication using HMAC MD5 algorithm

sha packet authentication using HMAC SHA algorithm

<password-string> user password,containing 1-32 character

Usage Guide: If the encryption and authentication is not selected, the default settings will be no encryption and no authentication. If the encryption is selected, the authentication must be done. When deleting a user, if correct username and incorrect group name is inputted, the user can still be deleted.

Example: Add a new user tester in the UserGroup with an encryption safety level and HMAC md5 for authentication, the password is hello.

Switch (Config)#snmp-server user tester UserGroup encrypted auth md5 hello

deletes an User

Switch (Config)#no snmp-server user tester UserGroup

2.4.3.20 snmp-server securityip

Command：snmp-server securityip {*<ipv4-address>*| *<ipv6-address>*}

no snmp-server securityip {*<ipv4-address>*| *<ipv6-address>*}

Function： Configure to permit to access security IPv4 or IPv6 address of the switch NMS administration station; the "**no snmp-server securityip {*<ipv4-address>*| *<ipv6-address>*}**" command deletes configured security IPv4 or IPv6 address.

Command Mode： Global Mode

Parameter： **<ipv4-address>** is NMS security IPv4 address, point separated decimal format

<ipv6-address> is NMS security IPv6 address, colon separated hex format.

Usage Guide： It is only the consistency between NMS administration station IPv4 or IPv6 address and security IPv4 or IPv6 address configured by the command, so it send SNMP package could be processed by switch, the command only applies to SNMP.

Example：

Configure security IP address of NMS administration station

Switch(config)#snmp-server securityip 1.1.1.5

Delete security IPv6 address

Switch(config)#no snmp-server securityip 2001::1

2.4.4 Typical SNMP Configuration Examples

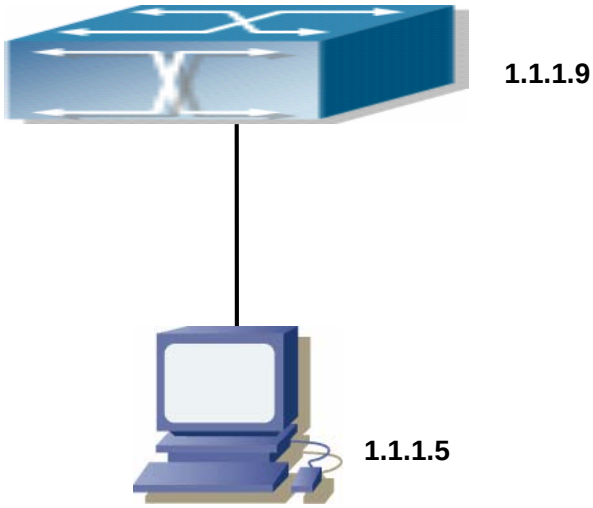


Fig 2-2 Typical SNMP Configuration

The IP address of the NMS is 1.1.1.5; the IP address of the switch (Agent) is 1.1.1.9

Scenario 1: The NMS network administrative software uses SNMP protocol to obtain data from the switch.

The configuration on the switch is listed below:

Switch(config)#snmp-server

Switch(Config)#snmp-server community private rw

Switch(Config)#snmp-server community public ro

Switch(Config)#snmp-server securityip 1.1.1.5

The NMS can use “private” as the community string to access the switch with read-write permission, or use “public” as the community string to access the switch with read-only permission.

Scenario 2: NMS will receive Trap messages from the switch (Note: NMS may have community string verification for the Trap messages. In this scenario, the NMS uses a Trap verification community string of “ectrap”).

The configuration on the switch is listed below:

Switch(config)#snmp-server

Switch(Config)#snmp-server host 1.1.1.5 ectrap

Switch(Config)#snmp-server enable traps

Scenario 3: NMS uses SNMP v3 to obtain information from the switch.

The configuration on the switch is listed below:

Switch(config)#snmp-server

Switch (Config)#snmp-server user tester UserGroup encrypted auth md5 hello

Switch (Config)#snmp-server group UserGroup AuthPriv read max write max notify max

Switch (Config)#snmp-server view max 1 include

Scenario 4: NMS wants to receive the v3Trap messages sent by the switch.

The configuration on the switch is listed below:

Switch(config)#snmp-server

Switch(config)#snmp-server host 10.1.1.2 v3 AuthPriv tester

Switch(config)#snmp-server enable traps

2.4.5 SNMP Troubleshooting

When users configure the SNMP, the SNMP server may fail to run properly due to physical connection failure and wrong configuration, etc. Users can troubleshoot the problems by following the guide below:

- ✧ Good condition of the physical connection.
- ✧ Interface and datalink layer protocol is Up (use the “show interface” command), and the connection between the switch and host can be verified by ping (use “ping”

command).

- ✧ The switch enabled SNMP Agent server function (use “snmp-server” command)
- ✧ Secure IP for NMS (use “snmp-server securityip” command) and community string (use “snmp-server community” command) are correctly configured, as any of them fails, SNMP will not be able to communicate with NMS properly.
- ✧ If Trap function is required, remember to enable Trap (use “snmp-server enable traps” command). and remember to properly configure the target host IP address and community string for Trap (use “snmp-server host” command) to ensure Trap message can be sent to the specified host.
- ✧ If RMON function is required, RMON must be enabled first (use “rmon enable” command).
- ✧ Use “show snmp” command to verify sent and received SNMP messages; Use “show snmp status” command to verify SNMP configuration information; Use “debug snmp packet” to enable SNMP debug function and verify debug information.
- ✧ If users still can’t solve the SNMP problems, Please contact our technical and service center.

2.5 Switch Upgrade

ES4626/ES4650 switch provides two ways for switch upgrade: BootROM upgrade and the TFTP/FTP upgrade under Shell.

2.5.1 Switch System Files

The system files includes system image file and boot file. The updating of the switch is to update the two files by overwrite the old files with the new ones.

The system image files refers to the compressed files of the switch hardware drivers, and software support program, etc, namely what we usually call the IMG update file. The IMG file can only be saved in the FLASH with a defined name of nos.img

The boot file is for initiating the switch, namely what we usually call the ROM update file ((It can be compressed into IMG file if it is of large size). The boot file can only be saved in the ROM in which the file name is defined as boot.rom

The update method of the system image file and the boot file is the same. The switch supplies the user with two modes of updating: 1. BootROM mode; 2. TFTP and FTP update at Shell mode. This two update method will be explained in details in following two sections.

2.5.2 BootROM Upgrade

There are two methods for BootROM upgrade: TFTP and FTP, which can be selected at BootROM command settings.

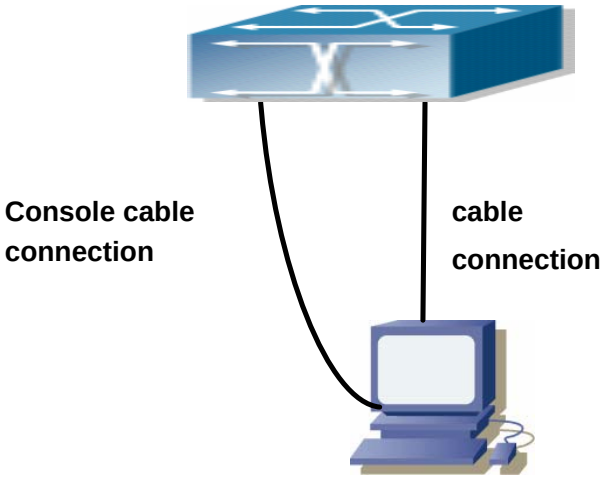


Fig 2-3 Typical topology for switch upgrade in BootROM mode

The upgrade procedures are listed below:

Step 1:

As shown in the figure, a PC is used as the console for the switch. A console cable is used to connect PC to the management port on the switch. The PC should have FTP/TFTP server software installed and has the image file required for the upgrade.

Step 2:

Press “ctrl+b” on switch boot up until the switch enters BootROM monitor mode. The operation result is shown below:

ES4650 Management Switch

Copyright (c) 2001-2004 by Accton Technology Corporation.

All rights reserved.

Reset chassis ... done.

Testing RAM...

134,217,728 RAM OK.

Loading BootROM...

Starting BootRom...

Attaching to file system ... done.

BootRom version: 1.0.4

Creation date: Jun 9 2006, 14: 54: 12

Attached TCP/IP interface to lnPci0.

[Boot]:

Step 3:

Under BootROM mode, run “setconfig” to set the IP address and mask of the switch under BootROM mode, server IP address and mask, and select TFTP or FTP upgrade. Suppose the switch address is 192.168.1.2/24, and PC address is 192.168.1.66/24, and select TFTP upgrade, the configuration should like:

[Boot]: setconfig

Host IP Address: 10.1.1.1 192.168.1.2

Server IP Address: 10.1.1.2 192.168.1.66

FTP(1) or TFTP(2): 1 2

Network interface configure OK.

[Boot]:

Step 4:

Enable FTP/TFTP server in the PC. For TFTP, run TFTP server program; for FTP, run FTP server program. Before start downloading upgrade file to the switch, verify the connectivity between the server and the switch by ping from the server. If ping succeeds, run “load” command in the BootROM mode from the switch; if it fails, perform troubleshooting to find out the cause. The following is the configuration for the system update image file.

[Boot]: load nos.img

Loading...

entry = 0x10010

size = 0x1077f8

Step 5:

Execute “write nos.img” in BootROM mode. The following saves the system update image file.

[Boot]: write nos.img

Programming...

Program OK.

[Boot]:

Step 6:

After successful upgrade, execute “run” command in BootROM mode to return to CLI configuration interface.

[Boot]: run（or reboot）

Other commands in BootROM mode

1. DIR command

Used to list existing files in the FLASH.

[Boot]: dir

boot.rom 327,440 1900-01-01 00: 00: 00 --SH
boot.conf 83 1900-01-01 00: 00: 00 --SH

nos.img 2,431,631 1980-01-01 00: 21: 34 ----

startup-config 2,922 1980-01-01 00: 09: 14 ----

temp.image 2,431,631 1980-01-01 00: 00: 32 ----

2. CONFIG RUN command

Used to set the IMAGE file to run upon system start-up, and the configuration file to run upon configuration recovery.

[Boot]: config run

Boot File: [nos.img] nos1.image

Config File: [boot.conf]

2.5.3 FTP/TFTP Upgrade

2.5.3.1 Introduction To FTP/TFTP

FTP(File Transfer Protocol)/TFTP(Trivial File Transfer Protocol) are both file transfer protocols that belonging to fourth layer(application layer) of the TCP/IP protocol stack, used for transferring files between hosts, hosts and switches. Both of them transfer files in a client-server model. Their differences are listed below.

FTP builds upon TCP to provide reliable connection-oriented data stream transfer service. However, it does not provide file access authorization and uses simple authentication mechanism(transfers username and password in plain text for authentication). When using FTP to transfer files, two connections need to be established between the client and the server: a management connection and a data connection. A transfer request should be sent by the FTP client to establish management connection on port 21 in the server, and negotiate a data connection through the management connection.

There are two types of data connections: active connection and passive connection.

In active connection, the client transmits its address and port number for data transmission to the sever, the management connection maintains until data transfer is complete. Then, using the address and port number provided by the client, the server establishes data connection on port 20 (if not engaged) to transfer data; if port 20 is engaged, the server automatically generates some other port number to establish data connection.

In passive connection, the client, through management connection, notify the server to establish a passive connection. The server then creates its own data listening port and informs the client about the port, and the client establishes data connection to the specified port.

As data connection is established through the specified address and port, there is a third party to provide data connection service.

TFTP builds upon UDP, providing unreliable data stream transfer service with no user authentication or permission-based file access authorization. It ensures correct data transmission by sending and acknowledging mechanism and retransmission of time-out packets. The advantage of TFTP over FTP is that it is a simple and low overhead file transfer service.

ES4626/ES4650 switch can operate as either FTP/TFTP client or server. When ES4626/ES4650 switch operates as a FTP/TFTP client, configuration files or system files can be downloaded from the remote FTP/TFTP servers(can be hosts or other switches) without affecting its normal operation. And file list can also be retrieved from the server in ftp client mode. Of course, ES4626/ES4650 switch can also upload current configuration files or system files to the remote FTP/TFTP servers(can be hosts or other switches). When ES4626/ES4650 switch operates as a FTP/TFTP server, it can provide file upload and download service for authorized FTP/TFTP clients, as file list service as FTP server.

Here are some terms frequently used in FTP/TFTP.

ROM: Short for EPROM, erasable read-only memory. EPROM is repalced by FLASH memory in ES4626/ES4650 switch.

SDRAM: RAM memory in the switch, used for system software operation and configuration sequence storage.

FLASH: Flash memory used to save system file and configuration file

System file: including system image file and boot file.

System image file: refers to the compressed file for switch hardware driver and software support program, usually refer to as IMAGE upgrade file. In ES4626/ES4650 switch, the system image file is allowed to save in FLASH only. ES4626/ES4650 switch mandates the name of system image file to be uploaded via FTP in Global Mode to be nos.img, other IMAGE system files will be rejected.

Boot file: refers to the file initializes the switch, also referred to as the ROM upgrade file (Large size file can be compressed as IMAGE file). In ES4626/ES4650 switch, the boot file is allowed to save in ROM only. ES4626/ES4650 switch mandates the name of the boot file to be boot.rom.

Configuration file: including start up configuration file and running configuration file. The distinction between start up configuration file and running configuration file can facilitate the backup and update of the configurations.

Start up configuration file: refers to the configuration sequence used in switch start up. ES4626/ES4650 switch start up configuration file stores in FLASH only, corresponding to the so called configuration save. To prevent illicit file upload and easier configuration, ES4626/ES4650 switch mandates the name of start up configuration file to be startup-config.

Running configuration file: refers to the running configuration sequence use in the

switch. In ES4626/ES4650 switch, the running configuration file stores in the RAM. In the current version, the running configuration sequence running-config can be saved from the RAM to FLASH by **write** command or **copy running-config startup-config** command, so that the running configuration sequence becomes the start up configuration file, which is called configuration save. To prevent illicit file upload and easier configuration, ES4626/ES4650 switch mandates the name of running configuration file to be running-config.

Factory configuration file: The configuration file shipped with ES4626/ES4650 switch in the name of factory-config. Run **set default** and **write**, and restart the switch, factory configuration file will be loaded to overwrite current start up configuration file.

2.5.3.2 FTP/TFTP Configuration

The configurations of ES4626/ES4650 switch as FTP and TFTP clients are almost the same, so the configuration procedures for FTP and TFTP are described together in this manual.

2.5.3.2.1 FTP/TFTP Configuration Task List

1. FTP/TFTP client configuration

Upload/download the configuration file or system file.

（1） For FTP client, server file list can be checked.

2. FTP server configuration

（1）Start FTP server

（2）Configure FTP login username and password

（3）Modify FTP server connection idle time

（4）Shut down FTP server

3. TFTP server configuration

（1）Start TFTP server

（2）Configure TFTP server connection idle time

（3）Configure retransmission times before timeout for packets without acknowledgement

（4）Shut down TFTP server

1. FTP/TFTP client configuration

（1）FTP/TFTP client upload/download file

Command	Explanation
Admin Mode	
copy <*source-url*> <*destination-url*> [ascii | binary]	FTP/TFTP client upload/download file

（2）For FTP client, server file list can be checked.

Global Mode	
dir <*ftpServerUrl*>	For FTP client, server file list can be checked. *FtpServerUrl* format looks like: ftp: //user: password@IP Address

2. FTP server configuration

（1）Start FTP server

Command	Explanation
Global Mode	
ftp-server enable **no ftp-server enable**	Start FTP server, the "**no ftp-server enable**" command shuts down FTP server and prevents FTP user from logging in.

（2）Modify FTP server connection idle time

Command	Explanation
Global Mode	
ftp-server timeout <*seconds*>	Set connection idle time

3. TFTP server configuration

（1）Start TFTP server

Command	Explanation
Global Mode	
tftp-server enable **no tftp-server enable**	Start TFTP server, the "**no ftp-server enable**" command shuts down TFTP server and prevents TFTP user from logging in.

（2）Modify TFTP server connection idle time

Command	Explanation
Global Mode	
tftp-server retransmission-number <*number*>	Set maximum retransmission time within timeout interval.

（3）Modify TFTP server connection retransmission time

Command	Explanation
Global Mode	
tftp-server retransmission-number <*number*>	Set maximum retransmission time within timeout interval.

2.5.3.2.2 Commands for Switch Upgrade

2.5.3.2.2.1 copy（FTP）

Command: copy <***source-url*> <*destination-url*> [ascii | binary]**

Function: Download files to the FTP client.

Parameter： <***source-url*>** is the location of the source files or directories to be copied;**<*destination-url*>** is the destination address to which the files or directories to be copied;forms of <***source-url*>** and **<*destination-url*>** vary depending on different locations of the files or directories. **ascii** indicates the ASCII standard will be adopted;**binary** indicates that the binary system will be adopted in the file transmission （default transmission method）.When URL represents an FTP address, its form should be:

ftp://<*username*>:<*password*>@{<*ipaddress*>|<*ipv6address*>|<*hostname*> }/<*filename*>,amongst <*username*> is the FTP user name,<*password*> is the FTP user password,<*ipaddress*>|<*ipv6address*> is the IPv4 or IPv6 address of the FTP server/client,<*hostname*> is the name of the host mapping with the IPv6 address,it does not support the file download and upload with hosts mapping with IPv4 addresses,<*filename*> is the name of the FTP upload/download file.

Special keywords of the filename

Keywords	**Source or destination addresses**
running-config	Running configuration files
startup-config	Startup configuration files
nos.img	System files
nos.rom	System startup files

Command Mode: Admin Mode

Usage Guide: This command supports command line hints,namely if the user can enter commands in following forms: **copy *<filename>* ftp:**// or **copy ftp:**// ***<filename>*** and press Enter,following hints will be provided by the system：

ftp server ip/ipv6 address [x.x.x.x]/[x:x::x:x] >

ftp username>

ftp password>

ftp filename>

Requesting for FTP server address, user name, password and file name

Examples:

（1）Save images in the FLASH to the FTP server of 2004:1:2:3::6

Switch#copy nos.img ftp://username:password@2004:1:2:3::6/ nos.img

（2）Obtain system file nos.img from the FTP server 2004:1:2:3::6

Switch#copy ftp:// username:password@2004:1:2:3::6/nos.img nos.img

（3）Save the running configuration files

Switch#copy running-config startup-config

2.5.3.2.2.2 copy（TFTP）

Command: copy <***source-url*> <*destination-url*> [ascii | binary]**

Function: Download files to the TFTP client

Parameter：<***source-url*>** is the location of the source files or directories to be cop ied;**<*destination-url*>** is the destination address to which the files or directories to be copied;forms of <***source-url*>** and **<*destination-url*>** vary depending on different locations of the files or directories. **ascii** indicates the ASCII standard will be adop ted;**binary** indicates that the binary system will be adopted in the file transmission （default transmission method）.When URL represents an TFTP address, its form s hould be: tftp://{<*ipaddress*>|<*ipv6address*>|<*hostname*> }/<*filename*>,amongst <*ipaddr ess*>|<*ipv6address*> is the IPv4 or IPv6 address of the TFTP server/client,<*hostnam e*> is the name of the host mapping with the IPv6 address,it does not support the file download and upload with hosts mapping with IPv4 addresses,<*filename*> is the name of the TFTP upload/download file.

Special keyword of the filename

Keywords	**Source or destination addresses**
running-config	Running configuration files
startup-config	Startup configuration files
nos.img	System files
nos.rom	System startup files

Command Mode: Admin Mode

Usage Guide: This command supports command line hints,namely if the user can enter commands in following forms: **copy <*filename*> tftp:**// or **copy tftp:**// **<*filename*>** and press Enter,following hints will be provided by the system：

tftp server ip/ipv6 address[x.x.x.x]/[x:x::x:x]>

tftp filename>

Requesting for TFTP server address, file name

Example:

（1）Save images in the FLASH to the TFTP server of 2004:1:2:3::6

Switch#copy nos.img tftp:// 2004:1:2:3::6/ nos.img

（2）Obtain system file nos.img from the TFTP server 2004:1:2:3::6

Switch#copy tftp:// 2004:1:2:3::6/nos.img nos.img

（3）Save running configuration files

Switch#copy running-config startup-config

2.5.3.2.2.3 dir

Command: dir <*ftp-server-url*>

Function: Browse the file list on the FTP server.

Parameter：The form of **< ftp-server-url >** is：ftp://<*username*>:<*password*>@{<*ipv4address*>|<*ipv6address*>},amongst <*username*> is the FTP user name,<*password*> is the FTP user password,

{<*ipv4address*>|<*ipv6address*>} is the IPv4 or IPv6 address of the FTP server.

Command Mode: Global Mode

Example: Browse the list of the files on the server with the FTP client

Switch(Config)# dir ftp://user:password@IPv6 Address.

2.5.3.2.2.4 ftp-server enable

Command: ftp-server enable

no ftp-server enable

Function: Start FTP server, the "**no ftp-server enable**" command shuts down FTP server and prevents FTP user from logging in.

Default: FTP server is not started by default.

Command mode: Global Mode

Usage Guide: When FTP server function is enabled, the switch can still perform ftp client functions. FTP server is not started by default.

Example: enable FTP server service.

Switch#config

Switch(Config)# ftp-server enable

2.5.3.2.2.5 ftp-server timeout

Command: ftp-server timeout <*seconds*>

Function: Set data connection idle time

Parameter: < *seconds*> is the idle time threshold (in seconds) for FTP connection, the valid range is 5 to 3600.

Default: The system default is 600 seconds.

Command mode: Global Mode

Usage Guide: When FTP data connection idle time exceeds this limit, the FTP management connection will be disconnected.

Example: Modify the idle threshold to 100 seconds.

Switch#config

Switch(Config)#ftp-server timeout 100

2.5.3.2.2.6 show ftp

Command: show ftp

Function: display the parameter settings for the FTP server

Command mode: Admin Mode

Default: No display by default.

Example:

Switch#show ftp

Timeout : 600

Displayed information	Description
Timeout	Timeout time.

2.5.3.2.2.7 show tftp

Command: show tftp

Function: display the parameter settings for the TFTP server

Default: No display by default.

Command mode: Admin Mode

Example:

Switch#show tftp

timeout : 60

Retry Times : 10

Displayed information	Explanation
Timeout	Timeout time.
Retry Times	Retransmission times.

2.5.3.2.2.8 tftp-server enable

Command: tftp-server enable

no tftp-server enable

Function: Start TFTP server, the "**no ftp-server enable**" command shuts down TFTP server and prevents TFTP user from logging in.

Default: TFTP server is not started by default.

Command mode: Global Mode

Usage Guide: When TFTP server function is enabled, the switch can still perform tftp client functions. TFTP server is not started by default.

Example: enable TFTP server service.

Switch#config

Switch(Config)#tftp-server enable

2.5.3.2.2.9 tftp-server retransmission-number

Command: tftp-server retransmission-number <*number*>

Function: Set the retransmission time for TFTP server

Parameter: < *number*> is the time to re-transfer, the valid range is 1 to 20.

Default: The default value is 5 retransmission.

Command mode: Global Mode

Example: Modify the retransmission to 10 times.

Switch#config

Switch(Config)#tftp-server retransmission-number 10

2.5.3.2.2.10 tftp-server transmission-timeout

Command: tftp-server transmission-timeout <*seconds*>

Function: Set the transmission timeout value for TFTP server

Parameter: < *seconds*> is the timeout value, the valid range is 5 to 3600s.

Default: The system default timeout setting is 600 seconds.

Command mode: Global Mode

Example: Modify the timeout value to 60 seconds.

Switch#config

Switch(Config)#tftp-server transmission-timeout 60

2.5.4 FTP/TFTP Configuration Examples

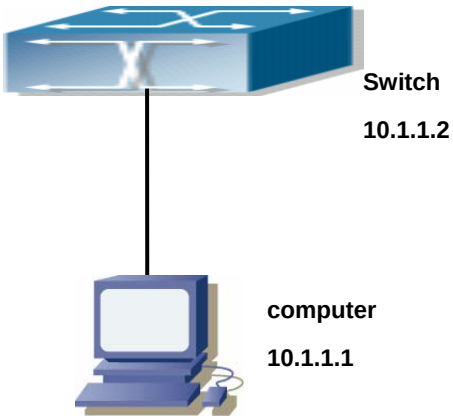


Fig 2-4 Download nos.img file as FTP/TFTP client

Scenario 1: The switch is used as FTP/TFTP client. The switch connects from one of its ports to a computer, which is a FTP/TFTP server with an IP address of 10.1.1.1; the switch acts as a FTP/TFTP client, the IP address of the switch management VLAN is 10.1.1.2. Download “nos.img” file in the computer to the switch.

- **FTP Configuration**

Computer side configuration:

Start the FTP server software on the computer and set the username “Switch”, and the password “switch”. Place the “12_30_nos.img” file to the appropriate FTP server directory on the computer.

The configuration procedures of the switch is listed below:

Switch(Config)#inter vlan 1
Switch (Config-If-Vlan1)#ip address 10.1.1.2 255.255.255.0
Switch (Config-If-Vlan1)#no shut
Switch (Config-If-Vlan1)#exit
Switch (Config)#exit
Switch#copy ftp: //Switch:switch@10.1.1.1/12_30_nos.img nos.img

With the above commands, the switch will have the “nos.img” file in the computer downloaded to the FLASH.

- **TFTP Configuration**

Computer side configuration:

Start TFTP server software on the computer and place the “nos.img” file to the appropriate TFTP server directory on the computer.

The configuration procedures of the switch is listed below:

Switch (Config)#inter vlan 1
Switch (Config-If-Vlan1)#ip address 10.1.1.2 255.255.255.0
Switch (Config-If-Vlan1)#no shut
Switch (Config-If-Vlan1)#exit
Switch (Config)#exit
Switch#copy tftp: //10.1.1.1/12_30_nos.img nos.img

Scenario 2: The switch is used as FTP server. The switch operates as the FTP server and connects from one of its ports to a computer, which is a FTP client. Transfer the “nos.img” file in the switch to the computer and save as 12_25_nos.img.

The configuration procedures of the switch is listed below:

Switch (Config)#inter vlan 1
Switch (Config-If-Vlan1)#ip address 10.1.1.2 255.255.255.0
Switch (Config-If-Vlan1)#no shut
Switch (Config-If-Vlan1)#exit
Switch (Config)#ftp-server enable
Switch(Config)# username Switch password 0 Admin

Computer side configuration:

Login to the switch with any FTP client software, with the username “Admin” and password “switch”, use the command “get nos.img 12_25_nos.img” to download

“nos.img” file from the switch to the computer.

Scenario 3: The switch is used as TFTP server. The switch operates as the TFTP server and connects from one of its ports to a computer, which is a TFTP client. Transfer the “nos.img” file in the switch to the computer.

The configuration procedures of the switch is listed below:

Switch(Config)#inter vlan 1

Switch (Config-If-Vlan1)#ip address 10.1.1.2 255.255.255.0

Switch (Config-If-Vlan1)#no shut

Switch (Config-If-Vlan1)#exit

Switch (Config)#tftp-server enable

Computer side configuration:

Login to the switch with any TFTP client software, use the “tftp” command to download “nos.img” file from the switch to the computer.

Scenario 4: The switch is used as FTP/TFTP client. The switch connects from one of its ports to a computer, which is a FTP/TFTP server with an IP address of 10.1.1.1; several switch user profile configuration files are saved in the computer. The switch operates as the FTP/TFTP client, the management VLAN IP address is 10.1.1.2. Download switch user profile configuration files from the computer to the switch FLASH.

- **FTP Configuration**

Computer side configuration:

Start the FTP server software on the computer and set the username “Switch”, and the password “Admin”. Save “nos.img”, “boot.rom” and “startup-config” in the appropriate FTP server directory on the computer.

The configuration procedures of the switch is listed below:

Switch (Config)#inter vlan 1

Switch (Config-If-Vlan1)#ip address 10.1.1.2 255.255.255.0

Switch (Config-If-Vlan1)#no shut

Switch (Config-If-Vlan1)#exit

Switch (Config)#exit

Switch#copy ftp: //Switch: Admin@10.1.1.1/nos.img nos.img

Switch#copy ftp: //Switch: Admin@10.1.1.1/boot.rom boot.rom

Switch#copy ftp: //Switch: Admin@10.1.1.1/startup-config startup-config

With the above commands, the switch will have the user profile configuration file in the computer downloaded to the FLASH.

- **TFTP Configuration**

Computer side configuration:

Start TFTP server software on the computer and place “nos.img”, “boot.rom” and

“startup-config” to the appropriate TFTP server directory on the computer.

The configuration procedures of the switch is listed below:

Switch (Config)#inter vlan 1

Switch (Config-If-Vlan1)#ip address 10.1.1.2 255.255.255.0

Switch (Config-If-Vlan1)#no shut

Switch (Config-If-Vlan1)#exit

Switch (Config)#exit

Switch#copy tftp: //10.1.1.1/ nos.img nos.img

Switch#copy tftp: //10.1.1.1/ boot.rom boot.rom

Switch#copy tftp: //10.1.1.1/ startup-config startup-config

Scenario 5: ES4626/ES4650 switch acts as FTP client to view file list on the FTP server.

Synchronization conditions: The switch connects to a computer by an Ethernet port, the computer is a FTP server with an IP address of 10.1.1.1; the switch acts as a FTP client, and the IP address of the switch management VLAN1 interface is 10.1.1.2.

FTP Configuration

PC side:

Start the FTP server software on the PC and set the username “Switch”, and the password “Admin”.

ES4626/ES4650 switch:

Switch (Config)#inter vlan 1

Switch (Config-If-Vlan1)#ip address 10.1.1.2 255.255.255.0

Switch (Config-If-Vlan1)#no shut

Switch (Config-If-Vlan1)#exit

Switch (Config)#dir ftp: //Switch: Admin@10.1.1.1

220 Serv-U FTP-Server v2.5 build 6 for WinSock ready...

331 User name okay, need password.

230 User logged in, proceed.

200 PORT Command successful.

150 Opening ASCII mode data connection for /bin/ls.

recv total = 480

nos.img

nos.rom

parsecommandline.cpp

position.doc

qmdict.zip

shell maintenance statistics.xls

… (some display omitted here)

show.txt

snmp.TXT
226 Transfer complete.
Switch (Config)#

2.5.5 FTP/TFTP Troubleshooting

2.5.5.1 FTP Troubleshooting

When upload/download system file with FTP protocol, the connectivity of the link must be ensured, i.e., use the "**Ping**" command to verify the connectivity between the FTP client and server before running the FTP program. If ping fails, you will need to check for appropriate troubleshooting information to recover the link connectivity.

☞ The following is what the message displays when files are successfully transferred. Otherwise, please verify link connectivity and retry "copy" command again.

220 Serv-U FTP-Server v2.5 build 6 for WinSock ready...
331 User name okay, need password.
230 User logged in, proceed.
200 PORT Command successful.
nos.img file length = 1526021
read file ok
send file
150 Opening ASCII mode data connection for nos.img.
226 Transfer complete.
close ftp client.

☞ The following is the message displays when files are successfully received. Otherwise, please verify link connectivity and retry "copy" command again.

220 Serv-U FTP-Server v2.5 build 6 for WinSock ready...
331 User name okay, need password.
230 User logged in, proceed.
200 PORT Command successful.
recv total = 1526037
****
write ok
150 Opening ASCII mode data connection for nos.img (1526037 bytes).
226 Transfer complete.

☞ If the switch is upgrading system file or system start up file through FTP, the switch must not be restarted until "close ftp client" or "226 Transfer complete." is displayed, indicating upgrade is successful, otherwise the switch may be rendered unable to

start. If the system file and system start up file upgrade through FTP fails, please try to upgrade again or use the BootROM mode to upgrade.

2.5.5.2 TFTP Troubleshooting

When upload/download system file with TFTP protocol, the connectivity of the link must be ensured, i.e., use the "**Ping**" command to verify the connectivity between the TFTP client and server before running the TFTP program. If ping fails, you will need to check for appropriate troubleshooting information to recover the link connectivity.

- ☞ The following is the message displays when files are successfully transferred. Otherwise, please verify link connectivity and retry "copy" command again.

  nos.img file length = 1526021
  read file ok
  begin to send file,wait...
  file transfers complete.
  close tftp client.

- ☞ The following is the message displays when files are successfully received. Otherwise, please verify link connectivity and retry "copy" command again.

  begin to receive file,wait...
  recv 1526037
  ****
  write ok
  transfer complete
  close tftp client.

If the switch is upgrading system file or system start up file through TFTP, the switch must not be restarted until "close tftp client" is displayed, indicating upgrade is successful, otherwise the switch may be rendered unable to start. If the system file and system start up file upgrade through TFTP fails, please try upgrade again or use the BootROM mode to upgrade

2.6 Security Feature Configuration

2.6.1 Security Feature Introduction

Before introducing the security features, we here first introduce the DoS. The DoS is short for Denial of Service, which is a simple but effective destructive attack on the internet. The server under DoS attack will drop normal user data packet due to non-stop

processing the attacker's data packet, leading to the denial of the service and worse can lead to leak of sensitive data of the server.

Security feature refers to applications such as protocol check which is for protecting the server from attacks such as DoS. The protocol check allows the user to drop matched packets based on specified conditions. The security features provide several simple and effective protections against Dos attacks while acting no influence on the linear forwarding performance of the switch.

2.6.2 Security Feature Configuration

2.6.2.1 Prevent IP Spoofing Function Configuration Task Sequence

1. Enable the IP spoofing function.

Command	Explanation
Global Mode	
dosattack-check srcip-equal-dstip enable	Enable the function of checking if the IP source address is the same as the destination address

2.6.2.2 Prevent TCP Unauthorized Label Attack Function Configuration Task Sequence

1. Enable the anti TCP unauthorized label attack function
2. Enable Checking IPv4 fragment function

Command	Explanation
Global Mode	
dosattack-check tcp-flags enable	Enable checking TCP label function
dosattack-check ipv4-first-fragment enable	Enable checking IPv4 fragment. This command has no effect when used separately, but if this function is not enabled, the switch will not drop the IPv4 fragment packet containing unauthorized TCP labels

2.6.2.3 Anti Port Cheat Function Configuration Task Sequence

1. Enable the anti port cheat function

Command	Explanation
Global Mode	

dosattack-check srcport-equal-dstport enable	Enable the prevent-port-cheat function

2.6.2.4 Prevent TCP Fragment Attack Function Configuration Task Sequence

1. Enable the prevent TCP fragment attack function
2. Configure the minimum permitted TCP head length of the packet

Command	Explanation
Global Mode	
dosattack-check tcp-fragment enable	Enable the prevent TCP fragment attack function
dosattack-check tcp-header <*size*>	**dosattack-check tcp-fragment enable** Configure the minimum permitted TCP head length of the packet. This command has no effect when used separately, the user should enable the **dosattack-check tcp-fragment enable**

2.6.2.5 Prevent ICMP Fragment Attack Function Configuration Task Sequence

1. Enable the prevent ICMP fragment attack function
2. Configure the max permitted ICMPv4 net load length
3. Configure the max permitted ICMPv6 net load length

Command	Explanation
Global Mode	
dosattack-check icmp-attacking enable	Enable the prevent ICMP fragment attack function
dosattack-check icmpv4-size <*size*>	Configure the max permitted ICMPv4 net length. This command has not effect when used separately, the user have to enable the **dosattack-check icmp-attacking enable**
dosattack-check icmpv6-size <*size*>	**dosattack-check icmp-attacking enable** Configure the max permitted ICMPv6 net length. This command has not effect when used separately, the user have to enable the **dosattack-check icmp-attacking enable**

2.6.3 Security Feature Commands

2.6.3.1 dosattack-check srcip-equal-dstip enable

Command: [no] dosattack-check srcip-equal-dstip enable

Function: Enable the function by which the switch checks if the source IP address is equal to the destination IP address; the “no” form of this command disables this function.

Parameter: None

Default: Disable the function by which the switch checks if the source IP address is equal to the destination IP address.

Command Mode: Global Mode

Usage Guide: By enabling this function, data packet whose source IP address is equal to its destination address will be dropped

Example: Drop the data packet whose source IP address is equal to its destination address

Switch(Config)# dosattack-check srcip-equal-dstip enable

2.6.3.2 dosattack-check ipv4-first-fragment enable

Command: [no] dosattack-check ipv4-first-fragment enable

Function: Enable the function by which the switch checks the first fragment packet of IPv4; the “no” form of this command disables this function.

Parameter: None

Command Mode: Global Mode

Usage Guide: This command has no effect when used separately. It should be used associating **dosattack-check tcp-flags enable** or **dosattack-check srcport-equal-dstport enable** command.

Example: Drop the IPv4 fragment or non-fragment data packet whose source port is equal to its destination port.

Switch(Config)# dosattack-check ipv4-first-fragment enable

Switch(Config)# dosattack-check srcport-equal-dstport enable

2.6.3.3 dosattack-check tcp-flags enable

Command: [no] dosattack-check tcp-flags enable

Function: Enable the function by which the switch will check the unauthorized TCP label function; the “no” form of this command will disable this function.

Parameter: None

Default: This function disable on the switch by default

Command Mode: Global Mode

Usage Guide: With this function enabled, the switch will be able to drop follow four data packets containing unauthorized TCP label: SYN=1 while source port is smaller than 1024;TCP label positions are all 0 while its serial No. =0;FIN=1,URG=1,PSH=1 and the TCP serial No.=0;SYN=1 and FIN=1. This function can be used associating the "dosattack-check ipv4-first-fragment enable" command

Example: Drop one or more types of above four packet types.

Switch(Config)# dosattack-check tcp-flags enable

2.6.3.4 dosattack-check srcport-equal-dstport enable

Command: dosattack-check srcport-equal-dstport enable

Function: Enable the function by which the switch will check if the source port is equal to the destination port; the "no" form of this command disables this function

Parameter: None

Default: Disable the function by which the switch will check if the source port is equal to the destination port

Command Mode: Global Mode

Usage Guide: With this function enabled, the switch will be able to drop TCP and UDP data packet whose destination port is equal to the source port. This function can be used associating the "dosattack-check ipv4-first-fragment enable" function so to block the IPv4 fragment TCP and UDP data packet whose destination port is equal to the source port

Example: Drop the non-fragment TCP and UDP data packet whose destination port is equal to the source port

Switch(Config)# dosattack-check srcport-equal-dstport enable

2.6.3.5 dosattack-check tcp-fragment enable

Command: [no] dosattack-check tcp-fragment enable

Function: Enable the function by which the switch detects TCP fragment attacks; the "no" form of this command disables this function

Parameter: None

Default: This function is not enabled on the switch by default

Command Mode: Global Mode

Usage Guide: By enabling this function the switch will be protected from the TCP fragment attacks, dropping the data packets whose TCP fragment offset value is 1 or the TCP head is shorter than the specified value. Use "dosattack-check tcp-header" command to specify the length.

Example: Enable the Checking TCP fragment attack function.

Switch(Config)# dosattack-check tcp-fragment enable

2.6.3.6 dosattack-check tcp-header

Command: dosattack-check tcp-header <size>

Function: Configure the minimum TCP head length permitted by the switch

Parameter: <size> is the minimum TCP head length permitted by the switch

Default: The length is 20 by default which is the shortest TCP head

Command Mode: Global Mode

Usage Guide: To use this function the “dosattack-check tcp-fragment enable” function must be enabled

Example: Set the minimum TCP head length permitted by the switch to 20

Switch(Config)# dosattack-check tcp-fragment enable

Switch(Config)# dosattack-check tcp-header 20

2.6.3.7 dosattack-check icmp-attacking enable

Command: [no] dosattack-check icmp-attacking enable

Function: Enable the ICMP fragment attack checking function on the switch; the “no” form of this command disables this function

Parameter: None

Default: Disable the ICMP fragment attack checking function on the switch

Command Mode: Global Mode

Usage Guide: With this function enabled the switch will be protected from the ICMP fragment attacks, dropping the fragment ICMPv4/v6 data packets whose net length is smaller than the specified value

Example: Enable the ICMP fragment attack checking function

Switch(Config)# dosattack-check icmp-attacking enable

2.6.3.8 dosattack-check icmpv4-size

Command: dosattack-check icmpv4-size <size>

Function: Configure the max net length of the ICMPv4 data packet permitted by the switch

Parameter: <size> is the max net length of the ICMPv4 data packet permitted by the switch

Default: The value is 0x200 by default

Command Mode: Global Mode

Usage Guide: To use this function you have to enable “dosattack-check icmp-attacking enable” first

Example: Set the max net length of the ICMPv4 data packet permitted by the switch to 100

Switch(Config)# dosattack-check icmp-attacking enable
Switch(Config)# dosattack-check icmpv4-size 100

2.6.3.9 dosattack-check icmpv6-size

Command:dosattack-check icmpv6-size <size>
Function: Configure the max net length of the ICMPv6 data packet permitted by the switch
Parameter:<size> is the max net length of the ICMPv6 data packet permitted by the switch
Default: The value is 0x200 by default
Command Mode: Global Mode
Usage Guide: To use this function you have to enable “dosattack-check icmp-attacking enable” first
Example: Set the max net length of the ICMPv6 data packet permitted by the switch to 100
Switch(Config)# dosattack-check icmp-attacking enable
Switch(Config)# dosattack-check icmpv6-size 100

2.6.4 Security Feature Example

Scenario:

The User has follows configuration requirements: the switch do not forward data packet whose source IP address is equal to the destination address, and those whose source port is equal to the destination port. Only the ping command with defaulted options is allowed within the IPv4 network, namely the ICMP request packet can not be fragmented and its net length is normally smaller than 100

Configuration procedure:
Switch(Config)# dosattack-check srcip-equal-dstip enable
Switch(Config)# dosattack-check srcport-equal-dstport enable
Switch(Config)# dosattack-check ipv4-first-fragment enable
Switch(Config)# dosattack-check icmp-attacking enable
Switch(Config)# dosattack-check icmpv4-size 100

2.7 Jumbo Configuration

2.7.1 Jumbo Introduction

So far the Jumbo (Jumbo Frame) has not reach a determined standard in the industry (including the format and length of the frame). Normally frames sized within 1519-8996 should be considered Jumbo frame. Networks with Jumbo frames will increase the speed of the whole network by 2% to 5%. Technically the Jumbo is just a lengthened frame sent and received by the switch. However considering the length of Jumbo frames, they will not be sent to CPU. We discarded the Jumbo frames sent to CPU in the packet receiving process.

2.7.2 Jumbo Configuration Task Sequence

1.Configure enable Jumbo function

Command	Explanation
jumbo enable **no jumbo enable**	Enable sending/receiving function of the Jumbo frames Disable the sending/receiving function of the Jumbo frames

2.7.3 Commands for Jumbo

Command：jumbo enable

no jumbo enable

Function：Enable the Jumbo receiving function, expanding the range of the frames received by the switch to 64-8996 bytes. The "**NO jumbo ENABLE**" command restores to the normal frame range of 64--1518

Parameter：None

Default：Jumbo function not enabled by default

Command Mode：Global Mode

Example：

Switch(Config)#jumbo enable

Switch(Config)#no jumbo enable

2.8 sFlow Configuration

2.8.1 sFlow Introduction

The sFlow (RFC 3176) is a protocol based on standard network export and used on

monitoring the network traffic information developed by the InMon Company.The monitored switch or router sends date to the client analyzer through its main operations such as sampling and statistic, then the analyzer will analyze acconrding to the user requirements so to monitor the network.

A sFlow monitor system includes: sFlow proxy, central data collector and sFlow analyzer. The sFlow proxy collects data from the switch using sampling technology. The sFlow collector is for formatting the sample data statistic which is to be forwarded to the sFlow analyzer which will analyze the sample data and perform corresponding measure according to the result. Our switch here acts as the proxy and central data collector in the sFlow system.

We have achieved data sampling and statistic targeting physical port.

Our data sample includes the IPv4 and IPv6 packets. Extensions of other types are not supported so far. As for non IPv4 and IPv6 packet, the unify HEADER mode will be adopted following the requirements in RFC3176, copying the head information of the packet based on analyzing the type of its protocol.

The latest SFLOW protocol presented by Inmon company is the version 5. Since it is the version 4 which is realized in the RFC3176, version conflict might exist in some case such as the structure and the packet format. This is because the version 5 has not become the official protocol, so, in order to be compatible with current applications, we will continue to follow the RFC3176.

2.8.2 sFlow Configuration Task

1. Configure sFlow Collector address

Command	Explanation
Global mode and interface mode	
sflow destination <*collector-address*> [<*collector-port*>] **no sflow destination**	Configure the IP address and port number of the host in which the sFlow analysis software is installed. As for the ports, if IP address is configured on the port, the port configuration will be applied, or else will be applied the global configuration. The "**no sflow destination**" command restores to the default port value and deletes the IP address.

2. Configure the sFlow proxy address

Command	Explanation
Global Mode	

sflow agent-address <*collector-address*> **no sflow agent-address**	Configure the source IP address applied by the sFlow proxy; the “no” form of the command deletes this address.

3. Configure the sFlow proxy priority

Command	Explanation
Global Mode	
sflow priority <*priority-vlaue*> **no sflow priority**	Configure the priority when sFlow receives packet from the hardware; the “**no sflow priority**” command restores to the default

4. Configure the packet head length copied by sFlow

Command	Explanation
Global Mode	
sflow header-len <*length-vlaue*> **no sflow header-len**	Configure the length of the packet data head copied in the sFlow data sampling; the “no” form of this command restores to the default value.

5. Configure the max data head length of the sFlow packet

Command	Explanation
Interface Mode	
sflow data-len <*length-vlaue*> **no sflow data-len**	Configure the max length of the data packet in sFlow; the “no” form of this command restores to the default.

6. Configure the sampling rate value.

Command	Explanation
Interface Mode	
sflow rate { input <*input-rate*> | output **<*output-rate* >}** **no sflow rate [input | output]**	Configure the sampling rate when sFlow performing hardware sampling. The “no” command deletes the rate value.

7. Configure the Sflow statistic sampling interval

Command	Explanation
Interface Mode	
sflow counter-interval <*interval-vlaue*> **no sflow counter-interval**	Configure the max interval when sFlow performing statistic sampling. The “no” form of this command deletes

2.8.3 Commands For sFlow

2.8.3.1 sflow destination

Command: sflow destination <*collector-address*> [<*collector-port*>]

no sflow destination

Function: Configure the IP address and port number of the host on which the sFlow analysis software is installed. If the port has been configured with IP address, the port configuration will be applied, or else the global configuration will be applied. The “no” form of this command restores the port to default and deletes the IP address.

Parameter:<*collector-address*> is the IP address of the analyzer,shown in dotted decimal notation.**<*collector-port*>** is the destination port of the sent sFlow packets

Command Mode: Global Mode and Interface Mode

Default: The destination port of the sFlow packet is defaulted at 6343, and the analyzer has no default address.

Usage Guide: If the analyzer address is configured at interface mode, this IP address and port configured at interface mode will be applied when sending the sample packet. Or else the address and port configured at global mode will be applied. The analyzer address should be configured to let the sFlow sample proxy work properly.

Example: Configure the analyzer address and port at global mode.

switch #config)#sflow destination 192.168.1.200 1025

2.8.3.2 sflow agent-address

Command: sflow agent-address <*agent-address*>

no sflow agent-address

Function: Configure the sFlow sample proxy address. The “no” form of this command deletes the proxy address

Parameter: <*agent-address* > is the sample proxy IP address which is shown in dotted decimal notation.

Command Mode: Global Mode

Default: None default value

Usage Guide: The proxy address is used to mark the sample proxy which is similar to OSPF or the Router ID in the BGP. However it is not necessary to make the sFlow sample proxy work properly.

Example: Sample the proxy address at global mode.

switch #config)#sflow agent-address 192.168.1.200

2.8.3.3 sflow priority

Command: sflow priority <*priority-value*>

no sflow priority

Function: Configure the priority when sFlow receives packet from the hardware. The "no" form of the command restores to the default

Parameter: <*priority-value*> is the priority value with a valid range of 0-3.

Command Mode: Global mode

Default: The default value is 0

Usage Guide: When sample packet is sent to the CPU, it is recommended not to assign high priority for the packet so that regular receiving and sending of other protocol packet will not be interfered. The higher the priority value is set, the higher its priority will be.

Example: Configure the priority when sFlow receives packet from the hardware at global mode,

switch #config)#sflow priority 1

2.8.3.4 sflow header-len

Command: sflow header-len <*length-value*>

no sflow header-len

Function: Configure the length of the head data packet copied in the sFlow data sampling. The "no" form of this command restores to the default value

Parameter: <*length-value*> is the value of the length with a valid range of 32-256.

Command Mode: Interface Mode

Default: 128 by default

Usage Guide: If the packet sample can not be identified whether it is IPv4 or IPv6 when sent to the CPU, certain length of the head of the group has to be copied to the sFlow packet and sent out. The length of the copied content is configured by this command

Example: Configure the length of the packet data head copied in the sFlow data sampling to 50.

Switch#(Config-If-Ethernet3/2)#sflow header-len 50

2.8.3.5 sflow data-len

Command: sflow data-len <*length-value*>

no sflow data-len

Function: Configure the max length of the sFlow packet data; the "**no sflow data-len**" command restores to the default value

Parameter: <*length-value*> is the value of the length with a valide range of 500-1470

Command Mode: Interface mode

Default: The value is 1400 by default

Usage Guide: When combining several samples to a sFlow group to be sent, the length of the group excluding the mac head and IP head parts should not exceed the configured value.

Example: Configure the max length of the sFlow packet data to 1000
switch #Config-If-Ethernet3/2)#sflow data-len 1000

2.8.3.6 sflow counter-interval

Command: sflow counter-interval <*interval-value*>
no sflow counter-interval
Function: Configure the max interval of the sFlow statistic sampling; the “no” form of this command deletes the statistic sampling interval value.
Parameter:<*interval-value*> is the value of the interval with a valid range of 20~120 and shown in second.
Command Mode: Interface Mode
Default: No default value
Usage Guide: If no statistic sampling interval is configured, there will not be any statistic sampling on the interface.
Example: Set the statistic sampling interval on the interface e3/1 to 20 seconds.
Switch#(Config-If-Ethernet3/2)#sflow counter-interval 20

2.8.3.7 sflow rate

Command: sflow rate { input <*input-rate*> | output **<*output-rate* >}**
no sflow rate [input | output]
Function: Configure the sample rate of the sFlow hardware sampling. The “no” form of this command deletes the sampling rate value.
Parameter:< *input-rate* > is the rate of ingress group sampling,the valid range is 1000~16383500
< *output-rate* > is the rate of engress group sampling, the valid range is 1000~16383500
Command Mode: Interface Mode
Default: No default value
Usage Guide: The traffic sampling will not be performed if the sampling rate is not configured on the port. And if the ingress group sampling rate is set to 10000, this indicates there will be one group be sampled every 10000 ingress groups.
Example: Configure the ingress sample rate on port e3/1 to 10000 and the egress sample rate to 20000
Switch#(Config-If-Ethernet3/2)#sflow rate input 10000
switch #Config-If-Ethernet3/2)#sflow rate output 20000

2.8.3.8 show sflow

Command: show sflow

Function: Display the sFlow configuration state

Parameter: None

Command Mode: All Modes

Usage Guide: This command is used to acknowledge the operation state of sFlow

switch #show sflow

Sflow version 1.2

Agent address is 172.16.1.100

Collector address have not configured

Collector port is 6343

Sampler priority is 2

Sflow DataSource: type 2, index 194(Ethernet3/2)

Collector address is 192.168.1.200

Collector port is 6343

Counter interval is 0

Sample rate is input 0, output 0

Sample packet max len is 1400

Sample header max len is 50

Sample version is 4

Displayed Information	Explanation
Sflow version 1.2	Indicates the sFlow version is 1.2
Agent address is 172.16.1.100	Address of the sFlow sample proxy is 172.16.1.100
Collector address have not configured	the sFlow global analyzer address is not configured
Collector port is 6343	the sFlow global destination port is the defaulted 6343
Sampler priority is 2	The priority of sFlow when receiving packets from the hardware is 2.
Sflow DataSource: type 2, index 194(Ethernet3/2)	One sample proxy data source of the sFlow is the interface e3/1 and its type is 2 (Ethernet), the interface index is 194.
Collector address is 192.168.1.200	The analyzer address of the sampling address of the E3/1 interface is 192.168.1.200
Collector port is 6343	Default value of the port on E3/1 interface sampling proxy is 6343.
Counter interval is 20	The statistic sampling interval on e3/1 interface is 20 seconds
Sample rate is input 10000, output 0	The ingress traffic rate of e3/1 interface sampling proxy is 10000 and no egress traffic sampling will be performed

Sample packet max len is 1400	The length of the sFlow group data sent by the e3/1 interface should not exceed 1400 bytes.
Sample header max len is 50	The length of the packet data head copied in the data sampling of the e3/1 interface sampling proxy is 50
Sample version is 4	The datagram version of the sFlow group sent by the E3/1 interface sampling proxy is 4.

2.8.4 sFlow Examples

Fig 2-5 sFlow configuration topology

As shown in the figure, sFlow sampling is enabled on the port 3/1 and 3/2 of the switch. Assume the sFlow analysis software is installed on the PC with the address of 192.168.1.200. The address of the layer 3 interface on the Switch connected with PC is 192.168.1.100. A loopback interface with the address of 10.1.144.2 is configured on the Switch. sFlow configuration is as follows:

Configuration procedure is as follows:

Switch#config
Switch (config)#sflow ageng-address 10.1.144.2
Switch (config)#sflow destination 192.168.1.200
Switch (config)#sflow priority 1
Switch (config)# (config)#in e3/1
Switch (Config-If-Ethernet3/1)#sflow rate input 10000
Switch (Config-If-Ethernet3/1)#sflow rate output 10000
Switch (Config-If-Ethernet3/1)#sflow rate counter-interval 20
Switch (Config-If-Ethernet3/1)#exit
Switch (config)# (config)#in e3/2
Switch (Config-If-Ethernet3/2)#sflow rate input 2000
Switch (Config-If-Ethernet3/2)#sflow rate output 20000
Switch (Config-If-Ethernet3/2)#sflow rate counter-interval 40

2.8.5 sFlow Troubleshooting

In configuring and using sFlow, the sFlow server may fail to run properly due to physical connection failure, wrong configuration, etc. The user should ensure the following:

- ✧ Ensure the physical connection is correct
- ✧ Guarantee the address of the sFlow analyzer configured under global or interface mode is accessible.
- ✧ If traffic sampling is required, the sampling rate of the interface must be configured
- ✧ If statistic sampling is required, the statistic sampling interval of the interface must be configured

If the examination remains unsolved, please contact with the technical service center of our company.

2.9 TACACS+ Configuration

2.9.1 TACACS+ Introduction

TACACS+ terminal access controller access control protocol is a protocol similar to the radius protocol for control the terminal access to the network. Three independent functions of Authentication, Authorization, Accounting are also available in this protocol. Compared with RADIUS, the transmission layer of TACACS+ protocol is adopted with TCP protocol, further with the packet head (except for standard packet head) encryption, this protocol is of a more reliable transmission and encryption characteristics, and is more adapted to security control.

According to the characteristics of the TACACS+ (Version 1.78), we provide TACACS+ authentication function on the switch, when the user logs, such as telnet, the authentication of user name and password can be carried out with TACACS+.

2.9.2 TACACS+ Configurations

1) Configure the TACACS+ authentication key
2) Configure the TACACS+ server
3) Configure the TACACS+ authentication timeout time

1) Configure the TACACS+ authentication key

Command	Explanation
Global Mode	

tacacs-server key <*string*> **no tacacs-server key**	Configure the TACACS+ server key; the "**no tacacs-server key**" command deletes the key

2) Configure TACACS+ server

Command	Explanation
Global Mode	
tacacs-server authentication host <*IPaddress*> [[port {<*portNum*>}] [primary]] **no tacacs-server authentication host <*IPaddress*>**	Configure the IP address and listen port number of the TACACS+ authentication server; the "no" form of this command deletes the TACACS+ authentication server

3) Configure the TACACS+ authentication timeout time

Command	Explanation
Global Mode	
tacacs-server timeout <*seconds*> **no tacacs-server timeout**	Configure the authentication timeout for the TACACS+ server, the "**no tacacs-server timeout**" command restores the default configuration

2.9.3 Commands for TACACS+

2.9.3.1 tacacs-server authentication host

Command:tacacs-server authentication host <*ip-address*> [port <*port-number*>] [primary]

no tacacs-server authentication host <*ip-address*>

Function: Configure the IP address and listening port number of the TACACS+ server; the "no" form of this command deletes TACACS+ authentication server.

Parameter: <*ip-address*> is the IP of the server;**<*port-number*>** is the listening port number of the server,the valid range is 0~65535,amongst 0 indicates it will not be an authentication server;**primary** indicates it's a primary server.

Command Mode: Global Mode

Default: No TACACS+ authentication configured on the system by default

Usage Guide: This command is for specifying the IP address and port number of the TACACS+ server used on authenticating with the switch. The parameter port is for define an authentication port number which must be in accordance with the authentication port number of specified TACACS+ server which is 49 by default. This command can configure several TACACS+ servers communicate with the switch. The configuration

sequence will be used as authentication server sequence, and in case **primary** is configured on one TACACS+ server, the server will be the primary server.

Example: Configure the TACACS+ authentication server address to 192.168.1.2

Switch(Config)#tacacs-server authentication host 192.168.1.2

2.9.3.2 tacacs-server key

Command: tacacs-server key <*string*>

no tacacs-server key

Function: Configure the key of TACACS+ authentication server; the "**no tacacs-server key**" command deletes the TACACS+ server key.

Parameter: <*string*> is the character string of the TACACS+ server key, containing maximum 16 characters.

Command Mode: Global Mode

Usage Guide: The key is used on encrypted packet communication between the switch and the TACACS+ server. The configured key must be in accordance with the one on the TACACS+ server or else no correct TACACS+ authentication will be performed. It is recommended to configure the authentication server key to ensure the data security.

Example: Configure test as the TACACS+ server authentication key.

Switch(Config)# tacacs-server key test

2.9.3.3 tacacs-server timeout

Command: tacacs-server timeout <*seconds*>

no tacacs-server timeout

Function: Configure a TACACS+ server authentication timeout timer; the "**no tacacs-server timeout**" command restores the default configuration

Parameter: <*seconds*> is the value of TACACS+ authentication timeout timer,shown in seconds and the valid range is 1~60.

Command Mode: Global Mode

Default: 3 seconds by default

Usage Guide: The command specifies the period the switch wait for the authentication through TACACS+ server. When connected to the TACACS+, and after sent the authentication query data packet to the TACACS+ server, the switch waits for the response. If no replay is received during specified period, the authentication is considered failed.

Example: Configure the timeout timer of the tacacs+ server to 30 seconds

Switch(Config)# tacacs-server timeout 30

2.9.3.4 debug tacacs-server

Command: debug tacacs=server

no debug tacacs-server

Function: Open the debug message of the TACACS+; the "**no debug tacacs-server**" command closes the TACACS+ debugging messages

Command Mode: Admin Mode

Parameter: None

Usage Guide: Enable the TACACS+ debugging messages to check the negotiation process of the TACACS+ protocol which can help detecting the failure.

Example: Enable the debugging messages of the TACACS+ protocol

Switch#debug tacacs-server

2.9.4 Typical TACACS+ Scenarios

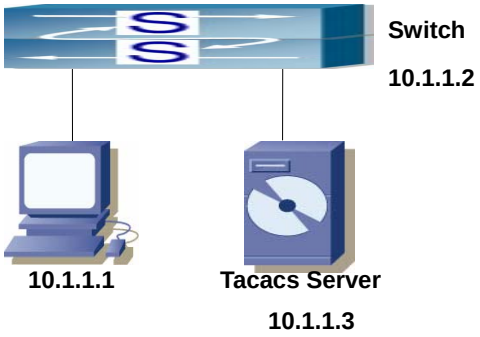


Fig 2-6 TACACS Configuration

A computer connects to a switch, of which the IP address is 10.1.1.2 and connected with a TACACS+ authentication server; IP address of the server is 10.1.1.3 and the authentication port is defaulted at 49, telnet log on authentication of the switch

Switch(Config)#interface vlan 1

Switch(Config-if-vlan1)#ip address 10.1.1.2 255.255.255.0

Switch(Config-if-vlan1)#exit

Switch(Config)#tacacs-server authentication host 10.1.1.3

Switch(Config)#tacacs-server key test

Switch(Config)#authentication login tacacs local

2.9.5 TACACS+ Troubleshooting

In configuring and using TACACS+, the TACACS+ may fail to authentication due to reasons such as physical connection failure or wrong configurations. The user should ensure the following:

✧ First good condition of the TACACS+ server physical connection

- ✧ Second all interface and link protocols are in the UP state (use “show interface” command)
- ✧ Then ensure the TACACS+ key configured on the switch is in accordance with the one configured on TACACS+ server
- ✧ Finally ensure to connect to the correct TACACS+ server

If the TACACS+ authentication problem remain unsolved, please use debug tacacs and other debugging command and copy the DEBUG message within 3 minutes, send the recorded message to the technical server center of our company.

2.10 Web Management

2.10.1 Switch Basic Configuration

Users should click “Switch basic configuration” table and configure the switch’s clock, prompts of command-line interface, timeout of quitting Admin mode, etc.

2.10.1.1 Basic Configuration

Users should click “Switch basic configuration” and “BasicConfig” to configure the switch’s clock, prompts of command-line interface and the mapping address relationship with the host.

Basic clock configuration -configure “date and clock” of the system.

Users should configure HH:MM:SS as 23:0:0 and YY.MM.DD as 2002/08/01. The complete configuration by clicking on the “Apply” button.

- Basic host configuration -configures the mapping relationship between the switch and the IP address.

Example: configure the Hostname as” test” and then click on the “Apply” button. This configuration will be applied to the switch.

2.10.1.2 Configure Exec Timeout

Example of configuring the timeout as 6 minutes and then click on the “Apply” button to complete the timeout of quitting Admin mode.

2.10.2 SNMP Configuration

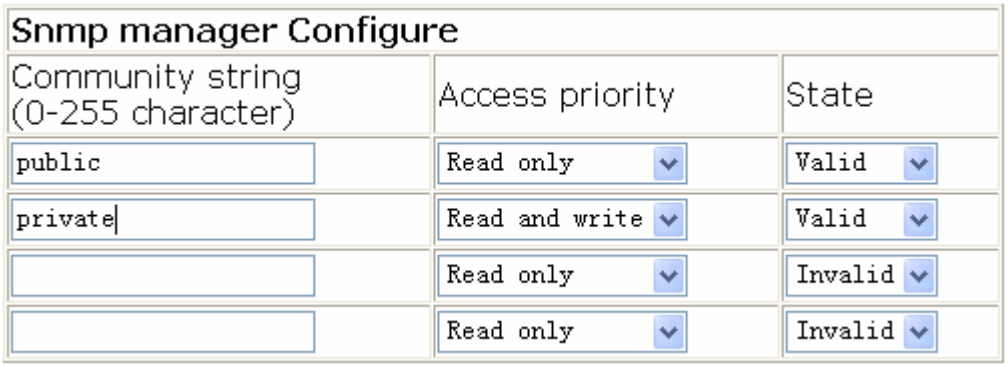
Users should click “Switch basic configuration” and “SNMP configuration” to configure the SNMP relating functions.

2.10.2.1 SNMP Manager Configuration

Users should click “Switch basic configuration”, “SNMP configuration”, and “SNMP manager configuration” to configure the community string of the switch.

- Community string (0-255 characters) -for configuration of the community string.
- Access priority -specifies access rights to MIB, including “Read only” and “Read and write.”
- State -”Valid” -to configure; “Invalid” -to remove.

Users should configure Community string as “public”, choose Access priority as “Read only” mode, and choose State as “Valid” or configure Community string as private, choose Access priority as “Read and write” mode, and choose State as “Valid”. The command will be applied to the switch by clicking on the “Apply” button.



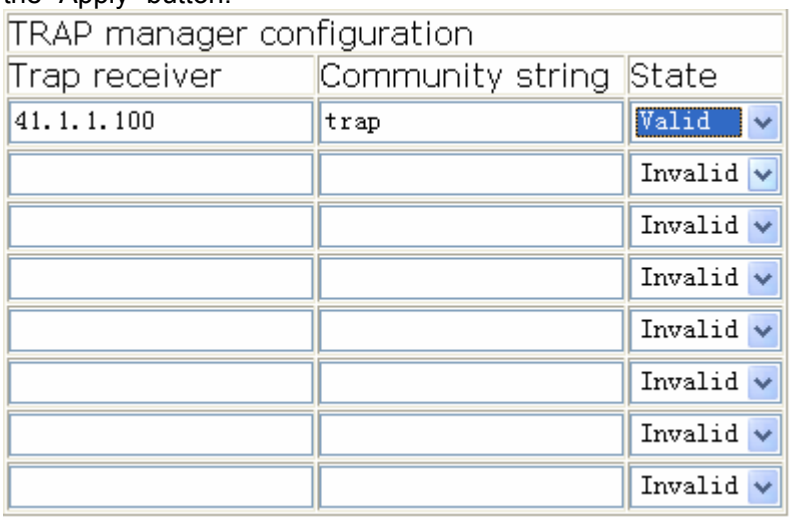
2.10.2.2 Trap Manager Configuration

Users should click “Switch basic configuration”, “SNMP configuration”, and “TRAP manager configuration” to configure the IP address of the management station which will receive SNMP Trap messages and Trap community strings.

- Trap receiver -the IP address of NMS management station that will receive Trap messages.
- Community string (0-255 character) -the community string used to send Trap messages.

- State -"Valid" -to configure; "Invalid" -to remove

Example: configure the Trap receiver as "41.1.1.100" and configure the community string as "trap" and State as "Valid." The command will be applied to the switch by clicking on the "Apply" button.

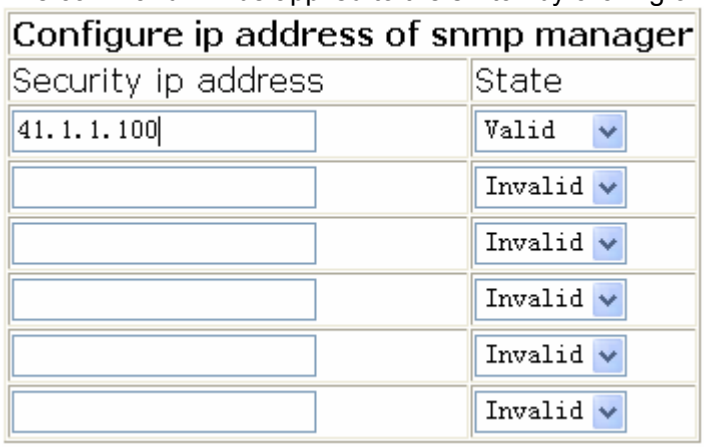


2.10.2.3 Configure IP address of SNMP manager

User should click "Switch basic configuration", "SNMP configuration", and "Configure ip address of snmp manager" to configure the security IP address which will be allowed to access to the NMS management station of the switch. 5.4.4.2.6.

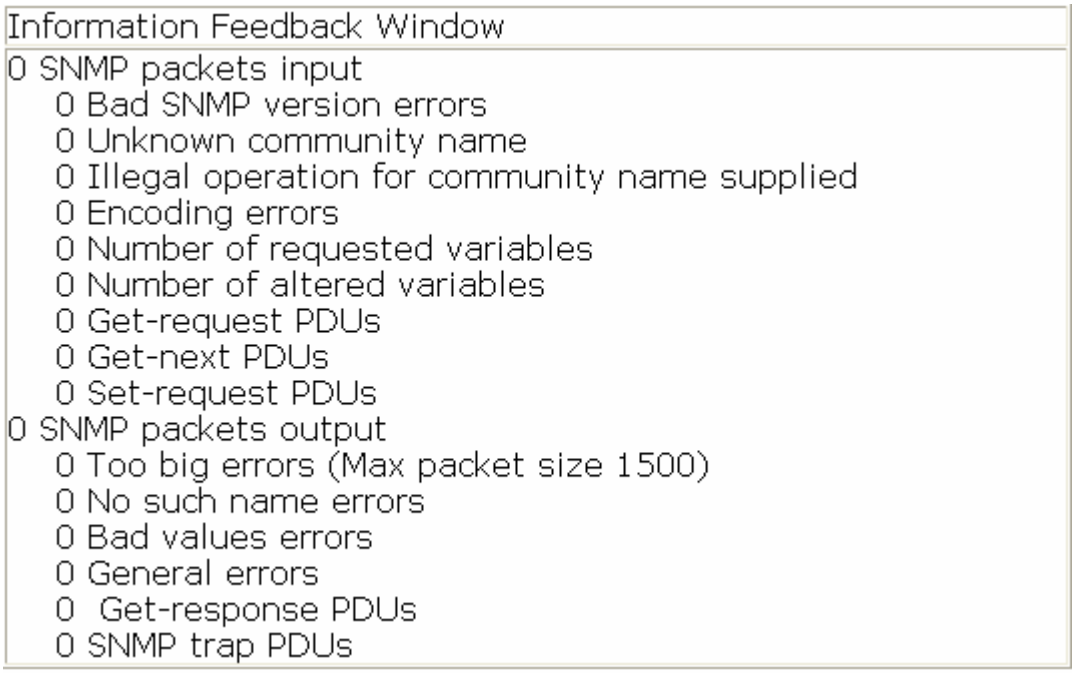
- Security ip address -Security IP address of NMS
- State –"Valid" -to configure; "Invalid" -to remove

Example: configure the security IP address as "41.1.1.100", and choose State as "Valid". The command will be applied to the switch by clicking on the "Apply" button.



2.10.2.4 SNMP statistics

When users click "Switch basic configuration", "SNMP configuration" and "SNMP statistics", a variety of counter information will appear.

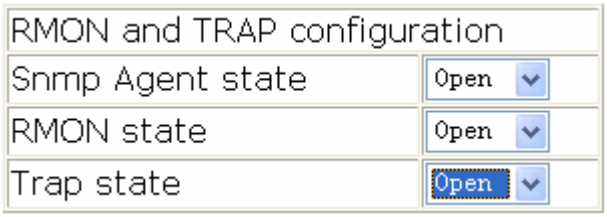


2.10.2.5 RMON and trap configuration

Users should click “Switch basic configuration”, “SNMP configuration” and “RMON and TRAP configuration” to configure the RMON function of the switch.

- Snmp Agent state –open/close the switch to be SNMP agent server function.
- RMON state -open/close RMON function of the switch.
- Trap state -allows device to send Trap messages

Example: choose Snmp Agent state as “Open”, choose RMON state as “Open”, and choose Trap state as “Open”. Then click on the “Apply” button.



2.10.3 Switch upgrade

Users should click “Switch basic configuration” and “Switch update” to configure the upgrade Node Tree Diagram. Two categories are explained below:

- TFTP Upgrade, including
  - ✓ TFTP client service -to configure TFTP client
  - ✓ TFTP server service -to configure TFTP server
- FTP Upgrade, including
  - ✓ FTP client service -to configure FTP client

✓ FTP server service -to configure FTP server

2.10.3.1 TFTP client configuration

Users should click “Switch basic configuration” and “TFTP client service” to enter into the configuration page.

Words and phrases are explained in the following:

Server IP address-IP address of the server.

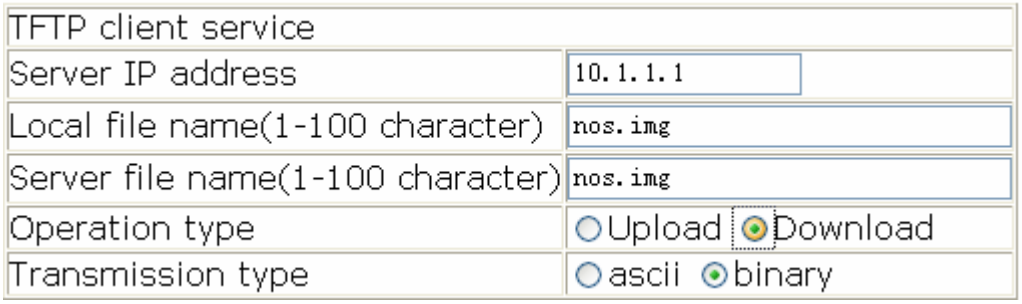
Local file name-the local file name

Server file name-the file name of the server

Operation type-”Upload” means to upload files; “Download” means to download files

Transmission type-”ascii” means to transit files by using ASCII standard. “binary” means the files are transmitted in the binary standard

Example: the Figure below shows how to get the system file from TFTP Server 10.1.1.1, which has server file name is “nos.img” and local file name “nos.img.” Click “Apply” to finish.



2.10.3.2 TFTP server configuration

Users should click “Switch basic configuration” and “TFTP server service” to enter into the configuration page.

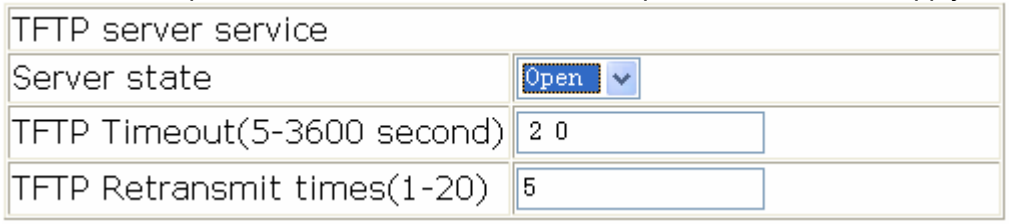
Words and phrases are explained in the following:

Server state-status of the server. (“Open” or “Close”)

TFTP Timeout-the timeout.

TFTP Retransmit times-times of retransmission.

Users should open the TFTP server, and choose “Open” and then click “Apply.”



2.10.3.3 FTP client configuration

Users should click “Switch basic configuration” and “FTP client service” to enter into this

configuration page.

Words and phrases are explained in the following:

Server IP address-IP address of the server

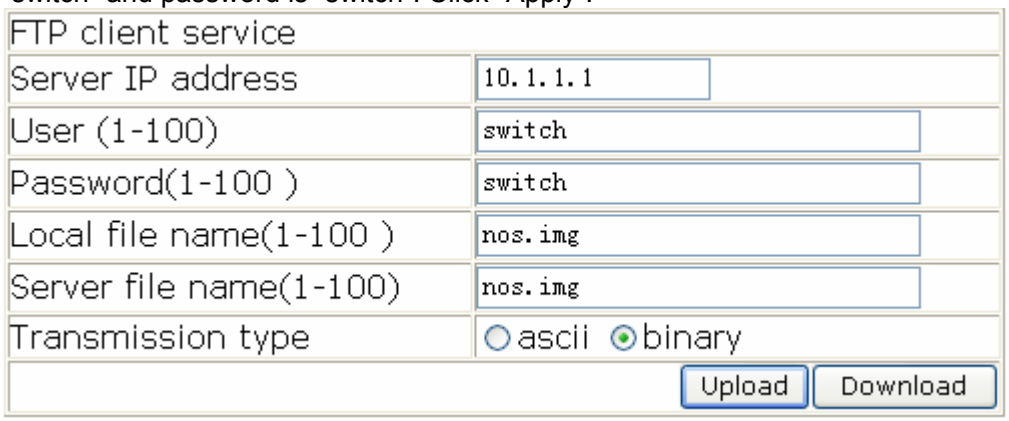
User name-the name of the user

Password-the specific password

Operation type-"Upload" means to upload files; "Download" means to download files

Transmission type-"ascii" means to transit files by using ASCII standard. "binary" means the files are transmitted in binary standard.

Users should follow the Figure below to get the system file from the FTP Server 10.1.1.1, with server file name is "nos.img" and local file name "nos.img." The ftp username is "switch" and password is "switch". Click "Apply".



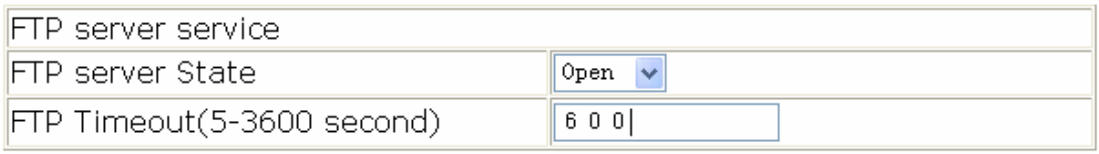
2.10.3.4 FTP server configuration

Users should click "Switch basic configuration" and "FTP server service" to enter into the configuration page and make configuration nodes, which include "server configuration" and "user configuration."

Words and phrases of "user configuration" are explained in the following:

- FTP Server state-status of the server. ("Open" or "Close".)
- FTP Timeout-the timeout.
- User name-the name of the user.
- Password-the specific password.
- State-display the status of the password. "Plain text" means proclaimed display and "encrypted" means "encrypted" display.
- Remove user-to remove a user.
- Add user-to add a user.

Example: open the TFTP server, input the username "switch" and password "switch", and then click "Apply."



2.10.4 Commands for Monitor And Debug

Users should click “Switch basic configuration” and “Basic configuration debug” to enter into the configuration page and make configuration nodes, which include the following segments:

- Debug command-a debugging command.
- Show calendar-to display the current time.
- Dir-to display FLASH files.
- Show history-to display the latest inputted commands.
- Show running-config-to display the current status of parameters configuration.
- Show switch port interface-to display properties of VLAN ports.
- Show tcp-to display the current TCP connection with the switch.
- Show udp-to display the current UDP connection with the switch.
- Show telnet login-to display the Telnet client messages connected through Telnet with the switch.
- Show telnet user-to display all Telnet client messages with authenticated switch access through Telnet.
- Show version to display the number/version of the switch.

2.10.4.1 Debug command

User should click “Switch basic configuration”, “Basic configuration debug”, and “Debug command” to enter into the configuration page and make configuration nodes, which include “ping” and “traceroute” segments.

Words and phrases of “Ping” segment are explained in the following:

IP address-the destination IP address

Hostname-the name of the host Words and phrases of “IP Traceroute” segment are explained in the following:

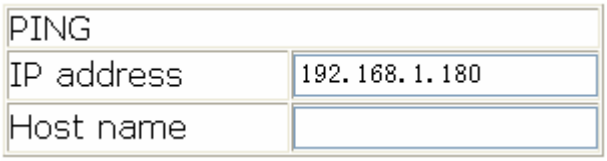
IP address-the destination IP address

Hostname-the name of the host

Hops-the maximum passing hops

Timeout- the timeout of data packets

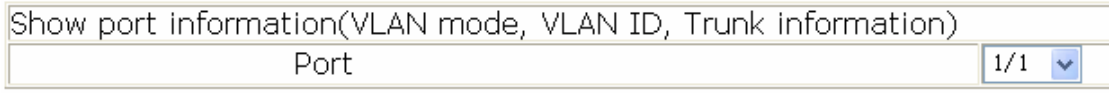
Example: “ping” 192.168.1.180 and then click “Apply.”



2.10.4.2 Show vlan port property

Users should click “Switch basic configuration”, “Basic configuration debug” and “show switchport interface” to enter into the configuration page and make configuration nodes. “Port” means the port table.

Example: User finds a VLAN port’s properties by choosing port1/1 and click “Apply.”

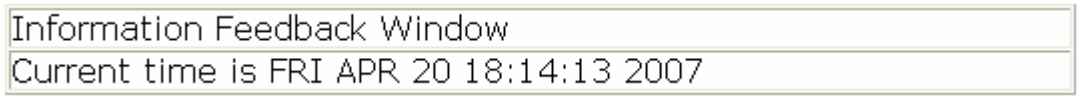


2.10.4.3 Others

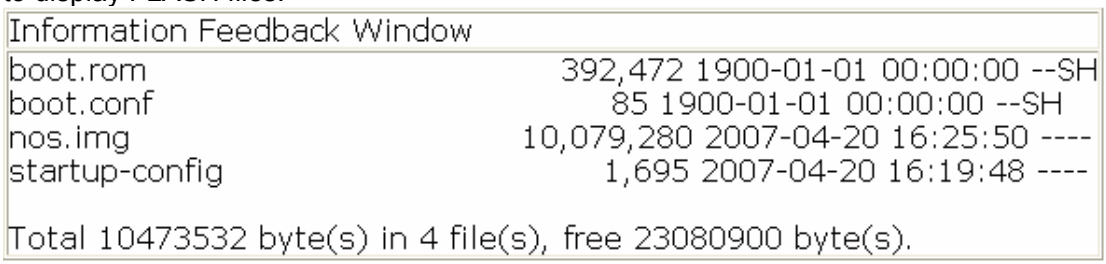
Other parts are easier to configure. Users just click a configuration node and the relating messages will appear.

Example:

to display the clock:



to display FLASH files:



2.10.5 Switch Maintenance

On the left directory of the root page, users should click “Switch maintenance” to configure maintenance nodes through web interface.

2.10.5.1 Exit current web configuration

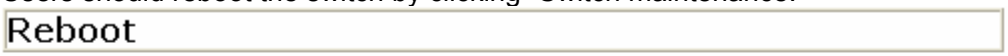
Users should quit the web-login by clicking “Switch maintenance” and “Exit current web configuration.”

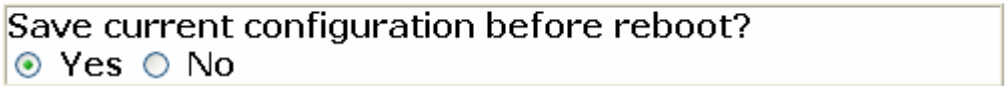
2.10.5.2 Save current running-config

Users should save the current running-config by clicking “Switch maintenance”, “Save current running-config” and “Apply”.

2.10.5.3 Reboot

Users should reboot the switch by clicking “Switch maintenance.”





2.10.5.4 Reboot with the default configuration

Users should clear all current configurations and reboot the switch again by clicking “Switch maintenance” and “Reboot with the default configuration.”

2.10.6 Telnet server configuration

On the left directory of the root page, users may click “Telnet server configuration” and configure the Telnet server configuration nodes through web interface.

2.10.7 Telnet server user configuration

Users should click “Telnet server configuration” and “Telnet server user configuration” to configure Telnet service start-up and users information. Words and phrases are explained in the following:

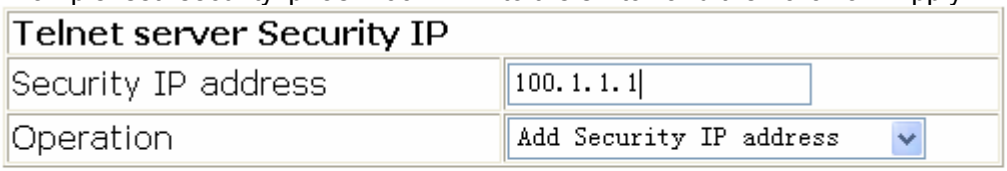
- Telnet server State-to choose from the drop-down list. (“Open” and “Close” service)
  - User name-a specific name of the Telnet user
  - Password-to configure a specific password
  - Encrypted text-to configure whether the password is encrypted when displaying configuration information.
  - Operation-includes “Remove user” and “Add user”

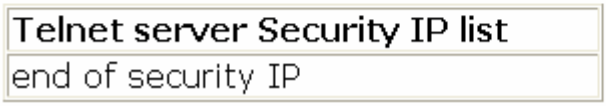
Example: set the Telnet user name as “switch” and password as “switch” and then click on the “Apply” button.

2.10.8 Telnet security IP

- Users should click “Telnet server configuration” and “Telnet security IP” to configure the security IP address of an allowed Telnet client for when the switch functions as the Telnet server. Words and phrases are explained in the following:
- Security IP address-a specific security IP address
- Operation-to choose from the drop-down list. (“Add Security IP address” and “Remove Security IP address”)

Example: set “security ip” as “100.1.1.1” to the switch and then click on “Apply”.





Chapter 3 Port Configuration

3.1 Introduction to Port

ES4626/ES4650 Switch comes with 8 Gigabit Combo ports , 16 SFP Gigabit fiber ports and （for ES4650） 2 SFP 10G fiber ports. The Combo ports can be configured to as either 1000GX-TX ports or Gigabit fiber ports.

If the user needs to configure some network ports, he/she can use the "**interface ethernet <*interface-list*>**" command to enter the appropriate Ethernet port configuration mode, where ***<interface-list>*** stands for one or more ports. If ***<interface-list>*** contains multiple ports, special characters such as ";" or "-" can be used to separate ports, ";" is used for discrete port numbers and "-" is used for consecutive port numbers. Suppose an operation should be performed on ports 2, 3, 4, 5, 8, 9, 10, the command would look like: **interface ethernet 1/2-5;1/8-10.** Port speed, duplex mode and traffic control can be configured under Ethernet Port Mode causing the performance of the corresponding network ports to change accordingly.

3.2 Port Configuration

3.2.1 Network Port Configuration

3.2.1.1 Network Port Configuration Task List

1. Enter the network port configuration mode
2. Configure the properties for the network ports
   （1） Configure combo mode for combo ports
   （2） Enable/Disable ports
   （3） Configure port names
   （4） Configure port cable types
   （5） Configure port speed and duplex mode
   （6） Configure bandwidth control
   （7） Configure traffic control
   （8） Enable/Disable port loopback function

（9） Configure broadcast storm control function for the switch

1. Enter the Ethernet port configuration mode

Command	Explanation
Interface Mode	
interface ethernet <*interface-list*>	Enters the network port configuration mode.

2. Configure the properties for the Ethernet ports

Command	Explanation
Interface Mode	
combo-forced-mode { copper-forced | copper-preferred-auto | sfp-forced | sfp-preferred-auto } **no combo-forced-mode**	Sets the combo port mode (combo ports only); the "**no combo-forced-mode**" command restores the default combo mode for combo ports, i.e., fiber ports first.
shutdown **no shutdown**	Enables/Disables specified ports
description <*string*> **no description**	Names or cancels the name of specified ports
mdi { auto | across | normal } **no mdi**	Sets the cable type for the specified port
speed-duplex {auto | force10-half | force10-full | force100-half | force100-full | { {force1g-half | force1g-full} [nonegotiate [master | slave]] } }	Sets port speed and duplex mode of 100/1000Base-TX ports. The "no" format of this command restores the default setting, i.e., negotiates speed and duplex mode automatically.
[no]negotiation	Enables/Disables the auto-negotiation function of 1000Base-T ports.
rate-limit<*bandwidth*> {input|output} **no rate-limit {input|output}**	Sets or cancels the bandwidth used for incoming/outgoing traffic for specified ports
flow control **no flow control**	Enables/Disables traffic control function for specified ports
loopback **no loopback**	Enables/Disables loopback test function for specified ports

rate-suppression {dlf | broadcast | multicast} <packets>	Enables the storm control function for broadcasts, multicasts and unicasts with unknown destinations (short for broadcast), and sets the allowed broadcast packet number; the “no” format of this command disables the broadcast storm control function.

3.2.1.2 Commands for Network Port Configuration

3.2.1.2.1 combo-forced-mode

Command:combo-forced-mode {copper-forced | copper-preferred-auto | sfp-forced | sfp-preferred-auto }

no combo-forced-mode

Function: Sets to combo port mode (combo ports only); the “**no combo-forced-mode**” command restores to default combo mode for combo ports, i.e., fiber ports first.

Parameters: copper-forced forces use of copper cable port; **copper-preferred-auto** for copper cable port first; **sfp-forced** forces use of fiber cable port; **sfp-preferred-auto** for fiber cable port first.

Command mode: Interface Mode

Default: The default setting for combo mode of combo ports is fiber cable port first.

Usage Guide: The combo mode of combo ports and the port connection condition determines the active port of the combo ports. A combo port consists of one fiber port and a copper cable port. It should be noted that the speed-duplex command applies to the copper cable port while the negotiation command applies to the fiber cable port, they should not conflict. For combo ports, only one, a fiber cable port or a copper cable port, can be active at a time, and only this port can send and receive data normally.

For the determination of the active port in a combo port, see the table below. The headline row in the table indicates the combo mode of the combo port, while the first column indicates the connection conditions of the combo port, in which “connected” refers to a good connection of fiber cable port or copper cable port to the other devices.

	Copper forced	**Copper preferred**	**SFP forced**	**SFP preferred**
Fiber connected, copper not connected	Copper cable port	Fiber cable port	Fiber cable port	Fiber cable port
Copper connected, fiber not connected	Copper cable port	Copper cable port	Fiber cable port	Copper cable port

Both fiber and copper are connected	Copper cable port	Copper cable port	Fiber cable port	Fiber cable port
Neither fiber nor copper are connected	Copper cable port	Fiber cable port	Fiber cable port	Fiber cable port

Note:

- ☞ Combo port is a conception involving the physical layer and the LLC sublayer of the datalink layer. The status of a combo port will not affect any operation in the MAC sublayer of the datalink layer and upper layers. If the bandwidth limit for a combo port is 1Mbps, then this 1Mbps applies to the active port of this combo port, regardless of the port type being copper or fiber.
- ☞ If a combo port connects to another combo port, it is recommended for both parties to use copper-forced or fiber-forced mode.
- ☞ Run "show interface" under Admin Mode to check for the active port of a combo port .The following result indicates if the active port for a combo port is the fiber cable port: Hardware is Gigabit-combo, active is fiber.

Example: setting ports 1/25 -28 to fiber-forced

Switch(Config)#interface ethernet 1/25-28

Switch(Config-Port-Range)#combo-forced-mode sfp-forced

3.2.1.2.2 clear counters

Command: clear counters [{ethernet <*interface-list*> | vlan <*vlan-id*> | port-channel <*port-channel-number*> | <*interface-name*>}]

Function: Clears the statistics of the specified port.

Parameters: <*interface-list*> stands for the Ethernet port number; **< *vlan-id* >** stands for the VLAN interface number; **<*port-channel-number*>** for trunk interface number; **<*interface-name*>** for interface name, such as port-channel 1.

Command mode: Admin Mode

Default: Port statistics are not cleared by default.

Usage Guide: If no port is specified, then statistics of all ports will be cleared.

Example: Clearing the statistics for Ethernet port 1/1.

Switch#clear counters ethernet 1/1

3.2.1.2.3 description

Command：description <*string*>

no description

Function： Set name for specified port; the "**no description**" command cancels this configuration.

Parameter：<*string*> is a character string, which should not exceeds 32 characters

Command Mode：interface Mode

Default：No port name by default

Usage Guide：This command is for helping the use manage switches, such as the user assign names according to the port application, e.g. financial as the name of 1/1-2 ports which is used by financial department, engineering as the name of 1/9 ports which belongs to the engineering department, while the name of 1/12 ports is assigned with Server, which is because they connected to the server. In this way the port distribution state will be brought to the table.

Example：Specify the name of 1/1-2 port as financial

Switch(Config)#interface ethernet 1/1-2

Switch(Config-If-Port-Range)#description financial

3.2.1.2.4 flow control

Command: flow control

no flow control

Function: Enables the flow control function for the port: the "**no flow control"** command disables the flow control function for the port**.**

Command mode: Interface Mode

Default: Port flow control is disabled by default.

Usage Guide: After the flow control function is enabled, the port will notify the sending device to slow down the sending speed to prevent packet loss when traffic received exceeds the capacity of port cache. ES4650's ports support IEEE802.3X flow control; the ports work in half-duplex mode, supporting back-pressure flow control. If flow control results in serious HOL, the switch will automatically start HOL control (discarding some packets in the COS queue that may result in HOL) to prevent drastic degradation of network performance.

Note: Port flow control function is NOT recommended unless the users need a slow speed, low performance network with low packet loss. Flow control will not work between different cards in the switch. When enable the port flow control function, speed and duplex mode of both ends should be the same.

Example: Enabling the flow control function in ports 1/1-8.

Switch(Config)#interface ethernet 1/1-8

Switch(Config-Port-Range)#flow control

3.2.1.2.5 interface Ethernet

Command: interface ethernet <*interface-list*>

Function: Enters Ethernet Interface Mode from Global Mode.

Parameters: <*interface-list*> stands for port number.

Command mode: Global Mode

Usage Guide: Run the *exit* command to exit the Ethernet Interface Mode to Global Mode.

Example: Entering the Ethernet Interface Mode for ports 1/1, 1/4-5, 1/8.

Switch(Config)#interface ethernet 1/1;1/4-5;1/8

Switch(Config-Port-Range)#

3.2.1.2.6 loopback

Command: loopback

no loopback

Function: Enables the loopback test function in an Ethernet port; the "**no loopback**" command disables the loopback test on an Ethernet port.

Command mode: Interface Mode

Default: Loopback test is disabled in Ethernet port by default.

Usage Guide: Loopback test can be used to verify the Ethernet ports are working normally. After loopback has been enabled, the port will assume a connection established to itself, and all traffic sent from the port will be received at the very same port.

Example: Enabling loopback test in Ethernet ports 1/1 -8

Switch(Config)#interface ethernet 1/1-8

Switch(Config-Port-Range)#loopback

3.2.1.2.7 mdi

Command: mdi { auto | across | normal }

no mdi

Function: Sets the cable types supported by the Ethernet port; the "**no mdi**" command sets the cable type to auto-identification. This command is not supported on ES4626/ES4650's ports of 1000Mbps or more, these ports have auto-identification set for cable types.

Parameters: auto indicates auto identification of cable types; **across** indicates crossover cable support only; **normal** indicates straight-through cable support only.

Command mode: Interface Mode

Default: Port cable type is set to auto-identification by default.

Usage Guide: Auto-identification is recommended. Generally, straight-through cable is used for switch-PC connection and crossover cable is used for switch-switch connection.

Example: Setting the cable type support of Ethernet ports 1/5 -8 to straight-through cable only.

Switch(Config)#interface ethernet 1/5-8

Switch(Config-Port-Range)#mdi normal

3.2.1.2.8 negotiation

Command: negotiation

no negotiation

Function: Enables/Disables the auto-negotiation function of a 1000Base-T port.

Parameters: None.

Command mode: Port configuration Mode

Default: Auto-negotiation is enabled by default.

Usage Guide: This command applies to 1000Base-T interface only. The**negotiation** command is not available for 1000Base-FX interface. For combo port, this command applies to the 1000Base-TX port only and has no effect on 1000Base-TX port. To change the negotiation mode, speed and duplex mode of 1000Base-TX port, use **speed-duplex** command instead.

Example: Port 1 of Switch 1 is connected to port 1 of Switch 2, the following will disable the negotiation for both ports.

SwitchA(Config)#interface e1/1

SwitchA(Config-Ethernet1/1)#no negotiation

SwitchB(Config)#interface e1/1

SwitchB(Config-Ethernet1/1)#no negotiation

3.2.1.2.9 rate-limit

Command：rate-limit <*bandwidth*> {input|output}

no rate-limit {input|output}

Function： Enable the bandwidth limit function on the port; the "**no rate-limit {input|output}**" command disables this function

Parameter：<*bandwidth*> is the bandwidth limit, which is shown in Mbps ranging between 1-10000M; **input** refers to the bandwidth limit will only performed when the switch receives data from out side, while **output** refers to the function will be perform on sending only.

Command Mode： Interface mode

Default： Bandwidth limit disabled by default

Usage Guide： When the bandwidth limit is enabled with a size set, the max bandwidth of the port is determined by this size other than by 10/100/1000M

Note: The bandwidth limit can not exceed the physic maximum speed possible on the port. For example, an 10/100M Ethernet port can not be set to a bandwidth limit at 101M (or higher), but applicable on a 10/100/1000 port working at a speed of 100M.

Example： Set the bandwidth limit of 1-8 port 1to 40M

Switch(Config)#interface ethernet 1/1-8

Switch(Config-If-Port-Range)#rate-limit 40 input

Switch(Config-If-Port-Range)#rate-limit 40 output

3.2.1.2.10 rate-suppression

Command: rate-suppression {dlf | broadcast | multicast} <packets>

no rate-suppression {dlf | broadcast | multicast}

Function: Sets the traffic limit for broadcasts, multicasts and unknown destination unicasts on all ports in the switch; the "**no rate-suppression**" command disables this traffic throttle function on all ports in the switch, i.e., enables broadcasts, multicasts and unknown destination unicasts to pass through the switch at line speed.

Parameters: use **dlf** to limit unicast traffic for unknown destination; **multicast** to limit multicast traffic; **broadcast** to limit broadcast traffic. ***<packets>*** stands for the number of packets allowed to pass through per second for non-10Gb ports. For 10 Gb ports, the number of packets allowed to pass through multiplies 1,000. The valid range for both port types is 1 to 262,143.

Command mode: Interface Mode

Default: no limit is set by default. So, broadcasts, multicasts and unknown destination unicasts are allowed to pass at line speed.

Usage Guide: All ports in the switch belong to a same broadcast domain if no VLAN has been set. The switch will send the abovementioned three traffics to all ports in the broadcast domain, which may result in broadcast storm and so may greatly degrade the switch performance. Enabling Broadcast Storm Control can better protect the switch from broadcast storm. Note the difference of this command in 10Gb ports and other ports. If the allowed traffic is set to 3, this means allow 3,120 packets per second and discard the rest for 10Gb ports. However, the same setting for non-10Gb ports means to allow 3 broadcast packets per second and discard the rest.

Example: Setting ports 8 -10 (1000Mbps) allow 3 broadcast packets per second.

Switch(Config)#interface ethernet 1/8-10

Switch(Config-Port-Range)#rate-suppression broadcast 3

3.2.1.2.11 show interface status

Command：show interface status[{ethernet <*interface-number*> | vlan <*vlan-id*> | port-channel <*port-channel-number*> | <*interface-name*>}]

Function：Show information of specific port on the switch

Parameter：***<interface-number>*** is the port number of the Ethernet, **< *vlan-id* >** is the VLAN interface number, ***<port-channel-number>*** is the number of the aggregation interface, ***<interface-name>*** is the name of the interface such as port-channel1.

Command Mode：Admin Mode

Default：Information not displayed by default

Usage Guide：As for Ethernet port, this command will show port speed rate, duplex mode, flow control switch state, broadcast storm restrain of the port and the statistic state of the data packets，furthermore, this command can also show some information about

SFP/XFP if the port plugged with it; while for vlan interfaces, the port MAC address, IP address and the statistic state of the data packet will be shown; for aggregated port, port speed rate, duplex mode, flow control switch state, broadcast storm restrain of the port and the statistic state of the data packets will be displayed. All information of all ports on the switch will be shown if no port is specified.

Example： Show the information of Port 1/1

Switch#show interface status ethernet 1/1

Hardware is Gigabit-TX,address is 00-00-00-00-00-02

PVID is 1

MTU 1500 bytes,BW 10000 Kbit

Encapsulation ARPA,Loopback not set

Auto-duplex:Negotiation half-duplex, Auto-speed: Negotiation 10M bits

FlowControl is off, MDI type is auto

3.2.1.2.12 shutdown

Command: shutdown

no shutdown

Function: Shuts down the specified Ethernet port; the "**no shutdown**" command opens the port.

Command mode: Interface Mode

Default: Ethernet port is open by default.

Usage Guide: When Ethernet port is shut down, no data frames are sent in the port, and the port status displayed when the user types the "**show interface**" command is "down".

Example: Opening ports 1/1-8.

Switch(Config)#interface ethernet1/1-8

Switch(Config-Port-Range)#no shutdown

3.2.1.2.13 speed-duplex

Command: speed-duplex {auto | force10-half | force10-full | force100-half | force100-full | { {force1g-half | force1g-full} [nonegotiate [master | slave]] } }

no speed-duplex

Function: Sets the speed and duplex mode for 1000Base-TX or 100Base-TX ports; the "**no speed-duplex**" command restores the default speed and duplex mode setting, i.e., auto speed negotiation and duplex.

Parameters: auto for auto speed negotiation; **force10-half** for forced 10Mbps at half-duplex; **force10-full** for forced 10Mbps at full-duplex mode; **force100-half** for forced 100Mbps at half-duplex mode; **force100-full** for forced 100Mbps at full-duplex mode; **force1g-half** for forced 1000Mbps at half-duplex mode; **force1g-full** for forced 1000Mbps at full-duplex mode; **nonegotiate** for disable auto-negotiation for 1000 Mb

port; **master** to force the 1000Mb port to be **master** mode; **slave** to force the 1000Mb port to be **slave** mode.

Command mode: Interface Mode

Default: Auto-negotiation for speed and duplex mode is set by default.

Usage Guide: This command applies to 1000Base-TX ports only. **speed-duple**x command is not available for 1000Base-X port. For combo port, this command applies to the 1000Base-TX port only and has no effect on 1000Base-X port. To change the negotiation mode of 1000Base-X port, use **negotiation** command instead.

When configuring port speed and duplex mode, the speed and duplex mode must be the same as the setting of the remote end, i.e., if the remote device is set to auto-negotiation, then auto-negotiation should be set at the local port. If the remote end is in forced mode, the same should be set in the local end.

1000Gb ports are by default **master** when configuring **nonegotiate** mode. If one end is set to **master** mode, the other end must be set to **slave** mode. **force1g-half** Is not supported yet.

Example: Port 1 of Switch 1 is connected to port 1 of SwitchB, the following will set both ports in forced 100Mbps at half-duplex mode.

```
SwitchA(Config)#interface e1/1
SwitchA(Config-Ethernet1/1)#speed-duplex force100-half
SwitchB(Config)#interface e1/1
SwitchB(Config-Ethernet1/1)#speed-duplex force100-half
```

3.2.2 VLAN Interface Configuration

3.2.2.1 VLAN Interface Configuration Task List

1. Enter VLAN Mode
2. Configure the IP address for VLAN interface and enable VLAN interface.

1. Enter VLAN Mode

Command	Explanation
Global Mode	
interface vlan <*vlan-id*> **no interface vlan <*vlan-id*>**	Enters Interface Mode; the "**no interface vlan <*vlan-id*>**" command deletes specified VLAN interface.

2. Configure the IP address for VLAN interface and enables VLAN interface.

Command	Explanation
VLAN Mode	

ip address <*ip-address*> <*mask*> [secondary] **no ip address [<*ip-address*> <*mask*>]**	Configures the VLAN interface IP address; the "**no ip address [<*ip-address*> <*mask*>]"** command deletes the VLAN interface IP address.
VLAN Mode	
Shutdown **no shutdown**	Enables/Disables VLAN interface

3.2.2.2 Commands for Vlan Interface

3.2.2.2.1 interface vlan

Command: interface vlan <*vlan-id*>

no interface vlan <*vlan-id*>

Function: Enters Interface Mode; the "**no interface vlan <*vlan-id*>**" command deletes existing VLAN interface.

Parameters: <*vlan-id*> is the VLAN ID for the establish VLAN, the valid range is 1 to 4094.

Command mode: Global Mode

Usage Guide: Before setting a VLAN interface, the existence of the VLAN must be verified. Run the *exit* command to exit the VLAN Mode to Global Mode.

Example: Entering into the Interface Mode for VLAN1.

Switch(Config)#interface vlan 1

Switch(Config-If-Vlan1)#

3.2.2.2.2 ip address

Command: ip address <*ip-address*> <*mask*> [secondary]

no ip address [<*ip-address*> <*mask*>] [secondary]

Function: Sets the IP address and mask for the switch; the "**no ip address [<*ip-address*> <*mask*>]"** command deletes the specified IP address setting.

Parameters: <*ip-address*> is the IP address in decimal format; **<*mask*>** is the subnet mask in decimal format; **[secondary]** indicates the IP configured is a secondary IP address.

Command mode: Interface Mode

Default: No IP address is configured by default.

Usage Guide: This command configures the IP address for VLAN interface manually. If the optional parameter secondary is not present, the IP address will be the primary IP of the VLAN interface, otherwise, the IP address configured will be the secondary IP address for the VLAN interface. A VLAN interface can have one primary IP address but

multiple secondary IP addresses. Both primary IP address and secondary IP addresses can be used for SNMP/Web/Telnet management. In addition, ES4626/ES4650 allows IP addresses to be obtained through BootP/DHCP.

Example: Setting the IP address of VLAN1 interface to 192.168.1.10/24.

Switch(Config-If-Vlan1)#ip address 192.168.1.10 255.255.255.0

3.2.2.2.3 shutdown

Command: shutdown

no shutdown

Function: Shuts down the specified VLAN Interface; the "**no shutdown**" command opens the VLAN interface.

Command mode: Interface Mode

Default: VLAN Interface is enabled by default.

Usage Guide: When VLAN interface is shutdown, no data frames will be sent by the VLAN interface. If the VLAN interface needs to obtain IP address via BootP/DHCP protocol, it must be enabled.

Example: Enabling VLAN1 interface of the switch.

Switch(Config-If-Vlan1)#no shutdown

3.2.3 Network Management Port Configuration

3.2.3.1 Network Management Port Configuration Task List

1. Enter the network management port configuration mode
2. Configure the properties for the network management ports
   （1） Enable/Disable ports
   （2） Configure port speed
   （3） Configure port duplex mode
   （4） Enable/Disable port loopback function
   （5） Configuring port IP Address

1. Enter the network management port configuration mode

Command	**Explanation**
Global Mode	
interface ethernet <*num*>	Enters the network management port configuration mode

2. Configure the properties for the network management port

Command	**Explanation**

Network Management Port Configuration	
shutdown **no shutdown**	Enables/Disables network management port
speed {auto| force10| force100| }	Sets network management port speed
duplex {auto| full| half}	Sets network management port duplex mode
loopback **no loopback**	Enables/Disables loopback test function for network management port
ip address <ip-address> <mask> **no ip address [<ip-address> <mask>]**	Configures or cancels the IP address for network management port.

3.2.3.2 Commands for Network Management Port Configuration

3.2.3.2.1 duplex

Command: duplex {auto| full| half }

Function: Sets network management port duplex mode

Parameters: auto for auto-negotiation full-duplex mode; **full** for forced full-duplex mode; **half** for forced half-duplex mode.

Command mode: Network management port configuration Mode

Default: The default duplex mode is set to auto-negotiation.

Usage Guide: According to IEEE 802.3, the auto-negotiation for port speed and duplex are linked. If the duplex setting of the port is auto-negotiation, the port speed will be set to auto-negotiation automatically; if the port duplex mode changes from auto-negotiation to forced full/half-duplex, the port speed will also become forced mode, the forced speed will be the port speed before this command.

It is strongly recommended for the users to set all port speed and duplex mode to auto-negotiation, this can minimize protocol-related connection problems. If forced speed/duplex mode needs to be set, the speed/duplex mode setting of both ends must be verified to be the same.

Example: Setting the network management port to forced full-duplex mode.

Switch(Config)#interface ethernet 0

Switch(Config-Ethernet0)#duplex full

3.2.3.2.2 interface Ethernet

Command: interface ethernet <*interface-name*>

Function: Enters network management port configuration mode from Global Mode.

Parameters: <*interface-name*> stands for port number, the default value is 0.

Command mode: Global Mode

Usage Guide: Run the *exit* command to exit the network management Interface Mode to Global Mode.

Example: Entering network management interface mode.

Switch(Config)#interface ethernet 0

Switch(Config-Ethernet0)#

3.2.3.2.3 ip address

Command: ip address <*ip-address*> <*mask*>

no ip address [<*ip-address*> <*mask*>]

Function: Sets the IP address and mask for the switch; the "**no ip address [<*ip-address*> <*mask*>]"** command deletes the specified IP address setting.

Parameters: <*ip-address*> is the IP address in decimal format; **<*mask*>** is the subnet mask in decimal format.

Command mode: Network management port configuration Mode

Default: No IP address is configured by default.

Usage Guide: This command configures the IP address for network management port.

Example: Setting the IP address of the network management interface to 192.168.1.10/24.

Switch(Config-Ethernet0)#ip address 192.168.1.10 255.255.255.0

3.2.3.2.4 loopback

Command: loopback

no loopback

Function: Enables the loopback test function for the network management port; the "**no loopback**" command disables the loopback test the on network management port.

Command mode: Network management port configuration Mode

Default: Loopback test is disabled in network management port by default.

Usage Guide: Loopback test can be used to verify the network management port is working normally. After loopback has been enabled, the port will assume a connection established to itself, and all traffic sent from the port will be received at this very port.

Example: Enabling loopback test in the network management port.

Switch(Config)#interface ethernet 0

Switch(Config-Ethernet0)#loopback

3.2.3.2.5 shutdown

Command: shutdown

no shutdown

Function: Shuts down the network management port; the "**no shutdown**" command opens the port.

Command mode: Network management port configuration Mode

Default: Network management port is open by default.

Usage Guide: When network management port is shut down, no data frames are sent in the port, and the port status displayed when the user typed "**show interface**" command is "down".

Example: Enabling the network management interface.

Switch(Config)#interface ethernet 0

Switch(Config-Ethernet0)#no shutdown

3.2.3.2.6 speed

Command: speed {auto| force10| force100}

Function: Sets port speed

Parameters: auto for auto-negotiation of speed; **force10** for forced 10Mbps; **force100** for forced half 100Mbps.

Command mode: Network management port configuration Mode

Default: Auto-negotiation for speed is set by default.

Usage Guide: According to IEEE 802.3, the auto-negotiation for port speed and duplex are linked. If the port speed setting is auto-negotiation, the port duplex mode will also be set to auto-negotiation automatically; if the port speed changes from auto-negotiation to forced, the port duplex mode will also become forced full/half-duplex.

It is strongly recommended for users to set all port speed and duplex mode to auto-negotiation, this can minimize protocol-related connection problems. If forced speed/duplex mode needs to be set, the speed/duplex mode setting of both ends must be verified to be the same.

Example: Setting the network management port to forced 100Mbps.

Switch(Config)#interface ethernet 0

Switch(Config-Ethernet0)#speed force100

3.3 Port Mirroring Configuration

3.3.1 Introduction to Port Mirroring

Port mirroring refers to the duplication of data frames sent/received on a port to another port. The duplicated port is referred to as mirror source port and the duplicating port is referred to as mirror destination port. A protocol analyzer (such as Sniffer) or RMON monitoring instrument is often attached to the mirror destination port to monitor and manage the network and diagnostic.

ES4626/ES4650 support one mirror destination port only. The number of mirror source ports are not limited, one or more may be used. Multiple source ports can be within the same VLAN or across several VLANs. The destination port and source port(s) can be located in different VLANs.

3.3.2 Port Mirroring Configuration Task List

1. Specify mirror source port and dentistination port

Command	**Explanation**
Port mode	
port monitor interface <*interface-list*> {rx| tx| both} **no port monitor interface <*interface-list*>**	Specifies mirror dentist port **port monitor interface <*interface-list*> {rx| tx| both},**the **<*interface-list*>** refer to the source ports ; the "**no port monitor interface <*interface-list*>}**" command deletes mirror port.

3.3.3 Command For Mirroring Configuration

3.3.3.1 port monitor

Command:port monitor interface <*interface-list*> {rx| tx| both}

no port monitor interface <*interface-list*>

Function: Specifies port of mirror source;the "**no port monitor interface <*interface-list*>**" command deletes the mirror source port.

Parameter:<*interface-list*> is the mirror source port list, in which special characters such as "-"、";" are available; **rx** is the flow received from the source port by the mirror;**tx** is the flow sent from the source port by the mirror;**both** refers to the flow both into and out from the mirror source

Command Mode: Port mode

Usage Guide: This command is for configuring the source port of the mirror. There is not limitation on the switch to the mirror source port, which can be one port or many ports, and not only can the bilateral flow be sent out from or received into the mirror source port,

but also the sent and received flows are available on single mirror source port. While mirroring several ports, their direction can vary but have to be configured by several times. The speed rate of the mirror source port and the destination port should be the same or else the packet may be lost.

Example: Configure the sent flow of the 1/1-4 mirror source port and the receiving flow of the 1/5 mirror port

Switch(Config-If-Ethernet1/5)#port monitor interface ethernet 1/1-4 tx

3.3.3.2 show port monitor

Command:show port monitor [interface <*interface-list*>]

Function: Show the mirror source and destination port information

Parameter:<*interface-list*> is the mirror source port list

Command Mode: Admin Mode

Usage Guide This command will show current mirror source port and destination port.

Example: Switch#show port monitor

3.3.4 Device Mirroring Troubleshooting

If problems occurs on configuring port mirroring, please check the following first for causes:

- ☞ Whether the mirror destination port is a member of a trunk group or not, if yes, modify the trunk group.
- ☞ If the throughput of mirror destination port is smaller than the total throughput of mirror source port(s), the destination port will not be able to duplicate all source port traffic; please decrease the number of source ports, duplicate traffic for one direction only or choose a port with greater throughput as the destination port.

3.4 Port Configuration Example

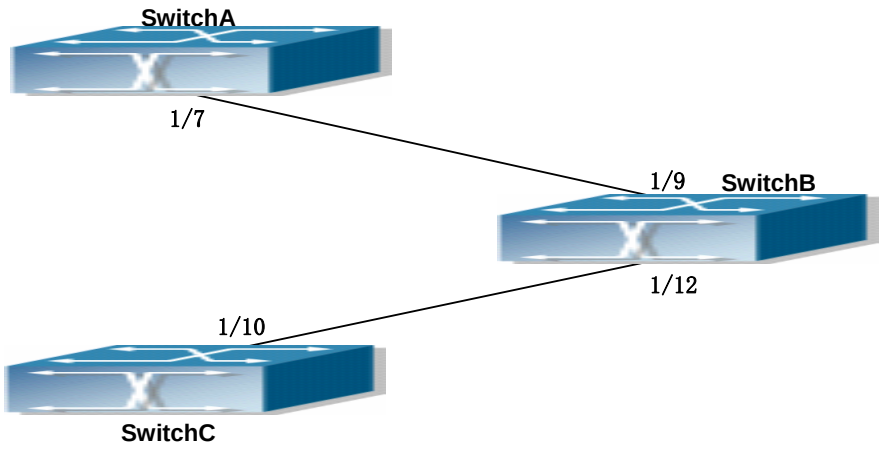


Fig 3-1 Port Configuration Example

No VLAN has been configured in the switches, default VLAN1 is used.

Switch	Port	Property
SwitchA	1/7	Ingress bandwidth limit: 150 M
SwitchB	1/8	Mirror source port
	1/9	100Mbps full, mirror source port
	1/12	1000Mbps full, mirror destination port
SwitchC	1/10	100Mbps full

The configurations are listed below:

SwitchA:

SwitchA(Config)#interface ethernet 1/7

SwitchA(Config-If-Ethernet1/7)#rate-limit 150 input

SwitchB:

SwitchB(Config)#interface ethernet 1/9

SwitchB(Config-If-Ethernet1/9)#speed-duplex force100-full

SwitchB(Config-If-Ethernet1/9)#exit

SwitchB(Config)#interface ethernet 1/12

SwitchB(Config-If-Ethernet1/12)# speed-duplex force1000-full

SwitchB(Config-If-Ethernet1/12)#port monitor interface ethernet 1/8-9 both

SwitchC:

SwitchC(Config)#interface ethernet 1/10

SwitchC(Config-If-Ethernet1/10)#speed-duplex force1000-full

3.5 Port Troubleshooting

Here are some situations that frequently occurs in port configuration and the advised solutions:

- ☞ Two connected fiber interfaces won't link up if one interface is set to auto-negotiation but the other to forced speed/duplex. This is determined by IEEE 802.3.
- ☞ The following combinations are not recommended: enabling traffic control as well as setting multicast limiting for the same port; setting broadcast, multicast and unknown destination unicast control as well as port bandwidth limiting for the same port. If such combinations are set, the port throughput may fall below the expected performance

3.6 Web Management

Click "Port configuration" to open the port configuration management table. Users can proceed to do port management, setup port speed, duplexes and so on.

3.6.1 Ethernet port configuration

Click "Port configuration", "Ethernet port configuration" to open the Ethernet port configuration management table to configure Ethernet port duplex, speed, bandwidth control and so on.

3.6.2 Physical port configuration

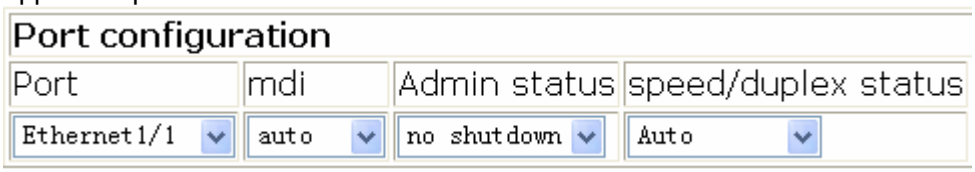
Click "port configuration", "Ethernet port configuration", "Physical port configuration" to configure the following information:

- Port: Specifies the configuration port
- MDI: Sets up the connection type of the Ethernet port. Auto means to auto-negotiate connection type; across means the port supporting cross-over cable only; normal means the port supporting straight-through cable only.
- Admin Status: Enables/Disables port.
- speed/duplex status: Sets up Ethernet sport speed and duplex including, auto-negotiation, 10Mbps Half, 10Mbps Full, 100Mbps Half, 100Mbps Full, 1000Mbps Half, 1000Mbps Full.
- Port flow control status: Sets up port flow control including disabled flow control and

enabled flow control.

- Loopback: Sets up Ethernet port to enable loopback testing function.

Example: Assign port to be Ethernet 1/1 and set up MDI as normal; Admin control status as no shutdown, speed/duplex as auto, port flow control status as disabled flow control and Loopback as no loopback. Then click Apply button and these set up items will be applied to port 1/1.



Port list table displays the related information of the switch physical ports.

Port list

Port	mdi	managementStatus	Speed	Mode	1000M Mode
Ethernet1/1	auto	NO SHUT DOWN	auto	auto	NULL
Ethernet1/2	auto	SHUT DOWN	auto	auto	NULL
Ethernet1/3	auto	NO SHUT DOWN	auto	auto	NULL
Ethernet1/4	auto	SHUT DOWN	auto	auto	NULL
Ethernet1/5	auto	SHUT DOWN	auto	auto	NULL
Ethernet1/6	auto	SHUT DOWN	auto	auto	NULL
Ethernet1/7	auto	NO SHUT DOWN	auto	auto	NULL
Ethernet1/8	auto	NO SHUT DOWN	auto	auto	NULL
Ethernet1/9	auto	SHUT DOWN	auto	auto	NULL
Ethernet1/10	auto	SHUT DOWN	auto	auto	NULL
Ethernet1/11	auto	SHUT DOWN	auto	auto	NULL
Ethernet1/12	auto	SHUT DOWN	auto	auto	NULL

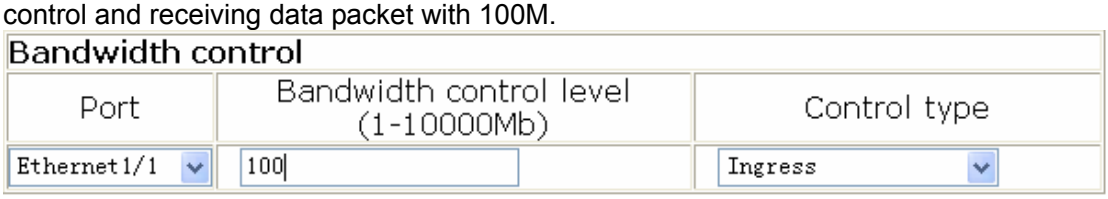
3.6.3 Bandwidth control

Click port configuration, Ethernet port configuration, Bandwidth control and proceed to do port bandwidth control. 1

- Port: Specifies configuration port
- Bandwidth control level: port bandwidth control. The unit is Mbps and the value range is 1~10000Mbps
- Control type: Ingress means to control port bandwidth when receiving data packet sent from outside the switch. Egress means to control port bandwidth when sending data packets to outside of the switch. Ingress and Egress means to control port bandwidth when both receiving and sending.

Example: Choose Port to be Ethernet 1/1, set up Bandwidth control level as 100Mb, Control type as Ingress, then click Apply button. So the port 1/1 will execute bandwidth

control and receiving data packet with 100M.



3.6.4 Vlan interface configuration

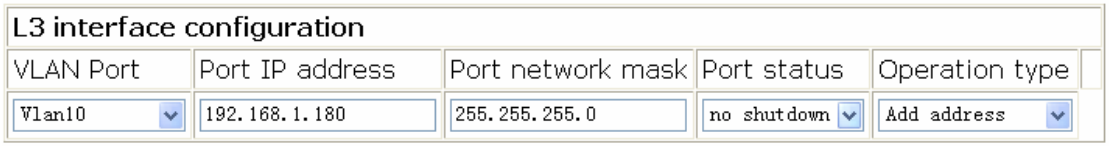
Click Port configuration, vlan interface configuration to open the VLAN port configuration management list to allocate IP address and mask on L3 port and so on.

3.6.5 Allocate IP address for L3 port

Click “Port configuration”, “vlan interface configuration”, Allocate IP address for L3 port to allocate IP address for L3 port. 2. This setup contains the following characteristics:

- Port: L3 port
- Port IP address: IP address for L3 port
- Port network mask
- Port status
- Operation type: add/delete address

Example: Assign Port as Vlan10, port IP address as 192.168.1.180, Port network mask as 255.255.255.0, Port status as no shutdown, Operation type selection as Add address then click Apply button and this set up will be applied to the switch.

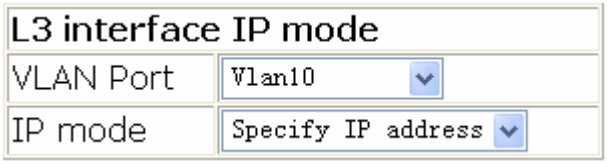


3.6.6 L3 port IP addr mode configuration

Click ”Port configuration”, “vlan interface configuration”, “L3 port IP addr mode configuration” to set up L3 port IP address mode configuration.

- Port: L3 port

IP mode: Specifies the Ip address, meaning users need to set up L3 IP address manually. Bootp-client means to gain an IP address and gateway address through BootP. dhcp-client means to gain IP address and gateway address through DHCP. Click the apply button and this setup will be applied to the switch.



3.6.7 Port mirroring configuration

Click “Port configuration”, “Port mirroring configuration” to enter port mirroring configuration management table to do port mirroring configurations.

3.6.8 Mirror configuration

Click Port configuration, Port mirroring configuration, Mirror configuration to configure port mirroring function including configuring mirroring source port and mirroring destination port functions.

Configure mirroring source port:

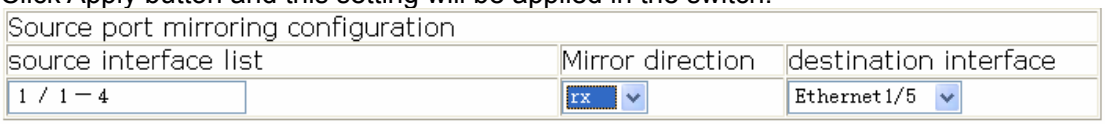
- Session: Mirror dialog value
- source interface list
- Mirror direction: rx means to mirror the port receiving data packets; tx means to mirror the port sending data packets; both means to mirror both receiving & sending

Example: Select mirror dialog session as one, set up source interface list as Ethernet ports 1/1~4 and the mirroring direction as rx. Click Apply button and this port will be added into the monitor session. Click the Default button to delete this port from the list.

Configure mirroring destination port. 2.

- Session: Mirroring dialog value
- destination interface
- tag: Setting the vlan tag function means all mirroring packets carry vlan tags; preserve means that if the Ingress mirroring packet, carrying a vlan tag, while Ingress, then Egress mirroring packet will carry vlan tag as well. Otherwise will be not.

Select mirror dialog session as 1 and set up port mirroring list as 1/5, tag as preserve. Click Apply button and this setting will be applied in the switch.



3.6.9 Port debug and maintenance

Click Port configuration, Port debug and maintenance and open the Port debug and

maintenance management list to get port information.

3.6.10 Show port information

Click “Port configuration”, “Port debug” and “maintenance”, Show port information to check the statistic information of the receiving/sending data packet information of the port.

Chapter 4 Port Channel Configuration

4.1 Introduction to Port Channel

To understand Port Channel, Port Group should be introduced first. Port Group is a group of physical ports in the configuration level; only physical ports in the Port Group can take part in link aggregation and become a member port of a Port Channel. Logically, Port Group is not a port but a port sequence. Under certain conditions, physical ports in a Port Group perform port aggregation to form a Port Channel that has all the properties of a logical port, therefore it becomes an independent logical port. Port aggregation is a process of logical abstraction to abstract a set of ports (port sequence) with the same properties to a logical port. Port Channel is a collection of physical ports and used logically as one physical port. Port Channel can be used as a normal port by the user, and can not only add network's bandwidth, but also provide link backup. Port aggregation is usually used when the switch is connected to routers, PCs or other switches.

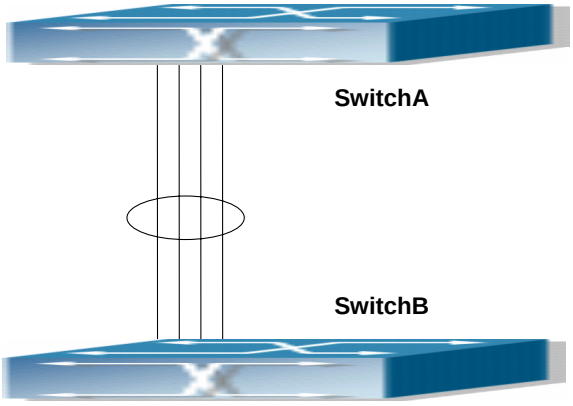


Fig 4-1 Port aggregation

As shown in the above figure2-1, SwitchA is aggregated to a Port Channel, the bandwidth of this Port Channel is the total of all the four ports. If traffic from SwitchA needs to be transferred to SwitchB through the Port Channel, traffic allocation calculation will be performed based on the source MAC address and the lowest bit of target MAC address. The calculation result will decide which port to convey the traffic. If a port in Port Channel fails, the other ports will undertake traffic of that port through a traffic allocation algorithm. This algorithm is carried out by the hardware.

ES4626/ES4650 switch offers 2 methods for configuring port aggregation: manual Port Channel creation and LACP (Link Aggregation Control Protocol) dynamic Port Channel creation. Port aggregation can only be performed on ports in full-duplex mode.

For Port Channel to work properly, member ports of the Port Channel must have the same properties as follows:

- ☞ All ports are in full-duplex mode.
- ☞ All Ports are of the same speed.
- ☞ All ports are Access ports and belong to the same VLAN or are all Trunk ports.
- ☞ If the ports are Trunk ports, then their “Allowed VLAN” and “Native VLAN” property should also be the same.

If Port Channel is configured manually or dynamically on ES4626/ES4650 switch, the system will automatically set the port with the smallest number to be Master Port of the Port Channel. If the spanning tree function is enabled in the switch, the spanning tree protocol will regard Port Channel as a logical port and send BPDU frames via the master port.

Port aggregation is closely related with switch hardware. ES4626/ES4650 switch allow physical port aggregation of any two switches, maximum 8 port groups and 8 ports in each port group are supported.

Once ports are aggregated, they can be used as a normal port. ES4626/ES4650 switch have a built-in aggregation interface configuration mode, the user can perform related configuration in this mode just like in the VLAN and physical port configuration mode.

4.2 Port Channel Configuration Task List

1. Create a port group in Global Mode.
2. Add ports to the specified group from the Port Mode of respective ports.
3. Enter port-channel configuration mode.

1. Creating a port group

Command	Explanation
Global Mode	
port-group *<port-group-number>* [load-balance { src-mac | dst-mac | dst-src-mac | src-ip| dst-ip|dst-src-ip}] **no port-group *<port-group-number >* [load-balance]**	Creates or deletes a port group and sets the load balance method for that group.

2. Add physical ports to the port group

Command	Explanation
Interface Mode	
port-group <*port-group-number*> mode {active|passive|on} **no port-group <*port-group-number*>**	Adds ports to the port group and sets their mode.

3. Enter port-channel configuration mode.

Command	Explanation
Global Mode	
interface port-channel <*port-channel-number*>	Enters port-channel configuration mode.

4.3 Commands for port channel

4.3.1 debug lacp

Command: debug lacp

no debug lacp

Function: Enables the LACP debug function: "**no debug lacp"** command disables this debug function**.**

Command mode: Admin Mode

Default: LACP debug information is disabled by default.

Usage Guide: Use this command to enable LACP debugging so that LACP packet processing information can be displayed.

Example: Enabling LACP debug.

Switch#debug lacp

4.3.2 port-group

Command:port-group <*port-group-number*> [load-balance { src-mac|dst-mac | dst-src-mac | src-ip| dst-ip|dst-src-ip}]

no port-group <*port-group-number*> [load-balance]

Function: Creates a port group and sets the load balance method for that group. If no method is specified, the default load balance method is used. The "**no port-group <*port-group-number*> [load-balance]**" command deletes that group or restores the default load balance setting. Enter "load-balance" for restoring default load balance,

otherwise, the group will be deleted.

Parameters: <*port-group-number*> is the group number of a port channel from 1 to 8, if the group number is already exist, an error message will be given. **dst-mac** performs load balancing according to destination MAC; **src-mac** performs load balance according to source MAC; **dst-src-mac** performs load balancing according to source and destination MAC; **dst-ip** performs load balancing according to destination IP; **src-ip** performs load balancing according to source IP; **dst-src-ip** performs load balancing according to destination and source IP. If a port group has formed a port-channel, the load balance setting cannot be modified, please set the load balance mode before port-channel.

Default: Switch ports do not belong to a port channel by default; LACP not enabled by default.

Command mode: Global Mode

Example: Creating a port group and setting the default load balance method.

Switch(Config)# port-group 1

Delete a port group.

Switch(Config)#no port-group 1

4.3.3 port-group mode

Command: port-group <*port-group-number*> mode {active|passive|on}

no port-group <*port-group-number*>

Function: Adds a physical port to port channel, the "**no port-group <*port-group-number*>**" removes specified port from the port channel.

Parameters: <*port-group-number*> is the group number of port channel, from 1 to 8; **active** enables LACP on the port and sets it in Active mode; **passive** enables LACP on the port and sets it in Passive mode; **on** forces the port to join a port channel without enabling LACP.

Command mode: Interface Mode

Default: Switch ports do not belong to a port channel by default; LACP not enabled by default.

Usage Guide: If the specified port group does not exist, a group will be created first to add the ports. All ports in a port group must be added in the same mode, i.e., all ports use the mode used by the first port added. Adding a port in "on" mode is a "forced" action, which means the local end switch port aggregation does not rely on the information of the other end, port aggregation will succeed as long as there are 2 or more ports in the group and all ports have consistent VLAN information. Adding a port in "active" or "passive" mode enables LACP. Ports of at least one end must be added in "active" mode, if ports of

both ends are added in “passive” mode, the ports will never aggregate.

Example: Under the Port Mode of Ethernet1/1, add current port to “port-group 1” in “active” mode.

Switch(Config-Ethernet1/1)#port-group 1 mode active

4.3.4 interface port-channel

Command: interface port-channel <*port-channel-number*>

Function: Enters the port channel configuration mode

Command mode: Global Mode

Usage Guide: On entering aggregated port mode, configuration to GVRP or spanning tree modules will apply to aggregated ports; if the aggregated port does not exist (i.e., ports have not been aggregated), an error message will be displayed and configuration will be saved and will be restored until the ports are aggregated. Note such restoration will be performed only once, if an aggregated group is ungrouped and aggregated again, the initial user configuration will not be restored. If it is configuration for modules, such as shutdown or speed configuration, then the configuration to current port will apply to all member ports in the corresponding port group.

Example: Entering configuration mode for port-channel 1.

Switch(Config)#interface port-channel 1

Switch(Config-If-Port-Channel1)#

4.3.5 show port-group

Command: show port-group [<*port-group-number*>] {brief | detail | load-balance | port | port-channel}

Parameters: <*port-group-number*> is the group number of port channel to be displayed, from 1 to 8; **“brief”** displays summary information; **“detail”** displays detailed information; **“load-balance”** displays load balance information; **“port”** displays member port information; **“port-channel”** displays port aggregation information.

Command mode: Admin Mode

Usage Guide: If “port-group-number” is not specified, then information for all port groups will be displayed.

Example: Adding port 1/1 and 1/2 to port-group 1.

1. Display summary information for port-group 1.

Switch#show port-group 1 brief

Port-group number : 1

Number of ports in porg-group : 2 Maxports in port-channel = 8

Number of port-channels : 0 Max port-channels : 1

Displayed information	Explanation
Number of ports in group	Port number in the port group
Maxports	Maximum number of ports allowed in a group
Number of port-channels	Whether aggregated to port channel or not
Max port-channels	Maximum port channel number can be formed by port group.

2. Display detailed information for port-group 1.

Switch# show port-group 1 detail

Sorted by the ports in the group 1:

Ethernet port 1/1 :

both of the port and the agg attributes are not equal

the general information of the port are as follows:

portnumber: 1 actor_port_agg_id:0 partner_oper_sys:0x000000000000

partner_oper_key: 0x0001 actor_oper_port_key: 0x0101

mode of the port: ACTIVE lacp_aware: enable

begin: FALSE port_enabled: FALSE lacp_ena: FALSE ready_n: TRUE

the attributes of the port are as follows:

mac_type: ETH_TYPE speed_type: ETH_SPEED_100M

duplex_type: FULL port_type: ACCESS

the machine state and port state of the port are as the follow

mux_state: DETCH rcvm_state: P_DIS prm_state: NO_PER

actor_oper_port_state : L_A___F_

partner_oper_port_state: _TA___F_

Ethernet port 1/2 :

both of the port and the agg attributes are not equal

the general information of the port are as follows:

portnumber: 2 actor_port_agg_id:0 partner_oper_sys:0x000000000000

partner_oper_key: 0x0002 actor_oper_port_key: 0x0102

mode of the port: ACTIVE lacp_aware: enable

begin: FALSE port_enabled: FALSE lacp_ena: TRUE ready_n: TRUE

the attributes of the port are as follows:

mac_type: ETH_TYPE speed_type: ETH_SPEED_100M

duplex_type: FULL port_type: ACCESS

the machine state and port state of the port are as follows:

mux_state: DETCH rcvm_state: P_DIS prm_state: NO_PER

actor_oper_port_state : L_A___F_

partner_oper_port_state: _TA___F_

Displayed information	Explanation
portnumber	Port number
actor_port_agg_id	The channel number to add the port to. If the port cannot be added to the channel due to inconsistent parameters between the port and the channel, 3 will be displayed.
partner_oper_sys	System ID of the other end.
partner_oper_key	Operational key of the other end.
actor_oper_port_key	Local end operational key
mode of the port	The mode in which port is added to the group
mac_type	Port type: standard Ethernet port and fiber-optical distributed data interface
speed_type	Port speed type: 10Mbps, 100Mbps, 1,000Mbps and 10Gbps.
duplex_type	Port duplex mode: full-duplex and half-duplex
port_type	Port VLAN property: access port or trunk port
mux_state	Status of port binding status machine
rcvm_state	Status of port receiving status machine
prm_state	Status of port sending status machine

3. Display load balance information for port-group 1.

Switch# show port-group 1 load-balance

The loadbalance of the group 1 based on src MAC address.

4. Display member port information for port-group 1.

Switch# show port-group 1 port

Sorted by the ports in the group 1 :

---

the portnum is 1

Ethernet port 1/1 related information:

Actor part	Administrative	Operational
port number	1	
port priority	0x8000	
aggregator id	0	
port key	0x0100	0x0101
port state		
LACP activity	.	1
LACP timeout	.	.
Aggregation	1	1
Synchronization	.	.
Collecting	.	.

Distributing . .
Defaulted 1 1
Expired . .
Partner part Administrative Operational
system 000000-000000 000000-000000
system priority 0x8000 0x8000
key 0x0001 0x0001
port number 1 1
port priority 0x8000 0x8000
port state
LACP activity . .
LACP timeout 1 1
Aggregation 1 1
Synchronization . .
Collecting . .
Distributing . .
Defaulted 1 1
Expired . .
Selected Unselected

Displayed information	Explanation
portnumber	Port number
port priority	Port Priority
system	System ID
system priority	System Priority
LACP activity	Whether port is added to the group in “active” mode, 1 for yes.
LACP timeout	Port timeout mode, 1 for short timeout.
Aggregation	Whether aggregation is possible for the port, 0 for independent port that does not allow aggregation.
Synchronization	Whether port is synchronized with the partner end.
Collecting	Whether status of port bound status machine is “collecting” or not.
Distributing	Whether status of port bound status machine is “distributing” or not.
Defaulted	Whether the local port is using default partner end parameter.
Expired	Whether status of port receiving status machine is “expire” or not.

Selected	Whether the port is selected or not..

5. Display port-channel information for port-group1.

Switch# show port-group 1 port-channel

Port channels in the group 1:

Port-Channel: port-channel1

Number of port : 2 Standby port : NULL

Port in the port-channel :

Index Port Mode

---

1 Ethernet1/1 active

2 Ethernet1/2 active

Displayed information	Explanation
Port channels in the group	If port-channel does not exist, the above information will not be displayed.
Number of port	Port number in the port-channel.
Standby port	Port that is in “standby” status, which means the port is qualified to join the channel but cannot join the channel due to the maximum port limit, thus the port status is “standby” instead of “selected”.

4.4 Port Channel Example

Scenario 1: Configuring Port Channel in LACP.

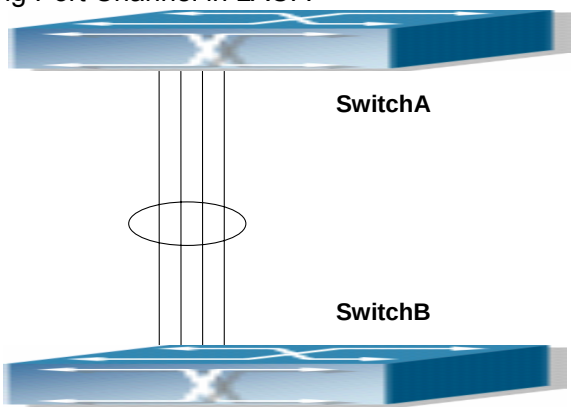


Fig 4-2 Configuring Port Channel in LACP

Example: The switches in the description below are all ES4626/ES4650 switch and as shown in the figure, ports 1, 2, 3, 4 of SwitchA are access ports that belong to vlan1. Add those four ports to group1 in active mode. Ports 1, 2, 3, 4 of SwitchB are access

ports that also belong to vlan1. Add these four ports to group2 in passive mode. All the ports should be connected with cables (shown as the four connecting lines in the figure)

The configuration steps are listed below:

SwitchA#config
SwitchA (Config)#interface eth 1/1-4
SwitchA (Config-Port-Range)#port-group 1 mode active
SwitchA (Config-Port-Range)#exit
SwitchA (Config)#interface port-channel 1
SwitchA (Config-If-Port-Channel1)#

SwitchB#config
SwitchB (Config)#port-group 2
SwitchB (Config)#interface eth 1/1-4
SwitchB (Config-Port-Range)#port-group 2 mode passive
SwitchB (Config-Port-Range)#exit
SwitchB (Config)#interface port-channel 2
SwitchB (Config-If-Port-Channel2)#

Configuration result:

Shell prompts ports aggregated successfully after a while, now ports 1, 2, 3, 4of SwitchA form an aggregated port named “Port-Channel1”, ports 1, 2, 3, 4 of SwitchB forms an aggregated port named “Port-Channel2”; configurations can be made in their respective aggregated port configuration mode.

Scenario 2: Configuring Port Channel in ON mode.

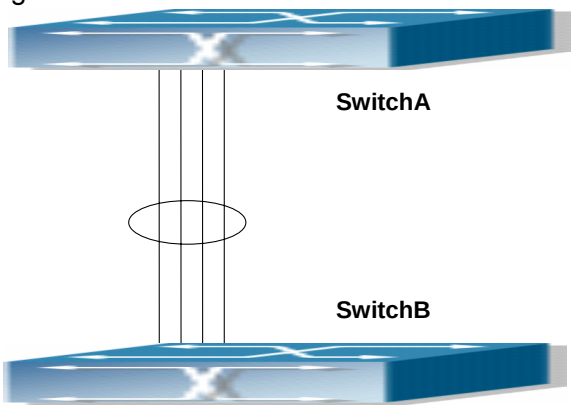


Fig 4-3 Configuring Port Channel in ON mode

Example: As shown in the figure, ports 1, 2, 3, 4 of SwitchA are access ports that belong to vlan1. Add those four port to group1 in “on” mode. Ports 1, 2, 3, 4 of SwitchB are access ports that also belong to vlan1, add these four ports to group2 in “on” mode.

The configuration steps are listed below:

SwitchA#config
SwitchA (Config)#interface eth 1/1
SwitchA (Config-Ethernet1/1)# port-group 1 mode on
SwitchA (Config-Ethernet1/1)#exit
SwitchA (Config)#interface eth 1/2
SwitchA (Config-Ethernet1/2)# port-group 1 mode on
SwitchA (Config-Ethernet1/2)#exit
SwitchA (Config)#interface eth 1/3
SwitchA (Config-Ethernet1/3)# port-group 1 mode on
SwitchA (Config-Ethernet1/3)#exit
SwitchA (Config-Ethernet1/4)# port-group 1 mode on
SwitchA (Config-Ethernet1/4)#exit

SwitchB#config
SwitchB (Config)#port-group 2
SwitchB (Config)#interface eth 1/1-4
SwitchB (Config-Port-Range)#port-group 2 mode on
SwitchB (Config-Port-Range)#exit

Configuration result:

Add ports 1, 2, 3, 4 of SwitchA to port-group 1 in order, and we can see a group in "on" mode is completely joined forcedly, switch in other ends won't exchange LACP BPDU to complete aggregation. Aggregation finishes immediately when the command to add port 2 to port-group 1 is entered, port 1 and port 2 aggregate to be port-channel 1, when port 3 joins port-group 1, port-channel 1 of port 1 and 2 are ungrouped and re-aggregate with port 3 to form port-channel 1. (It should be noted that whenever a new port joins in an aggregated port group, the group will be ungrouped first and re-aggregated to form a new group.) Now all four ports in both SwitchA and SwitchB are aggregated in "on" mode and become an aggregated port respectively.

4.5 Port Channel Troubleshooting

If problems occur when configuring port aggregation, please first check the following for causes.

- ☞ Ensure all ports in a port group have the same properties, i.e., whether they are in full-duplex mode, forced to the same speed, and have the same VLAN properties, etc. If inconsistency occurs, make corrections.
- ☞ Some commands cannot be used on a port in port-channel, such as arp, bandwidth, ip, ip-forward, etc.

- ☞ When port-channel is forced, as the aggregation is triggered manually, the port group will stay unaggregated if aggregation fails due to inconsistent VLAN information. Ports must be added to or removed from the group to trigger another aggregation, if VLAN information inconsistency persists, the aggregation will fail again. The aggregation will only succeed when VLAN information is consistent and aggregation is triggered due to port addition or removal.
- ☞ Verify that port group is configured in the partner end, and in the same configuration. If the local end is set in manual aggregation or LACP, the same should be done in the partner end; otherwise port aggregation will not work properly. Another thing to be noted is that if both ends are configured with LACP, then at least one of them should be in ACTIVE mode, otherwise LACP packet won't be initiated.
- ☞ LACP cannot be used on ports with Security and IEEE 802.1x enabled.

4.6 Web Management

Click "Port channel configuration" to open LACP port group configuration and LACP port configuration. LACP port group page will be used to configure and display group while LACP port configuration page will be used to configure and display port group members.

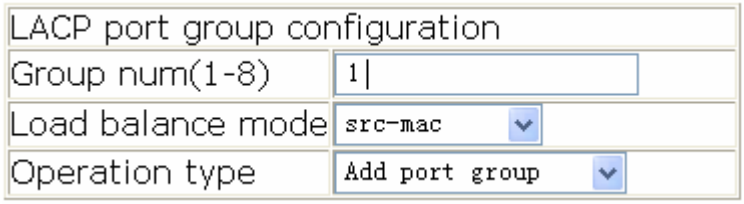
4.6.1 LACP port group configuration

Click "LACP port group configuration" to enter configuration page.

- Group Num: group number
- Load balance mode: includes src-mac, dst-mac, dst-src-mac, src-ip, dst-ip, dst-src-ip
- Operation type: Add port group or Remove port group

Fill in group Num, select load balance mode and select operation type as Add port group. Click Apply to add the group.

After finishing the group configuration, the configured port information will be shown under the configuration table.



4.6.2 LACP port configuration

Click LACP port configuration to enter configuration page

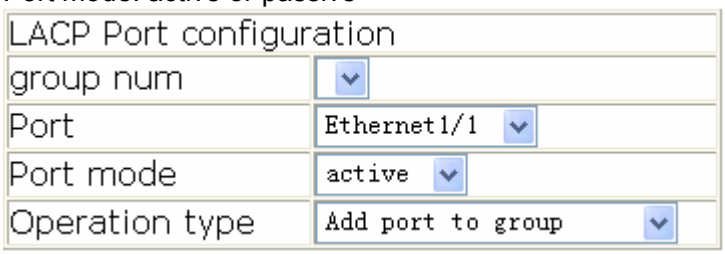
Click Apply button to add port into the group.

Display port member

Select a group num in port configuration and the information of port member will be shown under the configuration table.

- Port: name of port member

Port mode: active or passive



Chapter 5 VLAN Configuration

5.1 VLAN Configuration

5.1.1 Introduction To VLAN

VLAN (Virtual Local Area Network) is a technology that divides the logical addresses of devices within the network to separate network segments basing on functions, applications or management requirements. By this way, virtual workgroups can be formed regardless of the physical location of the devices. IEEE announced IEEE 802.1Q protocol to direct the standardized VLAN implementation, and the VLAN function of ES4626/ES4650 switch is implemented following IEEE 802.1Q.

The key idea of VLAN technology is that a large LAN can be partitioned into many separate broadcast domains dynamically to meet the demands.

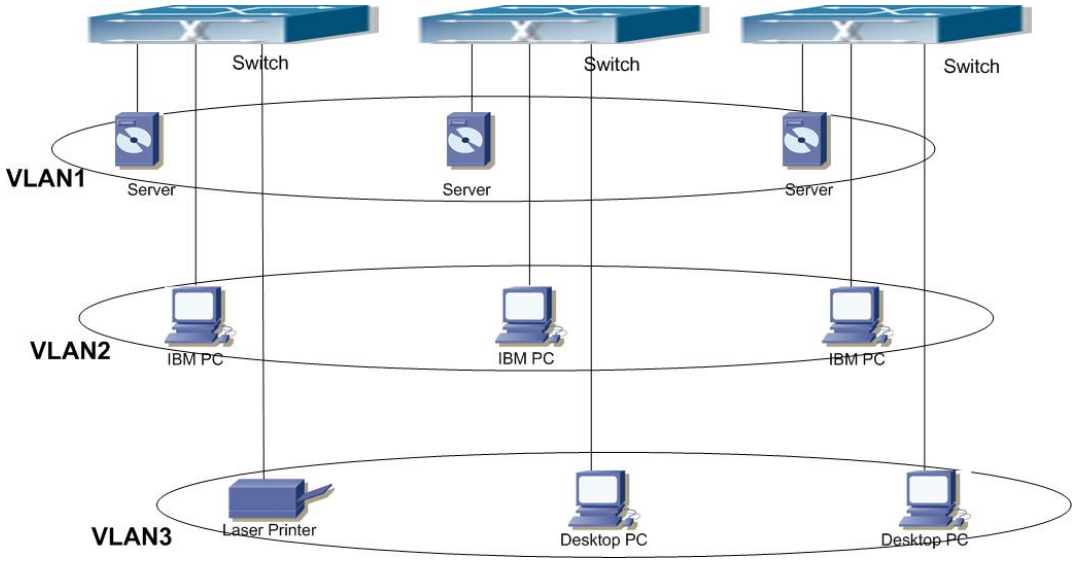


Fig 5-1 A VLAN network defined logically

Each broadcast domain is a VLAN. VLANs have the same properties as the physical LANs, except VLAN is a logical partition rather than physical one. Therefore, the partition of VLANs can be performed regardless of physical locations, and the broadcast, multicast and unicast traffic within a VLAN is separated from the other VLANs.

With the aforementioned features, VLAN technology provides us with the following convenience:

- Improving network performance
- Saving network resources
- Simplifying Network Management
- Lowering network cost
- Enhancing network security

VLAN and GVRP (GARP VLAN Registration Protocol) defined by 802.1Q are implemented in ES4626/ES4650 switch. The chapter will describe the use and configuration of VLAN and GVRP in details.

5.1.2 VLAN Configuration Task List

1. Creating or deleting VLAN
2. Assigning Switch ports for VLAN
3. Set The Switch Port Type
4. Set Trunk port
5. Set Access port
6. Enable/Disable VLAN ingress rules on ports
7. Configure Private VLAN
8. Set Private VLAN association

1. Creating or deleting VLAN

Command	Explanation
Global Mode	
vlan <*vlan-id*> [name <*vlan-name*>] **no vlan <*vlan-id*>[name]**	Create/delete VLAN or enter VLAN Mode and Set or delete VLAN name

2. Assigning Switch ports for VLAN

Command	Explanation
VLAN Mode	
switchport interface <*interface-list*> **no switchport interface <*interface-list*>**	Assign Switch ports to VLAN

3. Set The Switch Port Type

Command	Explanation
Interface Mode	
switchport mode {trunk|access}	Set the current port as Trunk or Access port.

4. Set Trunk port

Command	Explanation
Interface Mode	
switchport trunk allowed vlan {<*vlan-list*>|all} **no switchport trunk allowed vlan <*vlan-list*>**	Set/delete VLAN allowed to be crossed by Trunk. The “no” command restores the default setting.
switchport trunk native vlan <*vlan-id*> **no switchport trunk native vlan**	Set/delete PVID for Trunk port.

5. Set Access port

Command	Explanation
Interface Mode	
switchport access vlan <*vlan-id*> **no switchport access vlan**	Add the current port to specified VLAN the specified VLANs. The “no”. command restores the default setting.

6. Disable/Enable VLAN Ingress Rules

Command	Explanation
Global Mode	
switchport ingress-filtering **no switchport ingress-filtering**	Enable/Disable VLAN ingress rules

7. Configure Private VLAN

Command	Explanation
VLAN mode	
private-vlan {primary|isolated|community} **no private-vlan**	Configure current VLAN to Private VLAN. The “no” command delete private VLAN.

8. Set Private VLAN association

Command	Explanation
VLAN mode	
private-vlan association <*secondary-vlan-list*> **no private-vlan association**	Set/delete Private VLAN association

5.1.3 Commands For Vlan Configuration

5.1.3.1 vlan

Command: vlan <*vlan-id*>[name <*vlan-name*>]

no vlan <*vlan-id*>[name]

Function: Create a VLAN and enter VLAN configuration mode, and can set VLAN name. In VLAN Mode, the user can assign the switch ports to the VLAN. The "**no vlan <*vlan-id*>**" command deletes specified VLANs.

Parameter: <*vlan-id*> is the VLAN ID to be created/deleted, valid range is 1 to 4094.

<*vlan-name*> is the name that **create VLAN,** valid range is 1 to 16 characters

Command mode: Global Mode

Default: Only VLAN1 is set by default.

Usage Guide: VLAN1 is the default VLAN and cannot be configured or deleted by the user. The maximal VLAN number is 4094. It should be noted that dynamic VLANs learnt by GVRP cannot be deleted by this command.

Example: Create VLAN100 and enter the configuration mode for VLAN 100.

Switch(Config)#vlan 100

Switch(Config-Vlan100)#

5.1.3.2 private-vlan

Command: private-vlan {primary|isolated|community}

no private-vlan

Function: Configure current VLAN to Private VLAN. The "**no private-vlan**" command cancels the Private VLAN configuration.

Parameter: **primary** set current VLAN to Primary VLAN, **isolated** set current VLAN to Isolated VLAN, **community** set current VLAN to Community VLAN.

Command Mode: VLAN mode

Default: There are three Private VLANs: **Primary** VLAN, **Isolated** VLAN and **Community** VLAN. Ports in Primary there are three Private VLANs: Primary VLAN, Isolated VLAN and Community VLAN can communicate with ports of Isolated VLAN and Community VLAN related to this Primary VLAN; Ports in Isolated VLAN are isolated between each other and only communicate with ports in Primary VLAN they related to; ports in Community VLAN can communicate both with each other and with Primary VLAN ports they related to; there is no communication between ports in Community VLAN and port in Isolated VLAN.

Only VLANs containing empty Ethernet ports can be set to Private VLAN, and only the Private VLANs configured with associated private relationships can set the Access

Ethernet ports their member ports. Normal VLAN will clear its Ethernet ports when set to Private VLAN.

It is to be noted Private VLAN messages will not be transmitted by GVRP.

Example: Set VLAN100、200、300 to private vlans, with respectively primary、Isolated、Community types.

Switch(Config)#vlan 100
Switch(Config-Vlan100)#private-vlan primary
Switch(Config-Vlan100)#exit
Switch(Config)#vlan 200
Switch(Config-Vlan200)#private-vlan isolated
Switch(Config-Vlan200)#exit
Switch(Config)#vlan 300
Switch(Config-Vlan300)#private-vlan community
Switch(Config-Vlan300)#exit

5.1.3.3 private-vlan association

Command: private-vlan association <*secondary-vlan-list*>
no private-vlan association

Function: Set Private VLAN association; the "**no private-vlan association**" command cancels Private VLAN association.

Parameter: <*secondary-vlan-list*> Sets Secondary VLAN list which is associated to Primary VLAN. There are two types of Secondary VLAN: Isolated VLAN and Community VLAN. Users can set multiple Secondary VLANs by ";".

Command mode: VLAN Mode

Default: There is no Private VLAN association by default.

Usage Guide: This command can only used for Private VLAN. The ports in Secondary VLANs which are associated to Primary VLAN can communicate to the ports in Primary VLAN. Before setting Private VLAN association, three types of Private VLANs should have no member ports; the Private VLAN with Private VLAN association can't be deleted. When users delete Private VLAN association, all the member ports in the Private VLANs whose association is deleted are removed from the Private VLANs.

Example: Associate Isolated VLAN200 and Community VLAN300 to Primary VLAN100.

Switch(Config-Vlan100)#private-vlan association 200;300

5.1.3.4 show vlan

Command: show vlan [brief| summary] [id <*vlan-id*>] [name <*vlan-name*>]

Function: Display detailed information for all VLANs or specified VLAN.

Parameter: brief stands for brief information; **summary** for VLAN statistics; **<*vlan-id*>**

for VLAN ID of the VLAN to display status information, the valid range is 1 to 4094; ***<vlan-name>*** is the VLAN name for the VLAN to display status information, valid length is 1 to 11 characters.

Command mode: Admin Mode

Usage Guide: If no ***<vlan-id>*** or ***<vlan-name>*** is specified, then information for all VLANs in the switch will be displayed.

Example: Display the status for the current VLAN; display statistics for the current VLAN.

Switch#show vlan

VLAN	Name	Type	Media	Ports
1	default	Static	ENET	Ethernet1/1 Ethernet1/2
				Ethernet1/3 Ethernet1/4
				Ethernet1/9 Ethernet1/10
				Ethernet1/11 Ethernet1/12
2	VLAN0002	Static	ENET	Ethernet1/5 Ethernet1/6
				Ethernet1/7 Ethernet1/8

Switch#sh vlan summary

The max vlan entries: 4094

Universal Vlan:

1 2

Total Existing Vlans is: 2

Displayed information	Explanation
VLAN	VLAN number
Name	VLAN name
Type	VLAN type, statically configured or dynamically learned.
Media	VLAN interface type: Ethernet
Ports	Access port within a VLAN
Universal Vlan	Universal VLAN.
Dynamic Vlan	Dynamic VLAN (not shown in this example)

5.1.3.5 switchport access vlan

Command: switchport access vlan <*vlan-id*>

no switchport access vlan

Function: Add the current Access port to the specified VLAN. The "**no switchport access vlan**" command deletes the current port from the specified VLAN, and the port will be partitioned to VLAN1.

Parameter: <*vlan-id*> is the VID for the VLAN to be added the current port, valid range is 1 to 4094.

Command mode: Interface Mode

Default: All ports belong to VLAN1 by default.

Usage Guide: Only ports in Access mode can join specified VLANs, and an Access port can only join one VLAN at a time.

Example: Add some Access port to VLAN100.

Switch(Config)#interface ethernet 1/8

Switch(Config-ethernet1/8)#switchport mode access

Switch(Config-ethernet1/8)#switchport access vlan 100

Switch(Config-ethernet1/8)#exit

5.1.3.6 switchport interface

Command: switchport interface <*interface-list*>

no switchport interface <*interface-list*>

Function: Specify Ethernet port to VLAN; the "**no switchport interface <*interface-list*>**" command deletes one or one set of ports from the specified VLAN.

Parameter: <*interface-list*> is the port list to be added or deleted, ";" and "-" are supported, for **example:** ethernet 1/1;2;5 or ethernet 1/1-6;8.

Command mode: VLAN Mode

Default: A newly created VLAN contains no port by default.

Usage Guide: Access ports are normal ports and can join a VLAN, but a port can only join one VLAN for a time.

Example: Assign Ethernet port 1, 3, 4-7, 8 of VLAN100.

Switch(Config-Vlan100)#switchport interface ethernet 1/1;3;4-7;8

5.1.3.7 switchport mode

Command: switchport mode {trunk|access}

Function: Set the port in access mode or trunk mode.

Parameter: trunk means the port allows traffic of multiple VLAN; **access** indicates the port belongs to one VLAN only.

Command mode: Interface Mode

Default: The port is in Access mode by default.

Usage Guide: Ports in trunk mode is called Trunk ports. Trunk ports can allow traffic of multiple VLANs to pass through. VLAN in different switches can be interconnected with the Trunk ports. Ports under access mode are called Access ports. An access port can be assigned to one and only one VLAN at a time.

Example: Set port 1/5 to trunk mode and port 1/8 to access mode.

Switch(Config)#interface ethernet 1/5
Switch(Config-ethernet1/5)#switchport mode trunk
Switch(Config-ethernet1/5)#exit
Switch(Config)#interface ethernet 1/8
Switch(Config-ethernet1/8)#switchport mode access
Switch(Config-ethernet1/8)#exit

5.1.3.8 switchport trunk allowed vlan

Command: switchport trunk allowed vlan {<*vlan-list*>|all}
no switchport trunk allowed vlan

Function: Set trunk port to allow VLAN traffic; the "**no switchport trunk allowed vlan**" command restores the default setting.

Parameter: <*vlan-list*> is the list of VLANs allowed to pass through in the specified Trunk port; keyword "**all"** indicate allow all VLAN traffic on the Trunk port.

Command mode: Interface Mode

Default: Trunk port allows all VLAN traffic by default.

Usage Guide: The user can use this command to set the VLAN traffic allowed to pass though the trunk port; traffic of VLANs not included are prohibited.

Example: Set Trunk port to allow traffic of VLAN1, 3, 5-20.

Switch(Config)#interface ethernet 1/5
Switch(Config-ethernet1/5)#switchport mode trunk
Switch(Config-ethernet1/5)#switchport trunk allowed vlan 1;3;5-20
Switch(Config-ethernet1/5)#exit

5.1.3.9 switchport trunk native vlan

Command: switchport trunk native vlan <*vlan-id*>
no switchport trunk native vlan

Function: Set the PVID for Trunk port; the "**no switchport trunk native vlan**" command restores the default setting.

Parameter: <*vlan-id*> is the PVID for Trunk port.

Command mode: Interface Mode

Default: The default PVID of Trunk port is 1.

Usage Guide: PVID concept is defined in 802.1Q. PVID in Trunk port is used to tag untagged frames. When a untagged frame enters a Trunk port, the port will tag the untagged frame with the native PVID set with this commands for VLAN forwarding.

Example: Set the native VLAN for a Trunk port to 100.

Switch(Config)#interface ethernet 1/5
Switch(Config-ethernet1/5)#switchport mode trunk

Switch(Config-ethernet1/5)#switchport trunk native vlan 100
Switch(Config-ethernet1/5)#exit

5.1.3.10 switchport ingress-filtering

Command: switchport ingress-filtering
no switchport ingress-filtering

Function: Enable the VLAN ingress rule for a port; the "**no vlan ingress disable**" command disables the ingress rule.

Command mode: Interface Mode

Default: VLAN ingress rules are enabled by default.

Usage Guide: When VLAN ingress rules are enabled on the port, when the system receives data it will check source port first, and forwards the data to the destination port if it is a VLAN member port.

Example: Disable VLAN ingress rules on the port

Switch(Config-Ethernet1/1)# no switchport ingress-filtering

5.1.4 Typical VLAN Application

Scenario:

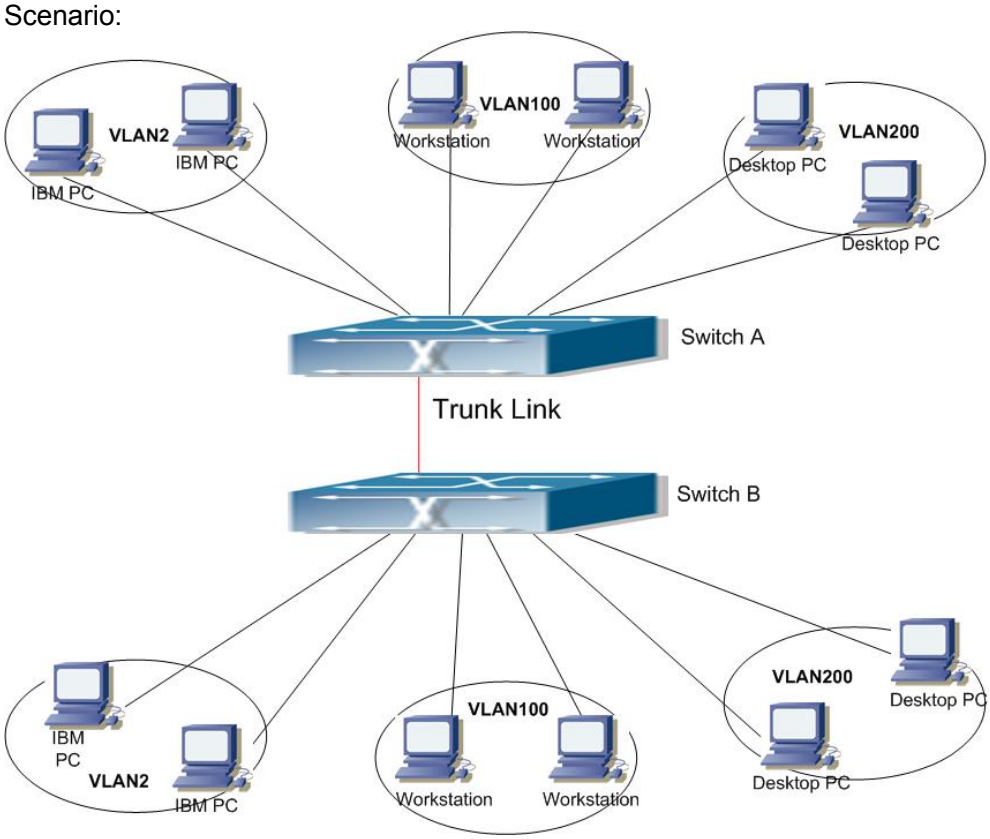


Fig 5-2 Typical VLAN Application Topology

The existing LAN is required to be partitioned to 3 VLANs due to security and application requirements. The three VLANs are VLAN2, VLAN100 and VLAN200. Those three VLANs are cross two different location A and B. One switch is placed in each site, and cross-location requirement can be met if VLAN traffic can be transferred between the two switches.

Configuration Item	**Configuration description**
VLAN2	Site A and site B switch port 2 -4.
VLAN100	Site A and site B switch port 5 -7.
VLAN200	Site A and site B switch port 8 -10.
Trunk port	Site A and site B switch port 11.

Connect the Trunk ports of both switches for a Trunk link to convey the cross-switch VLAN traffic; connect all network devices to the other ports of corresponding VLANs.

In this example, port 1 and port 12 is spared and can be used for management port or for other purposes.

The configuration steps are listed below:

Switch A:

```
Switch(Config)#vlan 2
Switch(Config-Vlan2)#switchport interface ethernet 1/2-4
Switch(Config-Vlan2)#exit
Switch(Config)#vlan 100
Switch(Config-Vlan100)#switchport interface ethernet 1/5-7
Switch(Config-Vlan100)#exit
Switch(Config)#vlan 200
Switch(Config-Vlan200)#switchport interface ethernet 1/8-10
Switch(Config-Vlan200)#exit
Switch(Config)#interface ethernet 1/11
Switch(Config-Ethernet1/11)#switchport mode trunk
Switch(Config-Ethernet1/11)#exit
Switch(Config)#
```

Switch B:

```
Switch(Config)#vlan 2
Switch(Config-Vlan2)#switchport interface ethernet 1/2-4
Switch(Config-Vlan2)#exit
Switch(Config)#vlan 100
Switch(Config-Vlan100)#switchport interface ethernet 1/5-7
Switch(Config-Vlan100)#exit
Switch(Config)#vlan 200
```

```
Switch(Config-Vlan200)#switchport interface ethernet 1/8-10
Switch(Config-Vlan200)#exit
Switch(Config)#interface ethernet 1/11
Switch(Config-Ethernet1/11)#switchport mode trunk
Switch(Config-Ethernet1/11)#exit
```

5.2 GVRP Configuration

5.2.1 Introduction to GVRP

GARP (Generic Attribute Registration Protocol) can be used to dynamically distribute, populate and register property information between switch members within a switch network, the property can be VLAN information, Multicast MAC address of the other information. As a matter of fact, GARP protocol can convey multiple property features the switch need to populate. Various GARP applications are defined on the basis of GARP, which are called GARP application entities, and GVRP is one of them.

GVRP (GARP VLAN Registration Protocol) is an application based on GARP working mechanism. It is responsible for the maintenance of dynamic VLAN register information and population of such register information to the other switches. Switches support GVRP can receive VLAN dynamic register information from the other switches, and update local VLAN register information according the information received. The switch enabled GVRP can also populate their own VLAN register information to the other switches. The populated VLAN register information includes local static information manually configured and dynamic information learnt from the other switches. Therefore, by populating the VLAN register information, VLAN information consistency can be achieved among all GVRP enabled switches.

5.2.2 GVRP Configuration Task List

1. Configuring GARP Timer Parameters.
2. Enable GVRP function

1. Configuring GARP Timer parameters.

Command	Explanation
Interface Mode	
bridge-ext garp timer join <*timer-value*> **no bridge-ext garp timer join** **bridge-ext garp timer leave <*timer-value*>** **no bridge-ext garp timer leave** **bridge-ext garp timer hold <*timer-value*>** **no bridge-ext garp timer hold**	Configure the hold, join and leave timers for GARP.
Global Mode	
bridge-ext garp timer leave all <*timer-value*> **no bridge-ext garp timer leave all**	Configure the leave all timer for GARP.

2. Enable GVRP function

Command	Explanation
Interface Mode	
bridge-ext gvrp **no bridge-ext gvrp**	Enable the GVRP function on current port.
Global Mode	
bridge-ext gvrp **no bridge-ext gvrp**	Enable the GVRP function for the switch.

5.2.3 Commands for GVRP

5.2.3.1 bridge-ext gvrp

Command: bridge-ext gvrp

no bridge-ext gvrp

Function: Enable the GVRP function for the switch or the current Trunk port; the "**no gvrp"** command disables the GVRP function globally or for the port**.**

Command mode: Interface Mode and Global Mode.

Default: GVRP is disabled by default.

Usage Guide: Port GVRP can only be enabled after global GVRP is enabled. When global GVRP is disabled, the GVRP configurations in the ports are also disabled. Note: GVRP can only be enabled on Trunk ports.

Example: Enable the GVRP function globally and for Trunk port 1/10.

Switch(Config)# bridge-ext gvrp

Switch(Config)#interface ethernet 1/10

Switch(Config-Ethernet1/10)# bridge-ext gvrp

Switch(Config)#exit

5.2.3.2 debug gvrp

Command: debug gvrp

no debug gvrp

Function: Enable the GVRP debugging function: the " no debug gvrp**"** command disables the function**.**

Command mode: Admin Mode

Default: GVRP debug information is disabled by default.

Usage Guide: Use this command to enable GVRP debugging, GVRP packet processing information can be displayed.

Example: Enable GVRP debugging.

Switch#debug gvrp

5.2.3.3 bridge-ext garp timer hold

Command:bridge-ext garp timer hold <*timer-value*>

no bridge-ext garp timer hold

Function: Set the hold timer for GARP; the " no garp timer hold" command restores the default timer setting.

Parameter:<*timer-value*> is the value for GARP **hold** timer, the valid range is 100 to 327650 ms.

Command mode: Interface Mode

Default: The default value for hold timer is 100 ms.

Usage Guide: When GARP application entities receive a join message, join message will not be sent immediately. Instead, hold timer is started. After hold timer timeout, all join messages received with the hold time will be sent in one GVRP frame, thus effectively reducing protocol message traffic.

Example: Set the GARP hold timer value of port 1/10 to 500 ms.

Switch(Config-Ethernet1/10)#bridge-ext garp timer hold 500

5.2.3.4 bridge-ext garp timer join

Command: bridge-ext garp timer join <*timer-value*>

no bridge-ext garp timer join

Function: Set the join timer for GARP; the "**no bridge-ext garp timer join**" command restores the default timer setting.

Parameter:<*timer-value*> is the value for join timer, the valid range is 100 to 327650 ms.

Command mode: Interface Mode

Default: The default value for join timer is 200 ms.

Usage Guide: GARP application entity sends a join message after join timer over, other GARP application entities received the join message will register this message.

Example: Set the GARP join timer value of port 1/10 to 1000 ms.

Switch(Config-Ethernet1/10)#bridge-ext garp timer join 1000

5.2.3.5 bridge-ext garp timer leave

Command:bridge-ext garp timer leave <*timer-value*>

no bridge-ext garp timer leave

Function: Set the leave timer for GARP;the "**no bridge-ext garp timer leave**" command restores the default timer setting.

Parameter:<*timer-value*>is the value for leave timer,the valid range is 100 to 327650 ms.

Command mode: Interface Mode

Usage Guide: When GARP application entity wants to cancel a certain property information, it sends a leave message.GARP application entities receiving this message will start the leave timer,if no join message is received before leave timer timeout, the property information will be canceled.Besides, the value of leave timer must be twice larger than the join timer. Otherwise,an error message will be displayed.

Example: Set the GARP leave timer value of port 1/10 to 3000 ms.

Switch(Config-Ethernet1/10)#bridge-ext garp timer leave 3000

5.2.3.6 bridge-ext garp timer leaveall

Command:bridge-ext garp timer leaveall <*timer-value*>

no bridge-ext garp timer leaveall

Function: Set the leaveall timer for GARP;the"**no bridge-ext garp timer leaveall**" command restores the default timer setting.

Parameter: <*timer-value*> is the value for GARP leaveall timer, the valid range is 100 to 327650 ms.

Command mode: Global Mode

Default: The default value for leaveall timer is 10000 ms.

Usage Guide: When a GARP application entity starts, the leaveall timer is started at the same time. When the leaveall timer is over, the GARP application entity will send a leaveall message. Other application entities will cancel all property information for that application entity, and the leaveall timer is cleared for a new cycle.

Example: Set the GARP leaveall timer value to 50000 ms.

Switch(Config)#bridge-ext garp timer leaveall 50000

5.2.3.7 show garp timer

Command: show garp timer [<*interface-name*>]

Function: Display the global and port information for GARP.

Parameter: <*interface-nam*> stands for the name of the Trunk port to be displayed.

Command mode: Admin Mode

Usage Guide: N/A.

Example: Display global GARP information.

Switch #show garp timer

5.2.3.8 show gvrp configuration

Command: show gvrp configuration [<*interface-name*>]

Function: Display the global and port information for GVRP.

Parameter: <*interface-nam*> stands for the name of the Trunk port to be displayed.

Command mode: Admin Mode

Usage Guide: N/A.

Example: Display global GVRP information.

Switch#show gvrp configuration

---------- Gvrp Information ----------

Gvrp status : enable

Gvrp Timers(milliseconds)

LeaveAll : 10000

5.2.4 Typical GVRP Application

Scenario:

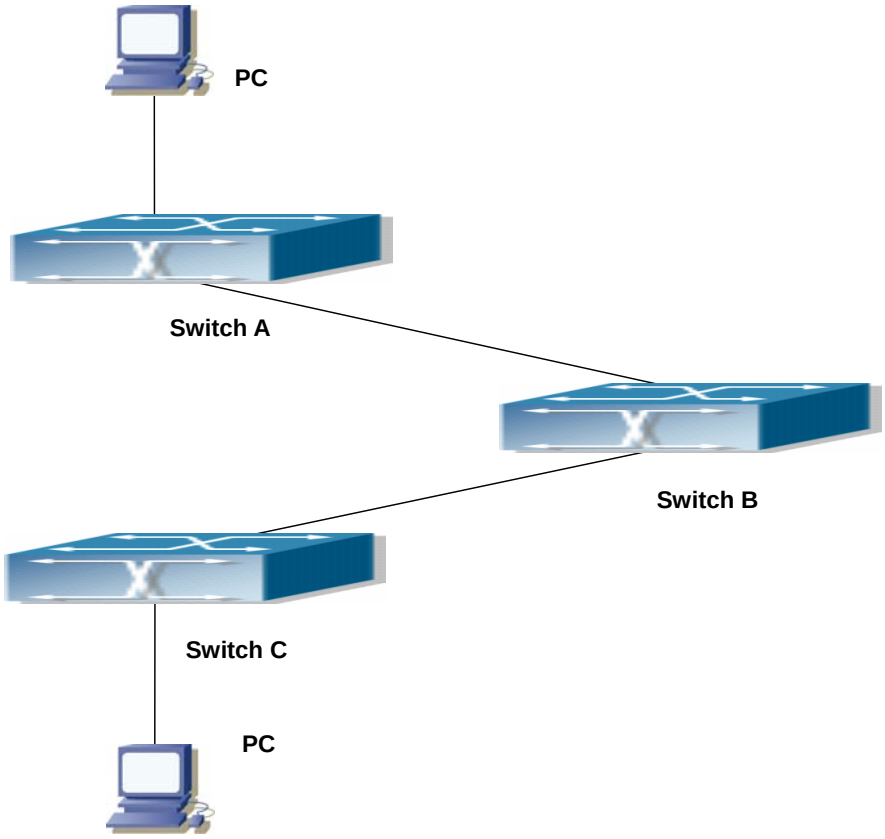


Fig 5-3 Typical GVRP Application Topology

To enable dynamic VLAN information register and update among switches, GVRP protocol is to be configured in the switch. Configure GVRP in Switch A, B and C, enable Switch B to learn VLAN100 dynamically so that the two workstation connected to VLAN100 in Switch A and C can communicate with each other through Switch B without static VLAN100 entries.

Configuration Item	Configuration description
VLAN100	Port 2 -6 of Switch A and C
Trunk port	Port 11 of Switch A and C, Port 10, 11 of Switch B
Global GVRP	Switch A, B, C:
Port GVRP	Port 11 of Switch A and C, Port 10, 11 of Switch B

Connect the two workstation to the VLAN100 ports in switch A and B, connect port 11 of Switch A to port 10 of Switch B, and port 11 of Switch B to port 11 of Switch C. All ports are on Switch A, B and C.

The configuration steps are listed below:

Switch A:

Switch(Config)# bridge-ext gvrp

Switch(Config)#vlan 100

Switch(Config-Vlan100)#switchport interface ethernet 1/2-6

```
Switch(Config-Vlan100)#exit
Switch(Config)#interface Ethernet 1/11
Switch(Config-Ethernet1/11)#switchport mode trunk
Switch(Config-Ethernet1/11)# bridge-ext gvrp
Switch(Config-Ethernet1/11)#exit
Switch B:
Switch(Config)# bridge-ext gvrp
Switch(Config)#interface ethernet 1/10
Switch(Config-Ethernet1/10)#switchport mode trunk
Switch(Config-Ethernet1/10)# bridge-ext gvrp
Switch(Config-Ethernet1/10)#exit
Switch(Config)#interface ethernet 1/11
Switch(Config-Ethernet1/11)#switchport mode trunk
Switch(Config-Ethernet1/11)# bridge-ext gvrp
Switch(Config-Ethernet1/11)#exit
Switch C:
Switch(Config)# bridge-ext gvrp
Switch(Config)#vlan 100
Switch(Config-Vlan100)#switchport interface ethernet 1/2-6
Switch(Config-Vlan100)#exit
Switch(Config)#interface ethernet 1/11
Switch(Config-Ethernet1/11)#switchport mode trunk
Switch(Config-Ethernet1/11)# bridge-ext gvrp
Switch(Config-Ethernet1/11)#exit
```

5.2.5 GVRP Troubleshooting

☞ The GARP counter setting in for Trunk ports in both ends of Trunk link must be the same, otherwise GVRP will not work properly.It is recommended to avoid enabling GVRP and RSTP at the same time in ES4626/ES4650 switch. If GVRP is to be enabled, RSTP function for the ports must be disabled first.

5.3 Dot1q-tunnel Configuration

5.3.1 Dot1q-tunnel Introduction

Dot1q-tunnel is also called QinQ (802.1Q-in-802.1Q), which is an expansion of 802.1Q. Its dominating idea is encapsulating the customer VLAN tag (CVLAN tag) to the service provider VLAN tag (SPVLAN tag). Carrying the two VLAN tags the packet is transmitted through the backbone network of the ISP internet, so to provide a simple layer-2 tunnel for the users. It is simple and easy to manage, applicable only by static configuration, and especially adaptive to small office network or small scale metropolitan area network using layer-3 switch as backbone equipment.

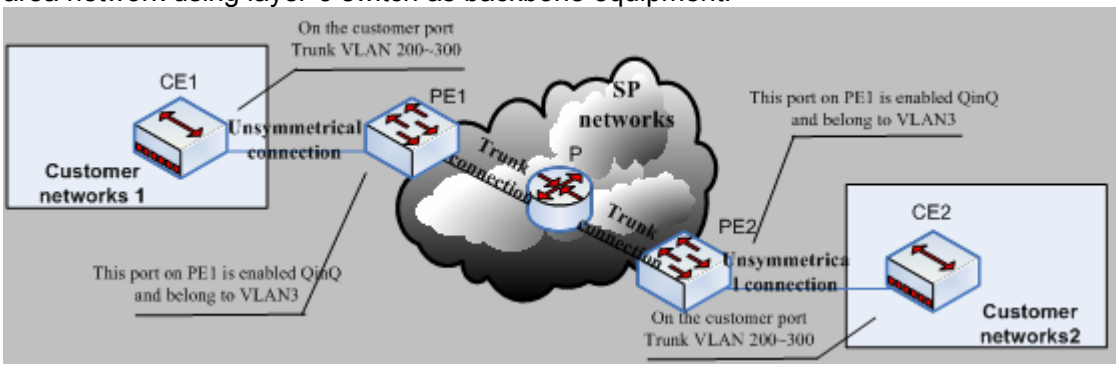


Fig 5-4 Dot1q-tunnel based Internetworking mode

As shown in Fig 5-4, after being enabled on the user port, dot1q-tunnel assigns each user an SPVLAN identification (SPVID). Here the identification of user is 3. Same SPVID should be assigned for the same network user on different PEs. When packet reaches PE1 from CE1, it carries the VLAN tag 200-300 of the user internal network. Since the dot1q-tunnel function is enabled, the user port on PE1 will add on the packet another VLAN tag, of which the ID is the SPVID assigned to the user. Afterwards, the packet will only be transmitted in VLAN3 when traveling in the ISP internet network while carrying two VLAN tags (the inner tag is added when entering PE1, and the outer is SPVID), whereas the VLAN information of the user network is open to the provider network. When the packet reaches PE2 and before being forwarded to CE2 from the client port on PE2, the outer VLAN tag is removed, then the packet CE2 receives is absolutely identical to the one sent by CE1. For the user, the role the operator network plays between PE1 and PE2,is to provide a reliable layer-2 link.

The technology of Dot1q-tunnel provides the ISP internet the ability of supporting many client VLANs by only one VLAN of themselves. Both the ISP internet and the clients can configure their own VLAN independently.

It is obvious that, the dot1q-tunnel function has got following characteristics:

- Applicable through simple static configuration, no complex configuration or maintenance to be needed.
- Operators will only have to assign one SPVID for each user, which increases the number of concurrent supportable users; while the users has got the ultimate freedom in selecting and managing the VLAN IDs (select within 1~4094

at users' will).

- The user network is considerably independent. When the ISP internet is upgrading their network, the user networks do not have to change their original configuration.

Detailed description on the application and configuration of dot1q-tunnel of ES4626 will be provided in this section

5.3.2 Dot1q-tunnel Configuration

5.3.2.1 Configuration task sequence of Dot1q-tunnel

1) Configure the dot1q-tunnel function on the ports
2) Configure the type of protocol (TPID) on the ports

1. Configure the dot1q-tunnel function on the ports

Command	Explanation
Port mode	
dot1q-tunnel enable **no dot1q-tunnel enable**	Enter/exit the dot1q-tunnel mode on the ports.

2. Configure the type of protocol (TPID) of the port

Command	Explanation
Port mode	
dot1q-tunnel tpid {8100|9100|9200|<0-65535>}	Configure the type of protocol on the ports.

5.3.3 Dot1q-Tunnel Configuration Command

5.3.3.1 dot1q-tunnel enable

Command: dot1q-tunnel enable
no dot1q-tunnel enable

Function: Set the access port of the switch to dot1q-tunnel mode; the "**no dot1q-tunnel enable**" command restores to default.

Parameter: None.

Command Mode: Port Mode.

Default: Dot1q-tunnel function disabled on the port by default.

Usage Guide: After enabling dot1q-tunnel on the port, data packets without VLAN tag

(referred to as tag) will be packed with a tag when entering through the port; those with tag will be packed with an external tag. The TPID in the tag is 8100 and the VLAN ID is the VLAN ID the port belongs to. Data packets with double tags will be forwarded according to MAC address and external tag, till the external tag is removed when transmitted outside from the access port. Since the length of the data packet may be over sized when packed with external tag, it is recommended to use this command associating the Jumbo function. Normally this command is used on access ports, and also on trunk ports however only when associating the VLAN translation function.

Example: Join port1 into VLAN3, enable dot1q-tunnel function.

Switch(Config)#vlan 3
Switch(Config-Vlan3)#switchport interface ethernet 1/1
Switch(Config-Vlan3)#exit
Switch(Config)#interface ethernet 1/1
Switch(Config-Ethernet1/1)# dot1q-tunnel enable
Switch(Config-Ethernet1/1)# exit

5.3.3.2 dot1q-tunnel tpid

Command: dot1q-tunnel tpid {8100|9100|9200|<0-65535>}

Function: Configure the type (TPID) of the protocol of switch trunk port.

Parameter: None.

Command Mode: Port Mode.

Default: TPID on the port is defaulted at 8100.

Usage Guide: This function is to facilitate internetworking with equipments of other manufacturers. If the equipment connected with the switch trunk port sends data packet with a TPID of 9100, the port TPID will be set to 9100, this way switch will receive and process data packets normally.

Example: Set port10 of the switch to trunk port and sends data packet with a TPID of 9100

Switch(Config)#interface ethernet 1/10
Switch(Config-Ethernet1/10)#switchport mode trunk
Switch(Config-Ethernet1/10)#dot1q-tunnel tpid 9100
Switch(Config-Ethernet1/10)#exit

5.3.3.3 show dot1q-tunnel

Command: show dot1q-tunnel

Function: Display the information of all the ports at dot1q-tunnel state.

Parameter: None.

Command Mode: Admin Mode.

Usage Guide: This command is used for displaying the information of the ports at dot1q-tunnel state.

Example: Display current dot1q-tunnel state.

Switch#show dot1q-tunnel

Interface Ethernet1/1:

dot1q-tunnel is enable

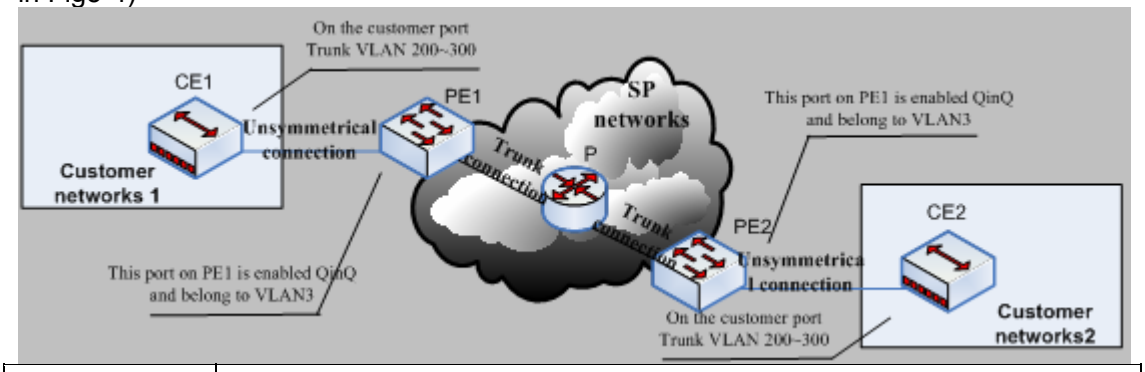
Interface Ethernet1/3:

dot1q-tunnel is enable

5.3.4 Typical Applications Of The Dot1q-tunnel

Scenario

Edge switch PE1 and PE2 of the ISP internet forward the VLAN200~300 data between CE1 and CE2 of the client network with VLAN3. The port1 of PE1 is connected to CE1, port10 is connected to public network, the TPID of the connected equipment is 9100; port1 of PE2 is connected to CE2, port10 is connected to public network.(as shown in Fig5-4)



Configuration Item	Configuration Explanation
VLAN3	Port1 of PE1 and PE2
dot1q-tunnel	Port1 of PE1 and PE2
tpid	Port10 of PE1
Trunk port	Port10 of PE1 and PE2

Configuration procedure is as follows:

PE1:

Switch (Config)#vlan 3

Switch (Config-Vlan3)#switchport interface ethernet 1/1

Switch (Config-Vlan3)#exit

Switch (Config)#interface ethernet 1/1

Switch (Config-Ethernet1/1)# dot1q-tunnel enable

Switch (Config-Ethernet1/1)# exit
Switch (Config)#interface ethernet 1/10
Switch (Config-Ethernet1/10)#switchport mode trunk
Switch (Config-Ethernet1/10)#dot1q-tunnel tpid 9100
Switch (Config-Ethernet1/10)#exit
Switch (Config)#
PE2:
Switch (Config)#vlan 3
Switch (Config-Vlan3)#switchport interface ethernet 1/1
Switch (Config-Vlan3)#exit
Switch (Config)#interface ethernet 1/1
Switch (Config-Ethernet1/1)# dot1q-tunnel enable
Switch (Config-Ethernet1/1)# exit
Switch (Config)#interface ethernet 1/10
Switch (Config-Ethernet1/10)#switchport mode trunk
Switch (Config-Ethernet1/10)#exit
Switch (Config)#

5.3.5 Dot1q-tunnel Troubleshooting

- Enabling dot1q-tunnel on Trunk port will make the tag of the data packet unpredictable which is not required in the application. So it is not recommended to enable dot1q-tunnel on Trunk port except the VLAN-translation is in operation.
  - STP/MSTP
  - PVLAN
  - QoS/ACL
  - GVRP
  - 802.1x
  - IGMP Snooping
- Configuring in port-channel is not supported

5.4 VLAN-translation Configuration

5.4.1 VLAN-translation Introduction

VLAN translation, as one can tell from the name, which translates the original VLAN

ID to new VLAN ID according to the user requirements so to exchange data across different VLANs. The VLAN translation is classified to ingress translation and egress translation, respectively translation the VLAN ID at the entrance or exit.

Application and configuration of VLAN translation will be explained in detail in this section.

5.4.2 VLAN-translation Configuration

5.4.2.1 Configuration task sequence of VLAN-translation

1. Configure the VLAN-translation function on the port
2. Configure the VLAN-translation relations on the port
3. Configure the VLAN-translation packet dropped on port if there is any failure.

1. Configure the VLAN-translation of the port

Command	Explanation
Port mode	
vlan-translation enable **no vlan-translation enable**	Enter/exit the port VLAN-translation mode

2. Configure the VLAN-translation relation of the port

Command	Explanation
Port mode	
vlan-translation <*old-vlan-id*> to <*new-vlan-id*> {in|out} **no vlan-translation *old-vlan-id* {in|out}**	Add/delete a VLAN-translation relation

3. Configure the VLAN-translation relation, check if there is any failure or packet dropped

Command	Explanation
Port mode	
vlan-translation miss drop {in|out|both} **no vlan-translation miss drop {in|out|both}**	Configure the VLAN-translation packet dropped on port if there is any failure.

5.4.3 Commands for VLAN-Translation Configuration

5.4.3.1 show vlan-translation

Command: show vlan-translation

Function: Display the information of all the ports at VLAN-translation state.

Parameter: None.

Command Mode: Admin Mode.

Usage Guide: Display the information of all the ports at VLAN-translation state, including enabling, packet dropped, direction and other information.

Example: Display current VLAN translation state information.

Switch#show vlan-translation

Interface Ethernet1/1:

vlan-translation is enable, miss drop is set in

Interface Ethernet1/2:

vlan-translation is enable, miss drop is not set

Interface Ethernet1/3:

vlan-translation is enable, miss drop is set both

5.4.3.2 vlan-translation

Command: vlan-translation <*old-vlan-id*> to <*new-vlan-id*> {in|out}

no vlan-translation <*old-vlan-id*> {in|out}

Function: Add VLAN translation by creating a mapping between original VLAN ID and current VLAN ID; the “no” form of this command deletes corresponding mapping.

Parameter: old-vlan-id is the original VLAN ID;new-vlan-id is the translated VLAN ID;in indicates entrance translation;out indicates exit translation.

Command Mode: Port Mode.

Default: The command is for configuring the in and out translation relation of the VLAN translation function. The data packets will be matched according to the configured translation relations, and its VLAN ID will be changed to the one in the configured item once matched, while the “vlan-translation miss drop” command will determine the next forwarding if not match. Same original VLAN ID and same current VLAN ID can be configured in different directions, however , the original and the current VLAN ID must not be the same.

Example: Move the VLAN100 data entered from the port1 to VLAN2 after entrance translation, and the data traffic out from VLAN2 to VLAN100 after exit translation.

Switch#config

Switch(config)#interface ethernet 4/1

Switch(Config-If-Ethernet4/1)#dot1q-tunnel enable

Switch(Config-If-Ethernet4/1)#vlan-translation enable

Switch(Config-If-Ethernet4/1)#vlan-translation 100 to 2 in

Switch(Config-If-Ethernet4/1)#vlan-translation 2 to 100 out

Switch(Config-If-Ethernet4/1)#exit
Switch(config)#

5.4.3.3 vlan-translation enable

Command: vlan-translation enable
no vlan-translation enable
Function: Enable VLAN translation on specified trunk port of the switch; the "**no vlan-translation enable**" command restores to the default value.
Parameter: None.
Command Mode: Port Mode.
Default: VLAN translation has not been enabled on the port by default.
Usage Guide: To apply VLAN translation on the port the dot1q-tunnel function must be first enabled and configured at trunk port.
Example: Enable VLAN translation function on port1
Switch#config
Switch(config)#interface ethernet 4/1
Switch(Config-If-Ethernet4/1)#dot1q-tunnel enable
Switch(Config-If-Ethernet4/1)#vlan-translation enable

5.4.3.4 vlan-translation miss drop

Command: vlan-translation miss drop {in|out|both}
no vlan-translation miss drop {in|out|both}
Function: Set to packet dropping upon translation failure; the "no" form of this command restores to the default value.
Parameter: In refers to entrance; out indicates exit; both represents bidirectional.
Command Mode: Port Mode.
Default: No packet dropping upon translation failure by default.
Usage Guide: When performing the mapping translation between the original and the current VID, if no translation correspondence is configured, the packet will not be dropped by default, but will after use this command.
Example: Set to packet dropped at entrance of port1 when translation fails.
Switch(Config-If-Ethernet4/1)#vlan-translation miss drop in

5.4.4 Typical application of VLAN-translation

Scenario

Edge switch PE1 and PE2 of the ISP internet support the VLAN20 data task between CE1 and CE2 of the client network with VLAN3. The port1 of PE1 is connected

to CE1, port10 is connected to public network; port1 of PE2 is connected to CE2, port10 is connected to public network.(as shown in Fig5-4).

Configuration Item	Configuration Explanation
VLAN-translation	Port1 of PE1 and PE2
Trunk port	Port1 and Port10 of PE1 and PE2

Configuration procedure is as follows

PE1、PE2:

Switch (Config)#interface ethernet 1/1
Switch (Config-Ethernet1/1)#switchport mode trunk
Switch (Config-Ethernet1/1)# dot1q-tunnel enable
Switch (Config-Ethernet1/1)# vlan-translation enable
Switch (Config-Ethernet1/1)# vlan-translation 20 to 3 in
Switch (Config-Ethernet1/1)# vlan-translation 3 to 20 out
Switch (Config-Ethernet1/1)# exit
Switch (Config)#interface ethernet 1/10
Switch (Config-Ethernet1/10)#switchport mode trunk
Switch (Config-Ethernet1/10)#exit
Switch (Config)#

5.4.5 VLAN-translation Troubleshooting

- ☞ Normally the VLAN-translation is applied on trunk ports.
- ☞ Normally before using the VLAN-translation, the dot1q-tunnel function needs to be enabled, becoming adaptable to double tag data packet and translating the VLAN normally.
- ☞ Configuring in port-channel is not supported.

5.5 Dynamic VLAN Configuration

5.5.1 Dynamic VLAN Introduction

The dynamic VLAN is named corresponding to the static VLAN (namely the port based VLAN). Dynamic VLAN supported by the ES4626/ES4650 switch includes MAC-based VLAN, IP-subnet-based VLAN and Protocol-based VLAN. Detailed description is as follows

The MAC-based VLAN division is based on the MAC address of each host, namely every host with a MAC address will be assigned to certain VLAN. By the means, the network user will maintain his membership in his belonging VLAN when moves from a physical location to another. As we can see the greatest advantage of this VLAN division is that the VLAN does not have to be re-configured when the user physic location change, namely shift from one switch to another, which is because it is user based, not switch port based

The IP subnet based VLAN is divided according to the source IP address and its subnet mask of every host. It assigns corresponding VLAN ID to the data packet according to the subnet segment, leading the data packet to specified VLAN. Its advantage is the same as that of the MAC-based VLAN: the user does not have to change configuration when relocated.

The VLAN is divided by the network layer protocol, assigning different protocol to different VLANs. This is very attractive to the network administrators who wish to organize the user by applications and services. Moreover the user can move freely within the network while maintaining his membership. Advantage of this method enables user to change physical position without changing their VLAN residing configuration, while the VLAN can be divided by types of protocols which is important to the network administrators. Further, this method has no need of added frame label to identify the VLAN which reduce the network traffic.

5.5.2 Dynamic VLAN Configuration

5.5.2.1 Dynamic VLAN Configuration Task Sequence

1. Configure the MAC-based VLAN function on the port
2. Configure the correspondence between the MAC address and the VLAN
3. Configure the IP-subnet-based VLAN function on the port
4. Configure the correspondence between the IP subnet and the VLAN
5. Configure the correspondence between the Protocols and the VLAN
6. Adjust the priority of the dynamic VLAN

1. Configure the MAC-based VLAN function on the port

Command	Explanation
Port Mode	
switchport mac-vlan enable **no switchport mac-vlan enable**	Enable/disable the MAC-based VLAN function on the port

2. Configure the correspondence between the MAC address and the VLAN

Command	Explanation
Global Mode	
mac-vlan mac <*mac-addrss*> vlan <*vlan-id*> priority <*priority-id*> **no mac-vlan {mac <*mac-addrss*>|all}**	Add/delete the correspondence between the MAC address and the VLAN, namely specified MAC address join/leave specified VLAN

3. Configure the IP-subnet-based VLAN function on the port

Command	Explanation
Port Mode	
switchport subnet-vlan enable **no switchport subnet-vlan enable**	Enable/disable the port IP-subnet-base VLAN function on the port

4. Configure the correspondence between the IP subnet and the VLAN

Command	Explanation
Global Mode	
subnet-vlan ip-address <*ipv4-addrss*> mask <*subnet-mask*> vlan <*vlan-id*> priority <*priority-id*> **no subnet-vlan {ip-address <*ipv4-addrss*> mask <*subnet-mask*>|all}**	Add/delete the correspondence between the IP subnet and the VLAN, namely specified IP subnet joins/leaves specified VLAN

5. Configure the correspondence between the Protocols and the VLAN

Command	Explanation
Global Mode	
protocol-vlan mode {ethernetii etype <*etype-id*>|llc {dsap <*dasp-id*> ssap <*ssap-id*>}|snap etype <*etype-id*>} vlan <*vlan-id*> **no protocol-vlan {mode {ethernetii etype <*etype-id*>|llc {dsap <*dasp-id*> ssap <*ssap-id*>}|snap etype <*etype-id*>}|all}**	Add/delete the correspondence between the Protocols and the VLAN, namely specified protocol joins/leaves specified VLAN

6. Adjust the priority of the dynamic VLAN

Command	Explanation
Global Mode	
dynamic-vlan mac-vlan prefer **dynamic-vlan subnet-vlan prefer**	Configure the priority of the dynamic VLAN

5.5.2.2 Commands for Dynamic VLAN Configuration

5.5.2.2.1 dynamic-vlan mac-vlan prefer

Command: dynamic-vlan mac-vlan prefer

Function: Set the MAC-based VLAN preferred.

Parameter: None

Command Mode: Global Mode

Default: MAC-based VLAN is preferred by default

Usage Guide: Configure the preference of dynamic-vlan on switch. The default priority sequence is MAC-based VLAN、IP-subnet-based VLAN、Protocol-based VLAN, namely the preferred order when several dynamic VLAN is available. After the IP-subnet-based VLAN is set to be preferred and the user wish to restore to preferring the MAC-based VLAN, please use this command

Example: Set the MAC-based VLAN preferred.

Switch#config

Switch(config)#dynamic-vlan mac-vlan prefer

5.5.2.2.2 dynamic-vlan subnet-vlan prefer

Command: dynamic-vlan subnet-vlan prefer

Function: Set the IP-subnet-based VLAN preferred.

Parameter: None

Command Mode: Global Mode

Default: MAC-based VLAN is preferred by default

Usage Guide: Configure the preference of dynamic-vlan on switch. The default priority sequence is MAC-based VLAN、IP-subnet-based VLAN、Protocol-based VLAN, namely the preferred order when several dynamic VLAN is available. This command is used to set to preferring the IP-subnet-based VLAN

Example: Set the IP-subnet-based VLAN preferred.

Switch #config

Switch (config)#dynamic-vlan subnet-vlan prefer

5.5.2.2.3 mac-vlan

Command: mac-vlan mac <*mac-addrss*> vlan <*vlan-id*> priority <*priority-id*>

no mac-vlan {mac <*mac-addrss*>|all}

Function: Add the correspondence between MAC address and VLAN, namely specify certain MAC address to join specified VLAN. The “no” form of this command deletes all/the correspondence.

Parameter:mac-address is the MAC address which is shown in the form of XX-XX-XX-XX-XX-XX,vlan-id is the ID of the VLAN with a valid range of

1~4094;priority-id is the level of priority and is used in the VLAN tag with a valid range of 0~7;all refers to all the MAC addresses.

Command Mode: Global Mode

Default: No MAC address joins the VLAN by default.

Usage Guide: With this command user can add specified MAC address to specified VLAN. If there is a non VLAN label data packet enters from the switch port from the specified MAC address, it will be assigned with specified VLAN ID so sent enter specified VLAN. Their belonging VLAN are the same no matter which port did they enter through. The command does not have any interfere on the VLAN label data packet

Example:

Switch #config

Switch (config)#mac-vlan mac 00-03-0f-11-22-33 vlan 100 priority 0

5.5.2.2.4 protocol-vlan

Command: protocol-vlan mode {ethernetii etype <*etype-id*>|llc {dsap <*dasp-id*> ssap <*ssap-id*>}|snap etype <*etype-id*>} vlan <*vlan-id*>

no protocol-vlan {mode {ethernetii etype <*etype-id*>|llc {dsap <*dasp-id*> ssap <*ssap-id*>}|snap etype <*etype-id*>}|all}

Function: Add the correspondence between the protocol and the VLAN namely specify the protocol to join specified VLAN. The “no” form of this command deletes all/the correspondence

Parameter: Mode is the encapsulate type of the configuration which is ethernetii、llc、snap;the encapsulate type of the ethernetii is EthernetII;etype-id is the type of the packet protocol, with a valid range of 1536~65535;llc is LLC encapsulate format;dasp-id is the access point of the destination service, the valid range is 0~255;aasp-id is the access point of the source service with a valid range of 0~255;snap is SNAP encapsulate format;etype-id is the type of the packet protocol, the valid range is 1536~65535;vlan-id is the ID of VLAN, the valid range is 1~4094;all indicates all the encapsulate protocols.

Command Mode: Global Mode

Default: No protocol joined the VLAN by default

Usage Guide: The command adds specified protocol into specified VLAN. If there is any non VLAN label packet from specified protocol enters through the switch port, it will be assigned with specified VLAN ID and enter the specified VLAN. No matter which port the packets go through, their belonging VLAN is the same. The command will not interfere with VLAN labeled data packets. It is recommended to configure ARP protocol together with the IP protocol or else some application may be affected

Example: Assign the IP protocol data packet encapsulated by the EthernetII to VLAN200

Switch #config

Switch (config)#protocol-vlan mode ethernetii etype 2048 vlan 200

5.5.2.2.5 show dynamic-vlan prefer

Command: show dynamic-vlan prefer

Function: Display the preference of the dynamic VLAN

Parameter: None

Command Mode: Admin Mode

Usage Guide: Display the dynamic VLAN preference

Example: Display current dynamic VLAN preference

Switch #show dynamic-vlan prefer

Mac Vlan/Voice Vlan

IP Subnet Vlan

Proto Vlan

5.5.2.2.6 show mac-vlan

Command: show mac-vlan

Function: Display the configuration of MAC-based VLAN on the switch

Parameter: None

Command Mode: Admin Mode

Usage Guide: Display the configuration of MAC-based VLAN on the switch

Example: Display the configuration of the current MAC-based VLAN

Switch #show mac-vlan

MAC-Address	VLAN_ID
00-e0-4c-77-ab-9d	2
00-0a-eb-26-8d-f3	2
00-03-0f-11-22-33	5

5.5.2.2.7 show mac-vlan interface

Command: show mac-vlan interface

Function: Display the ports at MAC-based VLAN

Parameter: None

Command Mode: Admin Mode

Usage Guide: Display the ports at MAC-based VLAN

Example: Display the ports currently at MAC-based VLAN

Switch #show mac-vlan interface

Ethernet1/1	Ethernet1/2
Ethernet1/3	Ethernet1/4
Ethernet1/5	Ethernet1/6

5.5.2.2.8 show protocol-vlan

Command: show protocol-vlan

Function: Display the configuration of Protocol-based VLAN on the switch

Parameter: None

Command Mode: Admin Mode

Usage Guide: Display the configuration of Protocol-based VLAN on the switch

Example: Display the configuration of the current Protocol-based VLAN

Switch #show protocol-vlan

Protocol_Type	VLAN_ID
mode ethernetii etype 0x800	200
mode ethernetii etype 0x860	200
mode snap etype 0xabc	100
mode llc dsap 0xac ssap 0xbd	100

5.5.2.2.9 show subnet-vlan

Command: show subnet-vlan

Function: Display the configuration of the IP-subnet-based VLAN on the switch

Parameter: None

Command Mode: Admin Mode

Usage Guide: Display the configuration of the IP-subnet-based VLAN on the switch

Example: Display the configuration of the current IP-subnet-based VLAN

Switch #show subnet-vlan

IP-Address	Mask	VLAN_ID
192.168.1.165	255.255.255.0	2
202.200.121.21	255.255.0.0	2
10.0.0.1	255.248.0.0	5

5.5.2.2.10 show subnet-vlan interface

Command: show subnet-vlan interface

Function: Display the port at IP-subnet-based VLAN

Parameter: None

Command Mode: Admin Mode

Usage Guide: Display the port at IP-subnet-based VLAN

Example: Display the port currently at IP-subnet-based VLAN

Switch#show subnet-vlan interface

Ethernet1/1	Ethernet1/2
Ethernet1/3	Ethernet1/4

5.5.2.2.11 subnet-vlan

Command: subnet-vlan ip-address *<ipv4-addrss>* mask *<subnet-mask>* vlan

<vlan-id> **priority** ***<priority-id>***

no subnet-vlan {ip-address ***<ipv4-addrss>*** **mask** ***<subnet-mask>*****|all}**

Function: Add a correspondence between the IP subnet and the VLAN, namely add specified IP subnet into specified VLAN; the “no" form of this command deletes all/the correspondence.

Parameter: ipv4-address is the IPv4 address shown in dotted decimal notation; the valid range of each section is 0~255;subnet-mask is the subnet mask code shown in dotted decimal notation; the valid range of each section is 0~255;priority-id is the priority applied in the VLAN tag with a valid range of 0~7;vlan-id is the VLAN ID with a valid range of 1~4094;all indicates all the subnets.

Command Mode: Global Mode

Default: No IP subnet joined the VLAN by default

Usage Guide: This command is used for adding specified IP subnet to specified VLAN. When packet without VLAN label and from the specified IP subnet enters through the switch port, it will be matched with specified VLAN id and enters specified VLAN. These packets will always come to the same VLAN no matter through which port did they enter. This command will not interfere with VLAN labeled data packets.

Example: Add the network equipment with IP subnet of 192.168.1.0/24 to VLAN 300.

Switch#config

Switch(config)#subnet-vlan ip-address 192.168.1.1 mask 255.255.255.0 vlan 300 priority 0

5.5.2.2.12 switchport mac-vlan enable

Command: switchport mac-vlan enable

no switchport mac-vlan enable

Function: Enable the MAC-based VLAN function on the port; the "no” form of this command will disable the MAC-based VLAN function on the port

Parameter: None

Command Mode: Port Mode.

Default: The MAC-base VLAN function is enabled on the port by default

Usage Guide: After adding a MAC address to specified VLAN, the MAC-based VLAN function will be globally enabled. This command can disable the MAC-based VLAN function on specified port to meet special user applications.

Example:

Disable the MAC-based VLAN function on port1.

Switch#config

Switch(config)#interface ethernet 4/1

Switch(Config-If-Ethernet4/1)#no switchport mac-vlan enable

5.5.2.2.13 switchport subnet-vlan enable

Command: switchport subnet-vlan enable

no switchport subnet-vlan enable

Function: Enable the IP-subnet-based VLAN on the port; the “no” form of this command disables the IP-subnet-based VLAN function on the port

Parameter: None

Command Mode: Port Mode.

Default: The IP-subnet-based VLAN is enabled on the port by default

Usage Guide: After adding the IP subnet to specified VLAN, the IP-subnet-based VLAN function will be globally enabled. This command can disable the IP-subnet-based VLAN function on specified port to meet special user applications.

Example: Disable the IP-subnet-based VLAN function on port1.

Switch#config

Switch(config)#interface ethernet 4/1

Switch(Config-If-Ethernet4/1)#no switchport subnet-vlan enable

5.5.3 Typical Application Of The Dynamic VLAN

Scenario

In the office network Department A belongs to VLAN100. Several members of this department often have the need to move within the whole office network. It is also required to ensure the resource for other members of the department to access VLAN 100. Assume one of the members is M, the MAC address of his PC is 00-03-0f-11-22-33, and similar configurations are assigned to other members.

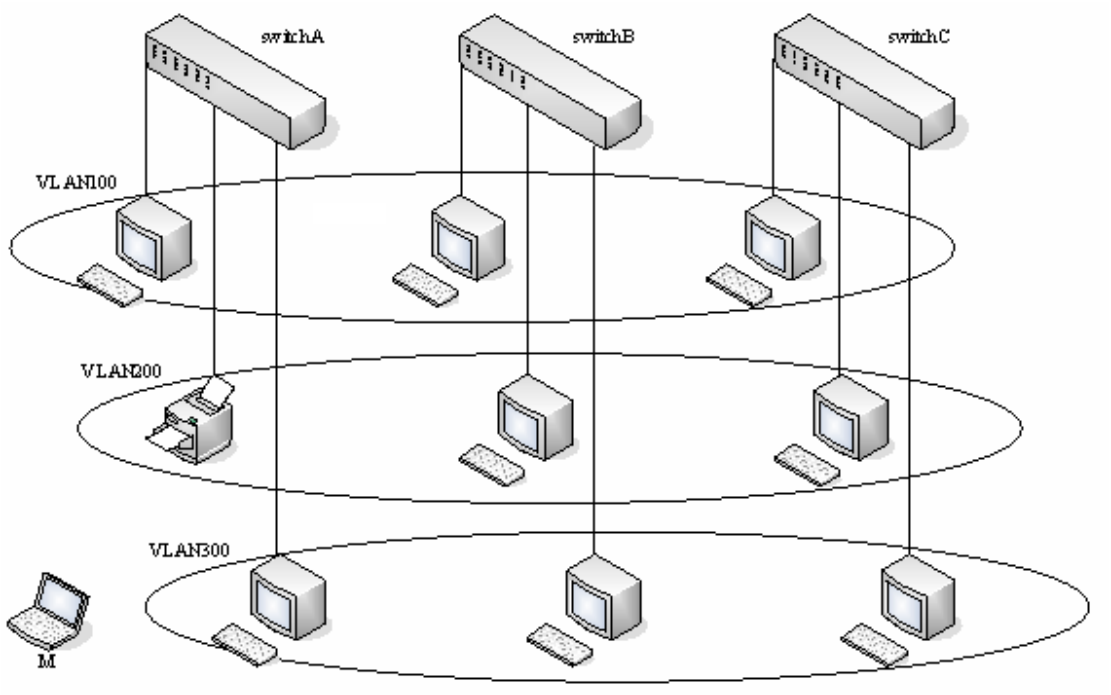


Fig 5-5 Typical topology application of dynamic VLAN

Configuration Items	Configuration Explanation
MAC-based VLAN	Global configuration on Switch A, Switch B, Switch C

Configuration procedure

Switch A, Switch B, Switch C:

Switch(Config)#mac-vlan mac 00-03-0f-11-22-33 vlan 100 priority 0

Switch (Config)#exit

5.5.4 Dynamic VLAN Troubleshooting

☞ On the switch configured with dynamic VLAN, if the two connected equipment (e.g. PC) are both belongs to the same dynamic VLAN, first communication between the two equipment may not be goes through. The solution will be letting the two equipment positively send data packet to the switch (such as ping), to let the switch learn their source MAC, then the two equipment will be able to communicate freely within the dynamic VLAN

5.6 Voice VLAN Configuration

5.6.1 Voice VLAN Introduction

Voice VLAN is specially configured for the user voice data traffic. By setting a Voice VLAN and adding the ports of the connected voice equipments to the Voice VLAN, the user will be able to configure QoS (Quality of service) service for voice data, and improve the voice data traffic transmission priority to ensure the calling quality

The switch can judge if the data traffic is the voice data traffic from specified equipment according to the source MAC address field of the data packet entering the port. The packet with the source MAC address complying with the system defined voice equipment OUI (Organizationally Unique Identifier) will be considered the voice data traffic and transmitted to the Voice VLAN.

The configuration is based on MAC address, acquiring a mechanism in which every voice equipment transmitting information through the network has got its unique MAC address. VLAN will trace the address belongs to specified MAC. By This means, VLAN allows the voice equipment always belong to Voice VLAN when relocated physically. The greatest advantage of the VLAN is the equipment can be automatically placed into Voice VLAN according to its voice traffic which will be transmitted at specified priority. Meanwhile, when voice equipment is physically relocated, it still belongs to the Voice VLAN without any further configuration modification, which is because it is based on voice equipment other than switch port.

5.6.2 Voice VLAN Configuration

5.6.2.1 Voice VLAN Configuration Task Sequence

1. Set the VLAN to Voice VLAN
2. Add a voice equipment to Voice VLAN
3. Enable the Voice VLAN on the port

1. Configure the VLAN to Voice VLAN

Command	Explanation
Global Mode	
voice-vlan vlan <*vlan-id*> **no voice-vlan**	Set/cancel the VLAN as a Voice VLAN

2. Add a voice equipment to a Voice VLAN

Command	Explanation
Global Mode	
voice-vlan mac <*mac-address*> mask <*mac-mask*> priority <*priority-id*> [name <*voice-name*>] **no voice-vlan {mac <*mac-address*> mask <*mac-mask*>|name <*voice-name*> |all}**	Specify certain voice equipment join/leave the Voice VLAN

3. Enable the Voice VLAN of the port

Command	Explanation
Port Mode	
switchport voice-vlan enable **no switchport voice-vlan enable**	Enable/disable the Voice VLAN function on the port

5.6.2.2 Commands for Voice VLAN Configuration

5.6.2.3 show voice-vlan

Command: show voice-vlan

Function: Display the configuration status of the Voice VLAN on the switch

Parameter: None

Command Mode: Admin Mode

Usage Guide: Display Voice VLAN Configuration

Example: Display the Current Voice VLAN Configuration

Switch#show voice-vlan

Voice VLAN ID:2

Ports:ethernet4/1;ethernet4/3

Voice name	MAC-Address	Mask	Priority
financePhone	00-e0-4c-77-ab-9d	0xff	5
manager	00-0a-eb-26-8d-f3	0xfe	6
Mr_Lee	00-03-0f-11-22-33	0x80	5
NULL	00-03-0f-11-22-33	0x0	5

5.6.2.3.1 switchport voice-vlan enable

Command: switchport voice-vlan enable

no switchport voice-vlan enable

Function: Enable the Voice VLAN function on the port; the “no” form of this command

disables Voice VLAN function on the port

Parameter: None

Command Mode: Port Mode

Default: Voice VLAN is enabled by default

Usage Guide: When voice equipment is added to the Voice VLAN, the Voice VLAN is enabled globally by default. This command disables Voice VLAN on specified port to meet specified application of the user.

Example: Disable the Voice VLAN function on port3

Switch#config

Switch(config)#interface ethernet 4/3

Switch(Config-If-Ethernet4/1)#no switchport voice-vlan enable

5.6.2.3.2 voice-vlan

Command: voice-vlan mac <*mac-address*> mask <*mac-mask*> priority <*priority-id*> [name <*voice-name*>]

no voice-vlan {mac <*mac-address*> mask <*mac-mask*>|name <*voice-name*> |all}

Function: Specify certain voice equipment to join in Voice VLAN; the "no" form of this command will let the equipment leave the Voice VLAN

Parameter: Mac-address is the voice equipment MAC address, shown in ”xx-xx-xx-xx-xx-xx” format; mac-mask is the last eight digit of the mask code of the MAC address, the valid values are: 0xff, 0xfe, 0xfc, 0xf8, 0xf0, 0xe0, 0xc0,0x80, 0x0; priority-id is the priority of the voice traffic, the valid range is 0–7; the voice-name is the name of the voice equipment, which is to facilitate the equipment management; all indicates all the MAC addresses of the voice equipments

Command Mode: Global Mode

Default: This command will add a specified voice equipment into the Voice VLAN, if a non VLAN labeled data packet from the specified voice equipment enters through the switch port, then no matter through which port the packet enters, it will belongs to Voice VLAN. The command will not interfere with the packets of VLAN labels.

Example: Add the 256 sets of voice equipments of the R&D department with MAC address ranging from 00-03-0f-11-22-00 to 00-03-0f-11-22-ff to the Voice VLAN

Switch#config

Switch(config)#voice-vlan vlan 100

Switch(config)#voice-vlan mac 00-03-0f-11-22-00 mask 255 priority 5 name test

5.6.2.3.3 voice-vlan vlan

Command: voice-vlan vlan <*vlan-id*>

no voice-vlan

Function: Configure the specified VLAN to Voice VLAN; the "**no voice-vlan** " command cancels the Voice VLAN configuration of this VLAN

Parameter: Vlan id is the number of the specified VLAN

Command Mode: Global Mode

Default: No Voice VLAN is configured by default

Usage Guide: Set specified VLAN for Voice VLAN, There can be only one Voice VLAN at the same time. The voice VLAN can not be applied concurrently with MAC-based VLAN

Example: Set VLAN100 to Voice VLAN

Switch#config

Switch(config)#voice-vlan vlan 100

5.6.3 Typical Applications Of The Voice VLAN

Scenario

A company realizes voice communication through configuring Voice VLAN. IP-phone1 and IP-phone2 can be connected to any port of the switch, namely normal communication and interconnected with other switches through the uplink port. IP-phone1 MAC address is 00-03-0f-11-22-33,IP-phone2 MAC address is 00-03-0f-11-22-55

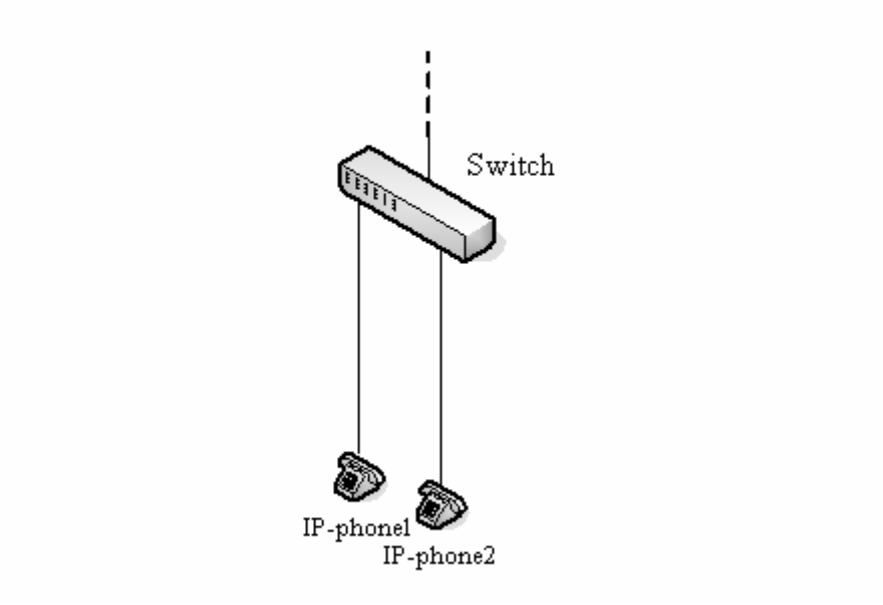


Fig 5-6 VLAN typical apply topology Figure

Configuration items	Configuration Explanation

Voice VLAN	Global configuration on the Switch

Configuration procedure

Switch A:

Switch(Config)#vlan 100

Switch(Config-Vlan100)#exit

Switch(Config)#voice-vlan vlan 100

Switch(Config)#voice-vlan mac 00-03-0f-11-22-33 mask 255 priority 5 name company

Switch(Config)#voice-vlan mac 00-03-0f-11-22-55 mask 255 priority 5 name company

Switch(Config)#interface ethernet 1/10

Switch(Config-If-Ethernet1/10)#switchport mode trunk

Switch(Config-If-Ethernet1/10)#exit

5.6.4 Voice VLAN Troubleshooting

- ☞ Voice VLAN can not be applied concurrently with MAC-base VLAN
- ☞ The Voice VLAN support maximum 1024 sets of voice equipments, the exceeded number of equipments will not be supported
- ☞ The Voice VLAN on the port is enabled by default. If the configured data can no longer enter the Voice VLAN during operation, please check if the Voice VLAN function has been disabled on the port.

Chapter 6 MAC Table Configuration

6.1 Introduction to MAC Table

MAC table is a table identifies the mapping relationship between destination MAC addresses and switch ports. MAC addresses can be categorized as static MAC addresses and dynamic MAC addresses. Static MAC addresses are manually configured by the user, have the highest priority and are permanently effective (will not be overwritten by dynamic MAC addresses); dynamic MAC addresses are entries learnt by the switch in data frame forwarding, and is effective for a limited period. When the switch receives a data frame to be forwarded, it stores the source MAC address of the data frame and creates a mapping to the destination port. Then the MAC table is queried for the destination MAC address, if hit, the data frame is forwarded in the associated port, otherwise, the switch forwards the data frame to its broadcast domain. If a dynamic MAC address is not learnt from the data frames to be forwarded for a long time, the entry will be deleted from the switch MAC table.

There are two MAC table operations:

1. Obtain a MAC address;
2. Forward or filter data frame according to the MAC table.

6.1.1 Obtaining MAC Table

The MAC table can be built up staticlly and dynamically. Static configuration is to set up a mapping between the MAC addresses and the ports; dynamic learning is the process in which the switch learns the mapping between MAC addresses and ports, and updates the MAC table regularly. In this section, we will focus on the dynamic learning process of MAC table.

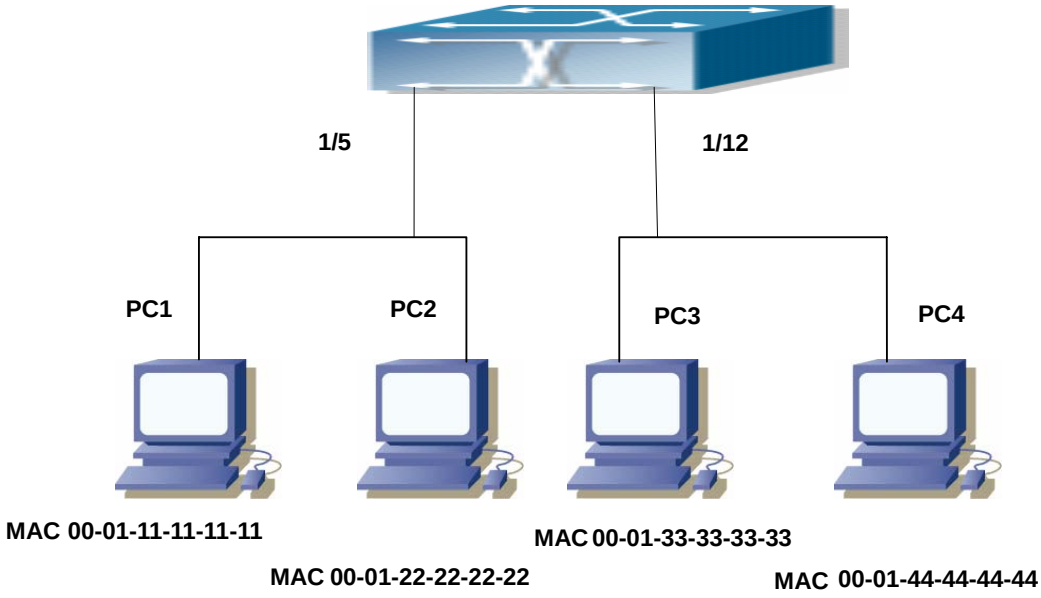


Fig 6-1 MAC Table dynamic learning

The topology of the figure above: 4 PCs connected to ES4626/ES4650 switch, where PC1 and PC2 belongs to a same physical segment (same collision domain), the physical segment connects to port 1/5 of ES4626/ES4650 switch; PC3 and PC4 belongs to the same physical segment that connects to port 1/12 of ES4626/ES4650 switch.

The initial MAC table contains no address mapping entries. Take the communication of PC1 and PC3 as an example, the MAC address learning process is as follow:

1. When PC1 sends message to PC3, the switch receives the source MAC address 00-01-11-11-11-11 from this message, the mapping entry of 00-01-11-11-11-11 and port 1/5 is added to the switch MAC table.
2. At the same time, the switch learns the message is destined to 00-01-33-33-33-33, as the MAC table contains only a mapping entry of MAC address 00-01-11-11-11-11 and port 1/5, and no port mapping for 00-01-33-33-33-33 present, the switch broadcast this message to all the ports in the switch (assuming all ports belong to the default VLAN1).
3. PC3 and PC4 on port 1/12 receive the message sent by PC1, but PC4 will not reply, as the destination MAC address is 00-01-33-33-33-33, only PC3 will reply to PC1. When port 1/12 receives the message sent by PC3, a mapping entry for MAC address 00-01-33-33-33-33 and port 1/12 is added to the MAC table.
4. Now the MAC table has two dynamic entries, MAC address 00-01-11-11-11-11 - port 1/5 and 00-01-33-33-33-33 -port 1/12.
5. After the communication between PC1 and PC3, the switch does not receive any message sent from PC1 and PC3. And the MAC address mapping entries in the MAC table are deleted after 300 seconds. The 300 seconds here is the default aging time for MAC address entry in ES4626/ES4650 switch. Aging time can be modified in

ES4626/ES4650 switch.

6.1.2 Forward or Filter

The switch will forward or filter received data frames according to the MAC table. Take the above figure as an example, assuming ES4626/ES4650 switch have learnt the MAC address of PC1 and PC3, and the user manually configured the mapping relationship for PC2 and PC4 to ports. The MAC table of ES4626/ES4650 switch will be:

MAC Address	Port number	Entry added by
00-01-11-11-11-11	1/5	Dynamic learning
00-01-22-22-22-22	1/5	Static configuration
00-01-33-33-33-33	1/12	Dynamic learning
00-01-44-44-44-44	1/12	Static configuration

1. Forward data according to the MAC table

If PC1 sends a message to PC3, the switch will forward the data received on port 1/5 from port 1/12.

2. Filter data according to the MAC table

If PC1 sends a message to PC2, the switch, on checking the MAC table, will find PC2 and PC1 are in the same physical segment and filter the message (i.e. drop this message).

Three types of frames can be forwarded by the switch:

- ✧ Broadcast frame
- ✧ Multicast frame
- ✧ Unicast frame

The following describes how the switch deals with all the three types of frames:

1. Broadcast frame: The switch can segregate collision domains but not broadcast domains. If no VLAN is set, all devices connected to the switch are in the same broadcast domain. When the switch receives a broadcast frame, it forwards the frame in all ports. When VLANs are configured in the switch, the MAC table will be adapted accordingly to add VLAN information. In this case, the switch will not forward the received broadcast frames in all ports, but forward the frames in all ports in the same VLAN.
2. Multicast frame: When IGMP Snooping function is not enabled, multicast frames are processed in the same way as broadcast frames; when IGMP Snooping is enabled, the switch will only forward the multicast frames to the ports belonging to the very multicast group.

Unicast frame: When no VLAN is configured, if the destination MAC addresses are in the switch MAC table, the switch will directly forward the frames to the associated ports;

when the destination MAC address in a unicast frame is not found in the MAC table, the switch will broadcast the unicast frame. When VLANs are configured, the switch will forward unicast frame within the same VLAN. If the destination MAC address is found in the MAC table but belonging to different VLANs, the switch can only broadcast the unicast frame in the VLAN it belongs to.

6.2 Mac Address Table Configuration Task List

1. Configure the MAC address aging-time
2. Configure static MAC forwarding or filter entry

1. Configure the MAC aging-time

Command	**Explanation**
Global Mode	
mac-address-table aging-time <*0|aging-time*> **no mac-address-table aging-time**	Configure the MAC address aging-time

2. Configure static MAC forwarding or filter entry

Command	**Explanation**
Global Mode	
mac-address-table static <*mac-address*> {interface <*interface-name* >| discard} vlan <*vlan-id*> **no mac-address-table {static|dynamic|discard} [address <WORD>] [vlan <1-4096>] [interface [ethernet|port-channel] <IFNAME>]**	Configure static MAC forwarding or filter entry

6.3 Commands for MAC address table configuration

6.3.1 mac-address-table aging-time

Command: mac-address-table aging-time {<*age*>| 0}

no mac-address-table aging-time

Function: Sets the aging-time for the dynamic entries of MAC address table; use the no form to restore the aging-time to 300s by default.

Parameter: <age> is the aging-time seconds ,range 10~100000; 0 to disable aging.

Command Mode: Global mode

Default: Default aging-time is 300 seconds.

Usage Guide: The user had better set the aging-time according to the network condition. A too small aging-time will affect the performance of the switch by causing too much broadcast, while a too large aging-time will make the unused entries stay too long in the address table.

The dynamic address does aging when the aging-time is set to 0.

Example: Set the aging-time to 400 seconds.

Switch (Config)#mac-address-table aging-time 400

6.3.2 mac-address-table

Command：mac-address-table static <*mac-address*> {interface <*interface-name* >| discard} vlan <*vlan-id*>

no mac-address-table {static|dynamic|discard} [address <WORD>] [vlan <1-4096>] [interface [ethernet|port-channel] <IFNAME>]

Function：Add or modify static address entries and filter address entries. The "**no mac-address-table {static|dynamic|discard} [address <WORD>] [vlan <1-4096>] [interface [ethernet|port-channel] <IFNAME>]**" command deletes the two entries

Parameter：static is the static entries;**discard** is filter entries, which is for discarding frames from specific MAC address;**dynamic** is dynamic address entries;***<mac-address>*** MAC address to be added or deleted;***<interface-name>*** name of the port transmitting the MAC data packet;***<vlan-id>*** is the vlan number.

Command Mode：Global mode

Default：When VLAN interface is configured and is up, the system will generate an static address mapping entry of which the inherent MAC address corresponds to the VLAN number

Usage Guide：In certain special applications or when the switch is unable to dynamically learn the MAC address, users can use this command to manually establish mapping relation between the MAC address and port and VLAN.

no mac-address-table command is for deleting all dynamic, static, filter MAC address entries existing in the switch MAC address list, except for the mapping entries retained in the system default

Example：Port 1/1 belongs to VLAN200, and establishes address mapping with MAC address 00-03-0f-f0-00-18.

Switch(Config)#mac-address-table static address 00-03-0f-f0-00-18 vlan 200 interface ethernet 1/1.

6.3.3 show mac-address-table

Command: show mac-address-table [static |dynamic |discard| aging-time| multicast| count] [address <WORD>] [vlan <1-4096>] [count] [interface<*interface-name*>]

Function: Show the current MAC table

Parameter: static entry; **dynamic** entry; **aging-time** address aging time; **discard** filter entry; **multicast** entry; ***<mac-addr>*** entry's MAC address; ***<vlan-id>*** entry's VLAN number; ***<interface-name>*** entry's interface name

Command mode: Admin mode

Default: MAC address table is not displayed by default.

Usage guide: This command can display various sorts of MAC address entries. Users can also use **show mac-address-table** to display all the MAC address entries.

Example: Display all the filter MAC address entries.

Switch#show mac-address-table discard

6.4 Typical Configuration Examples

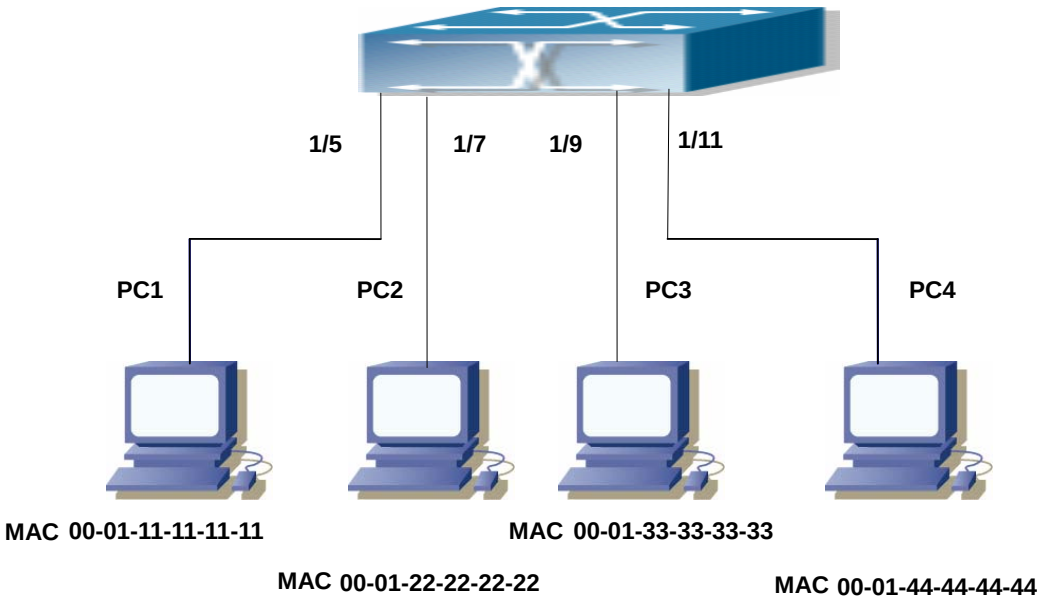


Fig 6-2 MAC Table typical configuration example

Scenario: Four PCs as shown in the above figure connect to port 1/5, 1/7, 1/9, 1/11 of switch, all the four PCs belong to the default VLAN1. As required by the network environment, dynamic learning is enabled. PC1 holds sensitive data and can not be accessed by any other PC that is in another physical segment; PC2 and PC3 have static mapping set to port 7 and port 9, respectively.

The configuration steps are listed below:

1. Set the MAC address 00-01-11-11-11-11 of PC1 as a filter address.

Switch(Config)#mac-address-table static 00-01-11-11-11-11 discard vlan 1.

2.Set the static mapping relationship for PC2 and PC3 to port 7 and port 9, respectively.

Switch(Config)#mac-address-table static 00-01-22-22-22-22 interface ethernet 1/7 vlan 1

Switch(Config)#mac-address-table static 00-01-33-33-33-33 interface ethernet 1/9 vlan 1

6.5 Troubleshooting

Using the show mac-address-table command, a port is found to be failed to learn the MAC of a device connected to it. Possible reasons:

- The connected cable is broken.
- Spanning Tree is enabled and the port is in “discarding” status; or the device is just connected to the port and Spanning Tree is still under calculation, wait until the Spanning Tree calculation finishes, and the port will learn the MAC address.
- If not the problems mentioned above , please check for the switch port and contact technical support for solution.

6.6 MAC Address Function Extension

6.6.1 MAC Address Binding

6.6.1.1 Introduction to MAC Address Binding

Most switches support MAC address learning, each port can dynamically learn several MAC addresses, so that forwarding data streams between known MAC addresses within the ports can be achieved. If a MAC address is aged, the packet destined for that entry will be broadcasted. In other words, a MAC address learned in a port will be used for forwarding in that port, if the connection is changed to another port, the switch will learn the MAC address again to forward data in the new port.

However, in some cases, security or management policy may require MAC addresses to be bound with the ports, only data stream from the binding MAC are allowed to be forwarded in the ports. That is to say, after a MAC address is bound to a port, only the data stream destined for that MAC address can flow in from the binding port, data stream destined for the other MAC addresses that not bound to the port will not be allowed to pass through the port.

6.6.1.2 MAC Address Binding Configuration Task List

1. Enable MAC address binding function for the ports
2. Lock the MAC addresses for a port
3. MAC address binding property configuration

1. Enable MAC address binding function for the ports

Command	Explanation
Interface Mode	
port security **no port-security**	Enable MAC address binding function for the port and lock the port. When a port is locked, the MAC address learning function for the port will be disabled: the "**no port-security"** command disables the MAC address binding function for the port**,** and restores the MAC address learning function for the port.

2. Lock the MAC addresses for a port

Command	Explanation
Interface Mode	
port-security convert	Convert dynamic secure MAC addresses learned by the port to static secure MAC addresses.
port-security timeout <*value*> **no port-security timeout**	Enable port locking timer function; the "**no port-security timeout**" restores the default setting.
port-security mac-address <*mac-address*> **no port-security mac-address <*mac-address*>**	Add static secure MAC address; the "**no port-security mac-address"** command deletes static secure MAC address.
Admin Mode	
clear port-security dynamic [address <*mac-addr*> | interface <*interface-id*>]	Clear dynamic MAC addresses learned by the specified port.

3. MAC address binding property configuration

Command	Explanation
Interface Mode	

port-security maximum <*value*> **no port-security maximum <*value*>**	Set the maximum number of secure MAC addresses for a port; the "**no port-security maximum**" command restores the default value.
port-security violation {protect | shutdown} **no port-security violation**	Set the violation mode for the port; the "**no port-security violation**" command restores the default setting.

6.6.1.3 Commands for Mac Address Binding configuration

6.6.1.3.1 clear port-security dynamic

Command:clear port-security dynamic[address<*mac-addr*>|interface <*interface-id*>]

Function: Clear the Dynamic MAC addresses of the specified port.

Command mode: Admin Mode

Parameter: <*mac-addr*> stands MAC address; **<*interface-id*>** for specified port number.

Usage Guide: The secure port must be locked before dynamic MAC clearing operation can be perform in specified port. If no ports and MAC are specified, then all dynamic MAC in all locked secure ports will be cleared; if only port but no MAC address is specified, then all MAC addresses in the specified port will be cleared.

Example: Delete all dynamic MAC in port1.

Switch#clear port-security dynamic interface Ethernet 1/1

6.6.1.3.2 port-security

Command: port security

no port security

Function: Enable MAC address binding function for the port and lock the port. When a port is locked, the MAC address learning function for the port will be disabled: the "**no port-security"** command disables the MAC address binding function for the port and restores the MAC address learning function for the port.

Command mode: Interface Mode

Default: MAC address binding is not enabled by default.

Usage Guide: The MAC address binding function, Spanning Tree and Port Aggregation functions are mutually exclusive. Therefore, if MAC binding function for a port is to be enabled, the Spanning Tree and Port Aggregation functions must be disabled, and the port enabling MAC address binding must not be a Trunk port.

Example: Enable MAC address binding function for port 1and and lock the port. When a port is locked, the MAC address learning function for the port will be disabled.

Switch(Config)#interface Ethernet 1/1

Switch(Config-Ethernet1/1)#port security

6.6.1.3.3 port-security convert

Command: port-security convert

Function: Converts dynamic secure MAC addresses learned by the port to static secure MAC addresses, and disables the MAC address learning function for the port.

Command mode: Interface Mode

Usage Guide: The port dynamic MAC convert command can only be executed after the secure port is locked. After this command has been executed, dynamic secure MAC addresses learned by the port will be converted to static secure MAC addresses. The command does not reserve configuration.

Example: Converting MAC addresses in port 1 to static secure MAC addresses.

Switch(Config)#interface Ethernet 1/1

Switch(Config-Ethernet1/1)# port-security convert

6.6.1.3.4 port-security mac-address

Command: port-security mac-address <*mac-address*>

no port-security mac-address <*mac-address*>

Function: Adds a static secure MAC address; the "**no port-security mac-address"** command deletes a static secure MAC address.

Command mode: Interface Mode

Parameters: <*mac-address*> stands for the MAC address to be added/deleted.

Usage Guide: The MAC address binding function must be enabled before static secure MAC address can be added.

Example: Adding MAC 00-03-0F-FE-2E-D3 to port1.

Switch(Config)#interface Ethernet 1/1

Switch(Config-Ethernet1/1)# port-security mac-address 00-03-0F-FE-2E-D3

6.6.1.3.5 port-security maximum

Command: port-security maximum <*value*>

no port-security maximum

Function: Sets the maximum number of secure MAC addresses for a port; the "**no maximum**" command restores the maximum secure address number of 1.

Command mode: Interface Mode

Parameter: < *value*> is the up limit for static secure MAC address, the valid range is 1 to 128.

Default: The default maximum port secure MAC address number is 1.

Usage Guide: The MAC address binding function must be enabled before maximum secure MAC address number can be set. If secure static MAC address number of the

port is larger than the maximum secure MAC address number set, the setting fails; extra secure static MAC addresses must be deleted, so that the secure static MAC address number is no larger than the maximum secure MAC address number for the setting to be successful.

Example: Set the maximum secure MAC address number for port 1 to 4.

Switch(Config)#interface Ethernet 1/1

Switch(Config-Ethernet1/1)# port-security maximum 4

6.6.1.3.6 port-security timeout

Command: port-security timeout <*value*>

no port-security timeout

Function: Set the timer for port locking; the "**no port-security timeout**" command restores the default setting.

Parameter: < *value*> is the timeout value, the valid range is 0 to 300s.

Command mode: Interface Mode

Default: Port locking timer is not enabled by default.

Usage Guide: The port locking timer function is a dynamic MAC address locking function. MAC address locking and conversion of dynamic MAC entries to secure address entries will be performed on locking timer timeout. The MAC address binding function must be enabled prior to running this command.

Example: Set port1 locking timer to 30 seconds.

Switch(Config)#interface Ethernet 1/1

Switch(Config-Ethernet1/1)# port-security timeout 30

6.6.1.3.7 port-security violation

Command：port-security violation {protect | shutdown}

no port-security violation

Function：Configure the port violation mode. The "**no port-security violation**" restore the violation mode to protect

Command Mode：Port mode

Parameter：protect refers to protect mode;**shutdown** refers to shutdown mode

Default：The port violation mode is **protect** by default

Usage Guide：The port violation mode configuration is only available after the MAC address binding function is enabled. when the port secure MAC address exceeds the security MAC limit, if the violation mode is **protect**, the port only disable the dynamic MAC address learning function; while the port will be shut if at **shutdown** mode. Users can manually open the port with **no shutdown** command.

Example：Set the violation mode of port 1 to shutdown

Switch(Config)#interface Ethernet 1/1

Switch(Config-Ethernet1/1)#port-security violation shutdown

6.6.1.3.8 show port-security

Command: show port-security

Function: Display the secure MAC addresses of the port.

Command mode: Admin Mode

Parameter: *<interface-list>* stands for the port to be displayed.

Usage Guide: This command displays the secure port MAC address information, if no port is specified, secure MAC addresses of all ports are displayed. The following is an example:

Switch#show port-security interface ethernet 1/3

Ethernet1/3 Security Mac Address Table

Vlan	Mac Address	Type	Ports
1	0000.0000.1111	SecureConfigured	Ethernet1/3

Total Addresses : 1

Displayed information	Explanation
Vlan	The VLAN ID for the secure MAC Address
Mac Address	Secure MAC address
Type	Secure MAC address type
Ports	The port that the secure MAC address belongs to
Total Addresses	Current secure MAC address number in the system.

6.6.1.3.9 show port-security address

Command: show port-security address [interface *<interface-id>*]

Function: Display the secure MAC addresses of the port.

Command mode: Admin Mode

Parameter: *<interface-list>* stands for the port to be displayed.

Usage Guide: This command displays the secure port MAC address information, if no port is specified, secure MAC addresses of all ports are displayed. The following is an example:

Switch#show port-security address interface ethernet 1/3

Ethernet1/3 Security Mac Address Table

Vlan	Mac Address	Type	Ports
1	0000.0000.1111	SecureConfigured	Ethernet1/3

Total Addresses : 1

Displayed information	Explanation
Vlan	The VLAN ID for the secure MAC Address
Mac Address	Secure MAC address
Type	Secure MAC address type
Ports	The port that the secure MAC address belongs to
Total Addresses	Current secure MAC address number in the system.

6.6.1.3.10 show port-security interface

Command: show port-security interface <*interface-id*>

Function: display the configuration of secure port.

Command mode: Admin Mode

Parameter: <*interface-list*> stands for the port to be displayed.

Default: Configuration of secure ports is not displayed by default.

Usage Guide: This command displays the detailed configuration information for the secure port.

Example:

Switch#show port-security interface ethernet 1/1

Ethernet1/1 Port Security : Enabled

Port status : Security Up

Violation mode : Protect

Maximum MAC Addresses : 1

Total MAC Addresses : 1

Configured MAC Addresses : 1

Lock Timer is ShutDown

Mac-Learning function is : Closed

Displayed information	Explanation
Port Security :	Is port enabled as a secure port?
Port status:	Port secure status
Violation mode :	Violation mode set for the port.
Maximum MAC Addresses :	The maximum secure MAC address number set for the port
Total MAC Addresses :	Current secure MAC address number for the port.
Configured MAC Addresses :	Current secure static MAC address number

	for the port.
Lock Timer	Whether locking timer (timer timeout) is enabled for the port.
Mac-Learning function	Is the MAC address learning function enabled?

6.6.1.4 Binding MAC Address Binding Troubleshooting

Enabling MAC address binding for ports may fail in some occasions. Here are some possible causes and solutions:

- ☞ If MAC address binding cannot be enabled for a port, make sure the port is not enabling Spanning tree or port aggregation and is not configured as a Trunk port. MAC address binding is exclusive to such configurations. If MAC address binding is to be enabled, the functions mentioned above must be disabled first.
- ☞ If a secure address is set as static address and deleted, that secure address will be unusable even though it exists. For this reason, it is recommended to avoid static address for ports enabling MAC address

Chapter 7 MSTP Configuration

7.1 MSTP Introduction

The MSTP (Multiple STP) is a new spanning-tree protocol which is based on the STP and the RSTP. It runs on all the bridges of a bridged-LAN. It calculates a common and internal spanning tree (CIST) for the bridge-LAN which consists of the bridges running the MSTP, the RSTP and the STP. It also calculates the independent multiple spanning-tree instances (MSTI) for each MST domain (MSTP domain). The MSTP, which adopts the RSTP for its rapid convergence of the spanning tree, enables multiple VLANs to be mapped to the same spanning-tree instance which is independent to other spanning-tree instances. The MSTP provides multiple forwarding paths for data traffic and enables load balancing. Moreover, because multiple VLANs share a same MSTI, the MSTP can reduce the number of spanning-tree instances, which consumes less CPU resources and reduces the bandwidth consumption.

7.1.1 MSTP Region

Because multiple VLANs can be mapped to a single spanning tree instance, IEEE 802.1s committee raises the MST concept. The MST is used to make the association of a certain VLAN to a certain spanning tree instance.

A MSTP region is composed of one or multiple bridges with the same MCID (MST Configuration Identification) and the bridged-LAN (a certain bridge in the MSTP region is the designated bridge of the LAN, and the bridges attaching to the LAN are not running STP). All the bridges in the same MSTP region have the same MSID.

MSID consists of 3 attributes:

- Configuration Name: Composed by digits and letters
- Revision Level
- Configuration Digest: VLANs mapping to spanning tree instances

The bridges with the same 3 above attributes are considered as in the same MST region.

When the MSTP calculates CIST in a bridged-LAN, a MSTP region is considered as a bridge. See the figure below:

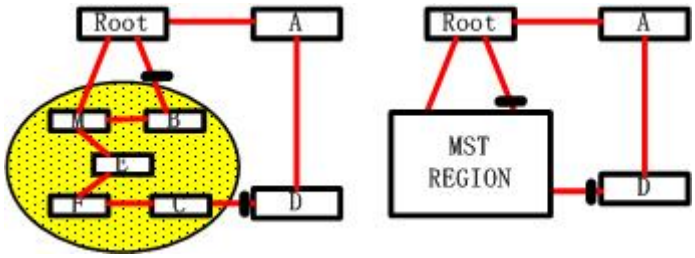


Figure7-1 Example of CIST and MST Region

In the above network, if the bridges are running the STP or the RSTP, one port between Bridge M and Bridge B should be blocked. But if the bridges in the yellow range run the MSTP and are configured in the same MST region, MSTP will treat this region as a bridge. Therefore, one port between Bridge B and Root is blocked and one port on Bridge D is blocked.

7.1.1.1 Operations Within An MSTP Region

The IST connects all the MSTP bridges in a region. When the IST converges, the root of the IST becomes the IST master, which is the switch within the region with the lowest bridge ID and path cost to the CST root. The IST master is also the CST root if there is only one region within the network. If the CST root is outside the region, one of the MSTP bridges at the boundary of the region is selected as the IST master.

When an MSTP bridge initializes, it sends BPDUs claiming itself as the root of the CST and the IST master, with both of the path costs to the CST root and to the IST master set to zero. The bridge also initializes all of its MST instances and claims to be the root for all of them. If the bridge receives superior MST root information (lower bridge ID, lower path cost, and so forth) than currently stored for the port, it relinquishes its claim as the IST master.

Within a MST region, the IST is the only spanning-tree instance that sends and receives BPDUs. Because the MST BPDU carries information for all instances, the number of BPDUs that need to be processed by a switch to support multiple spanning-tree instances is significantly reduced.

All MST instances within the same region share the same protocol timers, but each MST instance has its own topology parameters, such as root switch ID, root path cost, and so forth.

7.1.1.2 Operations between MST Regions

If there are multiple regions or legacy 802.1D bridges within the network, MSTP establishes and maintains the CST, which includes all MST regions and all legacy STP bridges in the network. The MST instances combine with the IST at the boundary of the region to become the CST.

The MSTI is only valid within its MST region. An MSTI has nothing to do with MSTIs in other MST regions. The bridges in a MST region receive the MST BPDU of other regions through Boundary Ports. They only process CIST related information and abandon MSTI information.

7.1.2 Port Roles

The MSTP bridge assigns a port role to each port which runs MSTP.

- CIST port roles: root port, designated port, alternate port and backup port
- On top of those roles, each MSTI port has one new role: master port.

The port roles in the CIST (root port, designated port, alternate port and backup port) are defined in the same ways as those in the RSTP.

7.1.3 MSTP Load Balance

In a MSTP region, VLANs can by mapped to various instances. That can form various topologies. Each instance is independent from the others and each distance can have its own attributes such as bridge priority and port cost etc. Consequently, the VLANs in different instances have their own paths. The traffic of the VLANs are load-balanced.

7.2 MSTP Configuration Task List

1. Enable the MSTP and set the running mode
2. Configure instance parameters
3. Configure MSTP region parameters
4. Configure MSTP time parameters
5. Configure the fast migrate feature for MSTP
6. Configure the format of port packet
7. Configure the snooping attribute of authentication key
8. Configure the FLUSH mode once topology changes

1. Enable MSTP and set the running mode

Command	**Explanation**
Global Mode and Interface Mode	
spanning-tree **no spanning-tree**	Enable/Disable MSTP

Global Mode	
spanning-tree mode {mstp|stp} **no spanning-tree mode**	Set MSTP running mode
Interface Mode	
spanning-tree mcheck	Force port migration to run under MSTP

2. Configure instance parameters

Command	**Explanation**
Global Mode	
spanning-tree mst <*instance-id*> priority <*bridge-priority*> **no spanning-tree mst <*instance-id*> priority**	Set bridge priority for specified instance
Interface Mode	
spanning-tree mst <*instance-id*> cost <*cost*> **no spanning-tree mst <*instance-id*> cost**	Set port path cost for specified instance
spanning-tree mst <*instance-id*> port-priority <*port-priority*> **no spanning-tree mst <*instance-id*> port-priority**	Set port priority for specified instance

3. Configure MSTP region parameters

Command	Explanation
Global Mode	
spanning-tree mst configuration **no spanning-tree mst configuration**	Enter MSTP region mode. The " **no spanning-tree mst configuration**" command restores the default setting.
MSTP region mode	
instance <*instance-id*> vlan <*vlan-list*> **no instance <*instance-id*> [vlan <*vlan-list*>]**	Create Instance and set mapping between VLAN and Instance
name <*name*> **no name**	Set MSTP region name
revision-level <*level*> **no revision-level**	Set MSTP region revision level
Abort	Quit MSTP region mode and return to Global mode without saving MSTP region configuration
Exit	Quit MSTP region mode and return to Global mode with saving MSTP region configuration

4. Configure MSTP time parameters

Command	Explanation
Global Mode	
spanning-tree forward-time <*time*> **no spanning-tree forward-time**	Set the value for switch forward delay time
spanning-tree hello-time <*time*> **no spanning-tree hello-time**	Set the Hello time for sending BPDU messages
spanning-tree maxage <*time*> **no spanning-tree maxage**	Set Aging time for BPDU messages
spanning-tree max-hop <*hop-count*> **no spanning-tree max-hop**	Set Maximum number of hops of BPDU messages in the MSTP region

5. Configure the fast migrate feature for MSTP

Command	Explanation
Interface Mode	
spanning-tree link-type p2p {auto|force-true|force-false} **no spanning-tree link-type**	Set the port link type
spanning-tree portfast **no spanning-tree portfast**	Set the port to be an boundary port

6. Configure the format of MSTP

Command	Explanation
Interface Mode	
spanning-tree format standard **spanning-tree format privacy** **spanning-tree format auto** **no spanning-tree format**	Configure the format of port spanning-tree packet，standard format is provided by IEEE,privacy is compatible with CISCO and auto means the format is determined by checking the received packet

7. Configure the snooping attribute of authentication key

Command	Explanation
Interface Mode	
spanning-tree digest-snooping **no spanning-tree digest-snooping**	Set the port to use the authentication string of partner port. **"no spanning-tree digest-snooping"** restores to use the generated string

8. Configure the FLUSH mode once topology changes

Command	Explanation
Global Mode	
spanning-tree tcflush enable **spanning-tree tcflush disable** **spanning-tree tcflush protect** **no spanning-tree tcflush**	Enable: the spanning-tree flush once the topology changes. Disable:the spanning tree don't flush when the topology changes. Protect: the spanning-tree flush every ten seconds **"no spanning-tree tcflush"** restores to default setting,enable flush once the topology changes
Interface Mode	
spanning-tree tcflush enable **spanning-tree tcflush disable** **spanning-tree tcflush protect** **no spanning-tree tcflush**	Configure the port flush mode. **"no spanning-tree tcflush"** restores to use the global configured flush mode

7.3 Commands for MSTP

7.3.1 abort

Command: abort

Function: Abort the current MSTP region configuration, quit MSTP region mode and return to global mode.

Command mode: MSTP Region Mode

Usage Guide: This command is to quit MSTP region mode without saving the current configuration. The previous MSTP region configuration is valid. This command is equal to "Ctrl+z".

Example: Quit MSTP region mode without saving the current configuration

Switch(Config-Mstp-Region)#abort

Switch(Config)#

7.3.2 exit

Command: exit

Function: Save current MSTP region configuration, quit MSTP region mode and return

to global mode.

Command mode: MSTP Region Mode

Usage Guide: This command is to quit MSTP region mode with saving the current configuration.

Example: Quit MSTP region mode with saving the current configuration.

Switch(Config-Mstp-Region)#exit

Switch(Config)#

7.3.3 instance vlan

Command: instance <instance-id> vlan <vlan-list>

no instance <*instance-id*> [vlan <*vlan-list*>]

Function: In MSTP region mode, create the instance and set the mappings between VLANs and instances; The command "**no instance <*instance-id*> [vlan <*vlan-list*>]**" removes the specified instance and the specified mappings between the VLANs and instances.

Parameter: Normally, ***<instance-id>*** sets the instance number. The valid range is from 0 to 48.; In the command "**no instance <*instance-id*> [vlan <*vlan-list*>]**", ***<instance-id>*** sets the instance number. The valid number is from 1 to 48. ***<vlan-list>*** sets consecutive or non-consecutive VLAN numbers. "-" refers to consecutive numbers, and ";" refers to non-consecutive numbers.

Command mode: MSTP Region Mode

Default: Before creating any Instances, there is only the instance 0, and VLAN 1~5094 all belong to the instance 0.

Usage Guide: This command sets the mappings between VLANs and instances. Only if all the mapping relationships and other attributes are same, the switches are considered in the same MSTP region. Before setting any instances, all the VLANs belong to the instance 0. MSTP can support maximum 48 MSTIs (except for CISTs). CIST can be treated as MSTI 0. All the other instances are considered as instance 1 to 48.

Example: Map VLAN1-10 and VLAN 100-110 to Instance 1.

Switch(Config)#spanning-tree mst configuration

Switch(Config-Mstp-Region)#instance 1 vlan 1-10;100-110

7.3.4 name

Command: name <*name*>

no name

Function: In MSTP region mode, set MSTP region name; The "**no name**" command

restores the default setting.

Parameter: *<name>* is the MSTP region name. The length of the name should be less than 32 characters.

Command mode: MSTP Region Mode

Default: Default MSTP region name is the MAC address of this bridge.

Usage Guide: This command is to set MSTP region name. The bridges with same MSTP region name and same other attributes are considered in the same MSTP region.

Example: Set MSTP region name to mstp-test.

Switch(Config)#spanning-tree mst configuration

Switch(Config-Mstp-Region)#description mstp-test

7.3.5 revision-level

Command: revision-level *<level>*

no revision-level

Function: In MSTP region mode, this command is to set revision level for MSTP configuration; The command "**no revision-level**" restores the default setting to 0.

Parameter: *<level>* is revision level. The valid range is from 0 to 65535.

Command mode: MSTP Region Mode

Default: The default revision level is 0.

Usage Guide: This command is to set revision level for MSTP configuration. The bridges with same MSTP revision level and same other attributes are considered in the same MSTP region.

Example: Set revision level to 2000.

Switch(Config)#spanning-tree mst configuration

Switch(Config-Mstp-Region)# revision-level 2000

7.3.6 spanning-tree

Command: spanning-tree

no spanning-tree

Function: Enable MSTP in global mode and in interface mode; The command "**no spanning-tree**" is to disable MSTP.

Command mode: Global Mode and Interface Mode

Default: MSTP is not enabled by default.

Usage Guide: If the MSTP is enabled in global mode, the MSTP is enabled in all the ports except for the ports which are set to disable the MSTP explicitly.

Example: Enable the MSTP in global mode, and disable the MSTP in the interface 1/2.

Switch(Config)#spanning-tree
Switch(Config)#interface ethernet 1/2
Switch(Config-Ethernet1/2)#no spanning-tree

7.3.7 spanning-tree format

Command:spanning-tree format standard | privacy | auto
no spanning-tree format

Function: Configure the format of the port packet so to be interactive with products of other companies.

Parameter：standard：The packet format provided by IEEE
privacy：Privacy packet format, which is compatible with CISCO equipments.
auto：Auto identified packet format, which is determined by checking the format of the received packets.

Default：Privacy Packet Format

Command Mode：Port Mode

Usage Guide:

As the CISCO has adopted the packet format different with the one provided by IEEE, while many companies also adopted the CISCO format to be CISCO compatible, we have to provide support to both formats. The standard format is originally the one provided by IEEE, and the privacy packet format is CISCO compatible. In case we are not sure about which the packet format is on partner, the AUTO configuration will be preferred so to identify the format by the packets they sent. The privacy packet format is set by default in the concern of better compatibility with previous products and the leading companies. Also the packet format will be privacy format before receiving the partner packet when configured to AUTO.

When the format is not AUTO and the received packet format from the partner does not match the configured format, we set the state of the port which receives the unmatched packet to DISCARDING to prevent both sides consider themselves the root which leads to circuits.

When the AUTO format is set, and over one equipment which is not compatible with each other are connected on the port (e.g. a equipment running through a HUB or Transparent Transmission BPDU is connected with several equipments running MSTP), the format alter counts will be recorded and the port will be disabled at certain count threshold. The port can only be re-enabled by the administrator.

Example: Switch(Config)#interface ethernet 1/2
Switch(Config-Ethernet-1/2)#spanning-tree format standard

7.3.8 spanning-tree forward-time

Command: spanning-tree forward-time <*time*>

no spanning-tree forward-time

Function: Set the switch forward delay time; The command "**no spanning-tree forward-time**" restores the default setting.

Parameter: <*time*> is forward delay time in seconds. The valid range is from 4 to 30.

Command mode: Global Mode

Default: The forward delay time is 15 seconds by default.

Usage Guide: When the network topology changes, the status of the port is changed from blocking to forwarding. This delay is called the forward delay. The forward delay is co working with hello time and max age. The parameters should meet the following conditions. Otherwise, the MSTP may work incorrectly.

2 * (Bridge_Forward_Delay - 1.0 seconds) >= Bridge_Max_Age

Bridge_Max_Age >= 2 * (Bridge_Hello_Time + 1.0 seconds)

Example: In global mode, set MSTP forward delay time to 20 seconds.

Switch(Config)#spanning-tree forward-time 20

7.3.9 spanning-tree hello-time

Command: spanning-tree hello-time <*time*>

no spanning-tree hello-time

Function: Set switch Hello time; The command "**no spanning-tree hello-time**" restores the default setting.

Parameter: <*time*> is Hello time in seconds. The valid range is from 1 to 10.

Command mode: Global Mode

Default: Hello Time is 2 seconds by default.

Usage Guide: Hello time is the interval that the switch sends BPDUs. Hello time is co working with forward delay and max age. The parameters should meet the following conditions. Otherwise, the MSTP may work incorrectly.

2 * (Bridge_Forward_Delay - 1.0 seconds) >= Bridge_Max_Age

Bridge_Max_Age >= 2 * (Bridge_Hello_Time + 1.0 seconds)

Example: Set MSTP hello time to 5 seconds in global mode.

Switch(Config)#spanning-tree hello-time 5

7.3.10 spanning-tree link-type p2p

Command: spanning-tree link-type p2p {auto|force-true|force-false}

no spanning-tree link-type

Function: Set the link type of the current port; The command "**no spanning-tree link-type**" restores link type to auto-negotiation.

Parameter: auto sets auto-negotiation, **force-true** forces the link as point-to-point type, **force-false** forces the link as non point-to-point type.

Command mode: Interface Mode

Default: The link type is auto by default, The MSTP detects the link type automatically.

Usage Guide: When the port is full-duplex, MSTP sets the port link type as point-to-point; When the port is half-duplex, MSTP sets the port link type as shared.

Example: Force the port 1/7-8 as point-to-point type.

Switch(Config)#interface ethernet 1/7-8

Switch(Config-Port-Range)#spanning-tree link-type p2p force-true

7.3.11 spanning-tree maxage

Command: spanning-tree maxage <*time*>

no spanning-tree maxage

Function: Set the max aging time for BPDU; The command "**no spanning-tree maxage**" restores the default setting.

Parameter: <*time*> is max aging time in seconds. The valid range is from 6 to 40.

Command mode: Global Mode

Default: The max age is 20 seconds by default.

Usage Guide: The lifetime of BPDU is called max age time. The max age is co working with hello time and forward delay. The parameters should meet the following conditions. Otherwise, the MSTP may work incorrectly.

2 * (Bridge_Forward_Delay - 1.0 seconds) >= Bridge_Max_Age

Bridge_Max_Age >= 2 * (Bridge_Hello_Time + 1.0 seconds)

Example: In global mode, set max age time to 25 seconds.

Switch(Config)#spanning-tree maxage 25

7.3.12 spanning-tree max-hop

Command: spanning-tree max-hop <*hop-count*>

no spanning-tree max-hop

Function: Set maximum hops of BPDU in the MSTP region; The command "**no spanning-tree max-hop**" restores the default setting.

Parameter: <*hop-count*> sets maximum hops. The valid range is from 1 to 40.

Command mode: Global Mode

Default: The max hop is 20 by default.

Usage Guide: The MSTP uses max-age to count BPDU lifetime. In addition, MSTP also uses max-hop to count BPDU lifetime. The max-hop is degressive in the network. The BPDU has the max value when it initiates from MSTI root bridge. Once the BPDU is received, the value of the max-hop is reduced by 1. When a port receives the BPDU with max-hop as 0, it drops this BPDU and sets itself as designated port to send the BPDU.

Example: Set max hop to 32.

Switch(Config)#spanning-tree max-hop 32

7.3.13 spanning-tree mcheck

Command: spanning-tree mcheck

Function: Force the port to run in the MSTP mode.

Command mode: Interface Mode

Default: The port is in the MSTP mode by default.

Usage Guide: If a network which is attached to the current port is running IEEE 802.1D STP, the port converts itself to run in STP mode. The command is used to force the port to run in the MSTP mode. But once the port receives STP messages, it changes to work in the STP mode again.

This command can only be used when the switch is running in IEEE802.1s MSTP mode. If the switch is running in IEEE802.1D STP mode, this command is invalid.

Example: Force the port 1/2 to run in the MSTP mode.

Switch(Config-Ethernet1/2)#spanning-tree mcheck

7.3.14 spanning-tree mode

Command: spanning-tree mode {mstp|stp}

no spanning-tree mode

Function: Set the spanning-tree mode in the switch; The command "**no spanning-tree mode**" restores the default setting.

Parameter: mstp sets the switch in IEEE802.1s MSTP mode; **stp** sets the switch in IEEE802.1D STP mode.

Command mode: Global Mode

Default: The switch is in the MSTP mode by default.

Usage Guide: When the switch is in IEEE802.1D STP mode, it only sends standard IEEE802.1D BPDU and TCN BPDU. It drops any MSTP BPDUs.

Example: Set the switch in the STP mode.

Switch(Config)#spanning-tree mode stp

7.3.15 spanning-tree mst configuration

Command: spanning-tree mst configuration

no spanning-tree mst configuration

Function: Enter the MSTP mode. Under the MSTP mode, the MSTP attributes can be set. The command "**no spanning-tree mst configuration**" restores the attributes of the MSTP to their default values.

Command mode: Global Mode

Default: The default values of the attributes of the MSTP region are listed as below:

Attribute of MSTP	Default Value
Instance	There is only the instance 0. All the VLANs (1~4094) are mapped to the instance 0.
Name	MAC address of the bridge
Revision	0

Usage Guide: Whether the switch is in the MSTP region mode or not, users can enter the MSTP mode, configure the attributes, and save the configuration. When the switch is running in the MSTP mode, the system will generate the MST configuration identifier according to the MSTP configuration. Only the switches with the same MST configuration identifier are considered as in the same MSTP region.

Example: Enter MSTP region mode.

Switch(Config)#spanning-tree mst configuration

Switch(Config-Mstp-Region)#

7.3.16 spanning-tree mst cost

Command: spanning-tree mst *<instance-id>* cost *<cost>*

no spanning-tree mst <instance-id> cost

Function: Sets path cost of the current port in the specified instance; The command "**no spanning-tree mst <instance-id> cost**" restores the default setting.

Parameter: *<instance-id>* sets the instance ID. The valid range is from 0 to 48. ***<cost>*** sets path cost. The valid range is from 1 to 200,000,000.

Command mode: Interface Mode

Default: By default, the port cost is relevant to the port bandwidth.

Port Type	Default Path Cost	Suggested Range
10Mbps	2000000	2000000~20000000
100Mbps	200000	200000~2000000
1Gbps	20000	20000~200000
10Gbps	2000	2000~20000

For the aggregation ports, the default costs are as below:

Port Type	Allowed Number Of Aggregation Ports	Default Port Cost
10Mbps	N	2000000/N
100Mbps	N	200000/N
1Gbps	N	20000/N
10Gbps	N	2000/N

Usage Guide: By setting the port cost, users can control the cost from the current port to the root bridge in order to control the elections of root port and the designated port of the instance.

Example: On the port 1/2, set the MSTP port cost in the instance 2 to 3000000.

Switch(Config-Ethernet1/2)#spanning-tree mst 2 cost 3000000

7.3.17 spanning-tree mst port-priority

Command: spanning-tree mst <*instance-id*> port-priority <*port-priority*>

no spanning-tree mst <*instance-id*> port-priority

Function: Set the current port priority for the specified instance; The command "**no spanning-tree mst <*instance-id*> port-priority**" restores the default setting.

Parameter: <*instance-id*> sets the instance ID. The valid range is from 0 to 48; **<*port-priority*>** sets port priority. The valid range is from 0 to 240. The value should be the multiples of 16, such as 0, 16, 32…240.

Command mode: Interface Mode

Default: The default port priority is 128.

Usage Guide: By setting the port priority, users can control the port ID of the instance in order to control the root port and designated port of the instance. The lower the value of the port priority is, the higher the priority is.

Example: Set the port priority as 32 on the port 1/2 for the instance 1.

Switch(Config)#interface ethernet 1/2

Switch(Config-Ethernet1/2)#spanning-tree mst 1 port-priority 32

7.3.18 spanning-tree mst priority

Command: spanning-tree mst <*instance-id*> priority <*bridge-priority*>

no spanning-tree mst <*instance-id*> priority

Function: Set the bridge priority for the specified instance; The command "**no spanning-tree mst <*instance-id*> priority**" restores the default setting.

Parameter: <*instance-id*> sets instance ID. The valid range is from 0 to 48;

<bridge-priority> sets the switch priority. The valid range is from 0 to 61440. The value should be the multiples of 4096, such as 0, 4096, 8192…61440.

Command mode: Global Mode

Default: The default bridge priority is 32768.

Usage Guide: By setting the bridge priority, users can change the bridge ID for the specified instance. And the bridge ID can influence the elections of root bridge and designated port for the specified instance.

Example: Set the priority for Instance 2 to 4096.

Switch(Config)#spanning-tree mst 2 priority 4096

7.3.19 spanning-tree portfast

Command: spanning-tree portfast

no spanning-tree portfast

Function: Set the current port as boundary port; The command "**no spanning-tree portfast**" sets the current port as non-boundary port.

Command mode: Interface Mode

Default: All the ports are non-boundary ports by default when enabling MSTP.

Usage Guide: When a port is set to be a boundary port, the port converts its status from discarding to forwarding without bearing forward delay. Once the boundary port receives the BPDU, the port becomes a non-boundary port.

Example: Set port 1/5-6 as boundary ports.

Switch(Config)#interface ethernet 1/5-6

Switch(Config-Port-Range)#spanning-tree portfast

7.3.20 spanning-tree digest-snooping

Command:spanning-tree digest-snooping

no spanning-tree digest-snooping

Function: Configure the port to use the authentication string of partner port .the command "**no spanning-tree digest-snooping**" restores to use the port generated authentication string.

Default: Don't use the authentication string of partner port .

Command mode: Interface mode

Usage Guide: According to MSTP protocol, the region authentication string is generated by MD5 algorithm with public authentication key,intstance ID, VLAN ID. Some manufactory don't use the public authentication key, this causes the incompatibility . After the command is executed the port can use the authentication string of partner port ,

realize compatibility with these manufactories equipment .

Note:Because the authentication string is related to instance ID and VLAN ID, the command may cause recognizing the equipment that with different instance and VLAN relation as in the same region. Before the command is executed, make sure that instance and VLAN relation is accord for all the equipment. If there are more than one equipment connected , all the connected ports should execute this command.

Example:

Switch(Config)#interface ethernet 1/2

Switch(Config-Ethernet-1/2)#spanning-tree digest-snooping

Switch(Config-Ethernet-1/2)#

7.3.21 spanning-tree tcflush (global mode)

Command:spanning-tree tcflush enable

spanning-tree tcflush disable

spanning-tree tcflush protect

no spanning-tree tcflush

Function: Configure the spanning-tree flush mode once the topology changes. “no spanning-tree tcflush” restores to default setting

Parameter:

Enable:the spanning-tree flush once the topology changes.

Disable:the spanning tree don’t flush when the topology changes.

Protect: the spanning-tree flush every ten seconds

Default: enable。

Command mode: Global mode。

Usage Guide: According to MSTP , when topology changes, the port that send change message clears MAC/ARP table (FLUSH). In fact it is not needed for some network environment to do FLUSH with every topology change. At the same time ,as a method to avoid network assault, we allow the network administrator to configure FLUSH mode by the command

Note:For the complicated network, especially need to switch from one spanning tree branch to another rapidly, the disable mode is not recommended.

Example:

Switch(Config)#spanning-tree tcflush disable

Switch(Config)#

7.3.22 spanning-tree tcflush (port mode)

Command:spanning-tree tcflush {enable| disable| protect}

no **spanning-tree tcflush**

Function: Configure the spanning-tree flush mode for port once the topology changes . “no spanning-tree tcflush” restores to default setting

Parameter:

Enable:the spanning-tree flush once the topology changes.

Disable:the spanning tree don’t flush when the topology changes.

Protect: the spanning-tree flush every ten seconds

Default: Global configuration

Command mode: Interface mode

Usage Guide: According to MSTP , when topology changes, the port that send change message clears MAC/ARP table (FLUSH). In fact it is not needed for some network environment to do FLUSH with every topology change. At the same time ,as a method to avoid network assault, we allow the network administrator to configure FLUSH mode by the command

Note:For the complicated network, especially need to switch from one spanning tree branch to another rapidly, the disable mode is not recommended.

Example:

Switch(Config)#interface ethernet 1/2

Switch(Config-Ethernet-1/2)#spanning-tree tcflush disable

Switch(Config-Ethernet-1/2)#

7.4 MSTP Example

The following is a typical MSTP application scenario:

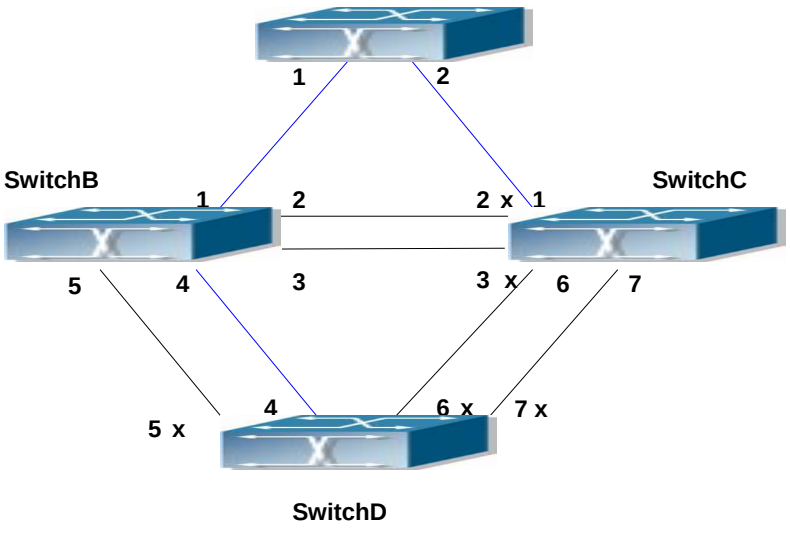


Figure 7-2 Typical MSTP Application Scenario

The connections among the switches are shown in the above figure. All the switches run in the MSTP mode by default, their bridge priority, port priority and port route cost are all in the default values (equal). The default configuration for switches is listed below:

Bridge Name		SwitchA	SwitchB	SwitchC	SwitchD
Bridge MAC Address		…00-00-01	…00-00-02	…00-00-03	…00-00-04
Bridge Priority		32768	32768	32768	32768
Port Priority	Port 1	128	128	128	
	Port 2	128	128	128	
	Port 3		128	128	
	Port 4		128		128
	Port 5		128		128
	Port 6			128	128
	Port 7			128	128
Route Cost	Port 1	200000	200000	200000	
	Port 2	200000	200000	200000	
	Port 3		200000	200000	
	Port 4		200000		200000
	Port 5		200000		200000
	Port 6			200000	200000
	Port 7			200000	200000

By default, the MSTP establishes a tree topology (in blue lines) rooted with SwitchA. The ports marked with “x” are in the discarding status, and the other ports are in the forwarding status.

Configurations Steps:

Step 1: Configure port to VLAN mapping:

- Create VLAN 20, 30, 40, 50 in SwitchB, SwitchC and SwitchD.
- Set ports 1-7 as trunk ports in SwitchB, SwitchC and SwitchD.

Step 2: Set SwitchB, SwitchC and SwitchD in the same MSTP:

- Set SwitchB, SwitchC and SwitchD to have the same region name as mstp.
- Map VLAN 20 and VLAN 30 in SwitchB, SwitchC and SwitchD to Instance 3; Map VLAN 40 and VLAN 50 in SwitchB, SwitchC and SwitchD to Instance 4.

Step 3: Set SwitchC as the root bridge of Instance 3; Set SwitchD as the root bridge of Instance 4

- Set the bridge priority of Instance 3 in SwitchC as 0.
- Set the bridge priority of Instance 4 in SwitchD as 0.

The detailed configuration is listed below:

SwitchB:

```
SwitchB(Config)#vlan 20
SwitchB(Config-Vlan20)#exit
SwitchB(Config)#vlan 30
SwitchB(Config-Vlan30)#exit
SwitchB(Config)#vlan 40
SwitchB(Config-Vlan40)#exit
SwitchB(Config)#vlan 50
SwitchB(Config-Vlan50)#exit
SwitchB(Config)#spanning-tree mst configuration
SwitchB(Config-Mstp-Region)#description mstp
SwitchB(Config-Mstp-Region)#instance 3 vlan 20;30
SwitchB(Config-Mstp-Region)#instance 4 vlan 40;50
SwitchB(Config-Mstp-Region)#exit
SwitchB(Config)#interface e1/1-7
SwitchB(Config-Port-Range)#switchport mode trunk
SwitchB(Config-Port-Range)#exit
SwitchB(Config)#spanning-tree
```

SwitchC:

```
SwitchC(Config)#vlan 20
SwitchC(Config-Vlan20)#exit
SwitchC(Config)#vlan 30
SwitchC(Config-Vlan30)#exit
SwitchC(Config)#vlan 40
SwitchC(Config-Vlan40)#exit
SwitchC(Config)#vlan 50
SwitchC(Config-Vlan50)#exit
SwitchC(Config)#spanning-tree mst configuration
SwitchC(Config-Mstp-Region)#description mstp
SwitchC(Config-Mstp-Region)#instance 3 vlan 20;30
SwitchC(Config-Mstp-Region)#instance 4 vlan 40;50
SwitchC(Config-Mstp-Region)#exit
SwitchC(Config)#interface e1/1-7
SwitchC(Config-Port-Range)#switchport mode trunk
SwitchC(Config-Port-Range)#exit
```

SwitchC(Config)#spanning-tree
SwitchC(Config)#spanning-tree mst 3 priority 0

SwitchD:

SwitchD(Config)#vlan 20
SwitchD(Config-Vlan20)#exit
SwitchD(Config)#vlan 30
SwitchD(Config-Vlan30)#exit
SwitchD(Config)#vlan 40
SwitchD(Config-Vlan40)#exit
SwitchD(Config)#vlan 50
SwitchD(Config-Vlan50)#exit
SwitchD(Config)#spanning-tree mst configuration
SwitchD(Config-Mstp-Region)#description mstp
SwitchD(Config-Mstp-Region)#instance 3 vlan 20;30
SwitchD(Config-Mstp-Region)#instance 4 vlan 40;50
SwitchD(Config-Mstp-Region)#exit
SwitchD(Config)#interface e1/1-7
SwitchD(Config-Port-Range)#switchport mode trunk
SwitchD(Config-Port-Range)#exit
SwitchD(Config)#spanning-tree
SwitchD(Config)#spanning-tree mst 4 priority 0

After the above configuration, SwitchA is the root bridge of the instance 0 of the entire network. In the MSTP region which SwitchB, SwitchC and SwitchD belong to, SwitchB is the region root of the instance 0, SwitchC is the region root of the instance 3 and SwitchD is the region root of the instance 4. The traffic of VLAN 20 and VLAN 30 is sent through the topology of the instance 3. The traffic of VLAN 40 and VLAN 50 is sent through the topology of the instance 4. And the traffic of other VLANs is sent through the topology of the instance 0. The port 1 in SwitchB is the master port of the instance 3 and the instance 4.

The MSTP calculation generates 3 topologies: the instance 0, the instance 3 and the instance 4 (marked with blue lines). The ports with the mark “x” are in the status of discarding. The other ports are the status of forwarding. Because the instance 3 and the instance 4 are only valid in the MSTP region, the following figure only shows the topology of the MSTP region.

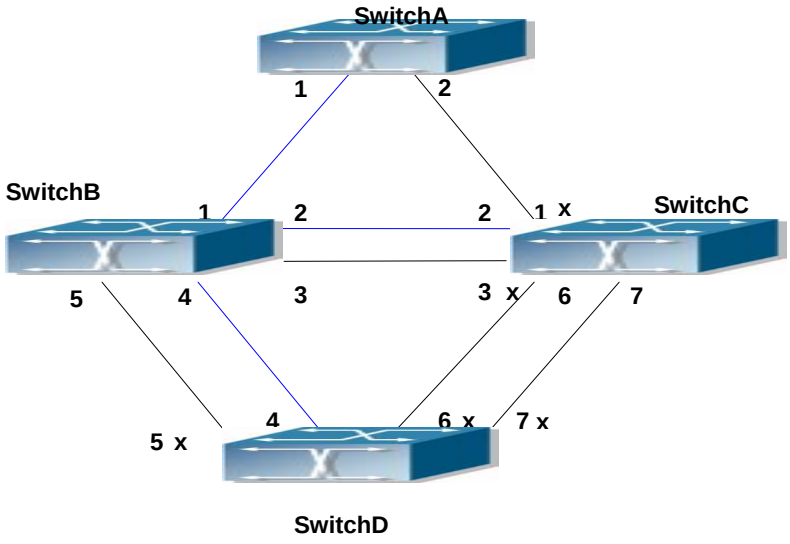


Figure 7-3 The Topology Of the Instance 0 after the MSTP Calculation

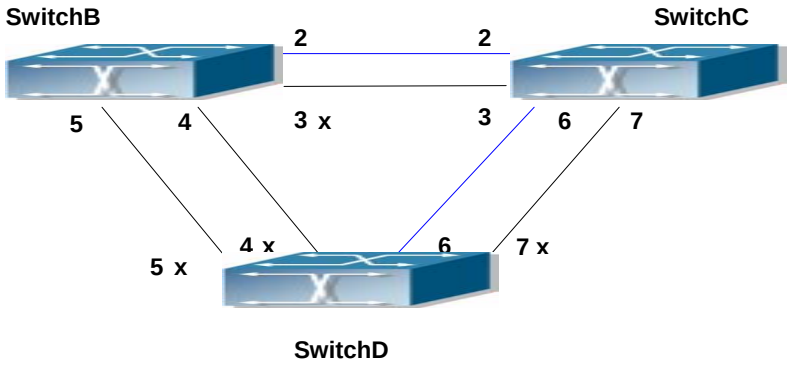


Figure 7-4 The Topology Of the Instance 3 after the MSTP Calculation

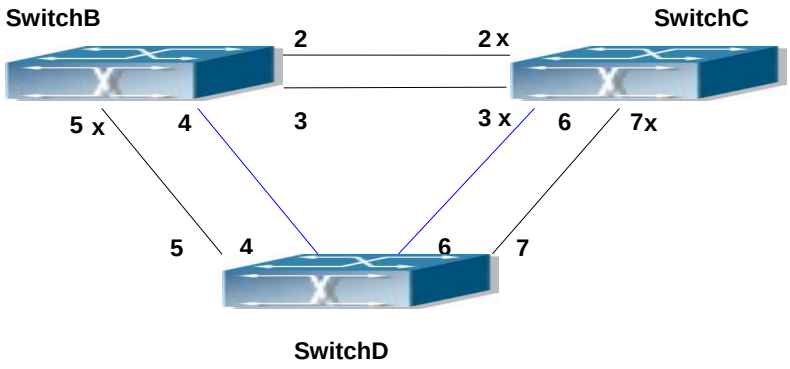


Figure 7-5 The Topology Of the Instance 4 after the MSTP Calculation

7.5 MSTP Troubleshooting

- In order to run the MSTP on the switch port, the MSTP has to be enabled globally. If the MSTP is not enabled globally, it can't be enabled on the port.
- The MSTP parameters co work with each other, so the parameters should meet the following conditions. Otherwise, the MSTP may work incorrectly.

  2×(Bridge_Forward_Delay -1.0 seconds) >= Bridge_Max_Age

  Bridge_Max_Age >= 2 ×(Bridge_Hello_Time + 1.0 seconds)
- When users modify the MSTP parameters, they have to be sure about the changes of the topologies. The global configuration is based on the bridge. Other configurations are based on the individual instances.
- The MSTP are mutually exclusive with MAC binding and IEEE 802.1x on the switch port. If MAC binding or IEEE 802.1x is enabled on the port, the MSTP can't apply to this port.

7.5.1 Commands for Monitor And Debug

7.5.1.1 show spanning-tree

Command: show spanning-tree [mst [<*instance-id*>]] [interface <*interface-list*>] [detail]

Function: Display the MSTP Information.

Parameter: ***<instance-id>*** sets the instance ID. The valid range is from 0 to 48; ***<interface-list>*** sets interface list; **detail** sets the detailed spanning-tree information.

Command mode: Admin Mode

Usage Guide: This command can display the MSTP information of the instances in the current bridge.

Example: Display the bridge MSTP.

```
Switch#sh spanning-tree
                        -- MSTP Bridge Config Info --
Standard        :   IEEE 802.1s
Bridge MAC      :   00: 03: 0f: 01: 0e: 30
Bridge Times :   Max Age 20, Hello Time 2, Forward Delay 15
Force Version:   3
############################ Instance 0 ############################
Self Bridge Id     : 32768 -   00: 03: 0f: 01: 0e: 30
Root Id                : 16384.00: 03: 0f: 01: 0f: 52
```

```
Ext.RootPathCost : 200000
Region Root Id     : this switch
Int.RootPathCost : 0
Root Port ID        : 128.1
Current port list in Instance 0:
Ethernet1/1 Ethernet1/2 (Total 2)
PortName          ID          ExtRPC     IntRPC    State Role        DsgBridge        DsgPort
-------------- ------- --------- --------- --- ---- ------------------ -------
Ethernet1/1    128.001              0              0 FWD ROOT 16384.00030f010f52 128.007
Ethernet1/2    128.002              0              0 BLK ALTR 16384.00030f010f52 128.011
############################## Instance 3 ##############################
Self Bridge Id     : 0.00: 03: 0f: 01: 0e: 30
Region Root Id     : this switch
Int.RootPathCost : 0
Root Port ID       : 0
Current port list in Instance 3:
Ethernet1/1 Ethernet1/2 (Total 2)
   PortName          ID       IntRPC     State Role        DsgBridge        DsgPort
-------------- ------- --------- --- ---- ------------------ -------
  Ethernet1/1    128.001              0 FWD MSTR        0.00030f010e30 128.001
  Ethernet1/2    128.002              0 BLK ALTR        0.00030f010e30 128.002
############################## Instance 4 ##############################
Self Bridge Id     : 32768.00: 03: 0f: 01: 0e: 30
Region Root Id     : this switch
Int.RootPathCost : 0
Root Port ID       : 0
Current port list in Instance 4:
Ethernet1/1 Ethernet1/2 (Total 2)
PortName          ID       IntRPC     State Role        DsgBridge        DsgPort
-------------- ------- --------- --- ---- ------------------ -------
Ethernet1/1 128.001              0 FWD MSTR 32768.00030f010e30 128.001
Ethernet1/2 128.002              0 BLK ALTR 32768.00030f010e30 128.002
```

Displayed Information	Description
Bridge Information	
Standard	STP version
Bridge MAC	Bridge MAC address
Bridge Times	Max Age, Hello Time and Forward Delay of the bridge
Force Version	Version of STP

Instance Information	
Self Bridge Id	The priority and the MAC address of the current bridge for the current instance
Root Id	The priority and the MAC address of the root bridge for the current instance
Ext.RootPathCost	Total cost from the current bridge to the root of the entire network
Int.RootPathCost	Cost from the current bridge to the region root of the current instance
Root Port ID	Root port of the current instance on the current bridge
MSTP Port List Of The Current Instance	
PortName	Port name
ID	Port priority and port index
ExtRPC	Port cost to the root of the entire network
IntRPC	Cost from the current port to the region root of the current instance
State	Port status of the current instance
Role	Port role of the current instance
DsgBridge	Upward designated bridge of the current port in the current instance
DsgPort	Upward designated port of the current port in the current instance

7.5.1.2 show spanning-tree mst config

Command: show spanning-tree mst config

Function: Display the configuration of the MSTP in the Admin mode.

Command mode: Admin Mode

Usage Guide: In the Admin mode, this command can show the parameters of the MSTP configuration such as MSTP name, revision, VLAN and instance mapping.

Example: Display the configuration of the MSTP on the switch.

```
Switch#show spanning-tree mst config
Name      switch
Revision  0
Instance  Vlans Mapped
---------------------------------
00        1-29, 31-39, 41-4094
```

03 30

04 40

7.5.1.3 show mst-pending

Command: show mst-pending

Function: In the MSTP region mode, display the configuration of the current MSTP region.

Command mode: MSTP Region Mode

Usage Guide: In the MSTP region mode, display the configuration of the current MSTP region such as MSTP name, revision, VLAN and instance mapping.

Note: Before quitting the MSTP region mode, the displayed parameters may not be effective.

Example: Display the configuration of the current MSTP region.

Switch(Config)#spanning-tree mst configuration

Switch(Config-Mstp-Region)#show mst-pending

Name switch

Revision 0

Instance Vlans Mapped

---

00 1-29, 31-39, 41-4093

03 30

04 40

05 4094

Switch(Config-Mstp-Region)#

7.5.1.4 debug spanning-tree

Command: debug spanning-tree

no debug spanning-tree

Function: Enable the MSTP debugging information; The command "**no debug spanning-tree**" disables the MSTP debugging information

Command mode: Admin Mode

Usage Guide: This command is the general switch for all the MSTP debugging. Users should enable the detailed debugging information, then they can use this command to display the relevant debugging information. In general, this command is used by skilled technicians.

Example: Enable to receive the debugging information of BPDU messages on the port

1/1

Switch#debug spanning-tree

Switch#debug spanning-tree bpdu rx interface e1/1

7.6 Web Management

Click “MSTP control” to enter MSTP control configuration mode to manage MSTP features for the switch.

7.6.1 MSTP field operation

Click “MSTP control” to enter MSTP field operation.

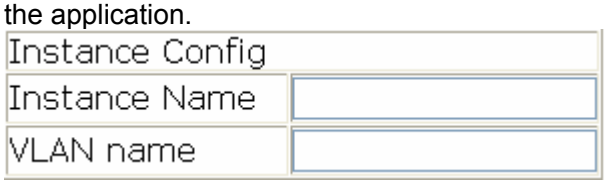
7.6.1.1 Instance configuration

Click “MSTP control” to enter MSTP field operation, then Instance configuration.

Create the Instance and configure the VLAN-Instance mapping or add VLAN table entry mapping to specified Instance.

Configure mapping between VLAN1-10;100-110 and Instance 1. Equivalent command 1.2.1.3.

Set Instance name to 1, VLAN name to VLAN1-10;100-110. Click "Apply" to commit the application.

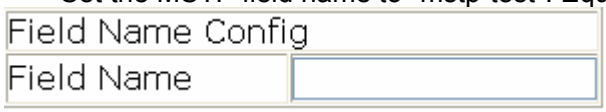


7.6.1.2 Field operation

Click “MSTP control” to enter the MSTP field operation.

Configure MSTP field name under MSTP field configuration mode.

Set the MSTP field name to "mstp-test". Equivalent command 1.2.1.4.

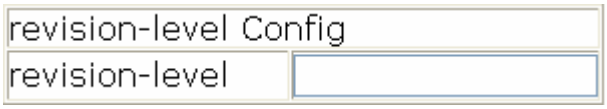


7.6.1.3 Revision level control

Click “MSTP control” to enter MSTP field operation, then "revision-level Config".

Configure the revision level value for calculating MST configuration ID under MST configuration mode.

Set the revision level to 2000.



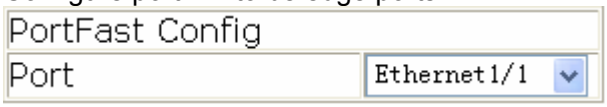
7.6.2 MSTP port operation

7.6.2.1 Edge port setting

Click “MSTP control” to enter MSTP field operation, then "PortFast Config".

Set the port to be an edge port

Configure port 1/1 to be edge ports.

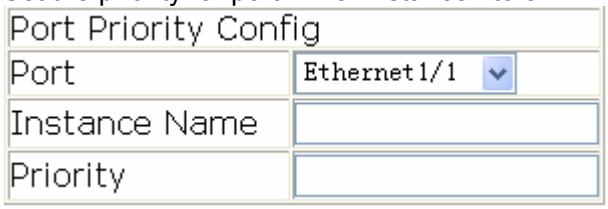


7.6.2.2 Port priority setting

Click “MSTP control” to enter MSTP port operation, then "Port Priority Config".

Set the priority for the current port on specified instance

Set the priority for port 1/1 of instance1 to 32.

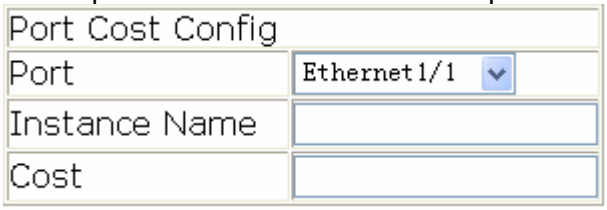


7.6.2.3 Port route cost setting

Click “MSTP control” to enter MSTP port operation, then "Port Cost Config".

Set the port route cost on specified instance for the current port

Set on port 1/1 route cost of the MSTP port corresponding to Instance 2 to 3000000.



7.6.2.4 MSTP mode

Click “MSTP control” to enter MSTP port operation, then "MSTP Mode".

Force switch port migrate to run under MSTP.

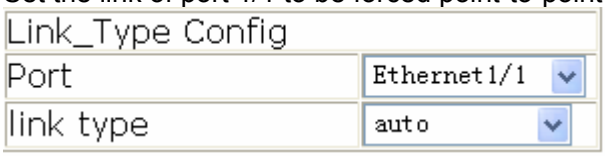
Force port 1/1 migrate to run under MSTP.

7.6.2.5 Link type configuration

Click “MSTP control” to enter MSTP port operation, then "Link_Type Config".

Set the link type of the current port.

Set the link of port 1/1 to be forced point-to-point type.

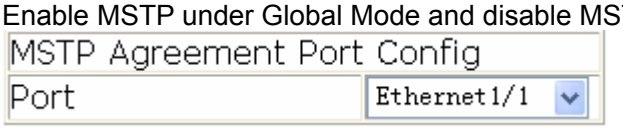


7.6.2.6 MSTP port configuration

Click “MSTP control” to enter MSTP port operation, then "MSTP Agreement Port Config".

Run the command to enable MSTP under the switch port configuration mode.

Enable MSTP under Global Mode and disable MSTP for port 1/1.



7.6.3 MSTP global control

7.6.3.1 MSTP global protocol port configuration

Click “MSTP control” to enter MSTP Global control, then "MSTP Global Agreement Port Config".

Run MSTP enable command under the switch port configuration mode.

Enable MSTP in Global mode.

7.6.3.2 Forward delay time configuration

Click “MSTP control” to enter MSTP Global control, then "Forward-time Config".

Set the value for switch forward delay time

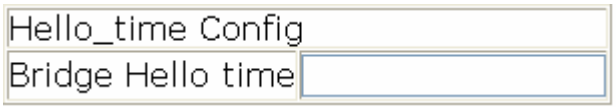
Set MSTP forward delay time to 20 seconds in Global Mode.

7.6.3.3 Hello_time configuration

Click “MSTP control” to enter MSTP Global control, then "Hello_time Config".

Set the Hello time for the switch.

Set MSTP Hello time to 5 seconds in Global Mode.

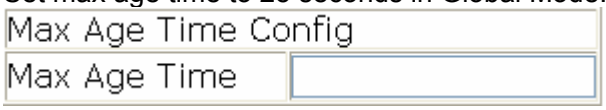


7.6.3.4 Set the max age time for BPDU information in the switch

Click “MSTP control”, MSTP Global Control, then enter the switch BPDU message "Max Age Time Config".

Set the max age time for BPDU information in the switch

Set max age time to 25 seconds in Global Mode.

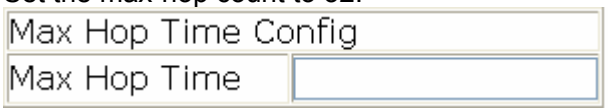


7.6.3.5 Set the max hop count support for BPDU transmitting in MSTP field

Click “MSTP control”, “MSTP Global control”, then set the BPDU "Max Hop Time Config" to support transmission in MSTP field.

Set the max hop count support for BPDU transmitting in MSTP field.

Set the max-hop count to 32.

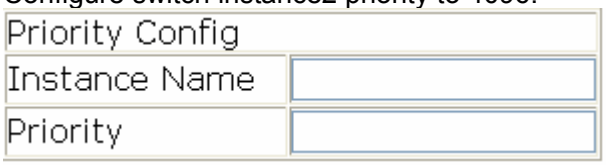


7.6.3.6 Set bridge priority of the specified instance for the switch

Click “MSTP control”, “MSTP Global control”, enter the "Priority Config" to set bridge priority for the switch for the specified instance.

Set bridge priority of the specified instance for the switch

Configure switch instance2 priority to 4096.



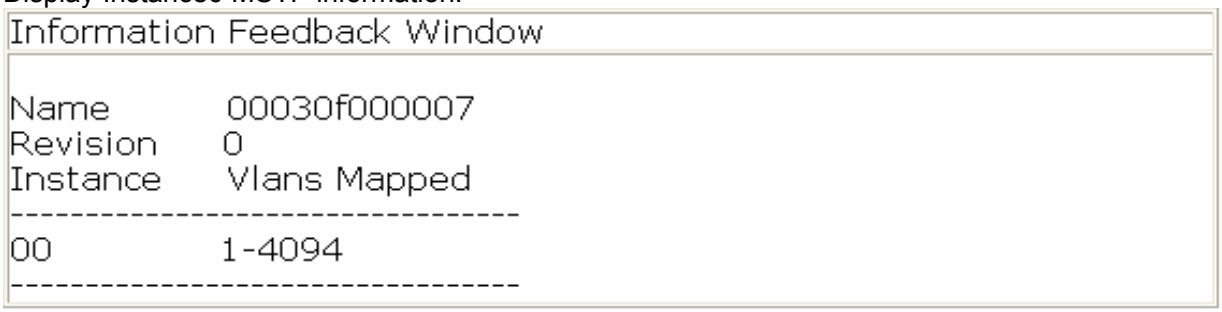
7.6.4 Show MSTP setting

7.6.4.1 Instance information

Click MSTPL control, “show MSTP settings”, enter "Instance Information".

Display MSTP and instances information.

Display Instance0 MSTP information.



7.6.4.2 MSTP field information

Click “MSTP control”, “show MSTP setting”, enter "MSTP Field Information".

Display effective MSTP field parameter configurations.

Chapter 8 QoS And PBR Configuration

8.1 QoS Configuration

8.1.1 Introduction to QoS

QoS (Quality of Service) is a set of capabilities that allow you to create differentiated services for network traffic, thereby providing better service for selected network traffic. QoS is a guarantee for service quality of consistent and predictable data transfer service to fulfill program requirements. QoS cannot generate extra bandwidth but provides more effective bandwidth management according to the application requirement and network management policy.

8.1.1.1 QoS Terms

CoS: Class of Service, the classification information carried by Layer 2 802.1Q frames, taking 3 bits of the Tag field in frame header, is called user priority level in the range of 0 to 7.

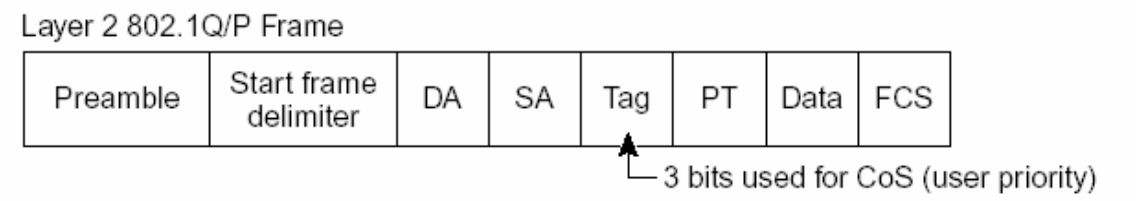


Fig 8-1 CoS priority

ToS: Type of Service, a one-byte field carried in Layer 3 IPv4 packet header to symbolize the service type of IP packets. Among ToS field can be IP Precedence value or DSCP value.

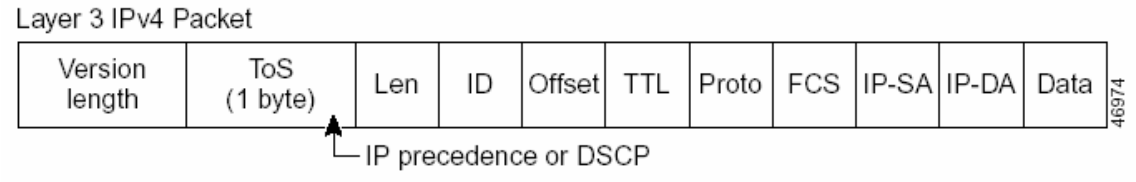


Fig 8-2 ToS priority

IP Precedence: IP priority.Classification information carried in Layer 3 IP packet header, occupying 3 bits, in the range of 0 to 7.

DSCP: Differentiated Services Code Point, classification information carried in Layer 3 IP packet header, occupying 6 bits, in the range of 0 to 63, and is downward compatible with IP Precedence.

Classification: The entry action of QoS, classifying packet traffic according to the classification information carried in the packet and ACLs.

Policing: Ingress action of QoS that lays down the policing policy and manages the classified packets.

Remark: Ingress action of QoS, perform allowing, degrading or discarding operations to packets according to the policing policies.

Queuing: Egress QoS action. Put the packets to appropriate egress queues according to the packet CoS value.

Scheduling: QoS egress action. Configure the weight for eight egress queues WRR (Weighted Round Robin).

In Profile: Traffic within the QoS policing policy range (bandwidth or burst value) is called “In Profile".

Out of Profile: Traffic out the QoS policing policy range (bandwidth or burst value) is called “Out of Profile".

8.1.1.2 QoS Implementation

To implement Layer 3 switch software QoS, a general, mature reference model should be given. QoS can not create new bandwidth, but can maximize the adjustment and configuration for the current bandwidth resource. Fully implemented QoS can achieve complete management over the network traffic. The following is as accurate as possible a description of QoS.

The data transfer specifications of IP cover only addresses and services of source and destination, and ensure correct packet transmission using OSI layer 4 or above protocols such as TCP. However, rather than provide a mechanism for providing and protecting packet transmission bandwidth, IP provide bandwidth service by the best effort. This is acceptable for services like Mail and FTP, but for increasing multimedia business data and e-business data transmission, this best effort method cannot satisfy the bandwidth and low-lag requirement.

Based on differentiated service, QoS specifies a priority for each packet at the ingress. The classification information is carried in Layer 3 IP packet header or Layer 2 802.1Q frame header. QoS provides same service to packets of the same priority, while offers different operations for packets of different priority. QoS-enabled switch or router can provide different bandwidth according to the packet classification information, and can remark on the classification information according to the policing policies configured,

and may discard some low priority packets in case of bandwidth shortage.

If devices of each hop in a network support differentiated service, an end-to-end QoS solution can be created. QoS configuration is flexible, the complexity or simplicity depends on the network topology and devices and analysis to incoming/outgoing traffic.

8.1.1.3 Basic QoS Model

The basic QoS consists of five parts: Classification, Policing, Remark, Queuing and Scheduling, where classification, policing and remark are sequential ingress actions, and Queuing and Scheduling are QoS egress actions.

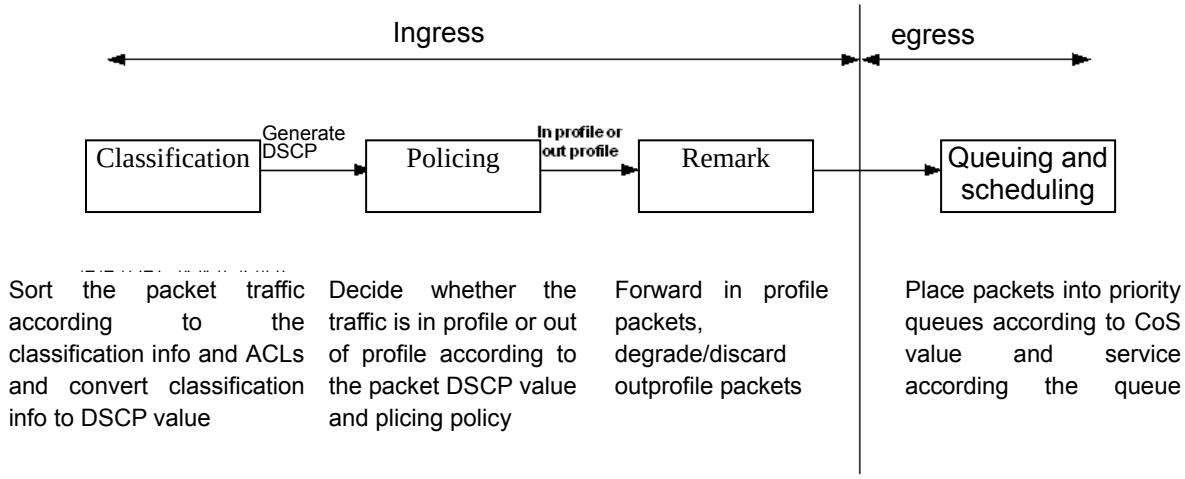


Fig 8-3 Basic QoS Model

Classification: Classify traffic according to packet classification information and generate internal DSCP value based on the classification information. For different packet types and switch configurations, classification is performed differently; the flowchart below explains this in detail.

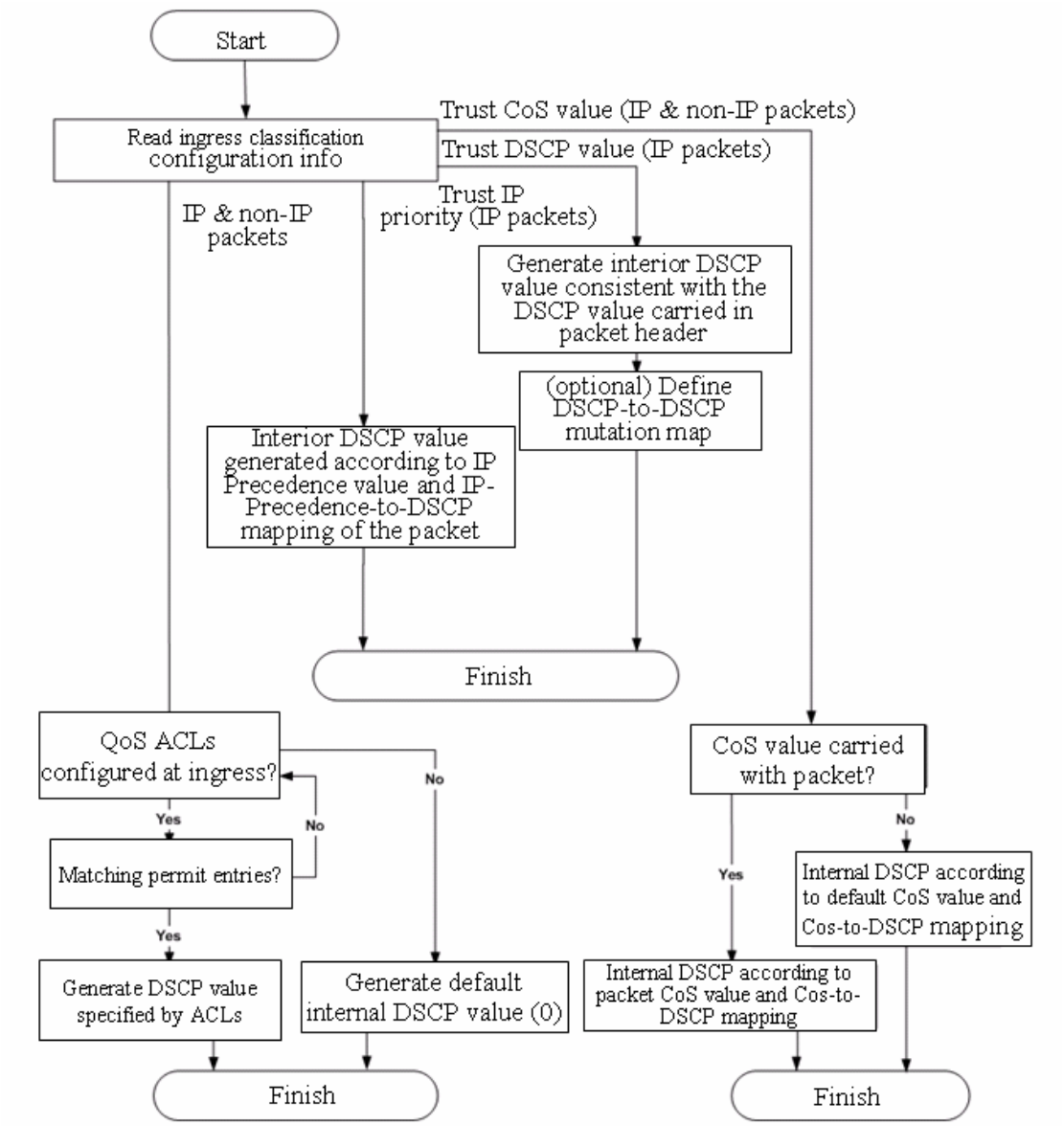


Fig 8-4 Classification process

Policing and remark: Each packet in classified ingress traffic is assigned an internal DSCP value and can be policed and remarked.

Policing can be performed based on DSCP value to configure different policies that allocate bandwidth to classified traffic. If the traffic exceeds the bandwidth set in the policy (out of profile), the out of profile traffic can be allowed, discarded or remarked. Remarking uses a new DSCP value of lower priority to replace the original higher level DSCP value in the packet; this is also called “marking down”. The following flowchart describes the operations during policing and remarking.

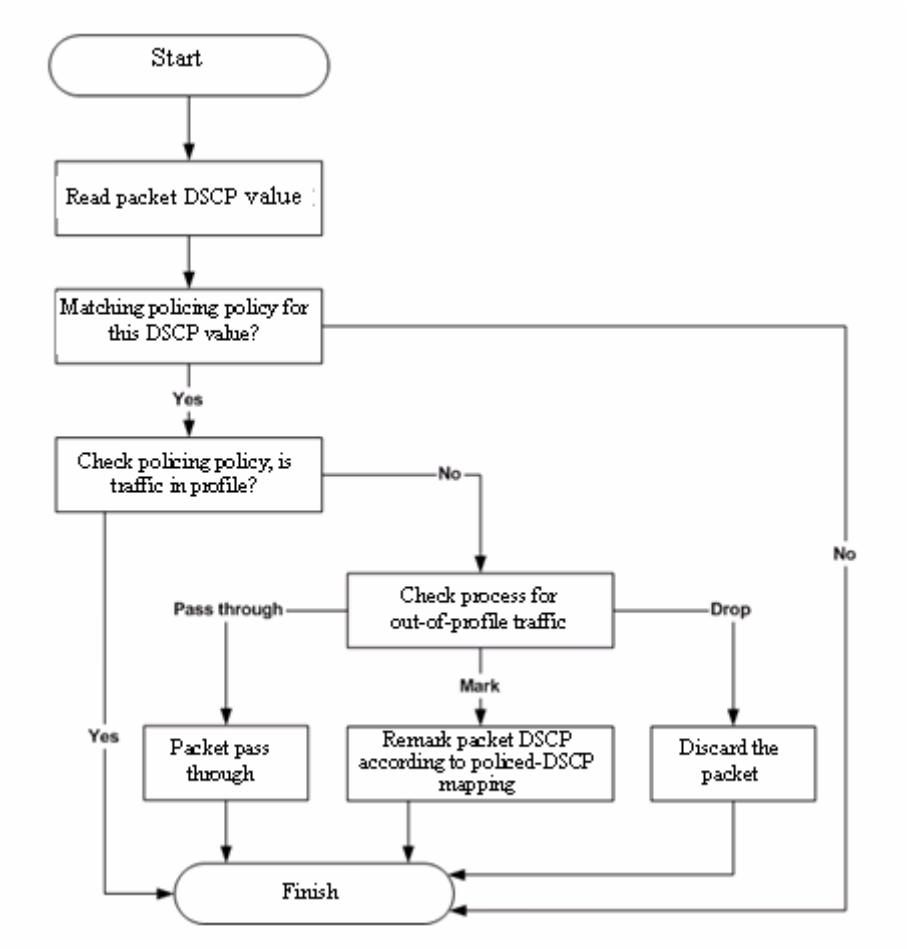


Fig 8-5 Policing and Remarking process

Queuing and scheduling: Packets at the egress will re-map the internal DSCP value to CoS value, the queuing operation assigns packets to appropriate queues of priority according to the CoS value; while the scheduling operation performs packet forwarding according to the prioritized queue weight. The following flowchart describes the operations during queuing and scheduling.

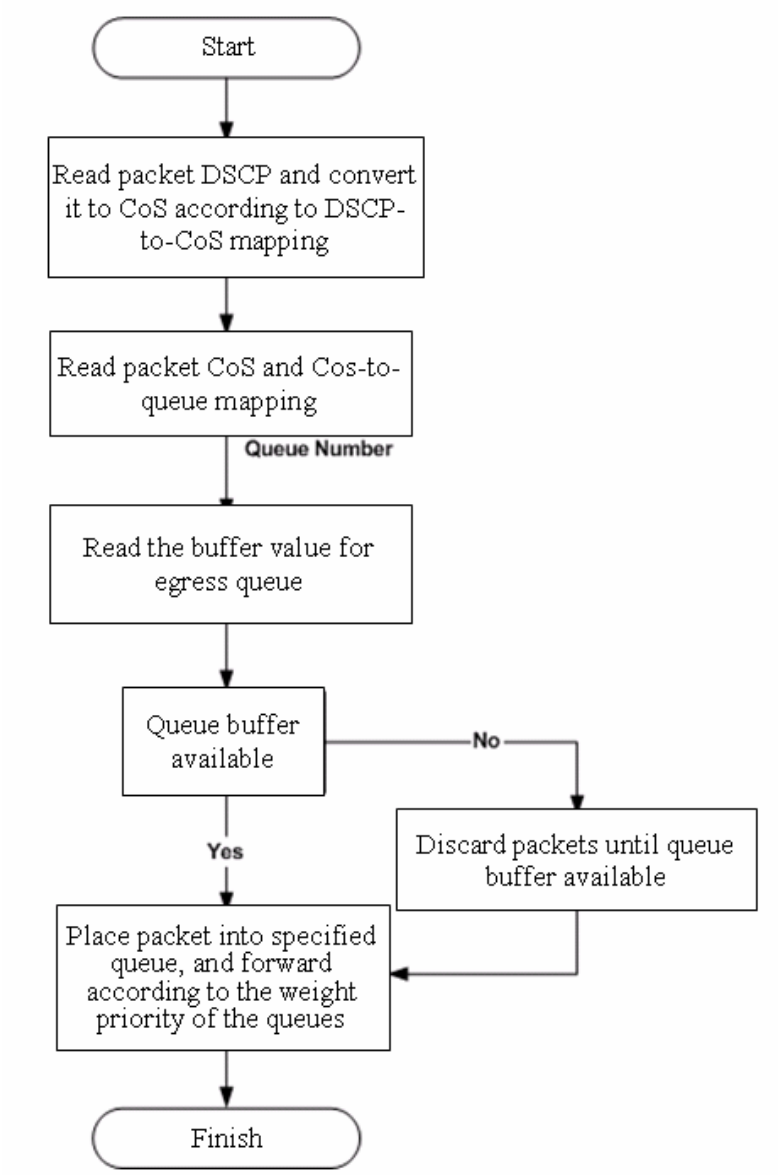


Fig 8-6 Queuing and Scheduling process

8.1.2 QoS Configuration Task List

1. Enable QoS

   QoS can be enabled or disabled in Global Mode. QoS must be enabled first in Global Mode to configure the other QoS commands.

2. Configure class map.

   Set up a classification rule according to ACL, VLAN ID, IP Precedence or DSCP to classify the data stream. Different classes of data streams will be processed with different policies.

3. Configure a policy map.

   After data steam classification, a policy map can be created to associate with the class map created earlier and enter class mode. Then different policies (such as bandwidth limit, priority degrading, assigning new DSCP value) can be applied to different data streams. You can also define a policy set that can be use in a policy map by several classes.

4. Apply QoS to the ports

   Configure the trust mode for ports or bind policies to ports. A policy will only take effect on a port when it is bound to that port.

5. Configure queue out method and weight

   Configure queue out to PQ or WRR, set the proportion of the 8 egress queues bandwidth and mapping from internal priority to egress queue.

6. Configure QoS mapping

   Configure the mapping from CoS to DSCP, DSCP to CoS, DSCP to DSCP mutation, IP precedence to DSCP, and policed DSCP.

1. Enable QoS

Command	Explanation
Global Mode	
mls qos **no mls qos**	Enable/disable QoS function.

2. Configure class map.

Command	Explanation
Global Mode	
class-map <*class-map-name*> **no class-map <*class-map-name*>**	Create a class map and enter class map mode; the "**no class-map <*class-map-name*>**" command deletes the specified class map.
match {access-group <*acl-index-or-name*> | ip dscp <*dscp-list*>| ip precedence <*ip-precedence-list*>| ipv6 access-group <*acl-index-or-name*> | ipv6 dscp <*dscp-list*>| ipv6 flowlabel <*flowlabel-list*>| vlan <*vlan-list*>|cos<*cost-list*>} **no match {access-group | ip dscp | ip precedence | ipv6 access-group | ipv6 dscp | ipv6 flowlabel | vlan |cos }**	Set matching criterion (classify data stream by ACL, DSCP, VLAN or priority, etc) for the class map; the "**no match {access-group | ip dscp | ip precedence | ipv6 access-group | ipv6 dscp | ipv6 flowlabel | vlan |cos }**" command deletes specified matching criterion.

3. Configure a policy map.

Command	Explanation

Global Mode	
policy-map <*policy-map-name*> **no policy-map <*policy-map-name*>**	Create a policy map and enter policy map mode; the "**no policy-map <*policy-map-name*>**" command deletes the specified policy map.
class <*class-map-name*> **no class <*class-map-name*>**	After a policy map is created, it can be associated to a class. Different policy or new DSCP value can be applied to different data streams in class mode; the "**no class <*class-map-name*>**" command deletes the specified class.
set {ip dscp <*new-dscp*> | ip precedence <*new-precedence*>|ipv6 dscp <*new-dscp*> | ipv6 flowlabel <*new-flowlabel*>|cos<*new cos*>} **no set {ip dscp | ip precedence|ipv6 dscp | ipv6 flowlabel |cos<*new cos*>}**	Assign a new DSCP and IP precedence value for the classified traffic; the "**no set {ip dscp | ip precedence|ipv6 dscp | ipv6 flowlabel |cos<*new cos*>}**" command cancels the newly assigned value.
police <*rate-kbps*> <*burst-kbyte*> [exceed-action {drop | policed-dscp-transmit}] **no police <*rate-kbps*> <*burst-kbyte*> [exceed-action {drop | policed-dscp-transmit}]**	Configure a policy to classify traffic, data stream exceeding the limit will be dropped or degraded; the "**no police <*rate-kbps*> <*burst-kbyte*> [exceed-action {drop | policed-dscp-transmit}]**" command deletes the specified policy.
mls qos aggregate-policer <*aggregate-policer-name*> <*rate-kbps*> <*burst-kbyte*> exceed-action {drop |policed-dscp-transmit} **no mls qos aggregate-policer <*aggregate-policer-name*>**	Define a policy set, perform different actions to out-of-profile data streams, such as discard or degrade. This policy can be used in one policy map by several classes; the "**no mls qos aggregate-policer <*aggregate-policer-name*>**" command deletes the specified policy set.
police aggregate <*aggregate-policer-name*> **no police aggregate <*aggregate-policer-name*>**	Apply a policy set to classified traffic; the "**no police aggregate <*aggregate-policer-name*>**" command deletes the specified policy

	set.

4. Apply QoS to ports

Command	Explanation
Interface Mode	
mls qos trust [cos [pass-through-dscp]|dscp [pass-through-cos]|ip-precedence [pass-through cos]|port priority <*cos*>] **no mls qos trust**	Configure port trust; the "**no mls qos trust**" command disables the current trust status of the port.
mls qos cos {<*default-cos*> } **no mls qos cos**	Configure the default CoS value of the port; the "**no mls qos cos**" command restores the default setting.
service-policy {input <*policy-map-name*> | output <*policy-map-name*>} **no service-policy {input <*policy-map-name*> | output <*policy-map-name*>}**	Apply a policy map to the specified port; the "**no service-policy {input <*policy-map-name*> | output <*policy-map-name*>}**" command deletes the specified policy map applied to the port. Egress policy map is not supported yet.
mls qos dscp-mutation <*dscp-mutation-name*> **no mls qos dscp-mutation <*dscp-mutation-name*>**	Apply DSCP mutation mapping to the port; the "**no mls qos dscp-mutation <*dscp-mutation-name*>**" command restores the DSCP mutation mapping default.

5. Configure queue out method and weight

Command	Explanation
Interface Mode	
queue bandwidth <*weight1 weight2 weight3 weight4 weight5 weight6 weight7 weight8*> **no queue bandwidth**	Set the WRR weight for specified egress queue; the "**no queue bandwidth**" command restores the default setting.
queue mode strict **queue mode wrr**	Configure queue out method to pq method; the "**queue mode wrr**" command restores the default WRR queue out method.
Global Mode	
wrr-queue cos-map <*queue-id*> <*cos1 ... cos8*>	Set CoS value mapping to specified egress queue; the "**no wrr-queue**

no wrr-queue cos-map	**cos-map**" command restores the default setting.

6. Configure QoS mapping

Command	Explanation
Global Mode	
mls qos map {cos-dscp <*dscp1...dscp8*> | dscp-cos <*dscp-list*> to <*cos*> | dscp-mutation <*dscp-mutation-name*> <*in-dscp*> to <*out-dscp*> |ip-prec-dscp <*dscp1...dscp8*> | policed-dscp <*dscp-list*> to <*mark-down-dscp*>} **no mls qos map {cos-dscp | dscp-cos | dscp-mutation <*dscp-mutation-name*> | ip-prec-dscp | policed-dscp}**	Set CoS to DSCP mapping, DSCP to CoS mapping, DSCP to DSCP mutation mapping, IP precedence to DSCP and policed DSCP mapping; the "**no mls qos map {cos-dscp | dscp-cos | dscp-mutation <*dscp-mutation-name*> | ip-prec-dscp | policed-dscp}**" command restores the default mapping.

8.1.3 Commands for QoS

8.1.3.1 class

Command: class <*class-map-name*>

no class <class-map-name>

Function: Associates a class to a policy map and enters the policy class map mode; the "**no class <*class-map-name*>**" command deletes the specified class.

Parameters: < *class-map-name*> is the class map name used by the class.

Default: No policy class is configured by default.

Command mode: Policy map configuration Mode

Usage Guide: Before setting up a policy class, a policy map should be created and the policy map mode entered. In the policy map mode, classification and policy configuration can be performed on packet traffic classified by class map.

Example: Entering a policy class mode.

Switch(Config)#policy-map p1

Switch(Config-PolicyMap)#class c1

Switch(Config-Policy-Class)#exit

8.1.3.2 class-map

Command: class-map <*class-map-name*>

no class-map <*class-map-name*>

Function: Creates a class map and enters class map mode; the "**no class-map <*class-map-name*>**" command deletes the specified class map.

Parameters: <*class-map-name*> is the class map name**.**

Default: No class map is configured by default.

Command mode: Global Mode

Usage Guide:

Example: Creating and then deleting a class map named "c1".

Switch(Config)#class-map c1

Switch(Config-ClassMap)# exit

Switch(Config)#no class-map c1

8.1.3.3 match

Command: match {access-group <*acl-index-or-name*> | ip dscp <*dscp-list*>| ip precedence <*ip-precedence-list*>| ipv6 access-group <*acl-index-or-name*> | ipv6 dscp <*dscp-list*>| ipv6 flowlabel <*flowlabel-list*>| vlan <*vlan-list*>|cos<*cost-list*>}

no match {access-group | ip dscp | ip precedence | ipv6 access-group | ipv6 dscp | ipv6 flowlabel | vlan |cos }

Function: Configure the match standard of the class map; the "no" form of this command deletes the specified match standard..

Parameter: access-group <*acl-index-or-name*> match specified ACL,the parameters are the number or name of the ACL;**ip dscp <*dscp-list*>** and **ipv6 dscp <*dscp-list*>** match specified DSCP value, the parameter is a list of DSCP consisting of maximum 8 DSCP values;**ip precedence <*ip-precedence-list*>** match specified IP Precedence, the parameter is a IP Precedence list consisting of maximum 8 IP Precedence values with a valid range of 0～7;**ipv6 access-group <*acl-index-or-name*>** match specified IPv6 ACL,the parameter is the number or name of the IPv6 ACL;**ipv6 flowlabel <*flowlabel-list*>** match specified IPv6 flow label, the parameter is IPv6 flow label value;**vlan <*vlan-list*>** match specified VLAN ID, the parameter is a VLAN ID list consisting of maximum 8 VLAN IDs. **<*cost-list*>** match specified cos value, the parameter is a COS list consisting of maximum 8 Cos.

Default: No match standard by default

Command Mode: Class-map Mode

Usage Guide: Only one match standard can be configured in a class map. When configuring match the ACL, only the permit rule is available in the ACL except for PBR.

Example: Create a class-map named c1, and configure the class rule of this class-map to match packets with IP Precedence of 0.1.

Switch(config)#class-map c1

Switch(config-ClassMap)#match ip precedence 0 1
Switch(config-ClassMap)#exit

8.1.3.4 set

Command: set {ip dscp <*new-dscp*> | ip precedence <*new-precedence*>|ipv6 dscp <*new-dscp*> | ipv6 flowlabel <*new-flowlabel*|cos<*new cos*>>}

no set {ip dscp | ip precedence|ipv6 dscp | ipv6 flowlabel |cos<*new cos*>}

Function: Assign a new DSCP, IP Precedence, IPv6 DSCP or IPv6 FL for the classified traffic; the “no” form of this command delete assigning the new values

Parameter: ***<new-dscp>*** new DSCP value;***<new-precedence>*** new IP Precedence;***<new-flowlabel>*** new IPv6 FL value. ***<new cos>}*** new COS value

Default: Not assigning by default

Command Mode: Policy Class-map Mode

Usage Guide: Only the classified traffic which matches the matching standard will be assigned with the new values.

Example: Set the IP Precedence of the packets matching the c1 class rule to 3.

Switch(config)#policy-map p1
Switch(config-PolicyMap)#class c1
Switch(config--Policy-Class)#set ip precedence 3
Switch(config--Policy-Class)#exit
Switch(config-PolicyMap)#exit

8.1.3.5 mls qos

Command: mls qos

no mls qos

Function: Enables QoS in Global Mode; the “**no mls qos**” command disables the global QoS.

Command mode: Global Mode

Default: QoS is disabled by default.

Usage Guide: QoS provides 8 queues to handle traffics of 8 priorities. This function cannot be used with the traffic control function.

Example: Enabling and then disabling the QoS function.

Switch(Config)#mls qos
Switch(Config)#no mls qos

8.1.3.6 mls qos cos

Command: mls qos cos {<*default-cos*> }

no mls qos cos

Function: Configures the default CoS value of the port; the "**no mls qos cos**" command restores the default setting.

Parameters: < *default-cos*> is the default CoS value for the port, the valid range is 0 to 7.

Default: The default CoS value is 0.

Command mode: Interface Mode

Usage Guide: none

Example: Setting the default CoS value of Ethernet port 1/1 to 5, i.e., packets coming in through this port will be assigned a default CoS value of 5 if no CoS value present.

Switch(Config)#interface ethernet 1/1

Switch(Config-Ethernet1/1)#mls qos cos 5

8.1.3.7 mls qos aggregate-policer

Command:mls qos aggregate-policer <*aggregate-policer-name*> <*rate-kbps*> <*burst-kbyte*> exceed-action {drop |policed-dscp-transmit}

no mls qos aggregate-policer <*aggregate-policer-name*>

Function: Defines a policy set that can be used in one policy map by several classes; the "**no mls qos aggregate-policer <*aggregate-policer-name*>**" command deletes the specified policy set.

Parameters: <*aggregate-policer-name*> is the name of the policy set; **<*rate-kbps*>** is the average baud rate (in kb/s) of classified traffic, range from 1 to 10,000,000; **<*burst-kbyte*>** is the burst value (in kb/s) for classified traffic, range from 1 to 1,000,000; **exceed-action drop** means drop packets when specified speed is exceeded; **exceed-action policed-dscp-transmit** specifies to mark down packet DSCP value according to **policed-dscp** mapping when specified speed is exceeded.

Default: No policy set is configured by default.

Command mode: Global Mode

Usage Guide: If a policy set is using by a policy map, it cannot be deleted unless the reference to the policy set is cleared in the appropriate policy map with "**no police aggregate <*aggregate-policer-name*>**" command. The delete should be performed in Global Mode with "**no mls qos aggregate-policer <*aggregate-policer-name*>**" command.

Example: Setting a policy set named "agg1", the policy set defines the bandwidth for packets of up to 20 Mbps, with a burst value of 2 MB. All packets exceeding this bandwidth setting will be dropped.

Switch(Config)#mls qos aggregate-policer agg1 20000 2000 exceed-action drop

8.1.3.8 mls qos trust

Command:mls qos trust [cos [pass-through-dscp]|dscp [pass-through-cos]| ip-precedence [pass-through-cos] |port priority <*cos*>]

[no] mls qos trust

Function: Configures port trust; the "**no mls qos trust**" command disables the current trust status of the port.

Parameters: cos configures the port to trust CoS value; **cos pass-through-dscp** configures the port to trust CoS value but does not change packet DSCP value; **dscp** configures the port to trust DSCP value; **dscp pass-through-cos** configures the port to trust DSCP value, but does not change packet CoS value; **ip-precedence** configures the port to trust IP precedence; **ip-precedence pass-through-cos** configures the port to trust IP precedence, but does not change packet CoS value.

port priority <*cos*> assigns a priority to the physical port, **cos** is the priority to be assigned. Priority of all incoming packets through the port will be set to this cos value. This is irrelevant to the priority of the packet itself, no modification is done to the packets.

Default: No trust.

Command mode: Interface Mode

Usage Guide: For packets with both CoS value and DSCP value, keyword **pass-through** should be used to protect the value if the value should not be changed after classification.

Example: Configuring Ethernet port 1/1 to trust CoS value, i.e., classifying the packets according to CoS value, DSCP value should not be changed.

Switch(Config)#interface ethernet 1/1

Switch(Config-Ethernet1/1)#mls qos trust cos pass-through-dscp

8.1.3.9 mls qos dscp-mutation

Command:mls qos dscp-mutation <*dscp-mutation-name*>

no mls qos dscp-mutation <*dscp-mutation-name*>

Function: Applies DSCP mutation mapping to the port; the "**no mls qos dscp-mutation <*dscp-mutation-name*>**" command restores the DSCP mutation mapping default.

Parameters: <*dscp-mutation-name*> is the name of DSCP mutation mapping.

Default: There is no policy by default.

Command mode: Interface Mode

Usage Guide: For configuration of DSCP mutation mapping on the port to take effect, the trust status of that port must be "**trust DSCP**". Applying DSCP mutation mapping allows DSCP values specified directly to be converted into new DSCP values without class and policy process. DSCP mutation mapping is effective to the local port only. The "trust DSCP" refers to the DSCP value before DSCP mutation in this case.

Example: Configuring Ethernet port 1/1 to trust DSCP, using DSCP mutation mapping of

mu1.

Switch(Config)#interface ethernet 1/1

Switch(Config-Ethernet1/1)#mls qos trust dscp pass-through cos

Switch(Config-Ethernet1/1)#mls qos dscp-mutation mu1

8.1.3.10 mls qos map

Command: mls qos map {cos-dscp <*dscp1...dscp8*> | dscp-cos <*dscp-list*> to <*cos*> | dscp-mutation <*dscp-mutation-name*> <*in-dscp*> to <*out-dscp*> |ip-prec-dscp <*dscp1...dscp8*> | policed-dscp <*dscp-list*> to <*mark-down-dscp*>}

no mls qos map {cos-dscp | dscp-cos | dscp-mutation <*dscp-mutation-name*> | ip-prec-dscp | policed-dscp}

Function: Sets **class of service (CoS)-to-Differentiated Services Code Point (DSCP)** mapping, **DSCP to CoS** mapping, **DSCP to DSCP mutation** mapping, **IP precedence to DSCP** and **policed DSCP** mapping; the "**no mls qos map {cos-dscp | dscp-cos | dscp-mutation <*dscp-mutation-name*> | ip-prec-dscp | policed-dscp}**" command restores the default mapping.

Parameters: cos-dscp <*dscp1...dscp8*> defines the mapping from CoS value to DSCP, **<*dscp1...dscp8*>** are the 8 DSCP value corresponding to the 0 to 7 CoS value, each DSCP value is delimited with space, ranging from 0 to 63; **dscp-cos <*dscp-list*> to <*cos*>** defines the mapping from DSCP to CoS value, **<*dscp-list*>** is a list of DSCP value consisting of up to 8 DSCP values, **<*cos*>** are the CoS values corresponding to the DSCP values in the list; **dscp-mutation <*dscp-mutation-name*> <*in-dscp*> to <*out-dscp*>** defines the mapping from DSCP to DSCP mutation, **<*dscp-mutation-name*>** is the name for mutation mapping, **<*in-dscp*>** stand for incoming DSCP values, up to 8 values are supported, each DSCP value is delimited with space, ranging from 0 to 63, **<*out-dscp*>** is the sole outgoing DSCP value, the 8 values defined in incoming DSCP will be converted to outgoing DSCP values; **ip-prec-dscp <*dscp1...dscp8*>** defines the conversion from IP precedence to DSCP value, **<*dscp1...dscp8*>** are 8 DSCP values corresponding to IP precedence 0 to 7, each DSCP value is delimited with space, ranging from 0 to 63; **policed-dscp <*dscp-list*> to <*mark-down-dscp*>** defines DSCP **mark down** mapping, where **<*dscp-list*>** is a list of DSCP values containing up to 8 DSCP values, **<*mark-down-dscp*>** are DSCP value after **mark down**.

Default: Default mapping values are:

Default CoS-to-DSCP Map

CoS Value	0	1	2	3	4	5	6	7
DSCP Value	0	8	16	24	32	40	48	56

Default DSCP-to-CoS Map

DSCP Value	0–7	8–15	16–23	24–31	32–39	40–47	48–55	56–63
CoS Value	0	1	2	3	4	5	6	7

Default IP-Precedence-to-DSCP Map

IP Precedence Value	0	1	2	3	4	5	6	7
DSCP Value	0	8	16	24	32	40	48	56

dscp-mutation and policed-dscp are not configured by default

Command mode: Global Mode

Usage Guide: In **police** command, classified packet traffic can be set to mark down if exceed specified average speed or burst value, **policed-dscp <*dscp-list*> to <*mark-down-dscp*>** can mark down the DSCP values of those packets to new DSCP values.

Example: Setting the ***CoS-to-DSCP*** mapping value to the default 0 8 16 24 32 40 48 56 to 0 1 2 3 4 5 6 7.

Switch(Config)#mls qos map cos-dscp 0 1 2 3 4 5 6 7

8.1.3.11 police

Command:police <*rate-kbps*> <*burst-kbyte*> [exceed-action {drop | policed-dscp-transmit}]

no police <*rate-kbps*> <*burst-kbyte*> [exceed-action {drop | policed-dscp-transmit}]

Function: Configures a policy to a classified traffic; the "**no police <*rate-kbps*> <*burst-kbyte*> [exceed-action {drop | policed-dscp-transmit}]**" command deletes the specified policy.

Parameters: <*rate-kbps*> is the average baud rate (kb/s) of classified traffic, ranging from 1 to 10,000,000; **<*burst-kbyte*>** is the burst baud rate (kbyte) of classified traffic, ranging from 1 to 1000,000; **exceed-action drop** means drop packets when specified speed is exceeded; **exceed-action policed-dscp-transmit** specifies to mark down packet DSCP value according to **policed-dscp** mapping when specified speed is exceeded.

Default: There is no policy by default.

Command mode: Policy class map configuration Mode

Usage Guide: The ranges of **<*rate-kbps*>** and **<*burst-kbyte*>** are quite large, if the setting exceeds the actual speed of the port, the policy map applying this policy will not bind to switch ports.

Example: Setting the bandwidth for packets that matching c1 class rule to 20 Mbps, with a burst value of 2 MB, all packets exceed this bandwidth setting will be dropped.

Switch(Config)#policy-map p1

Switch(Config-PolicyMap)#class c1

Switch(Config-Policy-Class)#police 20000 2000 exceed-action drop
Switch(Config-Policy-Class)#exit
Switch(Config-PolicyMap)#exit

8.1.3.12 police aggregate

Command: police aggregate <*aggregate-policer-name*>
no police aggregate <*aggregate-policer-name*>
Function: Applies a policy set to classified traffic; the "**no police aggregate <*aggregate-policer-name*>**" command deletes the specified policy set.
Parameters: <*aggregate-policer-name*> is the policy set name.
Default: No policy set is configured by default.
Command mode: Policy class map configuration Mode
Usage Guide: The same policy set can be referred to by different policy class maps.
Example: Appling a policy set "agg1" to packets satisfying c1 class rule.
Switch(Config)#policy-map p1
Switch(Config-PolicyMap)#class c1
Switch(Config--Policy-Class)#police aggregate agg1
Switch(Config--Policy-Class)#exit
Switch(Config-PolicyMap)#exit

8.1.3.13 policy-map

Command: policy-map <*policy-map-name*>
no policy-map <*policy-map-name*>
Function: Creates a policy map and enters the policy map mode; the "**no policy-map <*policy-map-name*>**" command deletes the specified policy map.
Parameters: < *policy-map-name*> is the policy map name.
Default: No policy map is configured by default.
Command mode: Global Mode
Usage Guide: QoS classification matching and marking operations can be done in the policy map configuration mode.
Example: Creating and deleting a policy map named "p1".
Switch(Config)#policy-map p1
Switch(Config-PolicyMap)#exit
Switch(Config)#no policy-map p1

8.1.3.14 queue mode

Command: queue mode {strict|wrr}
Function: Configure the queue out mode.

Parameter: strict configure queue out method to strict priority-queue method; wrr restores the default wrr queue out method.

Default: wrr out queue mode

Command mode: Interface Mode

Usage Guide: When priority-queue queue out mode is used, packets are no longer sent with WRR weighted algorithm, but send packets queue after queue.

Example: Set the queue out mode to strict priority-queue.

Switch(Config-Ethernet)# queue mode strict.

8.1.3.15 service-policy

Command: service-policy {input <*policy-map-name*> | output <*policy-map-name*>}

no service-policy {input <*policy-map-name*> | output <*policy-map-name*>}

Function: Applies a policy map to the specified port; the "**no service-policy {input <*policy-map-name*> | output <*policy-map-name*>}**" command deletes the specified policy map applied to the port.

Parameters: input <*policy-map-name*> applies the specified policy map to the ingress of switch port; **output <*policy-map-name*>** applies the specified policy map to the egress of switch port.

Default: No policy map is bound to ports by default.

Command mode: Interface Mode

Usage Guide: Configuring port trust status and applying policy map on the port are two conflicting operations; the later configuration will override the earlier configuration. Only one policy map can be applied to each direction of each port. Egress policy map is not supported yet.

Example: Bind policy p1 to ingress Ethernet port 1/1.

Switch(Config)#interface ethernet 1/1

Switch(Config-Ethernet1/1)# service-policy input p1

8.1.3.16 queue bandwidth

Command: queue bandwidth <*weight1 weight2 weight3 weight4 weight5 weight6 weight7 weight8*>

no queue bandwidth

Function: Sets the WRR weight for specified egress queue; the "**no queue bandwidth**" command restores the default setting.

Parameters: <*weight1 weight2 weight3 weight4 weight5 weight6 weight7 weight8*> are WRR weights, ranging from 0 to 15.

Default: The default values of weight1 to weight8 are 1 through 8.

Command mode: Interface Mode

Usage Guide: The absolute value of WRR is meaningless. WRR allocates bandwidth by using eight weight values. If a weight is 0, then the queue has the highest priority; when the weights of multiple queues are set to 0, then the queue of higher order has the higher priority.

Example: Setting the bandwidth weight proportion of the eight queue out to be 1:1:2:2:4:4:8:8.

Switch(Config-Ethernet1/1)#queue bandwidth 1 1 2 2 4 4 8 8

8.1.3.17 wrr-queue cos-map

Command:wrr-queue cos-map <*queue-id*> <*cos1 ... cos8*>

no wrr-queue cos-map

Function: Sets the CoS value mapping to the specified queue out; the "**no wrr-queue cos-map**" command restores the default setting.

Parameters: <*queue-id*> is the ID of queue out, ranging from 1 to 8; **<*cos1 ... cos8*>** are CoS values mapping to the queue out, ranging from 0 -7, up to 8 values are supported.

Default:

Default CoS-to-Egress-Queue Map when QoS is Enabled

CoS Value	0	1	2	3	4	5	6	7
Queue Selected	1	2	3	4	5	6	7	8

Command mode: Global Mode

Usage Guide: none

Example: Mapping packets with CoS value 2 and 3 to egress queue 1.

Switch(Config)#wrr-queue cos-map 1 2 3

8.1.4 QoS Example

Scenario 1:

Enable QoS function, change the queue out weight of port ethernet 1/1 to 1:1:2:2:4:4:8:8, and set the port in trust QoS mode without changing DSCP value, and set the default QoS value of the port to 5.

The configuration steps are listed below:

Switch#config

Switch(Config)#mls qos

Switch(Config)#interface ethernet 1/1

Switch(Config-Ethernet1/1)#queue bandwidth 1 1 2 2 4 4 8 8

Switch(Config-Ethernet1/1)#mls qos trust cos pass-through dscp

Switch(Config-Ethernet1/1)#mls qos cos 5
Configuration result:

When QoS enabled in Global Mode, the egress queue bandwidth proportion of port ethernet 1/1 is 1:1:2:2:4:4:8:8. When packets have CoS value coming in through port ethernet 1/1, it will be map to the queue out according to the CoS value, CoS value 0 to 7 correspond to queue out 1, 2, 3, 4, 5, 6, 7, 8, respectively. If the incoming packet has no CoS value, it is default to 5 and will be put in queue 6. All passing packets would not have their DSCP values changed.

Scenario 2:

In port ethernet 1/2, set the bandwidth for packets from segment 192.168.1.0 to 10 Mb/s, with a burst value of 4 MB, all packets exceed this bandwidth setting will be dropped.

The configuration steps are listed below:

Switch#config
Switch(Config)#access-list 1 permit 192.168.1.0 0.0.0.255
Switch(Config)#mls qos
Switch(Config)#class-map c1
Switch(Config-ClassMap)#match access-group 1
Switch(Config-ClassMap)# exit
Switch(Config)#policy-map p1
Switch(Config-PolicyMap)#class c1
Switch(Config--Policy-Class)#police 10000 4000 exceed-action drop
Switch(Config--Policy-Class)#exit
Switch(Config-PolicyMap)#exit
Switch(Config)#interface ethernet 1/2
Switch(Config-Ethernet1/2)#service-policy input p1
Configuration result:

An ACL name 1 is set to matching segment 192.168.1.0. Enable QoS globally, create a class map named c1, matching ACL1 in class map; create another policy map named p1 and refer to c1 in p1, set appropriate policies to limit bandwidth and burst value. Apply this policy map on port ethernet 1/2. After the above settings done, bandwidth for packets from segment 192.168.1.0 through port ethernet 1/2 is set to 10 Mb/s, with a burst value of 4 MB, all packets exceed this bandwidth setting in that segment will be dropped.

Scenario 3:

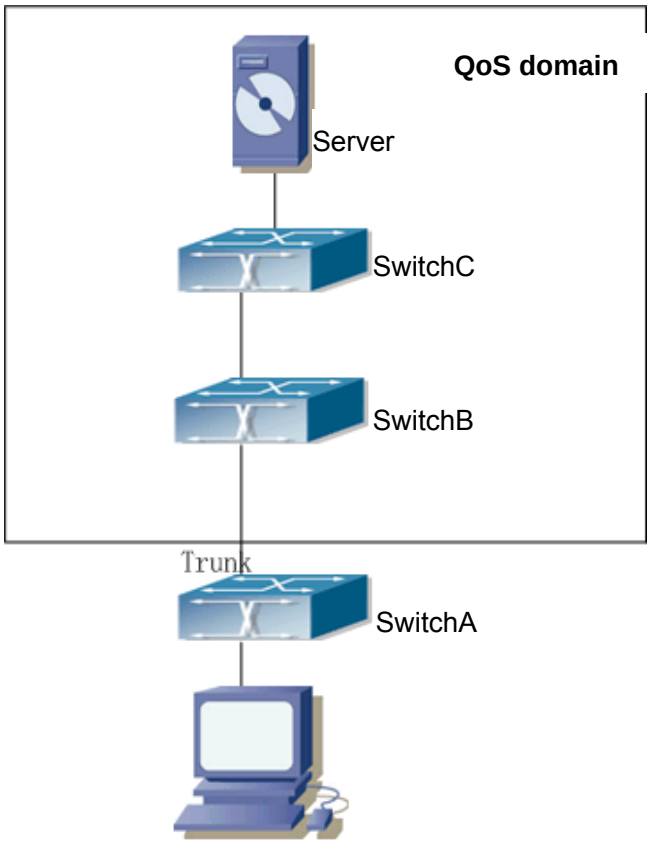


Fig 8-7 Typical QoS topology

As shown in the figure, inside the block is a QoS domain, switchA classifies different traffics and assigns different IP precedences. For example, set IP precedence for packets from segment 192.168.1.0 to 5 on port ethernet 1/1. The port connecting to switchB is a trunk port. In SwitchB, set port ethernet 1/1 that connecting to switchA to trust IP precedence. Thus inside the QoS domain, packets of different priorities will go to different queues and get different bandwidth.

The configuration steps are listed below:

QoS configuration in SwitchA:

Switch#config

Switch(Config)#access-list 1 permit 192.168.1.0 0.0.0.255

Switch(Config)#mls qos

Switch(Config)#class-map c1

Switch(Config-ClassMap)#match access-group 1

Switch(Config-ClassMap)# exit

Switch(Config)#policy-map p1

Switch(Config-PolicyMap)#class c1
Switch(Config--Policy-Class)#set ip precedence 5
Switch(Config--Policy-Class)#exit
Switch(Config-PolicyMap)#exit
Switch(Config)#interface ethernet 1/1
Switch(Config-Ethernet1/1)#service-policy input p1

QoS configuration in SwitchB:

SWITCH#CONFIG

Switch(Config)#mls qos
Switch(Config)#interface ethernet 1/1
Switch(Config-Ethernet1/1)#mls qos trust ip-precedence pass-through-cos

8.1.5 QoS Troubleshooting

- ☞ QoS is disabled on switch ports by default, 8 sending queues are set by default, queue1 forwards normal packets, other queues are used for some important control packets (such as BPDU).
- ☞ When QoS is enabled in Global Mode,. QoS is enabled on all ports with 8 traffic queues. The default CoS value of the port is 0; the port is in not Trusted state by default; the default queue weight values are 1, 2, 3, 4, 5, 6, 7, 8 in order, all QoS Map is using the default value.
- ☞ CoS value 7 maps to queue 8 that has the highest priority and usually reserved for certain protocol packets. It is not recommended for the user to change the mapping between CoS 7 to Queue 8, or set the default port CoS value to 7.
- ☞ Policy map can only be bound to ingress direction, egress is not supported yet.
- ☞ If the policy is too complex to be configured due to hardware resource limit, error massages will be provided.

8.1.5.1 Commands for Monitor And Debug

8.1.5.1.1 show class-map

Command: show class-map [<*class-map-name*>]
Function: Displays class map of QoS.
Parameters: < *class-map-name*> is the class map name.
Default: N/A.
Command mode: Admin Mode
Usage Guide: Displays all configured class-map or specified class-map information.
Example:

Switch # show class-map

Class map name:c1

Match acl name:1

Displayed information	Explanation
Class map name:c1	Name of the Class map
Match acl name:1	Classifying rule for the class map.

8.1.5.1.2 show policy-map

Command: show policy-map [<*policy-map-name*>]

Function: Displays policy map of QoS.

Parameters: < *policy-map-name*> is the policy map name.

Default: N/A.

Command mode: Admin Mode

Usage Guide: Displays all configured policy-map or specified policy-map information.

Example:

Switch # show policy -map

Policy Map p1

Class Map name: c1

police 16000000 2000 exceed-action drop

Displayed information	Explanation
Policy Map p1	Name of policy map
Class map name:c1	Name of the class map referred to
police 16000000 8000 exceed-action drop	Policy implemented

8.1.5.1.3 show mls qos aggregate-policer

Command: show mls qos aggregate-policer [<*aggregate-policer-name*>]

Function: Displays policy set configuration information for QoS.

Parameters: <*aggregate-policer-name*> is the policy set name.

Default: N/A.

Command mode: Admin Mode

Usage Guide:

Example:

Switch #show mls qos aggregate-policer policer1

aggregate-policer policer1 80000 80 exceed-action drop

Not used by any policy map

Displayed information	Explanation
aggregate-policer policer1 80000 80 exceed-action drop	Configuration for this policy set.
Not used by any policy map	Time that the policy set is being

	referred to

8.1.5.1.4 show mls qos interface

Command: show mls qos interface [<*interface-id*>] [buffers | policers | queueing | statistics]

Function: Displays QoS configuration information on a port.

Parameters: <***interface-id***> is the port ID; **buffers** is the queue buffer setting on the port; **policers** is the policy setting on the port; **queuing** is the queue setting for the port; **statistics** is the number of packets allowed to pass for in-profile and out-of-profile traffic according to the policy bound to the port.

Default: N/A.

Command mode: Admin Mode

Usage Guide: Statistics are available only when ingress policy is configured.

Example:

Switch #show mls qos interface ethernet 1/2

Ethernet1/2

default cos:0

DSCP Mutation Map: Default DSCP Mutation Map

Attached policy-map for Ingress: p1

Displayed information	Explanation
Ethernet1/2	Port name
default cos:0	Default CoS value of the port.
DSCP Mutation Map: Default DSCP Mutation Map	Port DSCP map name
Attached policy-map for Ingress: p1	Policy name bound to port.

Switch # show mls qos interface buffers ethernet 1/2

Ethernet1/2

packet number of 8 queue:

0x200 0x200 0x200 0x200 0x200 0x200 0x200 0x200

Displayed information	Explanation
packet number of 8 queue: 0x200 0x200 0x200 0x200 0x200 0x200 0x200 0x200	Available packet number for all 8 queues out on the port, this is a fixed setting that cannot be changed.

Switch # show mls qos interface queueing ethernet 1/2

Switch#show mls qos int queue e 1/2

Cos-queue map:

Cos 0 1 2 3 4 5 6 7

Queue 1 2 3 4 5 6 7 8

Queue and weight type:

Port	q1	q2	q3	q4	q5	q6	q7	q8	QType
Ethernet1/2	1	2	3	4	5	6	7	8	WFQ

Displayed information	Explanation
Cos-queue map:	CoS value to queue mapping.
Queue and weight type:	Queue to weight mapping.
QType	WFQ or PQ queue out method

Switch # show mls qos interface policers ethernet 1/2

Ethernet1/2

Attached policy-map for Ingress: p1

Displayed information	Explanation
Ethernet1/2	Port name
Attached policy-map for Ingress: p1	Policy map bound to the port.

Switch # show mls qos interface statistics ethernet 1/2

Device: Ethernet1/2

Classmap	classified	in-profile	out-profile (in packets)
c1	0	0	0

Displayed information	Explanation
Ethernet1/2	Port name
ClassMap	Name of the Class map
Classified	Total data packets match this class map.
In-profile	Total in-profile data packets match this class map.
out-profile	Total out-profile data packets match this class map.

8.1.5.1.5 show mls qos maps

Command: show mls qos maps [cos-dscp | dscp-cos | dscp-mutation *<dscp-mutation-name>* | ip-prec-dscp | policed-dscp]

Function: Displays mapping configuration information for QoS.

Parameters: **cos-dscp** CoS for CoS-DSCP; **dscp-cos** DSCP for DSCP-CoS, **dscp-mutation *<dscp-mutation-name>*** for DSCP-DSCP mutation, ***<dscp-mutation-name>*** is the name of mutation; **ip-prec-dscp** IP for IP precedence-DSCP; **policed-dscp** is DSCP mark down mapping.

Default: N/A.

Command mode: Admin Mode

Example:

Switch # show mls qos map

Cos-dscp map:

```
            cos:     0   1   2   3   4   5   6   7
-------------------------------------
           dscp:     0   8 16 24 32 40 48 56
IpPrecedence-dscp map:
         ipprec:     0   1   2   3   4   5   6   7
-------------------------------------
           dscp:     0   8 16 24 32 40 48 56
Dscp-cos map:
         d1 : d2 0   1   2   3   4   5   6   7   8   9
         0:        0   0   0   0   0   0   0   0   1   1
         1:        1   1   1   1   1   1   2   2   2   2
         2:        2   2   2   2   3   3   3   3   3   3
         3:        3   3   4   4   4   4   4   4   4   4
         4:        5   5   5   5   5   5   5   5   6   6
         5:        6   6   6   6   6   6   7   7   7   7
         6:        7   7   7   7
Policed-dscp map:
         d1 : d2 0   1   2   3   4   5   6   7   8   9
         0:        0   1   2   3   4   5   6   7   8   9
         1:       10 11 12 13 14 15 16 17 18 19
         2:       20 21 22 23 24 25 26 27 28 29
         3:       30 31 32 33 34 35 36 37 38 39
         4:       40 41 42 43 44 45 46 47 48 49
         5:       50 51 52 53 54 55 56 57 58 59
         6:       60 61 62 63
```

8.1.5.1.6 show mls-qos

Command: show mls-qos

Function: Displays global configuration information for QoS.

Parameters: N/A.

Default: N/A.

Command mode: Admin Mode

Usage Guide: This command indicates whether QoS is enabled or not.

Example:

Switch #show mls-qos

Qos is enabled

Displayed information	Explanation
Qos is enabled	QoS is enabled.

8.2 PBR Configuration

8.2.1 Introduction to PBR

PBR（Policy-Based Routing）is a method which determines the next-hop of the data packets by policy messages such as source address, destination address, IP priority, TOS value, IP protocol, source port No., destination port No, etc.

8.2.2 PBR configuration

The PBR configuration task list is as follows:

Initiate PBR function

Enable or disable PBR function automatically when turn on or turn off the QoS function at global mode.

Config classmap

Establish a class rule and apply different policies on different kinds of data streams thereafter.

Config policymap

A policymap can be established after the data streams are classified. Assign each stream to previously created classmap and then enter the policy classmap mode. In this way different data streams can now be assigned to different next-hop IP address and apply the policy to the port.

Apply policymap

A policy will not be valid until it is bonded to a specified port.

8.2.3 PBR examples

On port ethernet 1/1, apply policy-based routing on packages from 192.168.1.0/24 segment, and set the next-hop as 218.31.1.119, meanwhile the local network IP of this network ranges within 192.168.0.0/16. To assure normal communication in local network, messages from 192.168.1.0/24 to local IP 192.168.0.0/16 are not applied with policy routing.

Configuration procedure is as follows:

Switch#config

Switch(config)#access-list ip extended a1

Switch(Config-IP-Ext-Nacl-a1)#permit ip 192.168.1.0 0.0.0.255 any-destination

```
Switch(Config-IP-Ext-Nacl-a1)#deny ip 192.168.1.0 0.0.0.255 192.168.0.0 0.0.255.255
Switch(Config-IP-Ext-Nacl-a1)#exit
Switch(config)#mls qos
Switch(config)#class-map c1
Switch(config-ClassMap)#match access-group a1
Switch(config-ClassMap)# exit
Switch(config)#policy-map p1
Switch(config-PolicyMap)#class c1
Switch(config-Policy-Class)#set ip nexthop 218.31.1.119
Switch(config--Policy-Class)#exit
Switch(config-PolicyMap)#exit
Switch(config)#interface ethernet
Switch(Config-Ethernet1/1)#service-policy input p1
```

Configuration results

First set an ACL a1 with two items. The first item matches source IP segments 192.168.1.0/24（allowed）. The second item matches source IP segments 192.168.1.0/24 and destination IP segments 192.168.0.0/16（rejected）. Turn on QoS function in global mode and create a class-map: c1 in which matches ACL a1, and create a policy-map in which quote c1. Set the next-hop IP as 218.31.1.119 and apply the policy-map at port ethernet 1/1. After that, all messages on port ethernet 1/1 from segment 192.168.1.0/24 will be transmitted through 192.168.1.0/24 except those from 192.168.0.0/16 segment which are still be transmitted through normal L3 routing.

Chapter 9 Flow-based Redirection

9.1 Introduction to Flow-based Redirection

Flow-based redirection function enables the switch to transmit the data frames meeting some special condition (specified by ACL) to another specified port. The fames meeting a same special condition are called a class of flow, the ingress port of the data frame is called the source port of redirection, and the specified egress port is called the destination port of redirection. Usually there are two kinds of application of flow-based redirection: 1. connecting a protocol analyzer (for example, Sniffer) or a RMON monitor to the destination port of redirection, to monitor and manage the network, and diagnose the problems in the network; 2. Specifying transmission policy for a special type of data frames.

The switch can only designate a single destination port of redirection for a same class of flow within a source port of redirection, while it can designate different destination ports of redirection for different classes of flows within a source port of redirection. The same class of flow can be applied to different source ports.

9.2 Flow-based Redirection Configuration Task Sequence

1. Flow-based redirection configuration
2. Check the current flow-based redirection configuration

1. Flow-based redirection configuration

Command	Explanation
Physical interface configuration mode	
access-group <aclname> redirect to interface ethernet <ifname> **no access-group <aclname> redirect**	Specify flow-based redirection for the port; “ no access-group <aclname> redirect” command is used to delete flow-based redirection

2. Check the current flow-based redirection configuration

Command	Explanation
Global mode/Admin mode	
show flow-based-redirect {interface ethernet < *interface-list* > }	Display the information of current flow-based redirection in the system/port

9.3 Command for Flow-based Redirection

9.3.1 access-group <aclname> redirect to interface ethernet

Command：access-group <aclname> redirect to interface ethernet <ifname>
no access-group <aclname> redirect

Function： Specify flow-based redirection; “no access-group <aclname> redirect” command is used to delete flow-based redirection

Parameters：<aclname> name of the flow , only supports digital standard IP ACL, digital extensive IP ACL, nomenclatural standard IP ACL, nomenclatural extensive IP ACL, digital standard IPv6 ACL, and nomenclatural standard IPv6 ACL. Paramters of Timerange and Portrange can not be set in ACL, the type of ACL should be Permit. **<ifname>** the destination port of redirection.

Command Mode： Physical interface configuration mode

Usage Guide： “no access-group <aclname> redirect” command is used to delete flow-based redirection. Flow-based redirection function enables the switch to transmit the data frames meeting some special condition to another specified port.

Examples： Redirecting the frames whose source IP is 192.168.1.111 received from port 1 to port 6,

Switch(Config)#access-list 1 permit host 192.168.1.111

Switch(Config)# interface ethernet 1/1

Switch(Config-Ethernet1/1)# access-group 1 redirect to interface ethernet 1/6

9.3.2 show flow-based-redirect

Command：show flow-based-redirect {interface ethernet < interface-list > }

Function： Display the information of current flow-based redirection in the system/port

Parameters： 1. No specified port, display the information of all the flow-based redirection in the system

2. specify ports in ***<interface-list>***，display the information of the flow-based redirection configured in the ports listed in the interface-list.

Command Mode：Global mode/Admin mode

Usage Guide：This command is used to display the information of current flow-based redirection in the system/por

Examples：

Switch(Config)# show flow-based-redirect

Switch# show flow-based-redirect interface ethernet 1/1-5

9.4 Flow-based Redirection Examples

Scenario :

User's request of configuration is listed as follows: redirecting the frames whose source IP is 192.168.1.111 received from port 1 to port 6, that is sending the frames whose source IP is 192.168.1.111 received from port 1 through port 6

Modification of configuration:

1：Set an ACL, the condition to be matched is: source IP is 192.168.1.111;

2：Apply the redirection based on this flow to port 1.

The following is the configuration procedure:

Switch(Config)#access-list 1 permit host 192.168.1.111

Switch(Config)# interface ethernet 1/1

Switch(Config-Ethernet1/1)# access-group 1 redirect to interface ethernet 1/6

9.5 Flow-based Redirection Troubleshooting Help

When the configuration of flow-based redirection fails, please check that whether it is the following reasons causing the problem:

- ☞ The type of flow (ACL) can only be digital standard IP ACL, digital extensive IP ACL, nomenclatural standard IP ACL, nomenclatural extensive IP ACL, digital standard IPv6 ACL, and nomenclatural standard IPv6 ACL.
- ☞ Paramters of Timerange and Portrange can not be set in ACL, the type of ACL should be Permit；
- ☞ After a multi-cast data frame is redirected, this data frame will only be transmitted to the destination port of redirection.

Chapter 10 L3 Forward Configuration

ES4626/ES4650 switch supports Layer 3 forwarding which forwards Layer 3 protocol packets (IP packets) across VLANs. Such forwarding uses IP addresses, when a port receives an IP packet, it will index it in its own route table and decide the operation according to the index result. If the IP packet is destined to another subnet reachable from this switch, then the packet will be forwarded from the appropriate port. ES4626/ES4650 switch can forward IP packets by hardware, the forwarding chip of ES4626/ES4650 switch have a host route table and default route table. Host route table stores host routes to connect to the switch directly; default route table stores network routes (after aggregation algorithm process).

If the route (either host route or network route) for forwarding unicast traffic exists in the forwarding chip, rather than processing by the CPU in router, the forwarding of traffic will be completely handled by hardware,not like router forwarding by CPU. As a result, forwarding efficiency can be greatly improved, even to wire speed.

10.1 Layer 3 Interface

10.1.1 Introduction to Layer 3 Interface

Layer 3 interface can be created on ES4626/ES4650 switch. The Layer 3 interface is not a physical interface but a virtual interface. Layer 3 interface is built on VLANs. The Layer 3 interface can contain one or more layer2 interfaces which belongs to the same VLAN, or no layer2 interfaces. At least one of the Layer2 interfaces contained in Layer 3 interface should be in a UP state for Layer 3 interface in the UP state, otherwise, Layer 3 interface will be in the DOWN state. All layer 3 interfaces in the switch use the same MAC address by default, this address is selected from the reserved MAC address while creating Layer 3 interface. The Layer 3 interface is the base for layer 3 protocols. The switch can use the IP addresses set in the layer 3 interfaces to communicate with the other devices via IP. The switch can forward IP packets between different Layer 3 interfaces.

10.1.2 Layer 3 Interface Configuration Task List

1. Create Layer 3 Interface

Command	Explanation
Global Mode	
interface vlan <*vlan-id*> **no interface vlan <*vlan-id*>**	Creates a VLAN interface (VLAN interface is a Layer 3 interface); the "**no interface vlan <*vlan-id*>**" command deletes the VLAN interface (Layer 3 interface) created in the switch.

10.1.3 Commands for Layer 3 Interface

10.1.3.1 interface vlan

Command:interface vlan <*vlan-id*>

no interface vlan <*vlan-id*>

Function: Creates a VLAN interface (a Layer 3 interface); the "**no interface vlan <*vlan-id*>**" command deletes the Layer 3 interface specified.

Parameters: <*vlan-id*> is the VLAN ID of the established VLAN.

Default: No Layer 3 interface is configured upon switch shipment.

Command mode: Global Mode

Usage Guide: When crating a VLAN interface (Layer 3 interface), VLANs should be configured first, for details, see the VLAN chapters. When VLAN interface (Layer 3 interface) is created with this command, the VLAN interface (Layer 3 interface) configuration mode will be entered. After the creation of the VLAN interface (Layer 3 interface), interface vlan command can still be used to enter Layer 3 interface mode.

Example: Creating a VLAN interface (layer 3 interface).

Switch (Config)#interface vlan 1

10.2 IP Configuration

10.2.1 Introduction to IPv4, IPv6

IPv4 is the current version of global universal Internet protocol. The practice has proved that IPv4 is simple, flexible, open, stable, strong and easy to implement while collaborating well with various protocols of upper and lower layers. Although IPv4 almost has not been changed since it was established in 1980's, it has kept growing to the

current global scale with the promotion of Internet. However, as Internet infrastructure and Internet application services continue boosting, IPv4 has shown its deficiency when facing the present scale and complexity of Internet.

IPv6 refers to the sixth version of Internet protocol which is the next generation Internet protocol designed by IETF to replace the current Internet protocol version 4 (IPv4). IPv6 was specially developed to make up the shortages of IPv4 so that Internet can develop further.

The most important problem IPv6 has solved is to add the amount of IP address. IPv4 addresses have nearly run out, whereas the amount of Internet users has been increasing in geometric series. With the greatly and continuously boosting of Internet services and application devices (Home and Small Office Network, IP phone and Wireless Service Information Terminal which make use of Internet,) which require IP addresses, the supply of IP addresses turns out to be more and more tense. People have been working on the problem of shortage of IPv4 addresses for a long time by introducing various technologies to prolong the lifespan of existing IPv4 infrastructure, including Network Address Translation(NAT for short), and Classless Inter-Domain Routing(CIDR for short), etc.

Although the combination of CIDR, NAT and private addressing has temporarily mitigated the problem of IPv4 addresses space shortage, NAT technology has disrupted the end-to-end model which is the original intention of IP design by making it necessary for router devices that serve as network intermediate nodes to maintain every connection status which increases network delay greatly and decreases network performance. Moreover, the translation of network data packet addresses baffles the end-to-end network security check, IPSec authentication header is such an example.

Therefore, in order to solve all kinds of problems existing in IPv4 comprehensively, the next generation Internet Protocol IPv6 designed by IETF has become the only feasible solution at present.

First of all, the 128 bits addressing scheme of IPv6 Protocol can guarantee to provide enough globally unique IP addresses for global IP network nodes in the range of time and space. Moreover, besides increasing address space, IPv6 also enhanced many other essential designs of IPv4.

Hierarchical addressing scheme facilitates Route Aggregation, effectively reduces route table entries and enhances the efficiency and expansibility of routing and data packet processing.

The header design of IPv6 is more efficient compared with IPv4. It has less data fields and takes out header checksum, thus expedites the processing speed of basic IPv6 header. In IPv6 header, fragment field can be shown as an optional extended field, so that data packets fragmentation process won’t be done in router forwarding process,

and Path MTU Discovery Mechanism collaborates with data packet source which enhances the processing efficiency of router.

Address automatic configuration and plug-and-play is supported. Large amounts of hosts can find network routers easily by address automatic configuration function of IPv6 while obtaining a globally unique IPv6 address automatically as well which makes the devices using IPv6 Internet plug-and-play. Automatic address configuration function also makes the readdressing of existing network easier and more convenient, and it is more convenient for network operators to manage the transformation from one provider to another.

Support IPSec. IPSec is optional in IPv4, but required in IPv6 Protocol. IPv6 provides security extended header, which provides end-to-end security services such as access control, confidentiality and data integrity, consequently making the implement of encryption, validation and Virtual Private Network easier.

Enhance the support for Mobile IP and mobile calculating devices. The Mobile IP Protocol defined in IETF standard makes mobile devices movable without cutting the existing connection, which is a network function getting more and more important. Unlike IPv4, the mobility of IPv6 is from embedded automatic configuration to get transmission address (Care-Of-Address); therefore it doesn't need Foreign Agent. Furthermore, this kind of binding process enables Correspondent Node communicate with Mobile Node directly, thereby avoids the extra system cost caused by triangle routing choice required in IPv4.

Avoid the use of Network Address Translation. The purpose of the introduction of NAT mechanism is to share and reuse same address space among different network segments. This mechanism mitigates the problem of the shortage of IPv4 address temporally; meanwhile it adds the burden of address translation process for network device and application. Since the address space of IPv6 has increased greatly, address translation becomes unnecessary, thus the problems and system cost caused by NAT deployment are solved naturally.

Support extensively deployed Routing Protocol. IPv6 has kept and extended the supports for existing Internal Gateway Protocols(IGP for short), and Exterior Gateway Protocols(EGP for short). For example, IPv6 Routing Protocol such as RIPng, OSPFv3, IS-ISv6 and MBGP4+, etc.

Multicast addresses increased and the support for multicast has enhanced. By dealing with IPv4 broadcast functions such as Router Discovery and Router Query, IPv6 multicast has completely replaced IPv4 broadcast in the sense of function. Multicast not only saves network bandwidth, but enhances network efficiency as well.

10.2.2 IP Configuration

It can configure three-layer interface as IPv4 interface or IPv6 interface.

10.2.2.1 IPv4 Address Configuration

Configure the IPv4 address of three-layer interface

Command	Explanation
Interface Mode	
ip address <*ip-address*> <*mask*> [secondary] **no ip address [<*ip-address*> <*mask*>]**	Configure IP address of VLAN interface; the **no ip address [<*ip-address*> <*mask*>]** command cancels IP address of VLAN interface.

10.2.2.2 Commands For Ipv4 Address

10.2.2.2.1 ip address

Command：ip address <*ip-address*> <*mask*> [secondary]

no ip address [<ip-address> <mask>] [secondary]

Function：Set IP address and net mask of switch; the "**no ip address [<ip-address> <mask>] [secondary]**" command deletes the IP address configuration.

Parameter：<*ip-address*> is IP address, dotted decimal format; **<*mask*>** is subnet mask, dotted decimal format; what **[secondary]** represents means the configured IP address is slave IP address.

Command Mode： Interface Mode

Default：The system default is no IP address configuration.

Usage Guide：This command configures IP address on VLAN interface manually. If optional parameter **secondary** is not configured, then it is configured as the master IP address of VLAN interface; if optional parameter **secondary** is configured, then that means the IP address is the slave IP address of VLAN. One VLAN interface can only have one master IP address and more than one slave IP addresses. Master IP and Slave IP all can be used on SNMP/Web/Telnet management. Furthermore, the switch also provides BOOTP/DHCP manner to capture IP address.

Example：The IP address of switch VLAN1 interface is set to 192.168.1.10/24.

Switch(Config-If-Vlan1)#ip address 192.168.1.10 255.255.255.0

10.2.2.3 IPv6 Address Configuration

The configuration Task List of IPv6 is as follows:

1. IPv6 basic configuration
   （1） Globally enable IPv6
   （2） Configure interface IPv6 address
   （3） Configure IPv6 static routing
2. IPv6 Neighbor Discovery Configuration
   （1） Configure DAD neighbor query message number
   （2） Configure send neighbor query message interval
   （3） Enable and forbid router announce
   （4） Configure router announce lifespan
   （5） Configure router announce maximum interval
   （6） Configure router announce maximum interval
   （7） Configure prefix announce parameters
   （8） Set static neighbor table entries
   （9） Clear neighbor table entries
3. IPv6 Tunnel configuration
   （1） Create/Delete Tunnel
   （2） Configure Tunnel Source
   （3） Configure Tunnel Destination
   （4） Configure Tunnel Next-Hop
   （5） Configure 6to4 Tunnel Relay
   （6） Configure Tunnel Mode
   （7） Configure Tunnel Routing

1. IPv6 Basic Configuration

(1). Globally enable IPv6

Command	**Explanation**
Global mode	
[no] ipv6 enable	Enable functions such as IPv6 data packet transmission, neighbor discovery, router announcement, routing protocol, etc. The NO command shuts IPv6 function.

(2). Configure interface IPv6 address

Command	**Explanation**
Interface Configuration Mode	

ipv6 address <*ipv6-address*/*prefix-length*> **[eui-64]** **no ipv6 address <*ipv6-address/prefix-length*>**	Configure IPv6 address, including aggregatable global unicast addresses, local site addresses and local link addresses. The **no ipv6 address <*ipv6-address/prefix-length*>** command cancels IPv6 address.

(3). Set IPv6 Static Routing

Command	**Description**
Global mode	
[no] ipv6 route <*iPv6-prefix/prefix-length*> {<*nexthop-Ipv6-address*>|<*interface-type interface-number*>|{<*nexthop-Ipv6-address*> <*interface-type interface-number*>}} [*distance*]	Configure IPv6 static routing. The NO command cancels IPv6 static routing.

2. IPv6 Neighbor Discovery Configuration

（1）Configure DAD Neighbor Query Message number

Command	**Explanation**
Interface Configuration Mode	
[no] ipv6 nd dad attempts <*value*>	Set the neighbor query message number sent in sequence when the interface makes repeating address check. The NO command resumes default value (1).

（2）Configure Send Neighbor Query Message Interval

Command	**Explanation**
Interface Configuration Mode	
[no] ipv6 nd ns-interval <*seconds*>	Set the interval of the interface to send neighbor query message. The NO command resumes default value (1 second).

（3）Forbid Router announce

Command	**Explanation**
Interface Configuration Mode	
[no] ipv6 nd suppress-ra	Forbid IPv6 Router Announce. The NO command enables IPv6 router announce.

（4）Configure Router Announce Lifespan

Command	**Explanation**

Interface Configuration Mode	
[no] ipv6 nd ra-lifetime <*seconds*>	Configure Router Announce Lifespan. The NO command resumes default value (1800 seconds).

（5）Configure Router Announce Minimum Interval

Command	**Description**
Interface Configuration Mode	
[no] ipv6 nd min-ra-interval <*seconds*>	Configure the minimum interval for router announce. The NO command resumes default value (200 seconds).

（6）Configure Router Announce Maximum Interval

Command	**Explanation**
Interface Configuration Mode	
[no] ipv6 nd max-ra-interval <seconds>	Configure the maximum interval for router announce. The NO command resumes default value (600 seconds).

（7）Configure prefix announce parameters

Command	**Explanation**
Interface Configuration Mode	
[no] ipv6 nd prefix <ipv6-address/prefix-length> <valid-lifetime> <preferred-lifetime> [off-link] [no-autoconfig]	Configure the address prefix and announce parameters of router. The NO command cancels the address prefix of routing announce.

（8）Set Static Neighbor Table Entries

Command	**Explanation**
Interface Configuration Mode	
ipv6 neighbor <ipv6-address> <hardware-address> interface <interface-type interface-number>	Set static neighbor table entries, including neighbor IPv6 address, MAC address and two-layer port
no ipv6 neighbor <*ipv6-address*>	Delete neighbor table entries

（9）Clear Neighbor Table Entries

Command	**Explanation**
Admin Mode	
clear ipv6 neighbors	Clear all static neighbor table entries

3. IPv6 Tunnel Configuration

（1）Add/Delete tunnel

Command	Admin Mode
Global mode	
[no] interface tunnel <*tnl-id*>	Create a tunnel. The NO command deletes a tunnel.

（**2**）Configure tunnel source

Command	**Admin Mode**
Tunnel Configuration Mode	
[no] tunnel source <*ipv4-daddress*>	Configure tunnel source end IPv4 address. The NO command deletes the IPv4 address of tunnel source end.

（**3**）Configure Tunnel Destination

Command	**Description**
Tunnel Configuration Mode	
[no] tunnel destination <*ipv4-address*>	Configure tunnel destination end IPv4 address. The NO command deletes the IPv4 address of tunnel destination end.

（**4**）Configure Tunnel Next-Hop

Command	**Description**
Tunnel Configuration Mode	
[no] tunnel nexthop <*ipv4-daddress*>	Configure tunnel next-hop IPv4 address. The NO command deletes the IPv4 address of tunnel next-hop end.

（**5**）Configure Tunnel 6to4 Relay

Command	**Explanation**
Tunnel Configuration Mode	
[no] tunnel 6to4-relay <*ipv4-daddress*>	Configure 6to4 tunnel relay IPv4 address. The NO command deletes the IPv4 address of 6to4 tunnel relay.

（**6**）Configure Tunnel Mode

Command	**Explanation**
Tunnel Configuration Mode	
[no] tunnel mode ipv6ip | 6ot4 | isatap	Configure tunnel mode. The NO command clears tunnel mode.

（**7**）Configure Tunnel Routing

Command	**Explanation**
Global mode	

[no] ipv6 route <*ipv6-address/prefix-length*> {<*interface-type interface-number*> | tunnel <*tnl-id*>}	Configure tunnel routing. The NO command clears tunnel routing.

10.2.2.4 Commands For IPv6 Configuration

10.2.2.4.1 ipv6 enable

Command：[no] ipv6 enable

Function：This command enables functions such as Unicast IPv6 Data Packet Transmit, Neighbor Discover, Router Bulletin and Routing Protocol, etc.

Parameter：None

Command Mode：Global Mode

Default：Disable IPv6 Enable switch

Usage Guide：To enable ipv6 enable command will allow configuring IPv6 command and process IPv6 data transmission.

Example：Turn on IPv6 Enable switch under Global Mode.

Switch(Config)#ipv6 enable

10.2.2.4.2 ipv6 address

Command：ipv6 address <*ipv6-address/prefix-length*> [eui-64]

no ipv6 address <*ipv6-address/prefix-length*> [eui-64]

Function：Configure aggregatable global unicast address, local site address and local link address for the interface

Parameter：Parameter **<*ipv6-address*>** is the prefix of IPv6 address, parameter **<*prefix-length*>** is the distance of the prefix of IPv6 address, which is between 3-128, **eui-64** means IPv6 address is generated automatically based on eui64 interface identifier of the interface

Command Mode：Interface Configuration Mode

Default： None

Usage Guide：IIPv6 address prefix can not be multicast address or any other IPv6 address with specific usages, different vlan layer 3 interfaces can not configure the same address prefix. For global unicast address, the prefix must be in the range from 2001:: to 3fff::, and the length of the prefix must be bigger than or equal to 3. For local site address and local link address, the length of the prefix must be bigger than or equal to 3.

Example：Configure an IPv6 address on Vlan1 Layer 3 interface: the prefix is 2001:3f:ed8::99 and the length of the prefix is 64

Switch(Config-if-Vlan1)#ipv6 address 2001:3f:ed8::99/64

10.2.2.4.3 ipv6 route

Command：[no] ipv6 route <*ipv6-prefix/prefix-length*> {<*ipv6-address*>
|<*interface-type interface-number*>|{<*ipv6-address*> <*interface-type*
***interface-number*>}|tunnel <*tunnel no*> }} [<*precedence*>]**

Function：Set IPv6 static router

Parameters：Parameter ***<ipv6-prefix>*** is the destination address of IPv6 network static router, parameter ***<prefix-length>*** is the length of IPv6 prefix, parameter ***<ipv6-address>*** is the next hop IPv6 address of the reachable network, parameter ***<interface-type interface-number>*** is the interface name of directed static router exit, parameter ***<tunnel no>*** is the exit tunnel No. of tunnel router, parameter <***precedence>*** is the weight of this router, the range is 1-255, the default is 1

Default：There is not any IPv6 static router is configured.

Command Mode：Global Mode

Usage Guide： When the next hop IPv6 address is local link address, the interface name of the exit must be specified. When the next hop IPv6 address is global aggregatable unicast address and local site address, if no interface name of the exit is specified, it must be assured that the IP address of the next hop and the address of some interface of the switch must be in the same network segment. Interface name can be specified directly for tunnel router.

Example：Configure static router 1 with destination address 3ffe:589:dfc::88, prefix length 64 and next hop 2001:8fd:c32::99 (the router has been configured IPv6 address of 2001:8fd:c32::34/64)

Switch(Config)#ipv6 route 3ffe:589:dfc::88/64 2001:8fd:c32::99

Configure static router2 with destination 3ffe:ff7:123::55, prefix length 64, next hop fe80::203:ff:89fd:46ac and exit interface name Vlan1

Switch(Config)#ipv6 route 3ffe:ff7:123::55/64 fe80::203:ff:89fd:46ac Vlan1

10.2.2.4.4 ipv6 nd dad attempts

Command：ipv6 nd dad attempts <*value*>

no ipv6 nd dad attempts

Function：Set Neighbor Request Message number sent in succession by interface when setting Repeat Address Check..

Parameter：<*value*> is the Neighbor Request Message number sent in succession by Repeat Address Check, and the value of **<*value*>** must be in 0-10, NO command restores to default value 1.

Command Mode：Interface Configuration Mode

Default：The default request message number is 1

Usage Guide：When configuring an IPv6 address, it is required to process IPv6 Repeat Address Check, this command is used to configure the ND message number of Repeat Address Check to be sent, *value* being 0 means no Repeat Address Check is executed.

Example：The Neighbor Request Message number sent in succession by interface when setting Repeat Address Check is 3..

Switch(Config-if-Vlan1)# ipv6 nd dad attempts 3

10.2.2.4.5 ipv6 nd ns-interval

Command：**ipv6 nd ns-interval <*seconds*>**

no ipv6 nd ns-interval

Function：Set the time interval of Neighbor Request Message sent by the interface

Parameter：parameter **<*seconds*>** is the time interval of sending Neighbor Request Message, **<*seconds*>** value must be between 1-3600 seconds, *no* command restores the default value 1 second.

Command Mode：Interface Configuration Mode

Default：The default Request Message time interval is 1 seconds.

Default：The value to be set will include the situation in all routing announcement on the interface. Generally, very short time interval is not recommended.

Example：Set Vlan1 interface to send out Neighbor Request Message time interval to be 8 seconds.

Switch(Config-if-Vlan1)#ipv6 nd ns-interval 8

10.2.2.4.6 ipv6 nd suppress-ra

Command：**[no] ipv6 nd suppress-ra**

Function：Prohibit router announcement.

Parameter：None

Command Mode：Interface Configuration Mode

Default Situation：There is not Enable router announcement function.

Usage Guide：no ipv6 nd suppress-ra command enable router announcement function.

Example：Enable router announcement function.

Switch(Config-if-Vlan1)#no ipv6 nd suppress-ra

10.2.2.4.7 ipv6 nd ra-lifetime

Command：**ipv6 nd ra-lifetime <seconds>**

no ipv6 nd ra-lifetime

Function：Configure the lifetime of router announcement

Parameter： parameter <***seconds***> stands for the number of seconds of router announcement lifetime, **<*seconds*>** value must be between 9-9000.

Command Mode： Interface Configuration Mode

Default：The number of seconds of router default announcement lifetime is 1800.

Usage Guide：This command is used to configure the lifetime of the router on Layer 3 interface, seconds being 0 means this interface can not be used for default router, otherwise the value should not be smaller than the maximum time interval of sending router announcement. If no configuration is made, this value is equal to 3 times of the maximum time interval of sending routing announcement.

Example：Set the lifetime of routing announcement is 100 seconds.

Switch (Config-if-Vlan1)#ipv6 nd ra-lifetime 100

10.2.2.4.8 ipv6 nd min-ra-interval

Command：**ipv6 nd min-ra-interval <seconds>**

no ipv6 nd min-ra-interval

Function：Set the minimum time interval of sending routing message.

Parameter：Parameter **<*seconds*>** is number of seconds of the minimum time interval of sending routing announcement, **<*seconds*>** must be between 3-1350 seconds.

Command Mode：Interface Configuration Mode

Default：The default minimum time interval of sending routing announcement is 200 seconds.

Usage Guide：The minimum time interval of routing announcement should not exceed 1/4 of the maximum time interval.

Example：Set the minimum time interval of sending routing announcement is 10 seconds.

Switch (Config-if-Vlan1)#ipv6 nd min-ra-interval 10

10.2.2.4.9 ipv6 nd max-ra-interval

Command：**ipv6 nd max-ra-interval <seconds>**

no ipv6 nd max-ra-interval

Function：Set the maximum time interval of sending routing message.

Parameter：Parameter **<*seconds*>** is number of seconds of the time interval of sending routing announcement, **<*seconds*>** must be between 4-1800 seconds.

Command Mode：Interface Configuration Mode

Default：The default maximum time interval of sending routing announcement is 600 seconds.

Usage Guide：The maximum time interval of routing announcement should be smaller than the lifetime value routing announcement.

Example：Set the maximum time interval of sending routing announcement is 20 seconds.

Switch (Config-if-Vlan1)#ipv6 nd max-ra-interval 20

10.2.2.4.10 ipv6 nd prefix

Command：ipv6 nd prefix <ipv6-prefix/prefix-length> { [<valid-lifetime> <preferred-lifetime>] [no-autoconfig | off-link [no-autoconfig]]}

[no] ipv6 nd prefix <ipv6-prefix/prefix-length>

Function：Configure the address prefix and relative parameters for router announcement.

Parameter：Parameter ***<ipv6-prefix>*** is the address prefix of the specified announcement, parameter <***prefix-length***> is the length of the address prefix of the specified announcement, parameter <***valid-lifetime***> is the valid lifetime of the prefix, parameter <***preferred-lifetime***> is the preferred lifetime of the prefix, and the valid lifetime must be no smaller than preferred lifetime. Parameter **no-autoconfig** says this prefix can not be used to automatically configure IPv6 address on the host in local link. Parameter **off-link** says the prefix specified by router announcement message is not assigned to local link, the node which sends data to the address including this prefix consider local link as unreachable.

Command Mode：Interface Configuration Mode

Default：The default value of ***valid-lifetime*** is 2592000 seconds (30 days), the default value of ***preferred-lifetime*** is 604800 seconds (7 days). **off-link** is off by default, **no-autoconfig** is off by default.

Usage Guide：This command allows controlling the router announcement parameters of every IPv6 prefix. Note that valid lifetime and preferred lifetime must be configured simultaneously.

Example：Configure IPv6 announcement prefix as 2001:410:0:1::/64 on Vlan1, the valid lifetime of this prefix is 8640 seconds, and its preferred lifetime is 4320 seconds.

Switch (Config-if-Vlan1)#ipv6 nd prefix 2001:410:0:1::/64 8640 4320

10.2.2.4.11 ipv6 nd prefix

Command：ipv6 nd prefix <ipv6-prefix/prefix-length> { [<valid-lifetime> <preferred-lifetime>] [no-autoconfig | off-link [no-autoconfig]]}

[no] ipv6 nd prefix <ipv6-prefix/prefix-length>

Function：Configure the address prefix and relative parameters for router

announcement.

Parameter：Parameter ***<ipv6-prefix>*** is the address prefix of the specified announcement, parameter <***prefix-length>*** is the length of the address prefix of the specified announcement, parameter <***valid-lifetime>*** is the valid lifetime of the prefix, parameter <***preferred-lifetime>*** is the preferred lifetime of the prefix, and the valid lifetime must be no smaller than preferred lifetime. Parameter **no-autoconfig** says this prefix can not be used to automatically configure IPv6 address on the host in local link. Parameter **off-link** says the prefix specified by router announcement message is not assigned to local link, the node which sends data to the address including this prefix consider local link as unreachable.

Command Mode：Interface Configuration Mode

Default：The default value of ***valid-lifetime*** is 2592000 seconds (30 days), the default value of ***preferred-lifetime*** is 604800 seconds (7 days). **off-link** is off by default, **no-autoconfig** is off by default.

Usage Guide：This command allows controlling the router announcement parameters of every IPv6 prefix. Note that valid lifetime and preferred lifetime must be configured simultaneously.

Example：Configure IPv6 announcement prefix as 2001:410:0:1::/64 on Vlan1, the valid lifetime of this prefix is 8640 seconds, and its preferred lifetime is 4320 seconds.

Switch (Config-if-Vlan1)#ipv6 nd prefix 2001:410:0:1::/64 8640 4320

10.2.2.4.12 ipv6 neighbor

Command：**ipv6 neighbor <*ipv6-address*> <*hardware-address*> interface <** ***interface-type interface-number*>**

no ipv6 neighbor <*ipv6-address*>

Function：Set static neighbor table entry.

Parameters：Parameter ***ipv6-address*** is static neighbor IPv6 address, parameter ***hardware-address*** is static neighbor hardware address, ***interface-type*** is Ethernet type, ***interface-number*** is Layer 2 interface name.

Command Mode：Interface Configuration Mode

Default Situation：There is not static neighbor table entry.

Usage Guide：IPv6 address and multicast address for specific purpose and local address can not be set as neighbor.

Example：Set static neighbor 2001:1:2::4 on port E1/1, and the hardware MAC address is 00-03-0f-89-44-bc

Switch(Config-if-Vlan1)#ipv6 neighbor 2001:1:2::4 00-03-0f-89-44-bc interface Ethernet 1/1

10.2.2.4.13 interface tunnel

Command：[no] interface tunnel <*tnl-id*>

Function：Create/Delete tunnel.

Parameter：Parameter **<*tnl-id*>** is tunnel No.

Command Mode：Interface Configuration Mode

Default ：None

Usage Guide：This command creates a virtual tunnel interface. Since there is not information such as specific tunnel mode and tunnel source, ***show ipv6 tunnel*** does not show the tunnel, enter tunnel mode after creating, under that model information such as tunnel source and destination can be specified. NO command is to delete a tunnel.

Example：Create tunnel 1

Switch {Config}#interface tunnel 1

10.2.2.4.14 ping6

Command：ping6 [*ipv6-address]*

Function：Validate the reachability of the network.

Parameter：Parameter ***ipv6-address*** is destination IPv6 address.

Default：None

Command Mode：Admin Mode

Usage Guide：ping6 being followed by IPv6 address is the default situation, ping6 function can make settings for parameters of ping packets based on user choice. When ipv6-address is local link address, it is required to specify port number.

Example：

Switch#ping6

Target IPv6 address:fe80:0000:0000:0000:0203:0fff:fe01:2786

Repeat count [5]: 1

Datagram size in byte [56]: 80

Timeout in milli-seconds [2000]: 2500

Extended commands [n]: Type ^c to abort. n

Sending 1 80-byte ICMP Echoes to fe80:0000:0000:0000:0203:0fff:fe01:2786, timeout is 2 seconds.

!

Success rate is 100 percent (1/1), round-trip min/avg/max = 1/1/1 ms

Displayed information	Explanation
ping6	Execute ping6 function
Target IPv6 address	Destination IPv6 address
Repeat count	Number of ping packets being sent

Datagram size in byte	Size of Ping packets
Timeout in milli-seconds	Time delay allowed
Extended commands	Settings of extensive parameters
!	Indicate that the network is reachable
Success rate is 100 percent (1/1), round-trip min/avg/max = 1/1/1 ms	Statistics information, which shows the rate of ping packets arriving successfully is 100%, no loss.

10.2.2.4.15 tunnel source

Command：[no] tunnel source *<ipv4-daddress>*

Function：Configure tunnel source.

Parameter：***<ipv4-daddress>*** is the ipv4 address of tunnel source

Command Mode：Tunnel Configuration Mode

Default Situation： None

Usage Guide：None

Example：Configure tunnel source IPv4 address 202.89.176.6

Switch {Config-if-Tunnel1}#tunnel source 202.89.176.6

10.2.2.4.16 tunnel destination

Command： **[no] tunnel destination *<ipv4-daddress>***

Function：Configure tunnel destination.

Parameter：***<ipv4-daddress>*** is the ipv4 address of tunnel destination

Command Mode： Tunnel Configuration Mode

Default Situation：None

Usage Guide： None

Example：Configure tunnel destination 203.78.120.5

Switch {Config-if-Tunnel1}#tunnel destination 203.78.120.5

10.2.2.4.17 tunnel nexthop

Command：**[no] tunnel nexthop *<ipv4-daddress>***

Function：Configure tunnel next hop.

Parameter：***<ipv4-daddress>*** is the ipv4 address of tunnel next hop.

Command Mode：Tunnel Configuration Mode

Default Situation：None

Usage Guide：This command is for ISATAP tunnel, other tunnels won't check the configuration of nexthop.

Example：Configure tunnel next hop 178.99.156.8

Switch {Config-if-Tunnel1}#tunnel nexthop 178.99.156.8

10.2.2.4.18 tunnel 6to4-relay

Command：[no] tunnel 6to4-relay *<ipv4-daddress>*

Function： Configure 6to4 tunnel relay IPv4 address.

Parameter：*<ipv4-daddress>* is 6to4 tunnel relay IPv4 address.

Command Mode：Tunnel Configuration Mode

Default Situation：None

Usage Guide：This command is used to configure 6to4 tunnel relay IPv4 address. The IPv4 address won't be checked in configuring 6to4 tunnel relay. Relay IPv4 address will be used only if the data packets pass the default router and the destination address is not started with 2002.

Example：Configure 6to4 tunnel relay IPv4 address 178.99.156.8

Switch {Config-if-Tunnel1}#tunnel 6to4-relay 178.99.156.8

10.2.2.4.19 tunnel mode

Command：[no] tunnel mode {ipv6ip | 6to4 | isatap}

Function： Configure Tunnel Mode

Parameter：None

Command Mode：Tunnel Configuration Mode

Default：None

Usage Guide：In configuring tunnel mode, only specifying ipv6ip indicates configuring tunnel. Ipv6ip 6to4 indicates it is 6to4 tunnel, ipv6ip isatap indicates it is ISATAP tunnel.

Example：Configure tunnel mode

1、Switch {Config-if-Tunnel1}#tunnel mode ipv6ip

2、Switch {Config-if-Tunnel1}#tunnel mode ipv6ip 6to4

3、Switch {Config-if-Tunnel1}#tunnel mode ipv6ip isatap

10.2.2.4.20 clear ipv6 neighbor

Command：clear ipv6 neighbors

Function：Clear the neighbor cache of IPv6.

Parameter：None

Command Mode：Admin Mode

Default：None

Usage Guide：This command can not clear static neighbor.

Example：Clear neighbor list.

Switch #clear ipv6 neighbors

10.2.3 IP Configuration Examples

10.2.3.1 Configuration Examples of IPv4

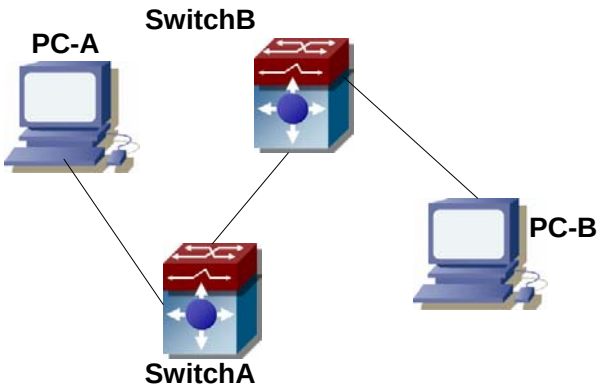


Fig 10-1IPv4 configuration example

The user's configuration requirements are: Configure IPv4 address of different network segments on switch1 and switch2, configure static routing and validate accessibility using ping function.

Configuration Description:

1、Configure two vlans on SwitchA, namely, vlan1 and vlan2.

2、Configure IPv6 address 192.168.1.1 255.255.255.0 in vlan1 of SwitchA, and configure IPv4 address 192.168.2.1 255.255.255.0 in vlan2.

3、Configure two vlans on SwitchB, respectively vlan2 and vlan3

4、Configure IPv4 address 192.168.2.2 255.255.255.0 in vlan2 of SwitchB, and configure IPv4 address 192.168.3.1 255.255.255.0 in vlan2.

5、The IPv4 address of PC-A is 192.168.1.100, and the IPv4 address of PC-B is 192.168.3.100

6、Configure static routing 192.168.3.0/24 on SwitchA, and configure static routing 192.168.1.0/24 on SwitchB.

7、Ping each other among PCs.

Note: First make sure PC-A and Switch can access each other by ping, and PC-B and SwitchB can access each other by ping.

The configuration procedure is as follows:

SwitchA(Config)#interface vlan 1

SwitchA(Config-if-Vlan1)#IP address 192.168.1.1 255.255.255.0

SwitchA(Config)#interface vlan 2

SwitchA(Config-if-Vlan2)#IP address 192.168.2.1 255.255.255.0

SwitchA(Config-if-Vlan2)#exit

SwitchA(Config)#IP route 192.168.3.0 255.255.255.0 192.168.2.2

SwitchB(Config)#interface vlan 2
SwitchB(Config-if-Vlan2)#IP address 192.168.2.2 255.255.2550
SwitchB(Config)#interface vlan 3
SwitchB(Config-if-Vlan3)#IP address 192.168.3.1 255.255.255.0
SwitchB(Config-if-Vlan3)#exit
SwitchB(Config)#IP route 192,168.1.0 255.255.255.0 192.168.2.1

10.2.3.2 Configuration Examples of IPv6

Example 1:

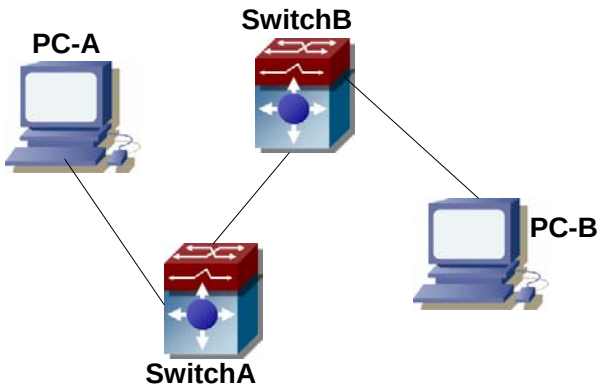


Fig 10-2 IPv6 configuration example

The user's configuration requirements are: Configure IPv6 address of different network segments on SwitchA and SwitchB, configure static routing and validate reachability using ping6 function.

Configuration Description:

1、Configure two vlans on SwitchA, namely, vlan1 and vlan2.
2、Configure IPv6 address 2001::1/64 in vlan1 of SwitchA, and configure IPv6 address 2002::1/64 in vlan.
3、Configure 2 vlans on SwitchB, namely, vlan2 and vlan3.
4、Configure IPv6 address 2002::2/64 in vlan2 of SwitchB, and configure IPv6 address 2003::1/64 in vlan2.
5、The IPv6 address of PC-A is 2001::11/64, and the IPv6 address of PC-B is 2003::33/64.
6、Configure static routing 2003:33/64 on SwitchA, and configure static routing 2001::11/64 on SwitchB.
7、ping6 2003::33

Note: First make sure PC-A and Switch can access each other by ping, and PC-B and SwitchB can access each other by ping.

The configuration procedure is as follows:

```
SwitchA(Config)#ipv6 enable
SwitchA(Config)#interface vlan 1
SwitchA(Config-if-Vlan1)#ipv6 address 2001::1/64
SwitchA(Config)#interface vlan 2
SwitchA(Config-if-Vlan2)#ipv6 address 2002::1/64
SwitchA(Config-if-Vlan2)#exit
SwitchA(Config)#ipv6 route 2003::33/64 2002::2

SwitchB(Config)#ipv6 enable
SwitchB(Config)#interface vlan 2
SwitchB(Config-if-Vlan2)#ipv6 address 2002::2/64
SwitchB(Config)#interface vlan 3
SwitchB(Config-if-Vlan3)#ipv6 address 2003::1/64
SwitchB(Config-if-Vlan3)#exit
SwitchB(Config)#ipv6 route 2001::33/64 2002::1

SwitchA#ping6 2003::33
```

Configuration results:

```
SwitchA#show run
interface Vlan1
 ipv6 address 2001::1/64
!
interface Vlan2
 ipv6 address 2002::2/64
!
interface Loopback
 mtu 3924
!
ipv6 route 2003::/64 2002::2
!
no login
!
end
SwitchB#show run
interface Vlan2
 ipv6 address 2002::2/64
!
```

```
interface Vlan3
 ipv6 address 2003::1/64
!
interface Loopback
 mtu 3924
!
ipv6 route 2001::/64 2002::1
!
no login
!
End
```

Example 2:

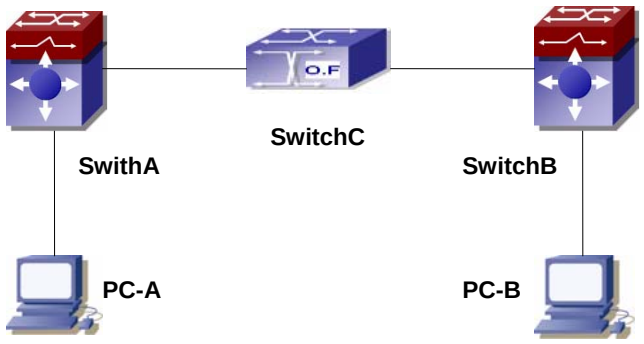


Fig 10-3 IPv6 tunnel

This case is IPv6 tunnel with the following user configuration requirements: SwitchA and SwitchB are tunnel nodes, dual-stack is supported. SwitchC only runs IPv4, PC-A and PC-B communicate.

Configuration Description:

1、Configure two vlans on SwitchA, namely, vlan1 and vlan2. Vlan1 is IPv6 domain, vlan2 connects to IPv4 domain.

2、Configure IPv6 address 2002:caca:ca01:2::1/64 in vlan1 of SwitchA and turn on RA function, configure IPv4 address 202.202.202.1 in vlan2.

3、Configure two vlans on SwitchB, namely, vlan3 and vlan4, vlan4 is IPv6 domain, and vlan3 connects to IPv4 domain.

4、Configure IPv6 address 2002:cbcb:cb01:2::1/64 in vlan4 of SwitchB and turn on RA function, configure IPv4 address 203.203.203.1 on vlan3.

5、Configure tunnel on SwitchA, the source IPv4 address of the tunnel is 202.202.202.1, the tunnel routing is ::/0

6、Configure tunnel on SwitchB, the source IPv4 address of the tunnel is 202.202.202.2, and the tunnel routing is ::/0

7、Configure two vlans on SwitchC, namely, vlan2 and vlan3. Configure IPv4 address 202.202.202.202 on vlan2 and configure IPv4 address 203.203.203.203 on vlan3.

8、PC-A and PC-B get the prefix of 2002 via SwitchA and SwitchB to configure IPv6 address automatically.

9、On PC-A, ping IPv6 address of PC-B

```
SwitchA(config)#ipv6 enable
SwitchA(Config-if-Vlan1)#ipv6 address 2002:caca:ca01:2::1/64
SwitchA(Config-if-Vlan1)#no ipv6 nd suppress-ra
SwitchA(Config-if-Vlan1)#interface vlan 2
SwitchA(Config-if-Vlan2)#ipv4 address 202.202.202.1 255.255.255.0
SwitchA(Config-if-Vlan1)#exit
SwitchA(config)# interface tunnel 1
SwitchA(Config-if-Tunnel1)#tunnel source 202.202.202.1
SwitchA(Config-if-Tunnel1)#tunnel destination 203.203.203.1
SwitchA(Config-if-Tunnel1)#tunnel mode ipv6ip
SwitchA(config)#ipv6 route ::/0 tunnel1

SwitchB(config)#ipv6 enable
SwitchB(Config-if-Vlan4)#ipv6 address 2002:cbcb:cb01::2/64
SwitchB(Config-if-Vlan4)#no ipv6 nd suppress-ra
SwitchB (Config-if-Vlan3)#interface vlan 3
SwitchB (Config-if-Vlan2)#ipv4 address 203.203.203.1 255.255.255.0
SwitchB (Config-if-Vlan1)#exit
SwitchB(Config)#interface tunnel 1
SwitchB(Config-if-Tunnel1)#tunnel source 203.203.203.1
SwitchB(Config-if-Tunnel1)#tunnel destination 202.202.202.1
SwitchB(Config-if-Tunnel1)#tunnel mode ipv6ip
SwitchB(config)#ipv6 route ::/0 tunnel1
```

10.2.4 IP Troubleshooting

IPv6 troubleshooting：

- IPv6 switch must be turned on when configuring IPv6 commands, otherwise the configuration is invalid.
- The router lifespan configured should not be smaller then the Send Router Announce Interval.
- If the connected PC has not obtained IPv6 address, you should check the RA

announce switch (the default is turned off)

10.2.4.1 Commands for Monitor And Debug

10.2.4.1.1 show ip traffic

Command: show ip traffic

Function: Display statistics for IP packets.

Command mode: Admin Mode

Usage Guide: Display statistics for IP and ICMP packets received/sent.

Example:

```
Switch#show ip traffic
IP statistics:
  Rcvd:  128 total, 128 local destination
         0 header errors, 0 address errors
         0 unknown protocol, 0 discards
  Frags:  0 reassembled, 0 timeouts
         0 fragment rcvd, 0 fragment dropped
         0 fragmented, 0 couldn't fragment, 0 fragment sent
  Sent:   0 generated, 0 forwarded
         0 dropped, 0 no route
ICMP statistics:
  Rcvd:  0 total 0 errors 0 time exceeded
         0 redirects, 0 unreachable, 0 echo, 0 echo replies
         0 mask requests, 0 mask replies, 0 quench
         0 parameter, 0 timestamp, 0 timestamp replies
  Sent:   0 total 0 errors 0 time exceeded
         0 redirects, 0 unreachable, 0 echo, 0 echo replies
         0 mask requests, 0 mask replies, 0 quench
         0 parameter, 0 timestamp, 0 timestamp replies
TCP statistics:
  TcpActiveOpens          0, TcpAttemptFails          0
  TcpCurrEstab            0, TcpEstabResets           0
  TcpInErrs               0, TcpInSegs                0
  TcpMaxConn              0, TcpOutRsts               0
  TcpOutSegs              0, TcpPassiveOpens          0
  TcpRetransSegs          0, TcpRtoAlgorithm          0
  TcpRtoMax               0, TcpRtoMin                0
UDP statics:
  UdpInDatagrams          0, UdpInErrors              0
```

UdpNoPorts 0, UdpOutDatagrams 0

Displayed information	Explanation
IP statistics：	IP packet statistics.
Rcvd： 290 total, 44 local destinations 0 header errors, 0 address errors 0 unknown protocol, 0 discards	Statistics of total packets received, number of packets reached local destination, number of packets have header errors, number of erroneous addresses, number of packets of unknown protocols; number of packets dropped.
Frags： 0 reassembled, 0 timeouts 0 fragment rcvd, 0 fragment dropped 0 fragmented, 0 couldn't fragment, 0 fragment sent	Fragmentation statistics: number of packets reassembled, timeouts, fragments received, fragments discarded, packets that cannot be fragmented, number of fragments sent, etc.
Sent： 0 generated, 0 forwarded 0 dropped, 0 no route	Statistics for total packets sent, including number of local packets, forwarded packets, dropped packets and packets without route.
ICMP statistics：	ICMP packet statistics.
Rcvd： 0 total 0 errors 0 time exceeded 0 redirects, 0 unreachable, 0 echo, 0 echo replies 0 mask requests, 0 mask replies, 0 quench 0 parameter, 0 timestamp, 0 timestamp replies	Statistics of total ICMP packets received and classified information
Sent： 0 total 0 errors 0 time exceeded 0 redirects, 0 unreachable, 0 echo, 0 echo replies 0 mask requests, 0 mask replies, 0 quench 0 parameter, 0 timestamp, 0 timestamp replies	Statistics of total ICMP packets sent and classified information
TCP statistics:	TCP packet statistics.
UDP statistics:	UDP packet statistics.

10.2.4.1.2 debug ip packet

Command: debug ip packet

no debug ip packet

Function: Enable the IP packet debug function: the “no debug IP packet” command disables this debug function.

Default: IP packet debugging information is disabled by default.

Command mode: Admin Mode

Usage Guide: Displays statistics for IP packets received/sent, including source/destination address and bytes, etc.

Example: Enabling IP packet debug.

Switch#debug ip pa

ip packet debug is on

Switch#

Switch#

Switch#

Switch#%Apr 19 15:56:33 2005 IP PACKET: rcvd, src 192.168.2.100, dst 192.168.2.1

, size 60, Ethernet0

10.2.4.1.3 debug ipv6 packet

Command：[no] debug ipv6 packet

Function：IPv6 data packets receive/send debug message.

Parameter：None

Default：None

Command Mode：Admin Mode

Usage Guide：

Example：

Switch#debug ipv6 packet

IPv6 PACKET: rcvd, src <fe80::203:fff:fe01:2786>, dst <fe80::1>, size <64>, proto <58>, from Vlan1

Displayed information	Explanation
IPv6 PACKET: rcvd	Receive IPv6 data report
Src <fe80::203:fff:fe01:2786>	Source IPv6 address
Dst <fe80::1>	Destination IPv6 address
size <64>	Size of data report
proto <58>	Protocol field in IPv6 header
from Vlan1	IPv6 data report is collected from Layer 3 port vlan1

10.2.4.1.4 debug ipv6 icmp

Command：[no] debug ipv6 icmp

Function：ICMP data packets receive/send debug message.

Parameter：None

Default： None

Command Mode：Admin Mode

Example：

Switch#debug ipv6 icmp

IPv6 ICMP: sent, type <129>, src <2003::1>, dst <2003::20a:ebff:fe26:8a49> from Vlan1

Displayed information	Explanation
IPv6 ICMP: sent	Send IPv6 data report
type <129>	Ping protocol No.
Src <2003::1>	Source IPv6 address
Dst <2003::20a:ebff:fe26:8a49>	Destination IPv6 address
from Vlan1	Layer 3 port being sent

10.2.4.1.5 debug ipv6 nd

Command：**[no] debug ipv6 nd**

Function：ND data packets receive/send debug message.

Parameter：None

Default：None

Command Mode：Admin Mode

Example：

Switch#debug ipv6 nd

IPv6 ND: rcvd, type <136>, src <fe80::203:fff:fe01:2786>, dst <fe80::203:fff:fe01:59ba>

Displayed information	Explanation
IPv6 ND: rcvd	Receive ND data report
type <136>	ND Type
Src <fe80::203:fff:fe01:2786>	Source IPv6 address
Dst <fe80::203:fff:fe01:59ba>	Destination IPv6 address

10.2.4.1.6 debug ipv6 tunnel packet

Command：**[no] debug ipv6 tunnel packet**

Function：tunnel data packets receive/send debug message.

Parameter：None

Default：None

Command Mode：Admin Mode

Example：

Switch#debug ipv6 tunnel packet

IPv6 tunnel: rcvd, type <136>, src <fe80::203:fff:fe01:2786>, dst

<fe80::203:fff:fe01:59ba>

IPv6 tunnel packet : rcvd src 178.1.1.1 dst 179.2.2.2 size 128 from tunnel1

Displayed information	Explanation
IPv6 tunnel packet : rcvd	Receive tunnel data report
type <136>	ND type
Src 178.1.1.1 dst	Tunnel source IPv4 address
Dst 179.2.2.2	Tunnel destination IPv4 address

10.2.4.1.7 show ipv6 interface

Command：show ipv6 interface {brief|{interface-name}}

Function：Show interface IPv6 parameters.

Parameter：Parameter brief is the brief summarization of IPv6 status and configuration, and parameter interface-name is Layer 3 interface name.

Default：None

Command Mode：Admin Mode

Usage Guide：If only brief is specified, then information of all three layers is displayed, and you can also specify a specific Layer 3 interface.

Example：

Switch#show ipv6 interface Vlan1

Vlan1 is up, line protocol is up, dev index is 2004

Device flag 0x1203(UP BROADCAST ALLMULTI MULTICAST)

IPv6 is enabled

Link-local address(es):

 fe80::203:fff:fe00:10 PERMANENT

Global unicast address(es):

 3001::1 subnet is 3001::1/64 PERMANENT

Joined group address(es):

 ff02::1

 ff02::16

 ff02::2

 ff02::5

 ff02::6

 ff02::9

 ff02::d

 ff02::1:ff00:10

 ff02::1:ff00:1

MTU is 1500 bytes

ND DAD is enabled, number of DAD attempts is 1

ND managed_config_flag is unset

ND other_config_flag is unset

ND NS interval is 1 second(s)

ND router advertisements is disabled

ND RA min-interval is 200 second(s)

ND RA max-interval is 600 second(s)

ND RA hoplimit is 64

ND RA lifetime is 1800 second(s)

ND RA MTU is 0

ND advertised reachable time is 0 millisecond(s)

ND advertised retransmit time is 0 millisecond(s)

Displayed information	Explanation
Vlan1	Layer 3 interface name
[up/up]	Layer 3 interface status
dev index	Internal index No.
fe80::203:fff:fe00:10	Automatically configured IPv6 address of Layer 3 interface
3001::1	Configured IPv6 address of Layer 3 interface

10.2.4.1.8 show ipv6 route

Command：show ipv6 route [<*destination*>|<*destination* >/<*length*>| database| fib [local]| nsm [connected | static | rip| ospf | bgp | isis| kernel| database]|statistics [vrf <vrfnum>]]

Function：Display IPv6 routing table

Parameter：**<*destination*>** is destination network address; **<*destination* >/<*length*>** is destination network address plus prefix length; **connected** is directly connected router; **static** is static router; **rip** is RIP router; **ospf** is OSPF router; **bgp** is BGP router;**isis** is ISIS router; **kernel** is kernel router; **statistics** shows router number; **database** is router database.

Default Situation：None

Command Mode：Admin Mode

Usage Guide：show ipv6 route only shows IPv6 kernel routing table (routing table in tcpip), database shows all routers except the local router, fib local shows the local router, statistics shows router statistics information

Example：

Switch#show ipv6 route

Codes: C - connected, L - Local, S - static, R - RIP, O - OSPF,

I - IS-IS, B - BGP

C ::/0 via ::, tunnel3 256

S 2001:2::/32 via fe80::789, Vlan2 1024
S 2001:2:3:4::/64 via fe80::123, Vlan2 1024
O 2002:ca60:c801:1::/64 via ::, Vlan1 1024
C 2002:ca60:c802:1::/64 via ::, tunnel49 256
C 2003:1::/64 via ::, Vlan4 256
C 2003:1::5efe:0:0/96 via ::, tunnel26 256
S 2004:1:2:3::/64 via fe80:1::88, Vlan2 1024
O 2006:1::/64 via ::, Vlan1 1024
S 2008:1:2:3::/64 via fe80::250:baff:fef2:a4f4, Vlan1 1024
C 2008:2005:5:8::/64 via ::, Ethernet0 256
S 2009:1::/64 via fe80::250:baff:fef2:a4f4, Vlan1 1024
C 2022:1::/64 via ::, Ethernet0 256
O 3333:1:2:3::/64 via fe80::20c:ceff:fe13:eac1, Vlan12 1024
C 3ffe:501:ffff:1::/64 via ::, Vlan4 256
O 3ffe:501:ffff:100::/64 via ::, Vlan5 1024
O 3ffe:3240:800d:1::/64 via ::, Vlan1 1024
O 3ffe:3240:800d:2::/64 via ::, Vlan2 1024
O 3ffe:3240:800d:10::/64 via ::, Vlan12 1024
O 3ffe:3240:800d:20::/64 via fe80::20c:ceff:fe13:eac1, Vlan12 1024
C fe80::/64 via ::, Vlan1 256
C fe80::5efe:0:0/96 via ::, tunnel26 256
C ff00::/8 via ::, Vlan1 256

Displayed information	Explanation
IPv6 Routing Table	IPv6 routing table status
Codes: K - kernel route, C - connected, S - static, R - RIP, O - OSPF,I - IS-IS, B - BGP > - selected route, * - FIB route, p - stale info	Abbreviation display sign of every entry
S 2009:1::/64 via fe80::250:baff:fef2:a4f4, Vlan1 1024	The static router in FIB table, of which the destination network segment is 2002::/64, via means passing fe80::250:baff:fef2:a4f4 is the next hop, Vlan1 is the exit interface name, 1024 is router weight.

10.2.4.1.9 show ipv6 neighbors

Command：show ipv6 neighbors [*interface-type interface-number* | *ipv6-address*]

Function：Display neighbor table entry information.

Parameter：Parameter ***interface-type interface-number*** specify the lookup based on

interface name. Parameter ***ipv6-address*** specifies the lookup based on IPv6 address.

Default Situation：None

Command Mode：Admin Mode

Usage Guide：

Example：

```
Switch#show ipv6 neighbors
IPv6 neighbour unicast items: 14, valid: 11, matched: 11, incomplete: 0, delayed: 0,
        manage items 5
IPv6 Address                            Hardware Addr        Interface       State
2002:ca60:c801:1:250:baff:fef2:a4f4     00-50-ba-f2-a4-f4                    Vlan1
reachable
3ffe:3240:800d:1::100                   00-03-0f-01-27-86                    Vlan1
reachable
3ffe:3240:800d:1::8888                  00-02-01-00-00-00                    Vlan1
permanent
3ffe:3240:800d:1:250:baff:fef2:a4f4     00-50-ba-f2-a4-f4                    Vlan1
reachable
3ffe:3240:800d:2::8888                  00-02-01-00-01-01                    Vlan2
permanent
3ffe:3240:800d:2:203:fff:fefe:3045      00-03-0f-fe-30-45                    Vlan2
reachable
fe80::203:fff:fe01:2786                 00-03-0f-01-27-86                    Vlan1
reachable
fe80::203:fff:fefe:3045                 00-03-0f-fe-30-45                    Vlan2
reachable
fe80::20c:ceff:fe13:eac1                00-0c-ce-13-ea-c1                    Vlan12
reachable
fe80::250:baff:fef2:a4f4                00-50-ba-f2-a4-f4                    Vlan1
reachable
IPv6 neighbour table: 11 entries
```

Displayed information	Explanation
IPv6 Address	Neighbor IPv6 address
Link-layer Addr.	Neighbor MAC address
Interface	Exit interface name
State	Neighbor status (reachable、statle、delay、probe、permanent、incomplete、unknow)

10.2.4.1.10 show ipv6 traffic

Command：show ipv6 traffic

Function：Display IPv6 transmission data packets statistics information.

Parameter： None

Default Situation：None

Command Mode：Admin Mode

Usage Guide：

Example：

```
Switch#show ipv6 traffic
IP statistics:
  Rcvd:  90 total, 17 local destination
         0 header errors, 0 address errors
         0 unknown protocol, 13 discards
  Frags: 0 reassembled, 0 timeouts
         0 fragment rcvd, 0 fragment dropped
         0 fragmented, 0 couldn't fragment, 0 fragment sent
  Sent:  110 generated, 0 forwarded
         0 dropped, 0 no route
ICMP statistics:
  Rcvd:  0 total 0 errors 0 time exceeded
         0 redirects, 0 unreachable, 0 echo, 0 echo replies
```

Displayed information	Explanation
IP statistics	IPv6 data report statistics
Rcvd: 90 total, 17 local destination0 header errors, 0 address errors0 unknown protocol, 13 discards	IPv6 received packets statistics
Frags: 0 reassembled, 0 timeouts 0 fragment rcvd, 0 fragment dropped0 fragmented, 0 couldn't fragment, 0 fragment sent	IPv6 fragmenting statistics
Sent: 110 generated, 0 forwarded 0 dropped, 0 no route	IPv6 sent packets statistics

10.2.4.1.11 show ipv6 enable

Command：show ipv6 enable

Function：Display IPv6 transmission function on/off status

Parameter：None

Default：None

Command Mode：Admin Mode

Example：

Switch#show ipv6 enable

ipv6 enable has been on

Displayed information	Explanation
ipv6 enable has been on	IPv6 transmission switch is at on status

10.2.4.1.12 show ipv6 tunnel

Command：show ipv6 tunnel [<tnl-id>]

Function：Display tunnel information.

Parameter：Parameter **tnl-id** is tunnel No.

Default Situation：None

Command Mode：Admin Mode

Usage Guide：If there is not tunnel number, then information of all tunnels are shown. If there is tunnel number, then the detailed information of specified tunnel is shown.

Example：

Switch#show ipv6 tunnel

name mode source destination nexthop

tunnel3 6to4 178.1.1.1

Displayed information	Explanation
Name	Tunnel name
Mode	Tunnel type
Source	Tunnel source ipv4 address
Destination	Tunnel destination ipv4 address
Nexthop	Tunnel next hop (only applies to ISATAP tunnel)

10.3 IP Forwarding

10.3.1 Introduction to IP Forwarding

Gateway devices can forward IP packets from one subnet to another; such forwarding uses routes to find a path. IP forwarding of ES4626/ES4650 switch is done with the participation of hardware, and can achieve wire speed forwarding . In addition, flexible management is provided to adjust and monitor forwarding. ES4626/ES4650 switch supports aggregation algorithm enabling/disabling optimization to adjust generation of network route entry in the switch chip and view statistics for IP forwarding and hardware forwarding chip status.

10.3.2 IP Route Aggregation Configuration Task

1. Set whether IP route aggregation algorithm with/without optimization should be used.

Command	Explanation
ip fib optimize **no ip fib optimize**	Enables the switch to use optimized IP route aggregation algorithm; the "**no ip fib optimize**" disables the optimized IP route aggregation algorithm.

10.3.3 Commands for IP Route Aggregation

10.3.3.1 ip fib optimize

Command: ip fib optimize

no ip fib optimize

Function: Enables the switch to use optimized IP route aggregation algorithm; the "**no ip fib optimize**" disables the optimized IP route aggregation algorithm.

Default: Optimized IP route aggregation algorithm is disabled by default.

Command mode: Global Mode

Usage Guide: This command is used to optimize the aggregation algorithm: if the route table contains no default route, the next hop most frequently referred to will be used to construct a virtual default route to simplify the aggregation result. This method has the benefit of more effectively simplifying the aggregation result. However, while adding a virtual default route to the chip segment route table reduces CPU load, it may introduce unnecessary data stream to switches of the next hop. In fact, part of local switch CPU load is transferred to switches of the next hop.

Example: Disabling optimized IP route aggregation algorithm.

Switch(Config)# no ip fib optimize

10.4 URPF

10.4.1 URPF Introduction

URPF (Unicast Reverse Path Forwarding) introduces the RPF technology applied in multicast to unicast, so to protect the network from the attacks which is based on source address cheat.

When switch receives the packet, it will search the route in the route table using the

source address as the destination address which is acquired from the packet. If the found router exit interface does not match the entrance interface acquired from this packet, the switch will consider this packet a fake packet and discard it.

10.4.2 URPF Operation Mechanism

At present the URPF operation mechanism is dependent on the ACL function provided by the switch chip when enabling URPF on layer 3 interface.

First apply deny-all rule on all layer 2 ports under the layer 3 interface. All data packet will be denied at the switch by default.

And then apply a rule to all the port under this layer 3 interface permitting the IP address configured to the layer 3 interface which forms a direct route, so to ensure the data packet sourced within the segment can enter the switch.

As for the route learnt by the switch which goes out through this layer 3 interface, if there is any route in the hardware forwarding table in the switch which goes out from a port under this layer 3 interface, then apply ACL rule on this port in which permitting address of the packets is the destination address of this route.

With above operation, we can ensure that before the data reaches the port, only those complying with above rules can enter the port and others will be dropped.

At present the URPF is applied with strict route check mechanism. Only the data complying with rules can enter the switch through the port or be forwarded by the switch

As the priority of the ACL rules corresponding with URPF is low which will not block various protocol data packet, so enabling this function will not affect the regular operation of the switch routing protocols.

10.4.3 URPF Configuration Task Sequence

1) Enable URPF

2) Display and debug URPF relevant information

1) Globally enable URPF

Command	Explanation
Port mode	
urpf enable **no urpf enable**	Enable and disable URPF on layer 3 interface (interface vlan)

2) Display and debug URPF relevant information

Command	Explanation
Admin mode	

debug urpf **no debug urpf**	Enable the debugging information of the URPF module, the “no” form of this command disables the URPF debugging information output
show urpf	Display which layer 3 interfaces has enabled with URPF
show urpf interface	Display the URPF rules generated by the interface or layer 2 interface

10.4.4 Commands For URPF

10.4.4.1 urpf enable

Command: urpf enable

no urpf enable

Function: Enable URPF on layer 3 interface, the “no” form of this command disables the URPF enabled on this interface

Command Mode: Interface Mode

Default: URPF protocol not enabled by system default

Example: Enable urpf on interface vlan2

Switch(Config)#interface vlan 2

Switch(Config-if-Vlan1)#urpf enable

10.4.4.2 show urpf

Command: show urpf

Function: Display which interfaces have been enabled with urpf function

Command Mode: Admin mode

Example:

Switch#show urpf

Vlan2 enable urpf

10.4.4.3 show urpf interface

Command: show urpf interface *{ethernet* | *port-channel|vlan}* ifname

Function: Display the urpf rule generated on certain port (interface).

Parameter: Port name or interface name

Command Mode: Admin Mode

Example: Display the urpf rule generated under vlan2

Switch#show urpf interface vlan 2

10.4.4.4 debug urpf

Command: debug urpf

no debug urpf

Function: Enable the URPF debugging information; the “no” form of this command disables the URPF debugging information

Command Mode: Admin Mode

Parameter: None

Usage Guide: Enable the URPF debugging information and view the URPF message process and the URPF item updating process, which facilitates to locate the failure.

Example: Enable URPF debugging information display

Switch#debug urpf

10.4.5 URPF Troubleshooting

Proper operation of the URPF protocol depends greatly on whether the corresponding URPF rules can be applied correctly. If after the URPF configuration is done and the function does not meet the expectation:

- ✧ Check if the switch has been configured with the rules conflicting with URPF (URPF priority is lower than ACL), the ACL rules will validate if confliction exits.
- ✧ Check if the hardware forward table has already generated a route related to the ports under the interface. Only when the hardware forwarding table has learnt the route, it will be applied corresponding ACL rules on this port.
- ✧ Check if the hardware ACL performance is full which lead to the newly generated route can not be applied with ACL rules
- ✧ If the configuration seems normal, however the URPF operation status still not matched the expectation, please enable the URPF debugging function and check if the generate URPF rule is correct with show urpf interface command, and send the result to the technical service center of our company.

10.5 ARP

10.5.1 Introduction to ARP

ARP (Address Resolution Protocol) is mainly used to resolve IP address to Ethernet

MAC address. ES4626/ES4650 switch supports both dynamic ARP and static ARP configuration. Furthermore, ES4626/ES4650 switch supports the configuration of proxy ARP for some applications. For instance, when an ARP request is received on the port, requesting an IP address in the same IP segment of the port but not the same physical network, if the port has enabled proxy ARP, the port would reply to the ARP with its own MAC address and forward the actual packets received. Enabling proxy ARP allows machines physically separated but of the same IP segment ignores the physical separation and communicate via proxy ARP interface as if in the same physical network.

10.5.2 ARP Configuration Task List

1. Configure static ARP
2. Configure proxy ARP

1. Configure static ARP

Command	Explanation
arp *<ip_address>* *<mac_address>* {[ethernet] *<portName>*} **no arp *<ip_address>***	Configures a static ARP entry; the "**no arp *<ip_address>*"** command deletes a static ARP entry.

2. Configure proxy ARP

Command	Explanation
ip proxy-arp **no ip proxy-arp**	Enables the proxy ARP function for Ethernet ports: the "**no ip proxy-arp"** command disables the proxy ARP.

3. Clear dynamic ARP

Command	Explanation
clear arp-cache	The command "**clear arp-cache"** clears the content of current ARP table, but it does not clear the current static ARP table

10.5.3 Commands for ARP Configuration

10.5.3.1 Arp

Command: arp *<ip_address>* *<mac_address>* {[ethernet] *<portName>*}

no arp *<ip_address>*

Function: Configures a static ARP entry; the "**no arp *<ip_address>*"** command deletes a static ARP entry.

Parameters: ***<ip_address>*** is the IP address; ***<mac_address>*** is the MAC address; **ethernet** stands for Ethernet port; ***<portName>*** for the name of layer2 port.

Default: No static ARP entry is set by default.

Command mode: Interface Mode

Usage Guide: Static ARP entries can be configured in the switch.

Example: Configuring static ARP for interface VLAN1.

Switch(Config-If-Vlan1)#arp 1.1.1.1 00-03-0f-f0-12-34 eth 1/2

10.5.3.2 clear arp-cache

Command: clear arp-cache

Function: Clears arp table.

Parameters: N/A.

Command mode: Admin Mode

Usage Guide: Clears the content of current ARP table, but it does not clear the current static ARP table.

Example:

Switch#clear arp-cache

10.5.3.3 ip proxy-arp

Command: ip proxy-arp

no ip proxy-arp

Function: Enables proxy ARP for VLAN interface; the “no ip proxy-arp” command disables proxy ARP.

Default: Proxy ARP is disabled by default.

Command mode: Interface Mode

Usage Guide: When an ARP request is received on the layer 3 interface, requesting an IP address in the same IP segment of the interface but not the same physical network, and the proxy ARP interface has been enabled, the interface will reply to the ARP with its own MAC address and forward the actual packets received. Enabling this function allows machines to physically be separated but in the same IP segment and communicate via the proxy ARP interface as if in the same physical network. Proxy ARP will check the route table to determine whether the destination network is reachable before responding to the ARP request; ARP request will only be responded if the destination is reachable. Note: the ARP request matching default route will not use proxy.

Example: Enabling proxy ARP for VLAN 1.

Switch(Config-If-Vlan1)#ip proxy-arp

10.5.3.4 ARP Troubleshooting

If ping from the switch to directly connected network devices fails, the following can be

used to check the possible cause and create a solution.

- Check whether the corresponding ARP has been learned by the switch.
- If ARP has not learned, then enabled ARP debugging information and view sending/receiving condition of ARP packets.

Defective cable is a common cause of ARP problems and may disable ARP learning.

Command

10.5.3.4.1 Commands for Monitor And Debug

10.5.3.4.1.1 debug arp

Command: debug arp

no debug arp

Function: Enables the ARP debugging function; the "**no debug arp**" command disables this debugging function.

Default: ARP debug is disabled by default.

Command mode: Admin Mode

Usage Guide: Display contents for ARP packets received/sent, including type, source and destination address, etc.

Example: Enabling ARP debugging

Switch#debug arp

ip arp debug is on

Switch#%Apr 19 15:59:42 2005 IP ARP: rcvd, type 1, src 192.168.2.100, 000A.EB5B.

780C, dst 192.168.2.1, 0000.0000.0000 flag 0x0.

%Apr 19 15:59:42 2005 IP ARP: sent, type 2, src 192.168.2.1, 0003.0F02.310A, dst

192.168.2.100, 000A.EB5B.780C.

10.5.3.4.1.2 show arp

Command: show arp

[<*ip-addr*>][<*vlan-id*>][<*hw-addr*>][type{static|dynamic}][count] }

Function: Displays the ARP table.

Parameters: <*ip-addr*> is a specified IP address; **<*vlan-id*>** stands for the entry for the identifier of specified VLAN; **<*hw-addr*>** for entry of specified MAC address; "static" for static ARP entry; "dynamic" for dynamic ARP entry; "count" displays number of ARP entries.

Command mode: Admin Mode

Usage Guide: Displays the content of current ARP table such as IP address, MAC address, hardware type, interface name, etc.

Example:

Switch#show arp

Total arp items: 3, matched: 3, Incomplete: 0

Address Hardware Addr Interface Port Flag

50.1.1.6	00-0a-eb-51-51-38	Vlan50	Ethernet1/11	Dynamic
50.1.1.9	00-00-00-00-00-09	Vlan50	Ethernet1/1	Static
150.1.1.2	00-00-58-fc-48-9f	Vlan150	Ethernet1/4	Dynamic

Displayed information	Explanation
Total arp items	Total number of Arp entries.
the matched	ARP entry number matching the filter conditions
InCompleted	ARP entries have ARP request sent without ARP reply
Address	IP address of Arp entries
Hardware Address	MAC address of Arp entries
Interface	Layer 3 interface corresponding to the ARP entry.
Port	Physical (Layer2) interface corresponding to the ARP entry.
Flag	Describes whether ARP entry is dynamic or static.

Chapter 11 DHCP Configuration

11.1 Introduction to DHCP

DHCP [RFC2131] is the acronym for Dynamic Host Configuration Protocol. It is a protocol that assigns IP address dynamically from the address pool as well as other network configuration parameters such as default gateway, DNS server, and default route and host image file position within the network. DHCP is the enhanced version of BootP. It is a mainstream technology that can not only provide boot information for diskless workstations, but can also release the administrators from manual recording of IP allocation and reduce user effort and cost on configuration. Anther benefit of DHCP is it can partially ease the pressure on IP demands, when the user of an IP leaves the network that IP can be assigned to another user.

DHCP is a client-server protocol, the DHCP client requests the network address and configuration parameters from the DHCP server; the server provides the network address and configuration parameters for the clients; if DHCP server and clients are located in different subnets, DHCP relay is required for DHCP packets to be transferred between the DHCP client and DHCP server. The implementation of DHCP is shown below:

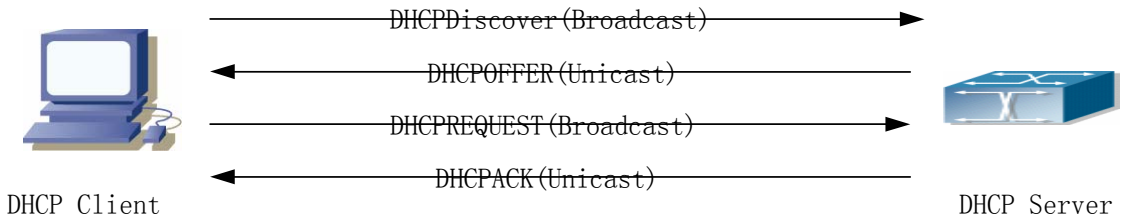


Fig 10-1 DHCP protocol interaction

Explanation:

1. DHCP client broadcasts DHCPDISCOVER packets in the local subnet.
2. On receiving the DHCPDISCOVER packet, DHCP server sends a DHCPOFFER packet along with IP address and other network parameters to the DHCP client.
3. DHCP client broadcast DHCPREQUEST packet with the information for the DHCP server it selected after selecting from the DHCPOFFER packets.
4. The DHCP server selected by the client sends a DHCPACK packet and the client gets an IP address and other network configuration parameters.

The above four steps finish a Dynamic host configuration assignment process. However, if the DHCP server and the DHCP client are not in the same network, the server will not receive the DHCP broadcast packets sent by the client, therefore no DHCP packets will

be sent to the client by the server. In this case, a DHCP relay is required to forward such DHCP packets so that the DHCP packets exchange can be completed between the DHCP client and server.

ES4626/ES4650 switch can act as both a DHCP server and a DHCP relay. DHCP server supports not only dynamic IP address assignment, but also manual IP address binding (i.e. specify a specific IP address to a specified MAC address or specified device ID over a long period. The differences and relations between dynamic IP address allocation and manual IP address binding are:

1) IP address obtained dynamically can be different every time; manually bound IP address will be the same all the time.

2) The lease period of IP address obtained dynamically is the same as the lease period of the address pool, and is limited; the lease of manually bound IP address is theoretically endless.

3) Dynamically allocated address cannot be bound manually.

4) Dynamic DHCP address pool can inherit the network configuration parameters of the dynamic DHCP address pool of the related segment.

11.2 DHCP Server Configuration

11.2.1 DHCP Sever Configuration Task List

1. Enable/Disable DHCP server
2. Configure DHCP Address pool
   (1) Create/Delete DHCP Address pool
   (2) Configure DHCP address pool parameters
   (3) Configure manual DHCP address pool parameters
3. Enable logging for address conflicts

1. Enable/Disable DHCP server

Command	**Explanation**
Global Mode	
service dhcp **no service dhcp**	Enables DHCP server

2. Configure DHCP Address pool

(1) Create/Delete DHCP Address pool

Command	**Explanation**
Global Mode	

ip dhcp pool <*name*> **no ip dhcp pool <*name*>**	Configures DHCP Address pool

(2) Configure DHCP address pool parameters

Command	Explanation
DHCP Address Pool Mode	
network-address <*network-number*> [mask | prefix-length] **no network-address**	Configures the address scope that can be allocated to the address pool
default-router [address1[address2[…address8]]] **no default-router**	Configures default gateway for DHCP clients
dns-server [address1[address2[…address8]]] **no dns-server**	Configures DNS server for DHCP clients
domain-name <*domain*> **no domain-name**	Configures Domain name for DHCP clients; the "**no domain-name**" command deletes the domain name.
netbios-name-server [address1[address2[…address8]]] **no netbios-name-server**	Configures the address for WINS server
netbios-node-type {**b-node|h-node|m-node|p-node|<*type-number*>**} **no netbios-node-type**	Configures node type for DHCP clients
bootfile <*filename*> **no bootfile**	Configures the file to be imported for DHCP clients on boot up
next-server [address1[address2[…address8]]] **no next-server [address1[address2[…address8]]]**	Configures the address of the server hosting file for importing
option <*code*> {ascii <*string*> | hex <*hex*> | ipaddress <*ipaddress*>} **no option <*code*>**	Configures the network parameter specified by the option code
lease (infinite | <0-365> (<0-23> (<0-59>|)|)) ***no lease***	Configures the lease period allocated to addresses in the address pool
Global Mode	

ip dhcp excluded-address <*low-address*> [<*high-address*>] **no ip dhcp excluded-address <*low-address*> [<*high-address*>]**	Excludes the addresses in the address pool that are not for dynamic allocation.

(3) Configure manual DHCP address pool parameters

Command	**Explanation**
DHCP Address Pool Mode	
hardware-address <*hardware-address*> [{Ethernet | IEEE802|<*type-number*>}] **no hardware-address**	Specifies the hardware address when assigning address manually
host <*address*> [<*mask*> | <*prefix-length*>] **no host**	Specifies the IP address to be assigned to the specified client when binding address manually
client-identifier <*unique-identifier*> **no client-identifier**	Specifies the unique ID of the user when binding address manually
client-name <*name*> **no client-name**	Configures a client name when binding address manually

3. Enable logging for address conflicts

Command	**Explanation**
Global Mode	
ip dhcp conflict logging **no ip dhcp conflict logging**	Enables logging for DHCP address to detect address conflicts
Admin Mode	
clear ip dhcp conflict <*address* | *all*>	Deletes a single address conflict record or all conflict records

11.2.2 DHCP Server Configuration Commands

11.2.2.1 bootfile

Command: bootfile <*filename*>

no bootfile

Function: Sets the file name for DHCP client to import on boot up; the "**no bootfile** " command deletes this setting.

Parameters: <*filename*> is the name of the file to be imported, up to 255 characters are allowed.

Command Mode: DHCP Address Pool Mode

Usage Guide: Specify the name of the file to be imported for the client. This is usually used for diskless workstations that need to download a configuration file from the server on boot up. This command is together with the “next sever”.

Example: The path and filename for the file to be imported is “c:\temp\nos.img”

Switch(dhcp-1-config)#bootfile c:\temp\nos.img

11.2.2.2 client-identifier

Command: client-identifier <*unique-identifier*>

no client-identifier

Function: Specifies the unique ID of the user when binding an address manually; the “**no client-identifier**” command deletes the identifier.

Parameters: <*unique-identifier*> is the user identifier, in dotted Hex format.

Command Mode: DHCP Address Pool Mode

Usage Guide: This command is used with “host” when binding an address manually. If the requesting client identifier matches the specified identifier, DHCP server assigns the IP address defined in “host” command to the client.

Example: Specifying the IP address 10.1.128.160 to be bound to user with the unique id of 00-10-5a-60-af-12 in manual address binding.

Switch(dhcp-1-config)#client-identifier 00-10-5a-60-af-12

Switch(dhcp-1-config)#host 10.1.128.160 24

11.2.2.3 client-name

Command: client-name <*name*>

no client-name

Function: Specifies the username when binding addresses manually; the “**no client-name**” command deletes the username.

Parameters: <*name*> is the name of the user, up to 255 characters are allowed.

Command Mode: DHCP Address Pool Mode

Usage Guide: Configure a username for the manual binding device, domain should not be included when configuring username.

Example: Giving the user, with unique id of 00-10-5a-60-af-12, a username of “network”.

Switch(dhcp-1-config)#client-name network

11.2.2.4 default-router

Command: default-router <*address1*>[<*address2*>[…<*address8*>]]

no default-router

Function: Configures default gateway(s) for DHCP clients; the “**no default-router**” command deletes the default gateway.

Parameters: ***address1…address8*** are IP addresses, in decimal format.

Default: No default gateway is configured for DHCP clients by default.

Command Mode: DHCP Address Pool Mode

Usage Guide: The IP address of default gateway(s) should be in the same subnet as the DHCP client IP, the switch supports up to 8 gateway addresses. The gateway address assigned first has the highest priority, and therefore address1 has the highest priority, and address2 has the second, and so on.

Example: Configuring the default gateway for DHCP clients to be 10.1.128.2 and 10.1.128.100.

Switch(dhcp-1-config)#default-router 10.1.128.2 10.1.128.100

11.2.2.5 dns-server

Command: dns-server <*address1*>[<*address2*>[…<*address8*>]]

no dns-server

Function: Configure DNS servers for DHCP clients; the "**no dns-server**" command deletes the default gateway.

Parameters: ***address1…address8*** are IP addresses, in decimal format.

Default: No DNS server is configured for DHCP clients by default.

Command Mode: DHCP Address Pool Mode

Usage Guide: Up to 8 DNS server addresses can be configured. The DNS server address assigned first has the highest priority, Therefore address 1 has the highest priority, and address 2 has the second, and so on.

Example: Set 10.1.128.3 as the DNS server address for DHCP clients.

Switch(dhcp-1-config)#dns-server 10.1.128.3

11.2.2.6 domain-name

Command: domain-name <*domain*>

no domain-name

Function: Configures the Domain name for DHCP clients; the "**no domain-name**" command deletes the domain name.

Parameters: **<*domain*>** is the domain name, up to 255 characters are allowed.

Command Mode: DHCP Address Pool Mode

Usage Guide: Specifies a domain name for the client.

Example: Specifying "edgecore.com" as the DHCP clients' domain name.

Switch(dhcp-1-config)#domain-name edgecore.com

11.2.2.7 hardware-address

Command: hardware-address <*hardware-address*> [{Ethernet |

IEEE802|<*type-number*>}]

no hardware-address

Function: Specifies the hardware address of the user when binding address manually; the "**no hardware-address**" command deletes the setting.

Parameters: <*hardware-address*> is the hardware address in Hex; **Ethernet | IEEE802** is the Ethernet protocol type, **<*type-number*>** should be the RFC number defined for protocol types, from 1 to 255, e.g., 0 for Ethernet and 6 for IEEE 802.

Default: The default protocol type is Ethernet,

Command Mode: DHCP Address Pool Mode

Usage Guide: This command is used with the "host" when binding address manually. If the requesting client hardware address matches the specified hardware address, the DHCP server assigns the IP address defined in "host" command to the client.

Example: Specify IP address 10.1.128.160 to be bound to the user with hardware address 00-00-e2-3a-26-04 in manual address binding.

Switch(dhcp-1-config)#hardware-address 00-00-e2-3a-26-04

Switch(dhcp-1-config)#host 10.1.128.160 24

11.2.2.8 host

Command:host <*address*> [<*mask*> | <*prefix-length*>]

no host

Function: Specifies the IP address to be assigned to the user when binding addresses manually; the "**no host**" command deletes the IP address.

Parameters: <*address*> is the IP address in decimal format; **<*mask*>** is the subnet mask in decimal format; **<*prefix-length*>** means mask is indicated by prefix. For example, mask 255.255.255.0 in prefix is "24", and mask 255.255.255.252 in prefix is "30".

Command Mode: DHCP Address Pool Mode

Usage Guide: If no mask or prefix is configured when configuring the IP address, and no information in the IP address pool indicates anything about the mask, the system will assign a mask automatically according to the IP address class.

This command is used with "hardware address" command or "client identifier" command when binding addresses manually. If the identifier or hardware address of the requesting client matches the specified identifier or hardware address, the DHCP server assigns the IP address defined in "host" command to the client.

Example: Specifying IP address 10.1.128.160 to be bound to user with hardware address 00-10-5a-60-af-12 in manual address binding.

Switch(dhcp-1-config)#hardware-address 00-10-5a-60-af-12

Switch(dhcp-1-config)#host 10.1.128.160 24

11.2.2.9 ip dhcp conflict logging

Command: ip dhcp conflict logging

no ip dhcp conflict logging

Function: Enables logging for address conflicts detected by the DHCP server; the "**no ip dhcp conflict logging"** command disables the logging.

Default: Logging for address conflict is enabled by default.

Command mode: Global Mode

Usage Guide: When logging is enabled, once the address conflict is detected by the DHCP server, the conflicting address will be logged. Addresses present in the log for conflicts will not be assigned dynamically by the DHCP server until the conflicting records are deleted.

Example: Disable logging for DHCP server.

Switch(Config)#no ip dhcp conflict logging

11.2.2.10 ip dhcp excluded-address

Command: ip dhcp excluded-address <low-address>[<*high-address*>]

no ip dhcp excluded-address <low-address> [<high-address>]

Function: Specifies addresses excluding from dynamic assignment; the "**no ip dhcp excluded-address <*low-address*> [<*high-address*>]**" command cancels the setting.

Parameters: <*low-address*> is the starting IP address, **[<*high-address*>]** is the ending IP address.

Default: Only individual address is excluded by default.

Command mode: Global Mode

Usage Guide: This command can be used to exclude one or several consecutive addresses in the pool from being assigned dynamically so that those addresses can be used by the administrator for other purposes.

Example: Reserving addresses from 10.1.128.1 to 10.1.128.10 from dynamic assignment.

Switch(Config)#ip dhcp excluded-address 10.1.128.1 10.1.128.10

11.2.2.11 ip dhcp pool

Command: ip dhcp pool <*name*>

no ip dhcp pool <*name*>

Function: Configures a DHCP address pool and enter the pool mode; the "**no ip dhcp pool <*name*>"** command deletes the specified address pool.

Parameters: <*name*> is the address pool name, up to 255 characters are allowed.

Command mode: Global Mode

Usage Guide: This command is used to configure a DHCP address pool under Global Mode and enter the DHCP address configuration mode.

Example: Defining an address pool named “1”.

Switch(Config)#ip dhcp pool 1

Switch(dhcp-1-config)#

11.2.2.12 loghost dhcp

Command: loghost dhcp <*ip-address*> <*port*>

no loghost dhcp

Function: Enables DHCP logging and specify the IP address and port number for the DHCP logging host; the “**no loghost dhcp”** command disables the DHCP logging function.

Parameters: <*ip-address*> is the DHCP log host IP address in decimal format. **<*port*>** is the port number, valid values range from 0 -65535.

Default: DHCP logging is disabled by default.

Command mode: Global Mode

Usage Guide: The user can check information about DHCP address assignment from the log host when this command is configured. Any host running logtest.exe provided by Edge-Core can be a DHCP log host.

Example: Enabling the DHCP logging, the log host is 192.168.1.101, port 45.

Switch(Config)#loghost dhcp 192.168.1.101 45

11.2.2.13 lease

Command: lease (infinite | <0-365> (<0-23> (<0-59>|)|))

no lease

Function: Sets the lease time for addresses in the address pool; the “**no lease**” command restores the default setting.

Parameters: <*days*> is number of days from 0 to 365; **<*hours*** is number of hours from 0 to 23; **<*minutes*>** is number of minutes from 0 to 59; **infinite** means perpetual use.

Default: The default lease duration is 1 day.

Command Mode: DHCP Address Pool Mode

Usage Guide: DHCP is the protocol to assign network addresses dynamically instead of permanently, hence the introduction of ease duration. Lease settings should be decided based on network conditions: too long lease duration offsets the flexibility of DHCP, while too short duration results in increased network traffic and overhead. The default lease duration of ES4626/ES4650 switch is 1 day.

Example: Setting the lease of DHCP pool “1” to 3 days 12 hours and 30 minutes.

Switch(dhcp-1-config)#lease 3 12 30

11.2.2.14 netbios-name-server

Command: netbios-name-server <*address1*>[<*address2*>[…<*address8*>]]

no netbios-name-server

Function: Configures WINS servers' address; the "**no netbios-name-server**" command deletes the WINS server.

Parameters: ***address1…address8*** are IP addresses, in decimal format.

Default: No WINS server is configured by default.

Command Mode: DHCP Address Pool Mode

Usage Guide: This command is used to specify WINS server for the client, up to 8 WINS server addresses can be configured. The WINS server address assigned first has the highest priority. Therefore, address 1 has the highest priority, and address 2 the second, and so on.

11.2.2.15 netbios-node-type

Command: netbios-node-type {**b-node|h-node|m-node|p-node|<*type-number*>**}

no netbios-node-type

Function: Sets the node type for the specified port; the "**no netbios-node-type**" command cancels the setting.

Parameters: **b-node** stands for broadcasting node, **h-node** for hybrid node that broadcasts after point-to-point communication; **m-node** for hybrid node to communicate in point-to-point after broadcast; **p-node** for point-to-point node; ***<type-number>*** is the node type in Hex from 0 to FF.

Default: No client node type is specified by default.

Command Mode: DHCP Address Pool Mode

Usage Guide: If client node type is to be specified, it is recommended to set the client node type to **h-node** that broadcasts after point-to-point communication.

Example: Setting the node type for client of pool 1 to broadcasting node.

Switch(dhcp-1-config)#netbios-node-type b-node

11.2.2.16 network-address

Command: network-address <*network-number*> [<*mask*> | <*prefix-length*>]

no network-address

Function: Sets the scope for assignment for addresses in the pool; the "**no network-address**" command cancels the setting.

Parameters: ***<network-number>*** is the network number; ***<mask>*** is the subnet mask in the decimal format; ***<prefix-length>*** stands for mask in prefix form. For example, mask 255.255.255.0 in prefix is "24", and mask 255.255.255.252 in prefix is "30". Note: When using DHCP server, the pool mask should be longer or equal to that of layer 3 interface IP address in the corresponding segment.

Default: If no mask is specified, default mask will be assigned according to the address class.

Command Mode: DHCP Address Pool Mode

Usage Guide: This command sets the scope of addresses that can be used for dynamic assignment by the DHCP server; one address pool can only have one corresponding segment. This command is exclusive with the manual address binding command “hardware address” and “host”.

Example: Configuring the assignable address in pool 1 to be 10.1.128.0/24.

Switch(dhcp-1-config)#network-address 10.1.128.0 24

11.2.2.17 next-server

Command: next-server <*address1*>[<*address2*>[…<*address8*>]]

no next-server

Function: Sets the server address for storing the client import file; the “**no next-server**” command cancels the setting.

Parameters: ***address1…address8*** are IP addresses, in the decimal format.

Command Mode: DHCP Address Pool Mode

Usage Guide: This command configures the address for the server hosting client import file. This is usually used for diskless workstations that need to download configuration files from the server on boot up. This command is used together with “bootfile”.

Example: Setting the hosting server address as 10.1.128.4.

Switch(dhcp-1-config)#next-server 10.1.128.4

11.2.2.18 option

Command: option <*code*> {ascii <*string*> | hex <*hex*> | ipaddress <*ipaddress*>}

no option <*code*>

Function: Sets the network parameter specified by the option code; the “**no option <*code*>**“ command cancels the setting for option.

Parameters: <*code*> is the code for network parameters; **<*string*>** is the ASCII string up to 255 characters; **<*hex*>** is a value in Hex that is no greater than 510 and must be of even length; **<*ipaddress*>** is the IP address in decimal format, up to 63 IP addresses can be configured.

Command Mode: DHCP Address Pool Mode

Usage Guide: The switch provides common commands for network parameter configuration as well as various commands useful in network configuration to meet different user needs. The definition of option code is described in detail in RFC2123.

Example: Setting the WWW server address as 10.1.128.240.

Switch(dhcp-1-config)#option 72 ip 10.1.128.240

11.2.2.19 service dhcp

Command: service dhcp

no service dhcp

Function: Enables DHCP server; the "**no service dhcp**" command disables the DHCP service.

Default: DHCP service is disabled by default.

Command mode: Global Mode

Usage Guide: Both DHCP server and DHCP relay are included in the DHCP service. When DHCP services are enabled, both DHCP server and DHCP relay are enabled. ES4626/ES4650 switch can only assign IP address for the DHCP clients and enable DHCP relay when DHCP server function is enabled.

Example: Enabling DHCP server.

Switch(Config)#service dhcp

11.3 DHCP Relay Configuration

When the DHCP client and server are in different segments, DHCP relay is required to transfer DHCP packets. Adding a DHCP relay makes it unnecessary to configure a DHCP server for each segment, one DHCP server can provide the network configuration parameter for clients from multiple segments, which is not only cost-effective but also management-effective.

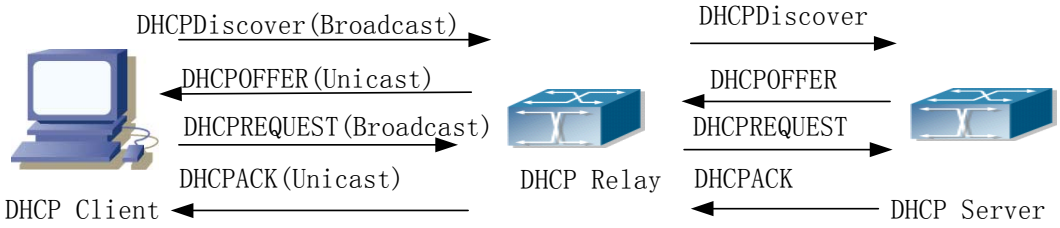


Fig 10-2 DHCP relay

As shown in the above figure, the DHCP client and the DHCP server are in different networks, the DHCP client performs the four DHCP steps as usual yet DHCP relay is added to the process.

1. The client broadcasts a DHCPDISCOVER packet, and DHCP relay inserts its own IP address to the relay agent field in the DHCPDISCOVER packet on receiving the packet, and forwards the packet to the specified DHCP server (for DHCP frame format, please refer to RFC2131).
2. On the receiving the DHCPDISCOVER packets forwarded by DHCP relay, the DHCP server sends the DHCPOFFER packet via DHCP relay to the DHCP client.
3. DHCP client chooses a DHCP server and broadcasts a DHCPREPLY packet, DHCP relay forwards the packet to the DHCP server after processing.

4. On receiving DHCPREPLY, the DHCP server responds with a DHCPACK packet via DHCP relay to the DHCP client.

DHCP relay can not only send DHCP broadcasting packets to the specified DHCP servers, but can also send other specified UDP broadcast packet to specified servers.

11.3.1 DHCP Relay Configuration Task List

1. Enable DHCP relay.
2. Configure DHCP relay to forward DHCP broadcast packet.
3. Configure DHCP relay to forward other UDP broadcast packet.
4. Disable DHCP relay from forwarding DHCP broadcast packet.

1. Enable DHCP relay.

DHCP server and DHCP relay is enabled as the DHCP service is enabled..

2. Configure DHCP relay to forward DHCP broadcast packet.

Command	Explanation
Global Mode	
ip forward-protocol udp <port> **no ip forward-protocol udp <port>**	The UDP port 67 is used for DHCP broadcast packet forwarding.
Interface Mode	
ip helper-address <ipaddress> **no ip helper-address <ipaddress>**	Set the destination IP address for DHCP relay forwarding; the “no ip helper-address <ipaddress>“ command cancels the setting.

3. Configure DHCP relay to forward other UDP broadcast packet.

Command	Explanation
Global Mode	
ip forward-protocol udp <port> **no ip forward-protocol udp <port>**	Specify the DHCP relay forwarding protocol by setting UDP port; the “no ip forward-protocol udp <port>“ command cancels the setting.
ip helper-address <ipaddress> **no ip helper-address <ipaddress>**	Set the destination IP address for DHCP relay forwarding; the “no ip helper-address <ipaddress>“ command cancels the setting.

4. Disable DHCP relay from forwarding DHCP broadcast packet.

Command	Explanation
Global Mode	

ip dhcp relay information policy drop **no ip dhcp relay information policy drop**	When layer 3 switches are used as DHCP relays, this command sets the relay forwarding policy to drop DHCP packets; the "no ip dhcp relay information policy drop" command allows DHCP packets forwarding.

11.3.2 DHCP Relay Configuration Commands

11.3.2.1 clear ip dhcp binding

Command: clear ip dhcp binding {<*address*> | all }

Function: Deletes the specified IP address-hardware address binding record or all IP address-hardware address binding records.

Parameters: <*address*> is the IP address that has a binding record in decimal format. **all** refers to all IP addresses that have a binding record.

Command mode: Admin Mode

Usage Guide: "**show ip dhcp binding**" command can be used to view binding information for IP addresses and corresponding DHCP client hardware addresses. If the DHCP server is informed that a DHCP client is not using the assigned IP address for some reason before the lease period expires, the DHCP server would not remove the binding information automatically. The system administrator can use this command to delete that IP address-client hardware address binding manually, if "all" is specified, then all auto binding records will be deleted, thus all addresses in the DHCP address pool will be reallocated.

Example: Removing all IP-hardware address binding records.

Switch#clear ip dhcp binding all

11.3.2.2 clear ip dhcp conflict

Command: clear ip dhcp conflict {<*address*> | all }

Function: Deletes an address present in the address conflict log.

Parameters: <*address*> is the IP address that has a conflict record; **all** stands for all addresses that have conflict records.

Command mode: Admin Mode

Usage Guide: "**show ip dhcp conflict**" command can be used to check which IP addresses are conflicting for use. The **"Clear ip dhcp conflict"** command can be used to delete the conflict record for an address. If "all" is specified, then all conflict records in the log will be removed. When records are removed from the log, the addresses are available for allocation by the DHCP server.

Example: The network administrator finds 10.1.128.160 that has a conflict record in the log and is no longer used by anyone, so he deletes the record from the address conflict log.

Switch#clear ip dhcp conflict 10.1.128.160

11.3.2.3 clear ip dhcp server statistics

Command: clear ip dhcp server statistics

Function: Deletes the statistics for DHCP server, clears the DHCP server count.

Command mode: Admin Mode

Usage Guide: DHCP count statistics can be viewed with "**show ip dhcp server statistics**" command, all information is accumulated. You can use the "**clear ip dhcp server statistics**" command to clear the count for easier statistics checking.

Example: clearing the count for DHCP server.

Switch#clear ip dhcp server statistics

11.3.2.4 debug ip dhcp server

Command: debug ip dhcp server { events|linkage|packets }

no debug ip dhcp server { events|linkage|packets }

Function: Enables DHCP server debug information: the "**no debug ip dhcp server { events|linkage|packets }"** command disables the debug information for DHCP server**.**

Default: Debug information is disabled by default.

Command mode: Admin Mode

11.3.2.5 ip forward-protocol udp

Command: ip forward-protocol udp <port>

no ip forward-protocol udp <port>

Function: Sets DHCP relay to forward UPD broadcast packets on the port; the "**no ip forward-protocol udp <port>**" command cancels the service.

Default: DHCP relay forwards DHCP broadcast packet to UDP port 67 by default.

Command mode: Global Mode

Usage Guide: The forwarding destination address is set in the "**ip helper-address**" command and described later.

Example: Setting TFTP packets to be forwarded to 192.168.1.5.

Switch(Config)#ip forward-protocol udp 69

Switch(Config)#interface vlan 1

Switch(Config-If-Vlan1)#ip helper-address 192.168.1.5

11.3.2.6 ip helper-address

Command: ip helper-address <*ip-address*>

no ip helper-address <*ip-address*>

Function: Specifies the destination address for the DHCP relay to forward UDP packets. The "**no ip helper-address <*ip-address*>**" command cancels the setting.

Default: Address for forwarding DHCP broadcast packet is set on DHCP relay by default.

Command mode: Interface Mode

Usage Guide: The DHCP relay forwarding server address corresponds to the port forwarding UDP, i.e. DHCP relay forwards corresponding UDP packets only to the corresponding server instead of all UDP packets to all servers. The default setting of DHCP relay is to forward DHCP packets on UDP port 67 to the DHCP server. When this command is run after "**ip forward-protocol udp <*port*>**" command, the forwarding address configured by this command receives the UDP packets from **<*port*>** instead of default DHCP packets. If a different set of UDP forwarding protocol and receiving server address is to be set, the combination of "**ip forward-protocol udp <*port*>**" command and this command should be used for configuration.

11.3.2.7 ip dhcp relay information policy drop

Command: ip dhcp relay information policy drop

no ip dhcp relay information policy drop

Function: When layer 3 switches are used as DHCP relays, this command sets the relay forwarding policy to drop DHCP packets; the "**no ip dhcp relay information policy drop**" command allows DHCP packets forwarding.

Default: DHCP relay forwards DHCP broadcast packet by default.

Command mode: Interface Mode

Usage Guide: When the DHCP relay should not forward DHCP packets for some reason, this command can be used to disable DHCP packet forwarding on DHCP relay.

Example: Disabling DHCP broadcast packet forwarding on the layer 3 switch.

```
Switch(Config)#interface vlan 1
Switch(Config-If-Vlan1)# ip dhcp relay information policy drop
```

11.4 DHCP Configuration Example

Scenario 1:

To save configuration efforts of network administrators and users, a company is using ES4626/ES4650 switch as a DHCP server. The Admin VLAN IP address is 10.16.1.2/16. The local area network for the company is divided into network A and B according to the office locations. The network configurations for location A and B are shown below.

PoolA(network 10.16.1.0)		PoolB(network 10.16.2.0)	
Device	IP address	Device	IP address
Default gateway	10.16.1.200 10.16.1.201	Default gateway	10.16.1.200 10.16.1.201
DNS server	10.16.1.202	DNS server	10.16.1.202
WINS server	10.16.1.209	WINS server	10.16.1.209
WINS node type	H-node	WINS node type	H-node
Lease	3 days	Lease	3 days

In location A, a machine with MAC address 00-03-22-23-dc-ab is assigned with a fixed IP address of 10.16.1.210 and named as “management”. (The interfaces in the following configurations are wrong; "no switch" command is not available.)

Switch(Config)#service dhcp
Switch(Config)#interface vlan 1
Switch(Config-Vlan-1)#ip address 10.16.1.2 255.255.0.0
Switch(Config-Vlan-1)#exit
Switch(Config)#ip dhcp pool A
Switch(dhcp-A-config)#network 10.16.1.0 24
Switch(dhcp-A-config)#lease 3
Switch(dhcp-A-config)#default-route 10.16.1.200 10.16.1.201
Switch(dhcp-A-config)#dns-server 10.16.1.202
Switch(dhcp-A-config)#netbios-name-server 10.16.1.209
Switch(dhcp-A-config)#netbios-node-type H-node
Switch(dhcp-A-config)#exit
Switch(Config)#ip dhcp excluded-address 10.16.1.200 10.16.1.210
Switch(Config)#ip dhcp pool B
Switch(dhcp-B-config)#network 10.16.2.0 24
Switch(dhcp-B-config)#lease 1
Switch(dhcp-B-config)#default-route 10.16.2.200 10.16.2.201
Switch(dhcp-B-config)#dns-server 10.16.2.202
Switch(dhcp-B-config)#option 72 ip 10.16.2.209
Switch(dhcp-config)#exit
Switch(Config)#ip dhcp excluded-address 10.16.2.200 10.16.2.210
Switch(Config)#ip dhcp pool A1
Switch(dhcp-A1-config)#host 10.16.1.210
Switch(dhcp-A1-config)#hardware-address 00-03-22-23-dc-ab
Switch(dhcp-A1-config)# client-name management
Switch(dhcp-A1-config)#exit

Scenario 2:

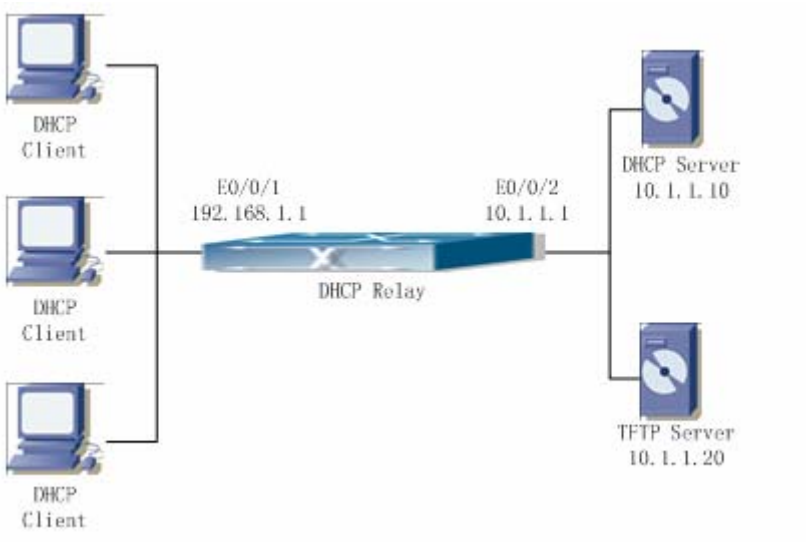


Fig 10-3 DHCP Relay Configuration

As shown in the above figure, route switch is configured as a DHCP relay. The DHCP server address is 10.1.1.10, TFTP server address is 10.1.1.20, the configuration steps is as follows:

Switch (Config)#service dhcp
Switch (Config)#interface vlan 1
Switch (Config-if-Vlan1)#ip address 192.168.1.1 255.255.255.0
Switch (Config-if-Vlan1)#exit
Switch (Config)#vlan 2
Switch (Config-Vlan-2)#exit
Switch (Config)#interface Ethernet 1/2
Switch (Config-Erthernet1/2)#switchport access vlan 2
Switch (Config-Erthernet1/2)#exit
Switch (Config)#interface vlan 2
Switch (Config-if-Vlan2)#ip address 10.1.1.1 255.255.255.0
Switch (Config-if-Vlan2)#exit
Switch (Config)#ip forward-protocol udp 67
Switch (Config)#interface vlan 1
Switch (Config-if-Vlan1)#ip help-address 10.1.1.10
Switch (Config-if-Vlan1)#exit
Switch (Config)#ip forward-protocol udp 69
Switch (Config)#interface vlan 1
Switch (Config-if-Vlan1)#ip help-address 10.1.1.20
Switch (Config-if-Vlan1)#exit

Note: DHCP server address and TFTP server address must be configured separately since their receiving UDP protocols are different. It is recommended to use the combination of command "**ip forward-protocol udp <*port*>**" and "**ip helper-address**

<ipaddress>". "**ip help-address**" can only be configured for ports on layer 3 and cannot be configured on layer 2 ports directly.

Usage Guide:

When a DHCP/BootP client is connected to a VLAN1 port of the switch, the client can only get its address from 10.16.1.0/24 instead of 10.16.2.0/24. This is because the broadcast packet from the client will be requesting the IP address in the same segment of the VLAN interface after VLAN interface forwarding, and the VLAN interface IP address is 10.16.1.2/24, therefore the IP address assigned to the client will belong to 10.16.1.0/24.

If the DHCP/BootP client wants to have an address in 10.16.2.0/24, the gateway forwarding broadcast packets of the client must belong to 10.16.2.0/24. The connectivity between the client gateway and the switch must be ensured for the client to get an IP address from the 10.16.2.0/24 address pool.

11.5 DHCP Troubleshooting

If the DHCP clients cannot obtain IP addresses and other network parameters, the following procedures can be followed when DHCP client hardware and cables have been verified ok.

- ☞ Verify the DHCP server is running, start the related DHCP server if not running.
- ☞ If the DHCP clients and servers are not in the same physical network, verify the router responsible for DHCP packet forwarding has DHCP relay function. If DHCP relay is not available for the intermediate router, it is recommended to replace the router or upgrade its software to one that has a DHCP relay function.
- ☞ In such case, DHCP server should be examined for an address pool that is in the same segment of the switch VLAN, such a pool should be added if not present, and (This does not indicate ES4626/ES4650 switch cannot assign IP address for different segments, see solution 2 for details.)

In DHCP service, pools for dynamic IP allocation and manual binding are conflicting, i.e., if command "**network-address**" and "**host**" are run for a pool, only one of them will take effect; furthermore, in manual binding, only one IP-MAC binding can be configured in one pool. If multiple bindings are required, multiple manual pools can be created and IP-MAC bindings set for each pool. New configuration in the same pool overwrites the previous configuration.

11.5.1 Commands for Monitor and Debug

11.5.1.1 show ip dhcp binding

Command: show ip dhcp binding [[<*ip-addr*>] + [type {all | manual | dynamic}] [count]]

Function: Displays IP-MAC binding information.

Parameters: <*ip-addr*> is a specified IP address in decimal format; “all” stands for all binding types (manual binding and dynamic assignment); “manual” for manual binding; “dynamic” for dynamic assignment; “count” displays statistics for DHCP address binding entries.

Command mode: Admin Mode

Example:

Switch# show ip dhcp binding

IP address	Hardware address	Lease expiration	Type
10.1.1.233	00-00-E2-3A-26-04	Infinite	Manual
10.1.1.254	00-00-E2-3A-5C-D3	60	Automatic

Displayed information	Explanation
IP address	IP address assigned to a DHCP client
Hardware address	MAC address of a DHCP client
Lease expiration	Valid time for the DHCP client to hold the IP address
Type	Type of assignment: manual binding or dynamic assignment.

11.5.1.2 show ip dhcp conflict

Command: show ip dhcp conflict

Function: Displays log information for addresses that have a conflict record.

Command mode: Admin Mode

Example:

Switch# show ip dhcp conflict

IP Address	Detection method	Detection Time
10.1.1.1	Ping	FRI JAN 02 00:07:01 2002

Displayed information	Explanation
IP Address	Conflicting IP address
Detection method	Method in which the conflict is detected.
Detection Time	Time when the conflict is detected.

11.5.1.3 show ip dhcp server statistics

Command: show ip dhcp server statistics

Function: Displays statistics of all DHCP packets for a DHCP server.

Command mode: Admin Mode

Example:

```
Switch# show ip dhcp server statistics
Address pools                   3
Database agents                 0
Automatic bindings              2
Manual bindings                 0
Conflict bindings               0
Expired bindings                0
Malformed message               0
Message                         Received
BOOTREQUEST                     3814
DHCPDISCOVER                    1899
DHCPREQUEST                     6
DHCPDECLINE                     0
DHCPRELEASE                     1
DHCPINFORM                      1
Message                         Send
BOOTREPLY                       1911
DHCPOFFER                       6
DHCPACK                         6
DHCPNAK                         0
DHCPRELAY                       1907
DHCPFORWARD                     0
Switch#
```

Displayed information	Explanation
Address pools	Number of DHCP address pools configured.
Database agents	Number of database agents.
Automatic bindings	Number of addresses assigned automatically
Manual bindings	Number of addresses bound manually
Conflict bindings	Number of conflicting addresses
Expired bindings	Number of addresses whose leases are expired
Malformed message	Number of error messages.
Message Received	Statistics for DHCP packets received
BOOTREQUEST	Total packets received

DHCPDISCOVER	Number of DHCPDISCOVER packets
DHCPREQUEST	Number of DHCPREQUEST packets
DHCPDECLINE	Number of DHCPDECLINE packets
DHCPRELEASE	Number of DHCPRELEASE packets
DHCPINFORM	Number of DHCPINFORM packets
Message Send	Statistics for DHCP packets sent
BOOTREPLY	Total packets sent
DHCPOFFER	Number of DHCPOFFER packets
DHCPACK	Number of DHCPACK packets
DHCPNAK	Number of DHCPNAK packets
DHCPRELAY	Number of DHCPRELAY packets
DHCPFORWARD	Number of DHCPFORWARD packets

11.6 Web Management

Click DHCP configuration. Users can configure DHCP on the switch.

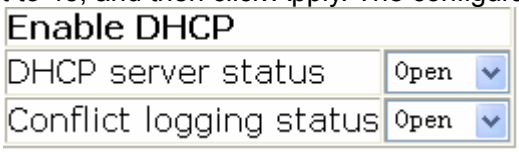
11.6.1 DHCP server configuration

Click DHCP configuration, DHCP server configuration, The DHCP server configuration page is shown.

11.6.1.1 Enable DHCP

Click DHCP configuration, DHCP server configuration, Enable DHCP. Users can enable or disable DHCP server, and configure logging server:

DHCP server status -Enable or disable DHCP server. 0.0.1; set Logging server port to 45, and then click Apply. The configuration is applied on the switch.



11.6.1.2 Address pool configuration

Click DHCP configuration, DHCP server configuration, Address pool configuration. Users can configure DHCP address pool:

DHCP pool name (1-32 character) - Configure DHCP pool name. ; for Address range for allocating, set IP address to 10.1.128.0; set Network mask to 255.255.255.0; set DHCP client node type to broadcast node; set Address lease timeout

to 3 day 12 hour 30 minute, and then click Apply. The configuration is applied on the switch.

DHCP Address pool configuration	
DHCP pool name	
DHCP pool domain name(1-255 character)	www.edge-core.com
Address range for allocating	IP address: 10.1.128.0 Network mask: 255.255.255.0
DHCP client node type	Broadcast node
Address lease timeout	Day: 3 Hour: 12 Minute: 30

11.6.1.3 Client's default gateway configuration

Click DHCP configuration, DHCP server configuration, Client's default gateway configuration. Users can configure DHCP client's default gateway. The default gateway IP address should be in the same subnet as DHCP clients. Users can configure maximum eight gateway addresses. Gateway 1 has the highest priority and Gateway 8 has the lowest priority.

For example: Select DHCP pool name to 1; set Gateway 1 to 10.1.128.3; Gateway 2 to 10.1.128.100, and then click Apply. The configuration is applied on the switch.

Client's default gateway configuration	
DHCP pool name	1
Gateway 1	10.1.128.3
Gateway 2(optional)	10.1.128.100
Gateway 3(optional)	
Gateway 4(optional)	
Gateway 5(optional)	
Gateway 6(optional)	
Gateway 7(optional)	
Gateway 8(optional)	

11.6.1.4 Client DNS server configuration

Click DHCP configuration, DHCP server configuration, Client DNS server configuration. Users can configure DHCP client DNS server. Users can configure maximum eight DNS servers. DNS server 1 has the highest priority and DNS server 8 has the lowest priority.

For example: Select DHCP pool name to 1; set DNS server 1 to 10.1.128.3, and then click Apply. The configuration is applied on the switch.

Client DNS server configuration	
DHCP pool name	1
DNS server 1	10.1.128.3
DNS server 2(optional)	
DNS server 3(optional)	
DNS server 4(optional)	
DNS server 5(optional)	
DNS server 6(optional)	
DNS server 7(optional)	
DNS server 8(optional)	

11.6.1.5 Client WINS server configuration

Click DHCP configuration, DHCP server configuration, Client WINS server configuration. Users can configure Wins server. Users can configure maximum eight WINS server. WINS server 1 has the highest priority and WINS server 8 has the lowest priority.

For example: Select DHCP pool name to 1; set WINS server 1 to 10.1.128.30, and then click Apply. The configuration is applied on the switch.

Client WINS server configuration	
DHCP pool name	1
WINS server 1	10.128.1.30
WINS server 2(optional)	
WINS server 3(optional)	
WINS server 4(optional)	
WINS server 5(optional)	
WINS server 6(optional)	
WINS server 7(optional)	
WINS server 8(optional)	

11.6.1.6 DHCP file server address configuration

Click DHCP configuration, DHCP server configuration, DHCP file server address configuration. Users can configure DHCP client bootfile name and file server:

DHCP pool name -Select DHCP pool name

DHCP client bootfile name (1-128 character) -Specify bootfile name. image; set File server1 to 10.1.128.4, and then click Apply. The configuration is applied on the switch.

DHCP file server address configuration	
DHCP pool name	1
DHCP client bootfile name(1-128 character)	C:\temp\nos.img
File server 1	10.1.128.4
File server 2(optional)	
File server 3(optional)	
File server 4(optional)	
File server 5(optional)	
File server 6(optional)	
File server 7(optional)	
File server 8(optional)	

11.6.1.7 DHCP network parameter configuration

Click DHCP configuration, DHCP server configuration, DHCP network parameter configuration. Users can specify DHCP network parameters. 1.128.240; set Operation type to Set network parameter, and then click Apply. The configuration is applied on the switch.

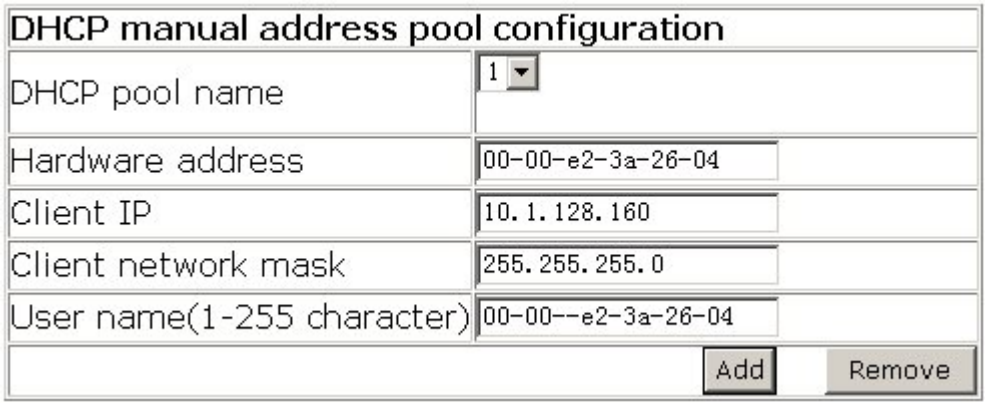
DHCP network parameter configuration	
DHCP pool name	1
Code(0-254)	72
Network parameter value type	ip address
Network parameter value	10.1.128.240
Operation type	Set network parameter

11.6.1.8 Manual address pool configuration

Click DHCP configuration, DHCP server configuration, Manual address pool configuration.Users can configure DHCP manual address pool:

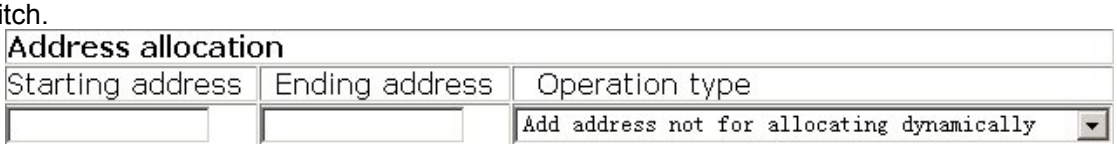
DHCP pool name -Select DHCP pool name

Hardware address -Specify hardware address.10.1.128.160; set Client network mask to 255.255.255.0; set User name to 00-00-e2-3a-26-04, and then Apply. The configuration is applied on the switch.



11.6.1.9 Excluded address

Click DHCP configuration, DHCP server configuration, Manual address pool configuration.Users can configure the exclusive addresses on the DCHP pool. 12.1.128.1; set Ending address to 10.1.128.10; set Operation type to Add address not for allocating dynamically, and then click Apply. The configuration is applied on the switch.



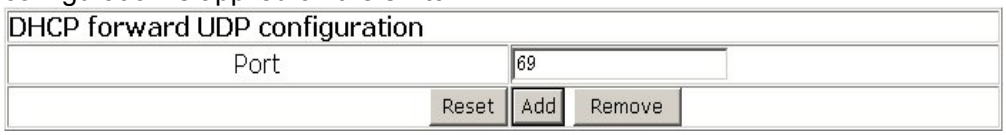
11.6.1.10 DHCP packet statistics

Click DHCP configuration, DHCP server configuration, DHCP packet statistics. Users can display DHCP packet statistics. Users can configure DHCP relay.

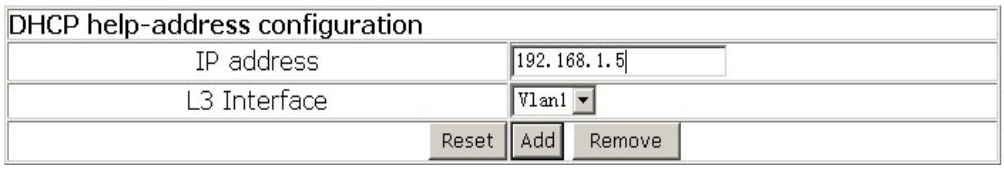
11.6.1.11 DHCP relay configuration

Click DHCP configuration, DHCP relay configuration, DHCP relay configuration. Users can configure DHCP relay:

DHCP forward UDP configuration: Configure DHCP port to forward UDP packets. The configuration is applied on the switch.

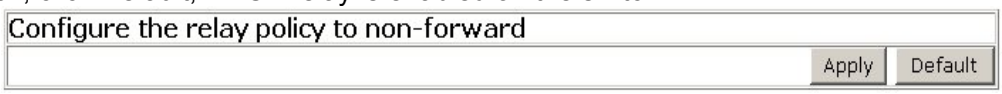


DHCP help-address configuration: Configure DHCP destination address of UDP packet. 168.1.5; set L3 Interface to Vlan1, and then click Add. The configuration is applied on the switch.



Configure the relay policy to non-forward: Click Apply, DHCP relay is disabled on the

switch; click Default, DHCP relay is enabled on the switch.



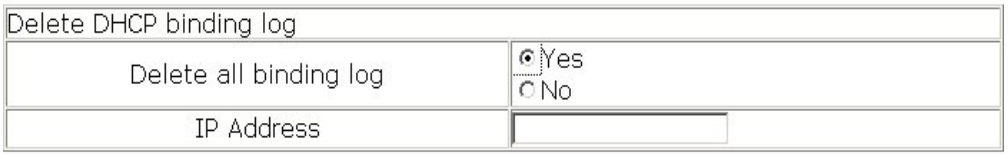
11.6.2 DHCP debugging

Click DHCP configuration, DHCP debugging. Users can display DHCP debug information.

11.6.2.1 Delete binding log

Click DHCP configuration, DHCP debugging, Delete binding log. Users can delete specified binding log or all binding logs.

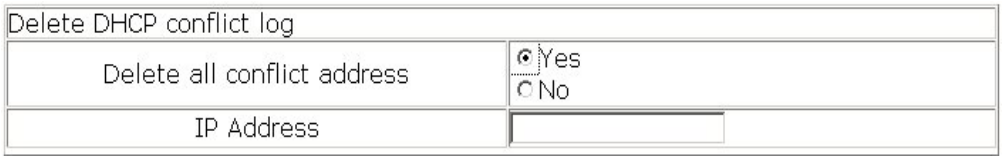
For example: Set Delete all binding log to Yes, and then click Apply. All the binding logs are deleted.



11.6.2.2 Delete conflict log

Click DHCP configuration, DHCP debugging, Delete conflict log. Users can delete conflict log.

For example: Delete all conflict address to Yes, and then click Apply. All the conflict logs are deleted.



11.6.2.3 Delete DHCP server statistics log

Click DHCP configuration, DHCP debugging, Delete DHCP server statistics log. Users can delete DHCP server statistics and restore the counter to zero.

For example: Click Apply. All the DHCP statistics are deleted.

11.6.2.4 Show IP-MAC binding

Click DHCP configuration, DHCP debugging, Show IP-MAC binding. Users can display IP-MAC binding.

Information display			
IP address	Hardware adress	Lease expiration	Type
Total dhcp binding items: 0, the matched: 0			

11.6.2.5 Show conflict-logging

Click DHCP configuration, DHCP debugging, Show conflict-logging. Users can display conflict logging.

Information display		
IP Address	Detection method	Detection Time

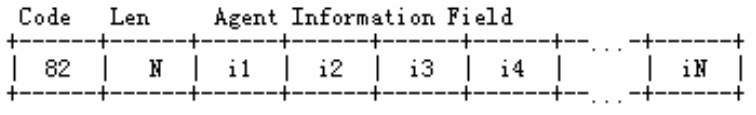
Chapter 12 DHCP option 82 Configuration

12.1 Introduction to DHCP option 82

DHCP option 82 is the Relay Agent Information Option, its option code is 82. DHCP option 82 is aimed at strengthening the security of DHCP servers and improving the IP address configuration policy. The Relay Agent adds option 82 (including the client's physical access port, the access device ID and other information),to the DHCP request message from the client then forwards the message to DHCP server. When the DHCP server which supports the option 82 function receives the message, it will allocate an IP address and other configuration information for the client according to preconfigured policies and the option 82 information in the message. At the same time, DHCP server can identify all the possible DHCP attack messages according to the information in option 82 and defend against them. DHCP Relay Agent will peel the option 82 from the reply messages it receives, and forward the reply message to the specified port of the network access device, according to the physical port information in the option. The application of DHCP option 82 is transparent for the client.

12.1.1 DHCP option 82 Message Structure

A DHCP message can have several option segments; option 82 is one of them. It has to be placed after other options but before option 255. The following is its format:



Code: represents the sequence number of the relay agent information option, the option 82 is called so because rfc3046 is defined as 82.

Len: the number of bytes in Agent Information Field, not including the two bytes in Code segment and Len segment.

option 82 can have several sub-options, and need at least one sub-option. rfc3046 defines the following two sub-options, whose formats are showed as follows:

```
  SubOpt  Len     Sub-option Value
+------+------+------+------+------+------+--...-+------+
|  1   |   N  |  s1  |  s2  |  s3  |  s4  |      |  sN  |
+------+------+------+------+------+------+--...-+------+
  SubOpt  Len     Sub-option Value
+------+------+------+------+------+------+--...-+------+
|  2   |   N  |  i1  |  i2  |  i3  |  i4  |      |  iN  |
+------+------+------+------+------+------+--...-+------+
```

SubOpt: the sequence number of sub-option, the sequence number of Circuit ID sub-option is 1, the sequence number of Remote ID sub-option is 2.

Len: the number of bytes in Sub-option Value, not including the two bytes in SubOpt segment and Len segment.

12.1.2 option 82 Working Mechanism

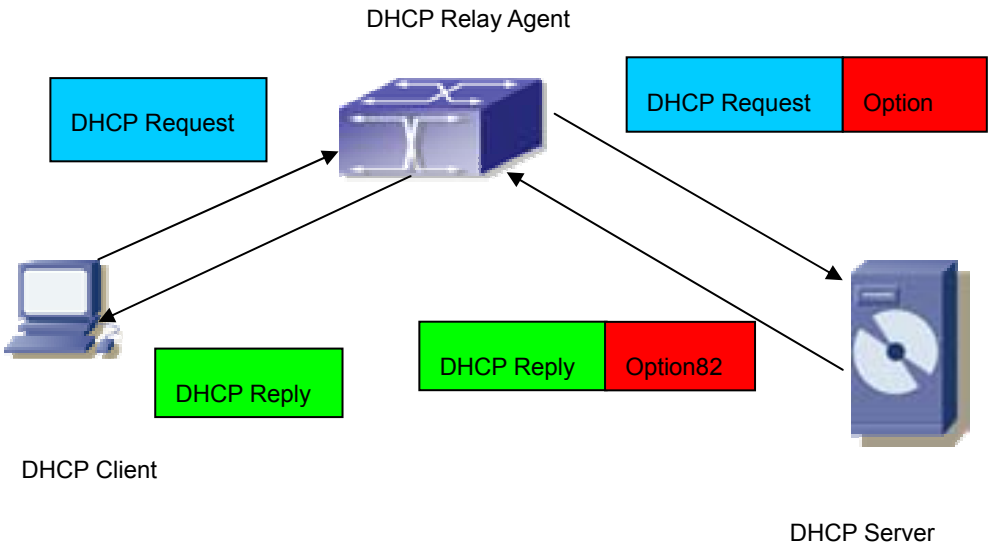


Fig 12-1 DHCP option 82 flow chart

If the DHCP Relay Agent supports option 82, the DHCP client should go through the following four steps to get its IP address from the DHCP server: discover, offer, select and acknowledge. The DHCP protocol follows the procedure below:

1）DHCP client sends a request broadcast message while initializing. This request message does not have option 82.

2）DHCP Relay Agent will add the option 82 to the end of the request message it receives, then relay and forward the message to the DHCP server. By default, the sub-option 1 of option 82 (Circuit ID) is the interface information of the switch connected to the DHCP client (VLAN name and physical port name), but the users can configure the Circuit ID as they wish. The sub-option 2 of option 82(Remote ID) is the MAC address of the DHCP relay device.

3）After receiving the DHCP request message, the DHCP server will allocate IP address and other information for the client according to the information and preconfigured policy in the option segment of the message. Then it will forward the reply message with DHCP configuration information and option 82 information to DHCP Relay Agent.

4）DHCP Relay Agent will peel the option 82 information from the replay message sent by DHCP server, and then forward the message with DHCP configuration information to the DHCP client.

12.2 DHCP option 82 Configuration

12.2.1 DHCP option 82 Configuration Task List

1. Enabling the DHCP option 82 of the Relay Agent.
2. Configure the DHCP option 82 attributes of the interface.
3. Enable the DHCP option 82 of server.
4. Diagnose and maintain DHCP option 82.

1. Enabling the DHCP option 82 of the Relay Agent.

Command	Explanation
Global configuration mode	
ip dhcp relay information option **no ip dhcp relay information option**	Set this command to enable the option 82 function of the switch Relay Agent. The “no ip dhcp relay information option” is used to disable the option 82 function of the switch Relay Agent.

2. Configure the DHCP option 82 attributes of the interface

Command	Explanation
Interface configuration mode	

ip dhcp relay information policy {drop | keep | replace} **no ip dhcp relay information policy**	This command is used to set the retransmitting policy of the system for the received DHCP request message which contains option 82. The drop mode means that if the message has option82, then the system will drop it without processing; keep mode means that the system will keep the original option 82 segment in the message, and forward it to the server to process; replace mode means that the system will replace the option 82 segment in the existing message with its own option 82, and forward the message to the server to process. The “no ip dhcp relay information policy” will set the retransmitting policy of the option 82 DCHP message as “replace”.
ip dhcp relay information option subscriber-id {standard | <circuit-id>} **no ip dhcp relay information option subscriber-id**	This command is used to set the format of option 82 sub-option1(Circuit ID option) added to the DHCP request messages from interface, standard means the standard vlan name and physical port name format, like”Vlan2+Ethernet1/12”,<circuit-id> is the circuit-id contents of option 82 specified by users, which is a string no longer than 64characters. The” no ip dhcp relay information option subscriber-id” command will set the format of added option 82 sub-option1 (Circuit ID option) as standard format.

3. Enable the DHCP option 82 of server.

Command	Explanation
Global configuration mode	

ip dhcp server relay information enable **no ip dhcp server relay information enable**	This command is used to enable the switch DHCP server to identify option82. The “no ip dhcp server relay information enable” command will make the server ignore the option 82.

4. Diagnose and maintain DHCP option 82

Command	Explanation
Admin mode	
show ip dhcp relay information option	This command will display the state information of the DHCP option 82 in the system, including option82 enabling switch, the interface retransmitting policy, the circuit ID mode and the DHCP server option82 enabling switch.
debug ip dhcp relay packet	This command is used to display the information of data packets processing in DHCP Relay Agent, including the “add” and “peel” action of option 82.

12.2.2 Command for DHCP option 82

12.2.2.1 ip dhcp relay information option

Command：ip dhcp relay information option

no ip dhcp relay information option

Function：Set this command to enable the option82 function of the switch Relay Agent. The “no ip dhcp relay information option” command is used to disable the option82 function of the switch Relay Agent

Parameters：None.

Default Settings：The system disables the option82 function by default.

Command Mode：Global configuration mode.

Usage Guide：Only the DHCP Relay Agents configuring with this command can add option82 to the DHCP request message, and let the server to process it. Before enabling this function, users should make sure that the DHCP service is enabled and the Relay Agent will transmit the udp broadcast messages whose destination port is 67.

Example：Enable the option82 function of the Relay Agent.

Switch(Config)#service dhcp
Switch(Config)# ip forward-protocol udp bootps
Switch(Config)# ip dhcp relay information option

12.2.2.2 ip dhcp relay information policy

Command：ip dhcp relay information policy {drop | keep | replace}
no ip dhcp relay information policy

Function：This command is used to set the retransmitting policy of the system for the received DHCP request message which contains option82. The drop mode means that if the message has option82, then the system will drop it without processing; keep mode means that the system will keep the original option82 segment in the message, and forward it to the server to process; replace mode means that the system will replace the option 82 segment in the existing message with its own option 82, and forward the message to the server to process. The “no ip dhcp relay information policy” will set the retransmitting policy of the option 82 DCHP message as “replace”.

Parameters：None

Command Mode: Interface configuration mode.

Default Settings：The system uses replace mode to replace the option 82 segment in the existing message with its own option 82.

User Guide：Since the DHCP client messages might go through several DHCP Relay Agents when passed to the DHCP server, the latter Relay Agents on the path should set policies to decide how to process the option82 added by Relay Agents before them. The selection of option 82 retransmitting policies should take the configuration policy of the DHCP server into account.

Example：Set the retransmitting policy of DHCP messages option 82 as keep.

Switch(Config-if-Vlan1)# ip dhcp relay information policy keep

12.2.2.3 ip dhcp relay information option subscriber-id

Command：ip dhcp relay information option subscriber-id {standard | <circuit-id>}
no ip dhcp relay information option subscriber-id

Function：This command is used to set the format of option82 sub-option1(Circuit ID option) added to the DHCP request messages from interface, **standard** means the standard vlan name and physical port name format, like”Vlan2+Ethernet1/12”,**<circuit-id>** is the circuit-id contents of option82 specified by users, which is a string no longer than 64 characters. The” **no ip dhcp relay information option subscriber-id**” command will set the format of added option82 sub-option1 (Circuit ID option) as standard format.

Parameters：None

Command Mode: Interface configuration mode.

Default Settings：The system uses the standard format to set the circuit-id of option 82 by default.

User Guide：Because the option 82 information added for the switch should cooperate with the third party DHCP server, if the standard circuit-id format of the switch cannot satisfy the server's request, this method will be provided for users to specify the contents of circuit-id according to the situation of the server.

Example：Set the sub-option circuit-id of DHCP option82 as foobar.

Switch(Config-if-Vlan1)# ip dhcp relay information option subscriber-id foobar

12.2.2.4 ip dhcp server relay information enable

Command：**ip dhcp server relay information enable**

no ip dhcp server relay information enable

Function：This command is used to enable the switch DHCP server to identify option82. The "no ip dhcp server relay information enable" command will make the server ignore the option 82.

Parameters: None

Command Mode：Global configuration mode.

Default Setting：The system disable the option82 identifying function by default.

User Guide：If the users want the switch DHCP server to identify option82 and return option 82 information in the reply message, this command needs to be set, or, the switch DHCP server will ignore the option82.

Example：Set the DHCP server to support option82

Switch(Config)# ip dhcp server relay information enable

12.2.2.5 show ip dhcp relay information option

Command：**show ip dhcp relay information option**

Function：This command will display the state information of the DHCP option 82 in the system, including option82 enabling switch, the interface retransmitting policy, the circuit ID mode and the switch DHCP server option82 enabling switch.

Parameters: None

Command Mode: Admin Mode

User Guide：Use this command to check the state information of Relay Agent option82 during operation.

Example：

Switch#show ip dhcp relay information option

ip dhcp server relay information option(i.e. option 82) is disabled

ip dhcp relay information option(i.e. option 82) is enabled

Vlan2:

ip dhcp relay information policy keep

ip dhcp relay information option subscriber-id standard

Vlan3:

ip dhcp relay information policy replace

ip dhcp relay information option subscriber-id foobar

12.2.2.6 debug ip dhcp relay packet

Command：debug ip dhcp relay packet

Function：This command is used to display the information of data packets processing in DHCP Relay Agent, including the “add” and “peel” action of option 82.

Parameters: None

Command Mode: Admin Mode

User Guide： Use this command during the operation to display the procedure of data packets processing of the server and to display the corresponding option82 operation information. identified option 82 information of the request message and the option 82 information returned by the reply message.

Example：

Switch(Config)# debug ip dhcp relay packet

12.3 DHCP option 82 Application Examples

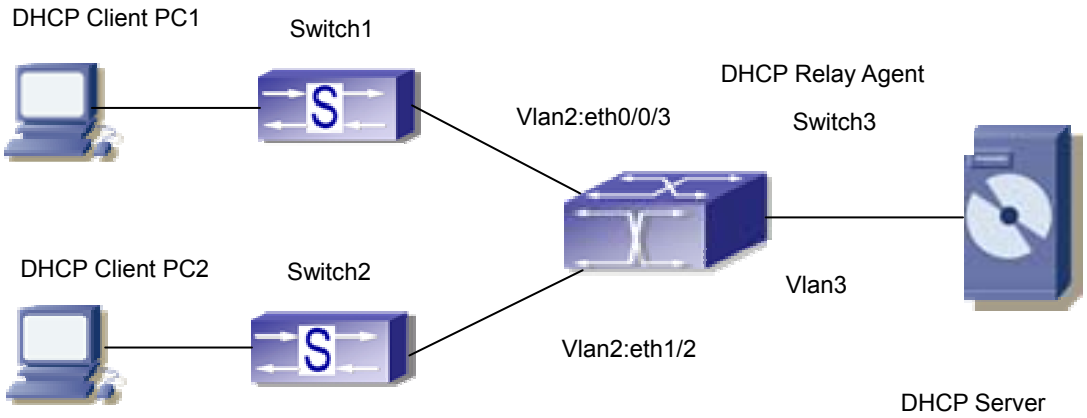


Fig 12-2 a DHCP option 82 typical application example

In the above example, layer 2 switches Switch1 and Switch2 are both connected to layer 3 switch Switch3, Switch 3 will transmit the request message from DHCP client to

DHCP serer as DHCP Relay Agent. It will also transmit the reply message from the server to DHCP client to finish the DHCP protocol procedure. If the DHCP option 82 is disabled, DHCP server cannot distinguish that whether the DHCP client is from the network connected to Switch1 or Switch2. So, all the PC terminals connected to Switch1 and Switch2 will get addresses from the public address pool of the DHCP server. After the DHCP option 82 function is enabled, since the Switch3 appends the port information of accessing Switch3 to the request message from the client, the server can tell that whether the client is from the network of Swich1 or Swich2, and thus can allocate separate address spaces for the two networks, to simplify the management of networks.

The following is the configuration of Switch3(MAC address is 00:03:0f:02:33:01):
Switch3(Config)#service dhcp
Switch3(Config)#ip dhcp relay information option
Switch3(Config)#ip forward-protocol udp bootps
Switch3(Config-if-vlan3)#ip address 192.168.10.222 255.255.255.0
Switch3(Config-if-vlan2)#ip address 192.168.102.2 255.255.255.0
Switch3(Config-if-vlan2)#ip helper 192.168.10.88

Linux ISC DHCP Server supports option 82, its configuration file /etc/dhcpd.con is
ddns-update-style interim;
ignore client-updates;

class "Switch3Vlan2Class1" {
match if option agent.circuit-id = "Vlan2+Ethernet1/2" and option agent.remote-id=00:03:0f:02:33:01;
}

class "Switch3Vlan2Class2" {
match if option agent.circuit-id = "Vlan2+Ethernet1/3" and option agent.remote-id=00:03:0f:02:33:01;
}

subnet 192.168.102.0 netmask 255.255.255.0 {
option routers 192.168.102.2;
option subnet-mask 255.255.255.0;
option domain-name "example.com.cn";
option domain-name-servers 192.168.10.3;
authoritative;

```
pool {
range 192.168.102.21 192.168.102.50;
default-lease-time 86400; #24 Hours
max-lease-time 172800; #48 Hours
allow members of "Switch3Vlan2Class1";
}
pool {
range 192.168.102.51 192.168.102.80;
default-lease-time 43200; #12 Hours
max-lease-time 86400; #24 Hours
allow members of "Switch3Vlan2Class2";
}
}
```

Now, the DHCP server will allocate addresses for the network nodes from Switch1 which are relayed by Switch3 within the range of 192.168.102.21 ~ 192.168.102.50, and allocate addresses for the network nodes from Switch1 within the range of 192.168.102.51～192.168.102.80.

12.4 DHCP option 82 Troubleshooting Help

DHCP option 82 is implemented as a sub-function module of DHCP Relay Agent. Before using it, users should make sure that the DHCP Relay Agent is configured correctly.

DHCP option 82 needs the DHCP Relay Agent and the DHCP server cooperate to finish the task of allocating IP addresses. The DHCP server should set allocating policy correctly depending on the network topology of the DHCP Relay Agent, or, even the Relay Agent can operate normally, the allocation of addresses will fail. When there is more than one kind of Relay Agent, please pay attention to the retransmitting policy of the interface DHCP request messages.

To implement the option 82 function of DHCP Relay Agent, the “debug dhcp relay packet” command can be used during the operating procedure, including adding the contents of option 82, the retransmitting policy adopted, the option 82 contents of the server peeled by the Relay Agent and etc., such information can help users to do troubleshooting.

To implement the option 82 function of DHCP server, the “debug ip dhcp server packet” command can be used during the operating procedure to display the procedure

of data packets processing of the server, including displaying the identified option 82 information of the request message and the option 82 information returned by the reply message.

Chapter 13 DHCP snooping Configuration

13.1 Introduction to DHCP Snooping

DHCP Snooping can effectively block attacks of fake DHCP Servers.

Defense against Fake DHCP Server：once the switch intercepts the DHCP Server reply packets（including DHCPOFFER, DHCPACK, and DHCPNAK）, it will alarm and respond according to the situation（shutdown the port or send Blackhole）。

Defense against DHCP over load attacks：To avoid too many DHCP messages attacking CPU, users should limit the DHCP speed of receiving packets on trusted and non-trusted ports.

Record the binding data of DHCP：DHCP SNOOPING will record the binding data allocated by DHCP SERVER while forwarding DHCP messages, it can also upload the binding data to the specified server to backup it. The binding data is mainly used to configure the dynamic users of dot1x userbased ports. Please refer to the chapter called“dot1x configuration” to find more about the usage of dot1x use-based mode.

Add binding ARP: DHCP SNOOPING can add static binding ARP according to the binding data after capturing binding data, thus to avoid ARP cheating.

Add trusted users：DHCP SNOOPING can add trusted user list entries according to the parameters in binding data after capturing binding data; thus these users can access all resources without DOT1X authentication.

Automatic Recovery：A while after the switch shut down the port or send blockhole, it should automatically recover the communication of the port or source MAC and send information to Log Server via syslog.

LOG Function：When the switch discovers abnormal received packets or automatically recovers, it should send syslog information to Log Server.

13.2 DHCP Snooping Configuration

13.2.1 DHCP Snooping Configuration Task Sequence

1. Enable DHCP Snooping
2. Enable DHCP Snooping binding function
3. Enable DHCP Snooping binding ARP function
4. Set helper server address
5. Set trusted ports
6. Enable DHCP Snooping binding DOT1X function
7. Enable DHCP Snooping binding USER function
8. Adding static list entries function
9. Set defense actions
10. Set rate limitation of DHCP messages
11. Enable the debug switch

1. Enable DHCP Snooping

Command	Explanation
Globe mode	
ip dhcp snooping enable **no ip dhcp snooping enable**	Enable or disable the dhcp snooping function

2. Enable DHCP Snooping binding

Command	Explanation
Globe mode	
ip dhcp snooping binding enable **no ip dhcp snooping binding enable**	Enable or disable the dhcp snooping binding function

3. Set HELPER SERVER address

Command	Explanation
Globe mode	
ip user helper-address A.B.C.D [port <udpport>] source <ipAddr> (secondary|) **no ip user helper-address (secondary|)**	Set or delete HELPER SERVER address

4. Enable DHCP Snooping binding ARP function

Command	Explanation
Globe mode	
ip dhcp snooping binding arp **no ip dhcp snooping binding arp**	Enable or disable the dhcp snooping binding ARP function

5. Set trusted ports

Command	Explanation
Port mode	
ip dhcp snooping trust **no ip dhcp snooping trust**	Set or delete the dhcp snooping trust attributes of ports.

6. Enable DHCP SNOOPING binding DOT1X function

Command	Explanation
Port mode	
ip dhcp snooping binding dot1x **no ip dhcp snooping binding dot1x**	Enable or disable the dhcp snooping binding dot1x function

7. Enable or disable the DHCP SNOOPING binding USER function

Command	Explanation
Port mode	
ip dhcp snooping binding user-control **no ip dhcp snooping binding user-control**	Enable or disable the dhcp snooping binding user function

8. Add static binding information

Command	Explanation
Globe mode	
ip dhcp snooping binding user <mac> address <ipAddr> <mask> vlan <vid> interface (ethernet|) <ifname> **no ip dhcp snooping binding user <mac> interface (ethernet|) <ifname>**	Add/delete dhcp snooping static binding list entries

9. Set defense actions

Command	Explanation
Port mode	
ip dhcp snooping action {shutdown|blackhole} [recovery <second>] **no ip dhcp snooping action**	Set or delete the dhcp snooping automatic defense actions of ports.

10. Set rate limitation of data transmission

Command	Explanation
Globe mode	
ip dhcp snooping limit-rate <pps> **no ip dhcp snooping limit-rate**	Set rate limitation of the transmission of DHCP SNOOPING messages

11. Enable the debug switch

Command	Explanation
Admin mode	
debug ip dhcp snooping packet **debug ip dhcp snooping event** **debug ip dhcp snooping binding**	Please refer to the chapter on system troubleshooting

13.2.2 Command for DHCP Snooping Configuration

13.2.2.1 debug ip dhcp snooping packet interface

Command：debug ip dhcp snooping packet interface <ifName>

no debug ip dhcp snooping packet <ifName>

Function：This command is used to enable the DHCP SNOOPING debug switch to debug the information that DHCP SNOOPING is receiving a packet.

Command Mode：Admin mode.

Usage Guide： the information that DHCP SNOOPING is receiving messages from a specific port.

13.2.2.2 debug ip dhcp snooping packet

Command：debug ip dhcp snooping packet

no debug ip dhcp snooping packet

Function：This command is used to enable the DHCP SNOOPING debug switch to debug the message-processing procedure of DHCP SNOOPING.

Command Mode：Admin mode.

Usage Guide： the debug information that the DHCP SNOOPING is processing messages, including every step in the message-processing procedure: adding alarm information, adding binding information, transmitting DHCP messages and etc.

13.2.2.3 debug ip dhcp snooping update

Command：debug ip dhcp snooping update

no debug ip dhcp snooping update

Function：This command is use to enable the DHCP snooping debug switch to debug the communication information between DHCP snooping and helper server.

Command Mode：Admin mode.

Usage Guide：Debug the information of communication messages received and sent by DHCP snooping and helper server.

13.2.2.4 debug ip dhcp snooping event

Command：debug ip dhcp snooping event

no debug ip dhcp snooping event

Function：This command is use to enable the DHCP SNOOPING debug switch to debug the state of DHCP SNOOPING task.

Command Mode：Admin mode.

Usage Guide: This command is mainly used to debug the state of DHCP SNOOPING task and available of outputting the state of checking binding data and executing port action and so on.

13.2.2.5 debug ip dhcp snooping binding

Command：debug ip dhcp snooping binding

no debug ip dhcp snooping binding

Function：This command is use to enable the DHCP SNOOPING debug switch to debug the state of binding data of DHCP SNOOPING.

Command Mode：Admin mode.

Usage Guide：This command is mainly used to debug the state of DHCP SNOOPING task when it adds ARP list entries, dot1x users and trusted user list entries according to binding data.

13.2.2.6 ip dhcp snooping

Command：ip dhcp snooping enable

no ip dhcp snooping enable

Function： Enable the DHCP Snooping function.

Parameters：None.

Command Mode：Globe mode.

Default Settings：DHCP Snooping is disabled by default.

Usage Guide：When this function is enabled, it will monitor all the DHCP Server packets of non-trusted ports.

Example：Enable the DHCP Snooping function.

switch(Config)#ip dhcp snooping enable

13.2.2.7 ip dhcp snooping binding

Command：ip dhcp snooping binding enable

no ip dhcp snooping binding enable

Function： Enable the DHCP Snooping binding funciton

Parameters：None.

Command Mode：Globe mode.

Default Settings：DHCP Snooping binding is disabled by default.

Usage Guide： When the function is enabled, it will record the binding information allocated by DHCP Server of all trusted ports.

Only after the DHCP SNOOPING function is enabled, the binding function can be enabled.

Example：Enable the DHCP Snooping binding funciton

switch(Config)#ip dhcp snooping binding enable

Relative Command：ip dhcp snooping enable

13.2.2.8 ip dhcp snooping binding user

Command：ip dhcp snooping binding user <mac> address <ipAddr> <mask> vlan <vid> interface [Ethernet] <ifname>

no lp dhcp snooping binding user <mac> interface [Ethernet] <ifname>

Function： Configure the information of static binding users

Parameters：

mac：The MAC address of the static binding user, which is the only index of the binding user.

ipAddr、mask：The IP address and mask of the static binding user;

vid：The VLAN ID which the static binding user belongs to；

i**fname：**The access interface of static binding user

Command Mode：Globe mode.

Default Settings：DHCP Snooping has no static binding list entry by default.

Usage Guide： The static binding users is deal in the same way as the dynamic binding users captured by DHCP SNOOPING; the follwoing actions are all allowed: notifying DOT1X to be a controlled user of DOT1X, adding a trusted user list entry directly, adding a bingding ARP list entry. The static binding uses will never be aged, and have a priority higher than dynamic binding users.

Only after the DHCP SNOOPING binding function is enabled, the static binding users can be enabled.

Example：Configure static binding users

switch(Config)#ip dhcp snooping binding user 00-03-0f-12-34-56 address 192.168.1.16 255.255.255.0 interface Ethernet 1/16

Relative Command：ip dhcp snooping binding enable

13.2.2.9 ip dhcp snooping binding arp

Command：ip dhcp snooping binding arp

no ip dhcp snooping binding arp

Function： Enable the DHCP Snooping binding ARP funciton.

Parameters：None

Command Mode：Globe mode

Default Settings： DHCP Snooping binding ARP funciton is disabled by default.

Usage Guide： When this function is enbaled, DHCP SNOOPING will add binding ARP list entries according to binding information. Only after the binding function is enabled, can the binding ARP function be enabled. Binding ARP list entries are static entries without configuration of reservation, and will be added to the NEIGHBOUR list directly. The priority of binding ARP list entries is lower than the static ARP list entries set by administrator, so can be overwritten by static ARP list entries; but, when static ARP list

entries are deleted, the binding ARP list entries can not be recovered untill the DHCP SNOOPING recapture the biding inforamtion. Adding binding ARP list entries is used to prevent these list entried from being attacked by ARP cheating. At the same time, these static list entries need no reauthenticaiton, which can prenvent the switch from the failing to reauthenticate ARP when it is being attacked by ARP scanning.

Only after the DHCP SNOOPING binding function is enabled, the binding ARP function can be set.

Example：Enable the DHCP Snooping binding ARP funciton.

switch(Config)#ip dhcp snooping binding arp

Relative Command：ip dhcp snooping binding enable

13.2.2.10 ip dhcp snooping binding dot1x

Command：**ip dhcp snooping binding dot1x**

no ip dhcp snooping binding dot1x

Function： Enable the DHCP Snooping binding DOT1X funciton.

Parameters：None

Command Mode：Port mode

Default Settings：By default, the binding DOT1X funciton is disabled on all ports.

Usage Guide： When this function is enabled, DHCP SNOOPING will notify the DOT1X module about the captured bindng information as a DOT1X controlled user. This command is mutually exclusive to”ip dhcp snooping binding user-contro“command.

Only after the DHCP SNOOPING binding function is enabled, the binding ARP function can be set.

Example：Enable the binding DOT1X funciton on port ethernet1/1

switch(Config)#interface ethernet 1/1

switch(Config- Ethernet 1/1)# ip dhcp snooping binding dot1x

Relative Command：ip dhcp snooping binding enable

ip dhcp snooping binding user-control

13.2.2.11 ip dhcp snooping binding user-control

Command：**ip dhcp snooping binding user-control**

no ip dhcp snooping binding user-control

Function： Enable the binding user funtion

Parameters：None

Command Mode：Port mode

Default Settings：By default, the binding user funciton is disabled on all ports.

Usage Guide： When this function is enabled, DHCP SNOOPING will treat the captured binding information as trusted users allowed to access all resources. This command is

mutually exclusive to“ ip dhcp snooping binding dot1x“ command.

Only after the DHCP SNOOPING binding function is enabled, the binding ARP function can be set.

Example：Enable the binding USER funciton on port ethernet1/1

switch(Config)#interface ethernet 1/1

switch(Config- Ethernet 1/1)# ip dhcp snooping binding user-control

Relative Command：ip dhcp snooping binding enable

ip dhcp snooping binding dot1x

13.2.2.12 ip dhcp snooping trust

Command：**ip dhcp snooping trust**

no ip dhcp snooping trust

Function： Set or delete the DHCP Snooping trust attributes of a port.

Parameters：None

Command Mode：Port mode

Default Settings：By default, all ports are non-trusted ports

Usage Guide：

Only when DHCP Snooping is globally enabled, can this command be set.

When a port turns into a trusted port from a non-trusted port, the original defense action of the port will be automatically deleted; all the security history records will be cleared (except the information in system log).

Example：Set port ethernet1/1 as a DHCP Snooping trusted port

switch(Config)#interface ethernet 1/1

switch(Config- Ethernet 1/1)#ip dhcp snooping trust

13.2.2.13 ip dhcp snooping action

Command：**ip dhcp snooping action {shutdown|blackhole} [recovery <second>]**

no ip dhcp snooping action

Function： Set or delete the automatic defense action of a port.

Parameters：

shutdown: When the port detects a fake DHCP Server, it will be shutdown

blackhole：When the port detects a fake DHCP Server, the vid and source MAC of the fake packet will be used to block the traffic from this MAC.

Recovery：Users can set to recover after the automatic defense action being executed.(no shut ports or delete correponding blackhole）

Second：Users can set how long after the execution of defense action to recover. The unit is second, and valid range is 10-3600.

Command Mode：Port mode

Default Settings：No default defense action.

Usage Guide：

Only when DHCP Snooping is globally enabled, can this command be set.

Trusted port will not detect fake DHCP Server, so, will never trigger the corresponding defense action. When a port turns into a trusted port from a non-trusted port, the original defense action of the port will be automatically deleted.

Example：Set the DHCP Snooping defense action of port ethernet1/1 as setting blackhole, and the recovery time is 30 seconds.

switch(Config)#interface ethernet 1/1

switch(Config- Ethernet 1/1)#ip dhcp snooping action blackhole recovery 30

13.2.2.14 ip dhcp snooping action MaxNum

Command：**ip dhcp snooping action {<maxNum>|default}**

Function： Set the number of defense action that can be simultaneously take effect.

Parameters：

<maxNum>: the number of defense action on each port, the range of which is 1-200, and the value of which is 10 by default

default：recover to the default value

Command Mode：Globe mode.

Default Settings：The default value is 10.

Usage Guide：Set the max number of defense actions to avoid the resource exhaustion of the switch caused by attacks. If the number of alarm information is larger than the set value, then the earliest defense action will be recovered forcibly in order to send new defense actions.

Example：Set the number of port defense actions as 100.

switch(Config)#ip dhcp snooping action maxnum 100

13.2.2.15 ip dhcp snooping limit-rate

Command：**ip dhcp snooping limit-rate <pps>**

no ip dhcp snooping limit-rate

Function： Set the DHCP message rate limit

Parameters：

<pps>：The number of DHCP messages transmitted in every minute, ranging from 0 to 100. Its default value is 100. 0 means that no DHCP message will be transmitted.

Command Mode：Globe mode.

Default Settings：The default value is 100.

Usage Guide：After enabling DHCP snooping, the switch will monitor all the DHCP messages and implement software transmission. The software performance of the switch

is relative to the type of the switch, its current load and so on.

Example：Set the message transmission rate as 50pps

switch(Config)#ip dhcp snooping limit-rate 50

13.2.2.16 ip user helper-address

Command： **ip user helper-address <*svr_addr*> [port <*udp_port*>] source <*src_addr*> [secondary]**

no ip user helper-address [secondary]

Function： Set the address and port of HELPER SERVER

Parameters：

<svr_addr>：the IP address of HELPER SERVER 的 IP in dotted-decimal notation.

udp_port：the UDP port of HELPER SERVER, the range of which is1－65535, and its default value is 9119.

src_addr：the local management IP address of the switch, in dotted-decimal notation

sencondary：whether it is a secondary SERVER address.

Command Mode：Globe mode.

Default Settings：There is no HELPER SERVER address by default.

Usage Guide：：DHCP SNOOPING will send the monitored binding information to HELPER SERVER to save it. If the switch starts abnormally, it can recover the binding data from HELPER SERVER. The HELPER SERVER function usually is integrated into DCBI package. The DHCP SNOOPING and HELPER SERVER use the UDP protocol to communicate, and guarantee the arrival of retransmitted data. **HELPER SERVER configuration can also be used to sent DOT1X user data from the server, the detail of usage is described in the chapter of "dot1x configuration".**

Two HELPER SERVER addresses are allowed, DHCP SNOOPING will try to connect to PRIMARY SERVER in the first place. Only when the PRIMARY SERVER is unreachable, will the switch c HELPER SERVER connects to SECONDARY SERVER.

Please pay attention：source address is the effective management IP address of the switch, if the management IP address of the switch changes, this configuration should be updated in time.

Example：Set the local management IP address as 100.1.1.1, primary HELPER SERVER address as 100.1.1.100 and the port as default value.

switch(Config)#interface vlan 1

switch(Config- If-Vlan1)#ip address 100.1.1.1 255.255.255.0

switch(Config-If-Vlan1)exit

switch(Config)#ip user helper-address 100.1.1.100 source 100.1.1.1

13.2.2.17 show ip dhcp snooping

Command：show ip dhcp snooping [interface [ethernet] <interfaceName>]

Function： Display the current cofiguration information of dhcp snooping or display the records of defense actions of a specific port.

Parameters：

<interfaceName>： the name of the specific port.

Command Mode： Admin mode.

Default Settings： None

Usage Guide： If there is no specific port, then display the current cofiguration information of dhcp snooping, otherwise, display the records of defense actions of the specific port.

Example：

```
switch#show ip dhcp snooping
DHCP Snooping is enabled

DHCP Snooping binding arp: disabled
DHCP Snooping maxnum of action info:10
DHCP Snooping limit rate: 100(pps), switch ID: 0003.0F12.3456
DHCP Snooping droped packets: 0, discarded packets: 0
DHCP Snooping alarm count: 0, binding count: 0,
      expired binding: 0, request binding: 0

interface          trust        action       recovery     alarm num    bind num
---------------- --------- --------- ---------- --------- ----------
Ethernet1/1      trust       none         0second      0            0
Ethernet1/2      untrust     none         0second      0            0
Ethernet1/3      untrust     none         0second      0            0
Ethernet1/4      untrust     none         0second      0            1
Ethernet1/5      untrust     none         0second      2            0
Ethernet1/6      untrust     none         0second      0            0
Ethernet1/7      untrust     none         0second      0            0
Ethernet1/8      untrust     none         0second      0            1
Ethernet1/9      untrust     none         0second      0            0
Ethernet1/10     untrust     none         0second      0            0
Ethernet1/11     untrust     none         0second      0            0
Ethernet1/12     untrust     none         0second      0            0
Ethernet1/13     untrust     none         0second      0            0
Ethernet1/14     untrust     none         0second      0            0
Ethernet1/15     untrust     none         0second      0            0
```

Ethernet1/16	untrust	none	0second	0	0
Ethernet1/17	untrust	none	0second	0	0
Ethernet1/18	untrust	none	0second	0	0
Ethernet1/19	untrust	none	0second	0	0
Ethernet1/20	untrust	none	0second	0	0
Ethernet1/21	untrust	none	0second	0	0
Ethernet1/22	untrust	none	0second	0	0
Ethernet1/23	untrust	none	0second	0	0
Ethernet1/24	untrust	none	0second	0	0

Displayed Information	Explanation
DHCP Snooping is enable	Whether the DHCP Snooping is globally enabled or disabled.
DHCP Snooping binding arp	Whether the ARP binding function is enabled.
DHCP Snooping maxnum of action info	The number limitation of port defense actions
DHCP Snooping limit rate	The rate limitation of receiving packets
switch ID	The switch ID is used to identify the switch, usually using the CPU MAC address.
DHCP Snooping droped packets	The number of dropped messages when the received DHCP messages exceeds the rate limit.
discarded packets	The number of discarded packets caused by the communication failure within the system. If the CPU of the switch is too busy to schedule the DHCP SNOOPING task and thus can not handle the received DHCP messages, such situation might happen.
DHCP Snooping alarm count:	The number of alarm information.
binding count	The number of binding information.
expired binding	The number of binding information which is already expired but has not been deleted. The reason why the expired information is not deleted

	immediately might be that the switch needs to notify the helper server about the information, but the helper server has not acknowledged it.
request binding	The number of REQUEST information
interface	The name of port
trust	The truest attributes of the port
action	The automatic defense action of the port
recovery	The automatic recovery time of the port
alarm num	The number of history records of the port automatic defense actions
bind num	The number of port-relative binding information.

switch#show ip dhcp snooping int Ethernet1/1
interface Ethernet1/1 user config:
trust attribute: untrust
action: none
binding dot1x: disabled
binding user: disabled
recovery interval:0(s)
Alarm info: 0

Binding info: 0

Expired Binding: 0

Request Binding: 0

Displayed Information	Explanation
interface	The name of port
trust attribute	The truest attributes of the port
action	The automatic defense action of the port
recovery interval	The automatic recovery time of the

	port
maxnum of alarm info	The max number of automatic defense actions that can be recorded by the port
binding dot1x	Whether the binding dot1x function is enabled on the port
binding user	Whether the binding user function is enabled on the port.
Alarm info	The number of alarm information.
Binding info	The number of binding information.
Expired Binding	The expired binding information
Request Binding	REQUEST information

13.3 DHCP Snooping Typical Application

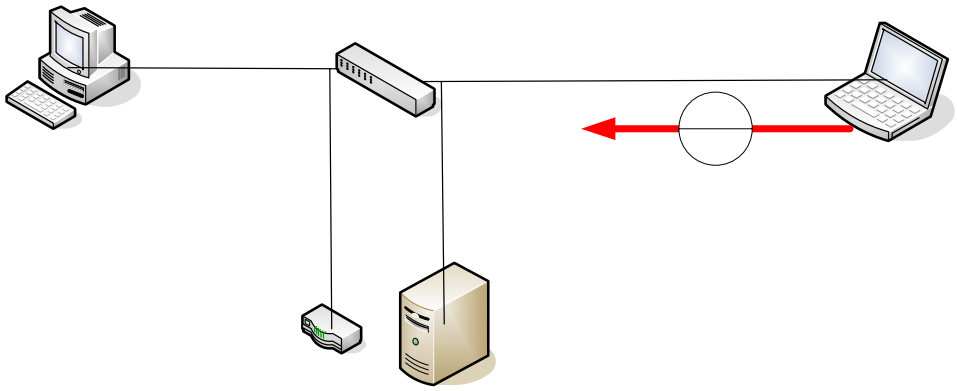


Fig 13-1 Sketch Map of TRUNK

As showed in the above chart, Mac-AA device is the normal user, connected to the non-trusted port 1/1 of the switch. It operates via DHCP Client, IP 1.1.1.5; DHCP Server and GateWay are connected to the trusted ports 1/11 and 1/12 of the switch; the malicious user Mac-BB is connected to the non-trusted port 1/10, trying to fake a DHCP Server（by sending DHCPACK）. Setting DHCP Snooping on the switch will effectively detect and block this kind of network attack.

Configuration sequence is：

switch#

```
switch#config
switch(Config)#ip dhcp snooping
switch(Config)#interface ethernet 1/11
switch(Config-Ethernet1/11)#ip dhcp snooping trust
switch(Config-Ethernet1/11)#exit
switch(Config)#interface ethernet 1/12
switch(Config-Ethernet1/12)#ip dhcp snooping trust
switch(Config-Ethernet1/12)#exit
switch(Config)#interface ethernet 1/1-10
switch(Config-Port-Range)#ip dhcp snooping action shutdown
switch(Config-Port-Range)#
```

13.4 DHCP Snooping Troubleshooting Help

13.4.1 Monitor And Debug Information

The ‘debug ip dhcp snooping’” command can be used to monitor the debug information.

13.4.2 DHCP Snooping Troubleshooting Help

If there is any problem happens when using DHCP Snooping function, please check if the problem is caused by the following reasons:

- ✧ Check that whether the global DHCP Snooping switch is enabled;
- ✧ If the port does not react to invalid DHCP Server packets, please check that whether the port is set as a non-trusted port of dhcp snooping.

Chapter 14 SNTP Configuration

14.1 Introduction to SNTP

The Network Time Protocol (NTP) is widely used for clock synchronization for global computers connected to the Internet. NTP can assess packet sending/receiving delay in the network, and estimate the computer's clock deviation independently, so as to achieve high accuracy in network computer clocking. In most positions, NTP can provide accuracy from 1 to 50ms according to the characteristics of the synchronization source and network route.

Simple Network Time Protocol (SNTP) is the simplified version of NTP, removing the complex algorithm of NTP. SNTP is used for hosts who do not require full NTP functions, it is a subset of NTP. It is common practice to synchronize the clocks of several hosts in local area network with other NTP hosts through the Internet, and use those hosts to provide time synchronization service for other clients in LAN. The figure below (Fig 3-1) depicts a NTP/SNTP application network topology, where SNTP mainly works between second level servers and various terminals since such scenarios do not require very high time accuracy, and the accuracy of SNTP (1 to 50 ms) is usually sufficient for those services.

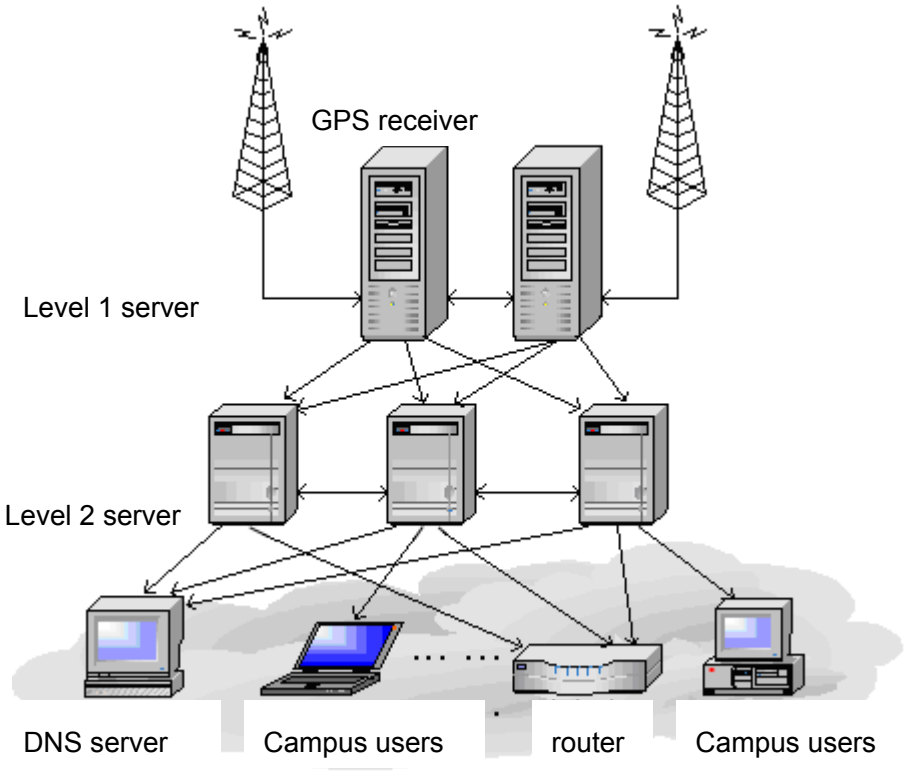


Fig 11-1 Working Scenario

ES4626/ES4650 switch implements SNTPv4 and supports SNTP client unicast as described in RFC2030; SNTP client multicast and unicast are not supported, nor is the SNTP server function.

14.2 Commands for SNTP

14.2.1 clock timezone

Command:clock timezone <*name*> hour <*hours*> [before-utc | after-utc]

Function:set the difference between local time and UTC time.

Parameter：<*name*> is the name of local tomezone, consist of max 16 characters. **<*hours*>** is the time difference to UTC time，range from 0 to 12 . **before-utc** means local time equals the UTC time subtracting the difference **, after-utc** means the local time equals the UTC time adding the difference

Default: 8 *hours* before-utc

Command Mode: Global Mode

Example: set the customer timezone 10 hours before-utc

Switch(Config)#clock timezone customer10 before-utc

14.2.2 sntp server

Command:sntp server {<*server_address*> | < *server_ipv6_addr*> } [version <*version_no*>]

no sntp server {<*server_address*> | < *server_ipv6_addr*>}

Function: Configure the IPv4/IPv6 addresses and the version of the SNTP/NTP server; the “no” form of this command cancels the configured SNTP/NTP server addresses.

Parameter： ***<server_address>*** is the IPv4 unicast address of the SNTP/NTP server,***<server_ipv6_addr>*** is the IPv6 unicast address of the SNTP/NTP server,***<version_no>*** is the version No. of the SNTP on current server,ranging between 1-4 and defaulted at 1.

Default: No sntp/ntp configured by default.

Command Mode: Global Mode

Example:

(1) Configure an IPv4 address of a SNTP/NTP server. SNTPv4 version is adopted on the server

Switch(Config)#sntp server 10.1.1.1 version 4

(2) Configure a SNTP/NTP server IPv6 address

Switch(Config)#sntp server 3ffe:506:1:2::5

14.2.3 sntp poll

Command: sntp poll <*poll_interval*>

no sntp poll

Function: Sets the interval for SNTP clients to send requests to NTP/SNTP; the “**no sntp poll**” command cancels the polltime sets and restores the default setting.

Parameters: <*poll_interval*> is the interval value from 16 to 16284.

Default: The default polltime is 64 seconds.

Command mode: Global Mode

Example: Setting the client to send request to the server every 128 seconds.

Switch#config

Switch(Config)#sntp poll 128

14.2.4 debug sntp

Command: debug sntp {adjust | packets | select }

no debug sntp {adjust | packets | select}

Function: Displays or disables SNTP debug information.

Parameters: adjust stands for SNTP clock adjustment information; **packet** for SNTP packets, **select** for SNTP clock selection.

Command mode: Admin Mode

Example: Displaying debugging information for SNTP packets.

Switch#debug sntp packets

14.2.5 show sntp

Command: show sntp

Function: Displays current SNTP client configuration and server status.

Parameters: N/A.

Command mode: Admin Mode

Example: Displaying current SNTP configuration.

Switch#show sntp

SNTP server	Version	Last Receive
2.1.0.2	1	never

14.3 Typical SNTP Configuration Examples

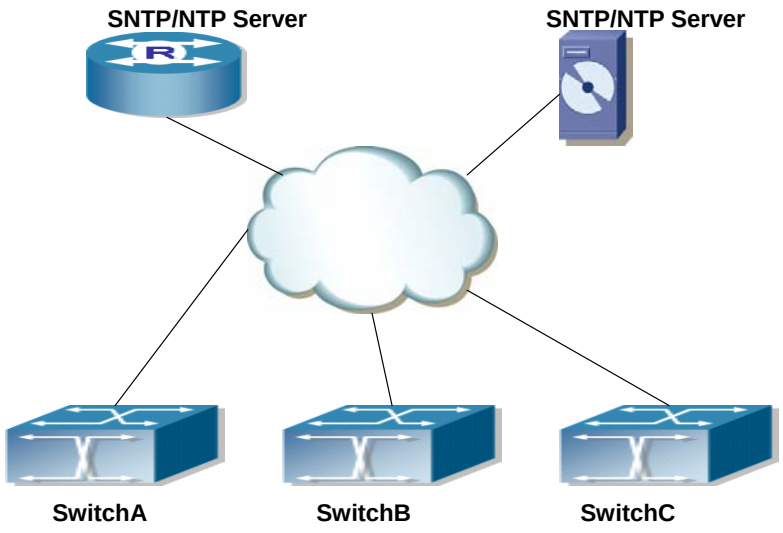


Fig 11-2 Typical SNTP Configuration

All ES4626/ES4650 switch in the autonomous zone are required to perform time synchronization, which is done through two redundant SNTP/NTP servers. For time to be synchronized, the network must be properly configured. There should be reachable route between any ES4626/ES4650 switch and the two SNTP/NTP servers.

Example: Assume the IP addresses of the SNTP/NTP servers are 10.1.1.1 and 20.1.1.1,

respectively, and SNTP/NTP server function (such as NTP master) is enabled, then configurations for any ES4626/ES4650 switch should like the following:

Switch#config

Switch (Config)#sntp server 10.1.1.1

Switch (Config)#sntp server 20.1.1.1

From now on, SNTP would perform time synchronization to the server according to the default setting (polltime 64s, version 1).

14.4 Web Management

Click “SNTP configuration” to open the switch SNTP configuration management list. Users may then make configuration to switch’s SNTP settings.

14.4.1 SNMP/NTP server configuration

Click “SNTP configuration”, “SNTP/NTP server configuration” to configure SNTP/NTP server address and server version.

Example: Configure Server address as 10.1.1.1, configure version as 4, and then, Click Apply button to apply the configuration to switch.

SNTP/NTP server and version configuration	
Server address	10.1.1.1
Version(1-4)	4

14.4.2 Request interval configuration

Click “SNTP configuration”, “Request interval configuration” to configure the sending request time interval from SNTP client to NTP/SNTP server.

Example: Configure Interval as 128 minutes, Click Apply to set the configuration in the switch.

Request interval from SNTP client to NTP/SNTP server	
Interval	128

14.4.3 Time difference

Click “SNTP configuration”, “Time difference” to configure the SNTP client time zone and UTC time difference.

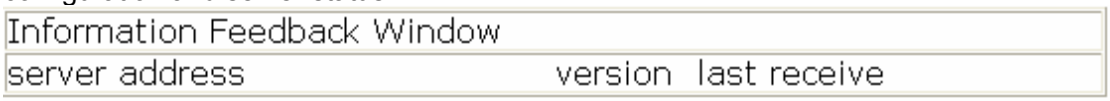
- Time zone-configures time zone

- Time difference -configures time difference
- before-utc –means: (Optional)Sets the offset as a negative number.For example,if the hour offset is 12, the before-UTC keyword sets it to -12.
- after-utc –means: (Optional)Sets the offset as a positive number. This is the default offset.

Example: Configure time zone as Beijing, select Add, set the time difference as 8, and then, click Apply to set the configuration in the switch .

14.4.4 Show SNTP

Click “SNTP configuration”, “Show sntp” to display the SNTP client current configuration and server status.



Chapter 15 ARP Scanning Prevention Function Configuration

15.1 Introduction to ARP Scanning Prevention Function

ARP scanning is a common method of network attack. In order to detect all the active hosts in a network segment, the attack source will broadcast lots of ARP messages in the segment, which will take up a large part of the bandwidth of the network. It might even do large-traffic-attack in the network via fake ARP messages to collapse of the network by exhausting the bandwidth. Usually ARP scanning is just a preface of other more dangerous attack methods, such as automatic virus infection or the ensuing port scanning, vulnerability scanning aiming at stealing information, distorted message attack, and DOS attack, etc.

Since ARP scanning threatens the security and stability of the network with great danger, so it is very significant to prevent it. ES4700BD series switch provides a complete resolution to prevent ARP scanning: if there is any host or port with ARP scanning features is found in the segment, the switch will cut off the attack source to ensure the security of the network.

There are two methods to prevent ARP scanning: port-based and IP-based. The port-based ARP scanning will count the number to ARP messages received from a port in a certain time range, if the number is larger than a preset threshold, this port will be “down”. The IP-based ARP scanning will count the number to ARP messages received from an IP in the segment in a certain time range, if the number is larger than a preset threshold, any traffic from this IP will be blocked, while the port related with this IP will not be “down”. These two methods can be enabled simultaneously. After a port or an IP is disabled, users can recover its state via automatic recovery function.

To improve the effect of the switch, users can configure trusted ports and IP, the ARP messages from which will not be checked by the switch. Thus the load of the switch can be effectively decreased.

15.2 ARP Scanning Prevention Configuration Task Sequence

1. Enable the ARP Scanning Prevention function.
2. Configure the threshold of the port-based and IP-based ARP Scanning Prevention
3. Configure trusted ports
4. Configure trusted IP
5. Configure automatic recovery time
6. Display relative information of debug information and ARP scanning

1. Enable the ARP Scanning Prevention function.

Command	Explanation
Global configuration mode	
anti-arpscan enable **no anti-arpscan enable**	Enable or disable the ARP Scanning Prevention function globally

2. Configure the threshold of the port-based and IP-based ARP Scanning Prevention

Command	Explanation
Global configuration mode	
anti-arpscan port-based threshold <threshold-value> **no anti-arpscan port-based threshold**	Set the threshold of the port-based ARP Scanning Prevention
anti-arpscan ip-based threshold <threshold-value> **no anti-arpscan ip-based threshold**	Set the threshold of the IP-based ARP Scanning Prevention

3. Configure trusted ports

Command	Explanation
Port configuration mode	
anti-arpscan trust <port | supertrust-port> **no anti-arpscan trust <port | supertrust-port>**	Set the trust attributes of the ports

4. Configure trusted IP

Command	Explanation
Global configuration mode	

anti-arpscan trust ip <ip-address [<netmask>]> **no anti-arpscan trust ip <ip-address [<netmask>]>**	Set the trust attributes of IP

5. Configure automatic recovery time

Command	Explanation
Global configuration mode	
anti-arpscan recovery enable **no anti-arpscan recovery enable**	Enable or disable the automatic recovery function
anti-arpscan recovery time <seconds> **no anti-arpscan recovery time**	Set automatic recovery time

6. Display relative information of debug information and ARP scanning

Command	Explanation
Global configuration mode	
anti-arpscan log enable **no anti-arpscan log enable**	Enable or disable the log function of ARP scanning prevention
anti-arpscan trap enable **no anti-arpscan trap enable**	Enable or disable the SNMP Trap function of ARP scanning prevention
show anti-arpscan [trust <ip | port | supertrust-port> | prohibited <ip | port>]	Display the state of operation and configuration of ARP scanning prevention
debug anti-arpscan <port | ip> **no debug anti-arpscan <port | ip>**	Enable or disable the debug switch of ARP scanning prevention

15.3 Command for ARP Scanning Prevention

15.3.1 anti-arpscan enable

Command：anti-arpscan enable

no anti-arpscan enable

Function：Globally enable ARP scanning prevention function; “no anti-arpscan enable” command globally disables ARP scanning prevention function.

Parameters：None.

Default Settings：Disable ARP scanning prevention function.

Command Mode：Global configuration mode

User Guide：

Example：

Enable the ARP scanning prevention function of the switch

Switch(Config)#anti-arpscan enable

15.3.2 anti-arpscan port-based threshold

Command：**anti-arpscan port-based threshold <*threshold-value*>**

no anti-arpscan port-based threshold

Function：Set the threshold of received messages of the port-based ARP scanning prevention. If the rate of received ARP messages exceeds the threshold, the port will be closed. The unit is packet/second. The “no anti-arpscan port-based threshold” command will reset the default value, 5 packets/second.

Parameters：rate threshold, ranging from 2 to 200.

Default Settings：5 packets/second

Command Mode：Global configuration mode

User Guide：the threshold of port-based ARP scanning prevention should be larger than the threshold of IP-based ARP scanning prevention, or, the IP-based ARP scanning prevention will fail.

Example：

Set the threshold of port-based ARP scanning prevention as10 packets/second.

Switch(Config)#anti-arpscan port-based threshold 10

15.3.3 anti-arpscan ip-based threshold

Command：**anti-arpscan ip-based threshold <*threshold-value*>**

no anti-arpscan ip-based threshold

Function：Set the threshold of received messages of the IP-based ARP scanning prevention. If the rate of received ARP messages exceeds the threshold, the IP messages from this IP will be blocked. The unit is packet/second. The “no anti-arpscan ip-based threshold” command will reset the default value, 3 packets/second.

Parameters：rate threshold, ranging from 2 to 200.

Default Settings：3 packets/second

Command Mode：Global configuration mode

User Guide：the threshold of port-based ARP scanning prevention should be larger than the threshold of IP-based ARP scanning prevention, or, the IP-based ARP scanning prevention will fail.

Example：

Set the threshold of IP-based ARP scanning prevention as 6 packets/second.

Switch(Config)#anti-arpscan ip-based threshold 6

15.3.4 anti-arpscan trust

Command：anti-arpscan trust <port | supertrust-port>

no anti-arpscan trust <port | supertrust-port>

Function：Configure a port as a trusted port or a super trusted port;" no anti-arpscan trust <port | supertrust-port>"command will reset the port as an untrusted port.

Parameters：None.

Default Settings：By default all the ports are non- trustful.

Command Mode：Port configuration mode.

User Guide：If a port is configured as a trusted port, then the ARP scanning prevention function will not deal with this port, even if the rate of received ARP messages exceeds the set threshold, this port will not be closed, but the non- trustful IP of this port will still be checked. If a port is set as a super non- trustful port, then neither the port nor the IP of the port will be dealt with. If the port is already closed by ARP scanning prevention, it will be opened right after being set as a trusted port.

Example：

Set port ethernet 1/5 of the switch as a trusted port

Switch(Config)#in e1/5

Switch(Config-if-ethernet 1/5)# anti-arpscan trust port

15.3.5 anti-arpscan trust ip

Command：anti-arpscan trust ip <ip-address [<netmask>]>

no anti-arpscan trust ip <ip-address [<netmask>]>

Function ： Configure trusted IP;" no anti-arpscan trust ip <ip-address [<netmask>]>"command reset the IP to non-trustful IP.

Parameters：Net mask of the IP

Default Settings：By default all the IP are non-trustful. Default mask is 255.255.255.255

Command Mode：Global configuration mode

User Guide：If a port is configured as a trusted port, then the ARP scanning prevention function will not deal with this port, even if the rate of received ARP messages exceeds the set threshold, this port will not be closed. If the port is already closed by ARP scanning prevention, its traffic will be recovered right immediately.

Example：

Set 192.168.1.100/24 as trusted IP

Switch(Config)#anti-arpscan trust ip 192.168.1.100 255.255.255.0

15.3.6 anti-arpscan recovery enable

Command：anti-arpscan recovery enable

no anti-arpscan recovery enable

Function：Enable the automatic recovery function, “no anti-arpscan recovery enable” command will disable the function.

Parameters：None

Default Settings：Enable the automatic recovery function

Command Mode：Global configuration mode

User Guide：If the users want the normal state to be recovered after a while the port is closed or the IP is disabled, they can configure this function.

Example：

Enable the automatic recovery function of the switch

Switch(Config)#anti-arpscan recovery enable

15.3.7 anti-arpscan recovery time

Command：anti-arpscan recovery time <*seconds*>

no anti-arpscan recovery time

Function：Configure automatic recovery time; “no anti-arpscan recovery time” command resets the automatic recovery time to default value.

Parameters：automatic recovery time, in second ranging from 5 to 86400

Default Settings：300 seconds

Command Mode：Global configuration mode

User Guide: Automatic recovery function should be enabled first.

Example：

Set the automatic recovery time as 3600 seconds

Switch(Config)#anti-arpscan recovery time 3600

15.3.8 anti-arpscan log enable

Command：anti-arpscan log enable

no anti-arpscan log enable

Function：Enable ARP scanning prevention log function;” no anti-arpscan log enable” command will disable this function.

Parameters：None.

Default Settings：Enable ARP scanning prevention log function

Command Mode：Global configuration mode

User Guide: After enabling ARP scanning prevention log function, users can check the detailed information of ports being closed or automatically recovered by ARP scanning prevention or IP being disabled and recovered by ARP scanning prevention. The level of the log is “Warning”.

Example：

Enable ARP scanning prevention log function of the switch

Switch(Config)#anti-arpscan log enable

15.3.9 anti-arpscan trap enable

Command：**anti-arpscan trap enable**

no anti-arpscan trap enable

Function：Enable ARP scanning prevention SNMP Trap function;” no anti-arpscan trap enable” command disable ARP scanning prevention SNMP Trap function.

Parameters：None.

Default Settings：Disable ARP scanning prevention SNMP Trap function

Command Mode：Global configuration mode

User Guide: After enabling ARP scanning prevention SNMP Trap function, users will receive Trap message whenever a port is closed or recovered by ARP scanning prevention, and whenever IP t is closed or recovered by ARP scanning prevention

Example：

Enable ARP scanning prevention SNMP Trap function of the switch

Switch(Config)#anti-arpscan trap enable

15.3.10 show anti-arpscan

Command：**show anti-arpscan [trust <ip | port | supertrust-port> |prohibited <ip | port>]**

Function：Display the operation information of ARP scanning prevention function

Parameters：None.

Default Settings: Display every port to tell whether it is a trusted port and whether it is closed. If the port is closed, then display how long it has been closed. Display all the trusted IP and disabled IP.

Command Mode：Admin Mode

User Guide：Use “show anti-arpscan trust port” if users only want to check trusted ports.

The reset follow the same rule.

Example：

Check the operating state of ARP scanning prevention function after enabling it.

Switch(Config)#show anti-arpscan

Total port: 36

Name	Port-property	beShut	shutTime(seconds)
Ethernet1/1	untrust	N	0
Ethernet1/2	untrust	N	0
Ethernet1/3	untrust	N	0
Ethernet1/4	untrust	N	0
Ethernet1/5	untrust	N	0
Ethernet1/6	untrust	N	0
Ethernet1/7	untrust	N	0
Ethernet1/8	untrust	N	0
Ethernet1/9	untrust	N	0
Ethernet1/10	untrust	N	0
Ethernet1/11	untrust	N	0
Ethernet1/12	untrust	N	0
Ethernet4/1	untrust	N	0
Ethernet4/2	untrust	N	0
Ethernet4/3	untrust	N	0
Ethernet4/4	trust	N	0
Ethernet4/5	untrust	N	0
Ethernet4/6	supertrust	N	0
Ethernet4/7	untrust	Y	30
Ethernet4/8	trust	N	0
Ethernet4/9	untrust	N	0
Ethernet4/10	untrust	N	0
Ethernet4/11	untrust	N	0
Ethernet4/12	untrust	N	0
Ethernet4/13	untrust	N	0
Ethernet4/14	untrust	N	0
Ethernet4/15	untrust	N	0
Ethernet4/16	untrust	N	0
Ethernet4/17	untrust	N	0
Ethernet4/18	untrust	N	0
Ethernet4/19	untrust	N	0

Ethernet4/20	untrust	N	0
Ethernet4/21	untrust	N	0
Ethernet4/22	untrust	N	0
Ethernet4/23	untrust	N	0
Ethernet4/24	untrust	N	0

Prohibited IP:

IP	shutTime(seconds)
1.1.1.2	132

Trust IP:

192.168.99.5	255.255.255.255
192.168.99.6	255.255.255.255
192.168.99.7	255.255.0.0

15.3.11 debug anti-arpscan

Command：debug anti-arpscan <port | ip>

no debug anti-arpscan <port | ip>

Function：Enable the debug switch of ARP scanning prevention;" no debug anti-arpscan <port | ip>" command disables the switch.

Parameters：None.

Default Settings: Disable the debug switch of ARP scanning prevention

Command Mode：Admin Mode

User Guide：After enabling debug switch of ARP scanning prevention users can check corresponding debug information or enable the port-based or IP-based debug switch separately whenever a port is closed by ARP scanning prevention or recovered automatically, and whenever IP t is closed or recovered .

Example：

Enable ARP scanning prevention function of the switch

Switch(Config)#debug anti-arpscan

15.4 ARP Scanning Prevention Typical Examples

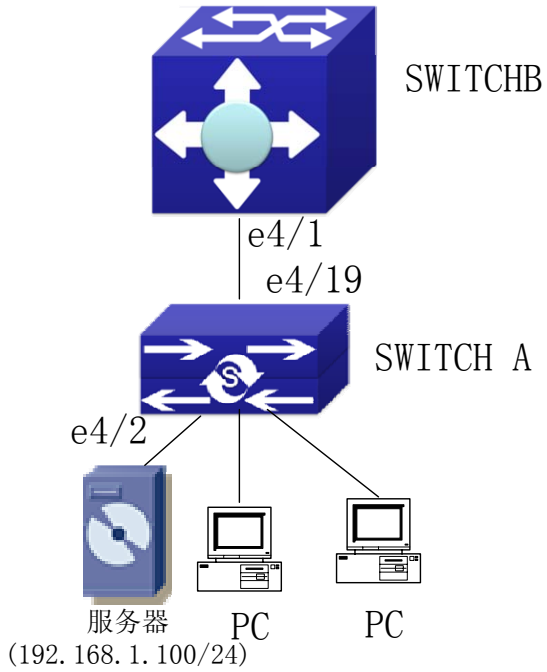


Fig 15-1 ARP scanning prevention typical configuration example

In the network topology above, port e4/1 of SWITCH B is connected to port e4/19 of SWITCH A, the port e4/2 of SWITCH A is connected to file server (IP address is 192.168.1.100/24), and all the other ports of SWITCH A are connected to common PC. The following configuration can prevent ARP scanning effectively without affecting the normal operation of the system.

SWITCH A configuration task sequence:

SwitchA(config)#anti-arpscan enable

SwitchA(config)#anti-arpscan recovery time 3600

SwitchA(config)#anti-arpscan trust ip 192.168.1.100 255.255.255.0

SwitchA(config)#in e4/2

SwitchA (Config-If-Ethernet4/2)#anti-arpscan trust port

SwitchA (Config-If-Ethernet4/2)#ex

SwitchA(config)#in e4/19

SwitchA (Config-If-Ethernet4/19)#anti-arpscan trust supertrust-port

Switch A(Config-If-Ethernet4/19)#ex

SWITCH B configuration task sequence:

Switch B(Config)# anti-arpscan enable

SwitchB(config)#in e4/1

SwitchB (Config-If-Ethernet4/2)#anti-arpscan trust port
SwitchB (Config-If-Ethernet4/2)ex

15.5 ARP Scanning Prevention Troubleshooting Help

ARP scanning prevention is disabled by default. After enabling ARP scanning prevention, users can enable the debug switch, “debug anti-arpscan”, to view debug information.

If the state of a port is showed as not closed when using “show anti-arpscan”, it means that the port is not closed by the ARP scanning prevention function. If the port is closed by other modules, users can check it with “show interface”.

The max number of IP that can be disabled by IP-based ARP scanning prevention is 64. If the limit is exceeded, users will see a prompt. Other modules can also disable IP, since the max number of IP that can be disabled by the switch is 256, if this limit is exceeded, a prompt will also be returned.

Chapter 16 Prevent ARP, ND Spoofing Configuration

16.1 Overview

16.1.1 ARP (Address Resolution Protocol)

Generally speaking, ARP (RFC-826) protocol is mainly responsible of mapping IP address to relevant 48-bit physical address, that is Mac address, for instance, IP address is 192.168.0.1, network card Mac address is 00-03-0F-FD-1D-2B. What the whole mapping process is that a host computer send broadcast data package involving IP address information of destination host computer, ARP request, and then the destination host computer send a data package involving its IP address and Mac address to the host, so two host computers can exchange data by MAC address.

16.1.2 ARP Spoofing

In terms of ARP Protocol design, to reduce redundant ARP data communication on networks, even though a host computer receives an ARP reply which is not requested by itself, it will also insert an entry to its ARP cache table, so it creates a possibility of “ARP spoofing”. If the hacker wants to snoop the communication between two host computers in the same network (even if are connected by the switches), it sends an ARP reply packet to two hosts separately, and make them misunderstand MAC address of the other side as the hacker host MAC address. In this way, the direct communication is actually communicated indirectly among the hacker host computer. The hackers not only obtain communication information they need, but also only need to modify some information in data packet and forward successfully. In this sniff way, the hacker host computer doesn’t need to configure intermix mode of network card, that is because the data packet between two communication sides are sent to hacker host computer on physical layer, which works as a relay.

16.1.3 How to prevent void ARP/ND Spoofing for our Layer 3 Switch

There are many sniff, monitor and attack behaviors based on ARP protocol in networks, and most of attack behaviors are based on ARP spoofing, so it is very important to prevent ARP spoofing. ARP spoofing accesses normal network environment by counterfeiting legal IP address firstly, and sends a great deal of counterfeited ARP application packets to switches, after switches learn these packets, they will cover previously corrected IP, mapping of MAC address, and then some corrected IP, MAC address mapping are modified to correspondence relationship configured by attack packets so that the switch makes mistake on transfer packets, and takes an effect on the whole network. Or the switches are made used of by vicious attackers, and they intercept and capture packets transferred by switches or attack other switches, host computers or network equipment.

What the essential method on preventing attack and spoofing switches based on ARP in networks is to disable switch automatic update function; the cheater can't modify corrected MAC address in order to avoid wrong packets transfer and can't obtain other information. At one time, it doesn't interrupt the automatic learning function of ARP and ND. Thus it prevents ARP spoofing and attack to a great extent.

ND is neighbor discovering protocol in IPv6 protocol, and it's similar to ARP on operation principle, therefore we do in the same way as preventing ARP spoofing to prevent ND spoofing and attack.

16.2 Prevent ARP, ND Spoofing configuration

16.2.1 Prevent ARP, ND Spoofing Configuration Task List

The steps of preventing ARP, ND spoofing configuration as below:

1. Disable ARP, ND automatic update function
2. Disable ARP, ND automatic learning function
3. changing dynamic ARP, ND to static ARP, ND
4. Clear dynamic ARP, ND

1. Disable ARP, ND automatic update function

Command	Explanation
Admin Mode and Interface Mode	

ip arp-security updateprotect **no ip arp-security updateprotect** **ipv6 nd-security updateprotect** **no ipv6 nd-security updateprotect**	Disable and enable ARP, Nd automatic update function

2. Disable ARP, ND automatic learning function

Command	Explanation
Admin mode and Interface Mode	
ip arp-security learnprotect **no Ip arp-security learnprotect** **ipv6 nd-security learnprotect** **no ipv6 nd-security learnprotect**	Disable and enable ARP, ND automatic learning function

3. Function on changing dynamic ARP, ND to static ARP, ND

Command	Explanation
Admin Mode and Interface Mode	
ip arp-security convert **ipv6 nd-security convert**	Change dynamic ARP, ND to static ARP, ND

4. Clear dynamic ARP, ND

Command	Explanation
Admin Mode and Interface Mode	
clear ip arp dynamic **clear ipv6 nd dynamic**	Clear dynamic ARP, ND

16.3 Commands For Preventing ARP, ND Spoofing

16.3.1 ip arp-security updateprotect

Command：ip arp-security updateprotect

no ip arp-security updateprotect

Function： Forbid ARP automatic learning function of IPv4 Version, the "no ip arp-security updateprotect " command re-enables ARP automatic learning function.

Parameter： None

Default： Learn ARP and update normally

Command Mode： Global Mode/ Interface configuration

Example：Switch(Config-if-Vlan1)# ip arp-security updateprotect
Switch(Config)# ip arp-security updateprotect

16.3.2 ipv6 nd-security updateprotect

Command：ipv6 nd-security updateprotect
no ipv6 nd-security updateprotect
Function： Forbid ND automatic learning function of IPv6 Version, the “no ipv6 nd-security updateprotect ” command re-enables ND automatic learning function.
Parameter： None
Default： Learn ND and update normally
Command Mode： Global Mode/ Interface configuration
Example：Switch(Config-if-Vlan1)#ipv6 nd -security updateprotect
Switch(Config)#ipv6 nd -security updateprotect

16.3.3 ip arp-security learnprotect

Command：ip arp-security learnprotect
no ip arp-security learnprotect
Function： Forbid ARP automatic learning function of IPv4 Version, the “no ip arp-security learning ” command re-enables ARP automatic learning function.
Parameter： None
Default： Learn ARP and update normally
Command Mode： Global Mode/ Interface configuration
Example：Switch(Config-if-Vlan1)# ip arp-security learnprotect
Switch(Config)# ip arp-security learnprotect

16.3.4 ipv6 nd learnprotect

Command：ipv6 nd-security learnprotect
no ipv6 nd-security learnprotect
Function：Forbid ND automatic learning function of IPv6 Version, the “no ipv6 nd-security learning ” command re-enables ND automatic learning function.
Parameter： None
Default： Learn ND and update normally
Command Mode：Global Mode/ Interface configuration

Example：Switch(Config-if-Vlan1)#ipv6 nd -security learnprotect

Switch(Config)#ipv6 nd -security learnprotect

16.3.5 ip arp-security convert

Command：ip arp-security convert

Function： Change all of dynamic arp to static arp

Parameter： None

Command Mode：Global Mode/ Interface configuration

Example：Switch(Config-if-Vlan1)# ip arp -security convert

Switch(Config)# ip arp -security convert

16.3.6 ipv6 nd-security convert

Command：ipv6 nd-security convert

Function： Change all of dynamic nd to static nd

Parameter： None

Command Mode： Global Mode/ Interface Configuration

Example：Switch(Config-if-Vlan1)#ipv6 nd -security convert

Switch(Config)#ipv6 nd -security conver

16.3.7 clear ip arp dynamic

Command：clear ip arp dynamic

Function： Clear all of dynamic arp on interface

Parameter： None

Command Mode：Interface Configuration

Example：Switch(Config-if-Vlan1)#clear ip arp dynamic

16.3.8 clear ipv6 nd dynamic

Command：clear ipv6 nd dynamic

Function： Clear all of dynamic nd on interface.

Parameter： None

Command mode： Interface Configuration

Example：Switch(Config-if-Vlan1)#clear ipv6 nd dynamic

16.4 Prevent ARP, ND Spoofing Example

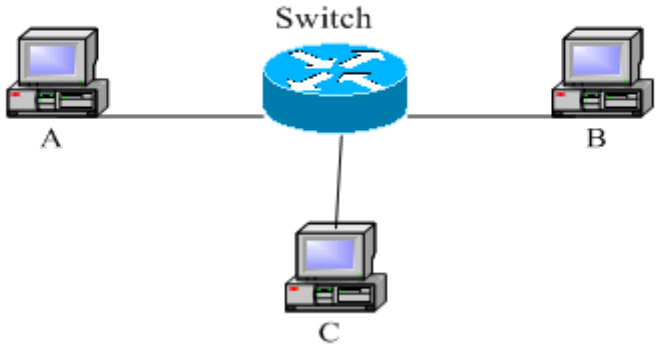


Fig 16-1 Prevent ARP ,ND Spoofing

Equipment Explanation

Equipment	Configuration	Quality
switch	IP:192.168.2.4; IP:192.168.1.4; mac: 04-04-04-04-04-04	1
A	IP:192.168.2.1; mac: 01-01-01-01-01-01	1
B	IP:192.168.1.2; mac: 02-02-02-02-02-02	1
C	IP:192.168.2.3; mac: 03-03-03-03-03-03	some

There is a normal communication between B and C on above diagram. A wants switch to forward packets sent by B to itself, so need switch sends the packets transfer from B to A. firstly A sends ARP reply package to switch, format is: 192.168.2.3, 01-01-01-01-01-01, mapping its MAC address to C's IP, so the switch changes IP address when it updates ARP list.,then data packet of 192.168.2.3 is transferred to 01-01-01-01-01-01 address (A MAC address).

In further, A transfers its received packets to C by modifying source address and destination address, the mutual communicated data between B and C are received by A unconsciously. Because the ARP list is update timely, another task for A is to continuously send ARP reply packet, and refreshes switch ARP list.

So it is very important to protect ARP list, configure to forbid ARP learning command in stable environment, and then change all dynamic ARP to static ARP, the learned ARP will not be refreshed, and protect for users.

```
Switch#config
Switch(config)#ip arp-security learnprotect
Switch(config)#ip arp-security convert
```

If the environment changing, it enable to forbid ARP refresh, once it learns ARP

property, it wont be refreshed by new ARP reply package, and protect use data from sniffing.

```
Switch#config
Switch(config)#ip arp-security updateprotect
```

Chapter 17 Routing Protocol

17.1 Routing Protocol Overview

To communicate with a remote host over the Internet, a host must choose a proper route via a set of routers or Layer3 switches.

Both routers and layer3 switches calculate the route using CPU, the difference is that layer3 switch adds the calculated route to the switch chip and forward by the chip at wire speed, while the router always store the calculated route in the route table or route buffer, and data forwarding is performed by the CPU. For this reason, although both routers and switches can perform route selection, layer3 switches have great advantage over routers in data forwarding. The following describes basic principle and methods used in layer3 switch route selection.

In route selection, the responsibility of each layer3 switch is to select a proper midway route according to the destination of the package received; and send the package to the next layer3 switch until the last layer3 switch in the route send the package to the destination host. A route is the path selected by each layer3 switch to pass the package to the next layer3 switch. Route can be grouped into direct route, static route and dynamic route.

Direct route refer to the path directly connects to the layer3 switch, and can be obtained with no calculation.

Static route is the manually specified path to a network or a host; static route cannot be changed freely. The advantage of static route is simple and consistent, and it can limit illegal route modification, and is convenient for load balance and route backup. However, as this is set manually, it is not suitable for mid- or large-scale networks for the route in such conditions are too huge and complex.

Dynamic route is the path to a network or a host calculated by the layer3 switch according to the routing protocols enabled. If the next hop layer3 switch in the path is not reachable, layer3 switch will automatically discard the path to that next hop layer3 switch and choose the path through other layer3 switches.

There are two dynamic routing protocols: Interior Gateway Protocol (IGP) and Exterior Gateway protocol (EGP). IGP is the protocol used to calculate the route to a destination inside an autonomous system. IGP supported by ES4626/ES4650 switch include RIP and OSPF, RIP and OSRF can be configured according to the requirement. ES4626/ES4650 switch supports running several IGP dynamic routing protocols at the

same time. Or, other dynamic routing protocols and static route can be introduced to a dynamic routing protocol, so that multiple routing protocols can be associated.

EGP is used to exchange routing information among different autonomous systems, such as BGP protocol. EGP supported by ES4626/ES4650 switch include BGP-4, BGP-4+..

17.1.1 Routing Table

As mentioned before, layer3 switch is mainly used to establish the route from the current layer3 switch to a network or a host, and to forward packages according to the route. Each layer3 switch has its own route table containing all routes used by that switch. Each route entry in the route table specifies the physical port should be used for forwarding package to reach a destination host or the next hop layer3 switch to the host.

The route table mainly consists of the following:

Destination address: used to identify the destination address or destination network of an IP package.

Network mask: used together with destination address to identify the destination host or the network the layer3 switch resides. Network mask consists of several consecutive binary 1's, and usually in the format of dotted decimal (an address consists of 1 to 4 255’s.) When “AND” the destination address with network mask, we can get the network address for the destination host or the network the layer3 switch resides. For example, the network address of a host or the segment the layer3 switch resides with a destination address of 200.1.1.1 and mask 255.255.255.0 is 200.1.1.0..

Output interface: specify the interface of layer3 switch to forward IP packages.

IP address of the next layer3 switch (next hop): specify the next layer3 switch the IP package will pass.

Route entry priority: There may be several different next hop routes leading to the same destination. Those routes may be discovered by different dynamic routing protocols or static routes manually configured. The entry with the highest priority (smallest value) becomes the current best route. The user can configure several routes of different priority to the same destination; layer3 switch will choose one route for IP package forwarding according to the priority order.

To avoid too large route table, a default route can be set. Once route table lookup fails, the default route will be chosen for forwarding packages.

The table below describes the routing protocols supported by ES4626/ES4650 switch and the default route lookup priority value.

Routing Protocols or route type	Default priority value

Direct route	0
OSPF	110
Static route	1
RIP	120
OSPF ASE	150
IBGP	200
EBGP	20
Unknown route	255

17.2 IP Routing Policy

17.2.1 Introduction To Routing Policy

Some policies have to be applied when the router publishing and receiving routing messages so to filter routing messages, such as only receiving or publishing routing messages meets the specified conditions. A routing protocol maybe need redistribute other routing messages found by other protocols such as OSPF so to increase its own routing knowledge; when the router redistributing routing messages from other routing protocols there may be only part of the qualified routing messages is needed, and some properties may have to be configured to suit this protocol.

To achieve routing policy, first we have to define the characteristics of the routing messages to be applied with routing policies, namely define a group matching rules. We can configure by different properties in the routing messages such as destination address, the router address publishing the routing messages. The matching rules can be previously configured to be applied in the routing publishing, receiving and distributing policies.

Five filters are provided in ES4626/ES4650 switch: route-map, acl, as-path, community-list and ip-prefix for use. We will introduce each filter in following sections:

1. route-map

For matching certain properties of the specified routing information and setting some routing properties when the conditions are fulfilled.

Route-map is for controlling and changing the routing messages while also controlling the redistribution among routes. A route-map consists of a series of match and set commands in which the match command specifies the conditions required matching, and the set command specifies the actions to be taken when matches. The route-map is also for controlling route publishing among different route process. It can also used on policy routing which select different routes for the messages other than the shortest route.

A group matches and set clauses make up a node. A route-map may consist of several nodes each of which is a unit for matching test. We match among nodes with by sequence-number. Match clauses define matching rules. The matching objects are some properties of routing messages. Different match clause in the same node is “and” relation logically, which means the matching test of a node, will not be passed until conditions in its entire match clause are matched. Set clause specifies actions, namely configure some properties of routing messages after the matching test is passed.

Different nodes in a route-map is an “or” relation logically. The system checks each node of the route-map in turn and once certain node test is passed the route-map test will be passed without taking the next node test.

2. access control list(acl)

ACL (Access Control Lists) is a data packet filter mechanism in the switch which is by permitting or denying certain data packet transmtting out from or into the network, the switch controls the network access and secure the network service. Users can establish a group of rules by certain messages in the packet, in which each rule to be applied on certain amount of matching messages: permit or deny. The users can apply these rules to the entrance or exit of specified switch, with which data stream in certain direction on certain port would have to follow the specified ACL rules in-and-out the switch. Please refer to chapter “ACL Configuration”.

3. Ip-prefix list

The ip-prefix list acts similarly to acl while more flexible and more understandable. The match object of ip-prefix is the destination address messages field of routing messages when applied in routing messages filtering.

An ip-prefix is identified by prefix list name. Each prefix list may contain multiple items, each of which specifies a matching range of a network prefix type and identifies with a sequence-number which specifies the matching check order of ip-prefix.

In the process of matching, the switch check each items identified by sequence-number in ascending order and the filter will be passed once certain items is matched(without checking rest items)

4. Autonomic system path information access-list as-path

The autonomic system path information access-list as-path is only used in BGP. In the BGP routing messages packet there is an autonomic system path field (in which autonomic system path the routing messages passes through is recorded). As-path is specially for specifying matching conditions for autonomic system path field.

As for relevant as-path configurations, please refer to the ip as-path command in BGP configuration.

5. community-list

Community-list is only for BGP. There is a community property field in the BGP

routing messages packet for identifying a community. The community list is for specifying matching conditions for Community-list field.

As for relevant Community-list configuration, please refer to the ip as-path command in BGP configuration

17.2.2 IP Routing Policy Configuration Task List

1、 Define route-map

2、Define the match clause in route-map

3、Define the set clause in route-map

4、Define address prefix list

1.Define route-map

Command	**Explanation**
Global mode	
route-map <*map_name*> {deny | permit} <*sequence_num*> **no route-map <*map_name*> [{deny | permit} <*sequence_num*>]**	Configure route-map; the **no route-map <*map_name*> [{deny | permit} <*sequence_num*>]** command deletes the route-map

2. Define the match clause in route-map

Command	**Explanation**
Route-map configuration mode	
match as-path <*list-name*> **no match as-path [<*list-name*>]**	Match the autonomous system as path access-list the BGP route passes through; the **no match as-path [<*list-name*>]** command deletes match condition
match community <*community-list-name* | **<*community-list-num* > [exact-match]** **no match community [<*community-list-name* |** **<*community-list-num* > [exact-match]]**	Match a community property access-list. The **no match community [<*community-list-name* |** ***community-list-num* > [exact-match]]** command deletes match condition

match interface <*interface-name* > no match interface [<*interface-name* >]	Match by ports; The **no match interface [<*interface-name* >]** command deletes match condition
match ip <address | next-hop> <*ip-acl-name* | *ip-acl-num* | prefix-list *list-name*> no match ip <address | next-hop> [<*ip-acl-name* | *ip-acl-num* | prefix-list [*list-name*]>]	Match the address or next-hop; The **no match ip <address | next-hop> [<*ip-acl-name* | *ip-acl-num* | prefix-list [*list-name*]>]** command deletes match condition
match metric <*metric-val* > no match metric [<*metric-val* >]	Match the routing metric value; The **no match metric [<*metric-val* >]** command deletes match condition
match origin <egp | igp | incomplete > no match origin [<egp | igp | incomplete >]	Match the route origin; The **no match origin [<egp | igp | incomplete >]** command deletes match condition
match route-type external <type-1 | type-2 > no match route-type external [<type-1 | type-2 >]	Match the route type; The **no match route-type external [<type-1 | type-2 >]** command deletes match condition
match tag <*tag-val* > no match tag [<*tag-val* >]	Match the route tag; The **no match tag [<*tag-val* >]** command deletes match condition

3. Define the match clause in route-map

Command	**Explanation**
Route-map configuration mode	

set aggregator as <*as-number*> <*ip_addr*> **no set aggregator as [<*as-number*> <*ip_addr*>]**	Distribute an AS No. for BGP aggregator; The **no set aggregator as [<*as-number*> <*ip_addr*>]** command deletes the configuration
set as-path prepend <*as-num*> **no set as-path prepend [<*as-num*>]**	Add a specified AS No. before the BGP routing messages as-path series; The **no set as-path prepend [<*as-num*>]** command deletes the configuration
set atomic-aggregate **no set atomic-aggregate**	Configure the BGP atomic aggregate property; The **no set atomic-aggregate** command deletes the configuration
set comm-list <*community-list-name* | ***community-list-num* > delete** **no set comm-list <*community-list-name* |** ***community-list-num* > delete**	Delete BGP community list value; The **no set comm-list <*community-list-name* | *community-list-num* > delete** command deletes the configuration
set community [*AA:NN*] [internet] [local-AS] **[no-advertise] [no-export] [none] [additive]** **no set community [*AA:NN*] [internet] [local-AS]** **[no-advertise] [no-export] [none] [additive]**	Configure BGP community list value; The **no set community [*AA:NN*] [internet] [local-AS] [no-advertise] [no-export] [none] [additive]** command deletes the configuration

set extcommunity <rt | soo> <*AA:NN*> **no set extcommunity <rt | soo> [<*AA:NN*>]**	Configure BGP extended community list property; The **no set extcommunity <rt | soo> [<*AA:NN*>]** command deletes the configuration
set ip next-hop <*ip_addr*> **no set ip next-hop [<*ip_addr*>]**	Set next-hop IP address; The **no set ip next-hop [<*ip_addr*>]** command deletes the configuration
set local-preference <*pre_val*> **no set local-preference [<*pre_val*>]**	Set local preference; The **no set local-preference [<*pre_val*>]** command deletes the configuration
set metric < +/- *metric_val* | *metric_val*> **no set metric [+/- *metric_val* | *metric_val*]**	Set routing metric value; The **no set metric [+/- *metric_val* | *metric_val*]** command deletes the configuration
set metric-type <type-1 | type-2> **no set metric-type [<type-1 | type-2>]**	Set OSPF metric type; The **no set metric-type [<type-1 | type-2>]** command deletes the configuration
set origin <egp | igp | incomplete > **no set origin [<egp | igp | incomplete >]**	Set BGP routing origin; The **no set origin [<egp | igp | incomplete >]** command deletes the configuration
set originator-id <*ip_addr*> **no set originator-id [<*ip_addr*>]**	Set routing originator ID; The **no set originator-id [<*ip_addr*>]** command deletes the configuration
set tag <*tag_val*> **no set tag [<*tag_val*>]**	Set OSPF routing tag value; The **no set tag [<*tag_val*>]** command deletes the configuration

set vpnv4 next-hop <*ip_addr*> **no set vpnv4 next-hop [<*ip_addr*>]**	Set BGP VPNv4 next-hop address; the **no set vpnv4 next-hop [<*ip_addr*>]** command deletes the configuration
set weight < *weight_val*> **no set weight [< *weight_val*>]**	Set BGP routing weight; The **no set weight [< *weight_val*>]** command deletes the configuration

4. Define address prefix list

Command	**Explanation**
Global mode	
ip prefix-list <*list_name*> description <*description*> **no ip prefix-list <*list_name*> description**	Describe the prefix list; The **no ip prefix-list <*list_name*> description** command deletes the configuration
ip prefix-list <*list_name*> [seq <*sequence_number*>] <deny | permit> < any | *ip_addr/mask_length* [ge *min_prefix_len*] [le *max_prefix_len*]> **no ip prefix-list <*list_name*> [seq <*sequence_number*>] [<deny | permit> < any | *ip_addr/mask_length* [ge *min_prefix_len*] [le *max_prefix_len*]>]**	Set the prefix list; The **no ip prefix-list <*list_name*> [seq <*sequence_number*>] [<deny | permit> < any | *ip_addr/mask_length* [ge *min_prefix_len*] [le *max_prefix_len*]>]** command deletes the configuration

17.2.3 Commands for Routing Policy

17.2.3.1 ip prefix-list description

Command: ip prefix-list <*list_name*> description <*description*>

no ip prefix-list <*list_name*> description

Function: Configure the description of the prefix-list. The "**no ip prefix-list <*list_name*>**" command deletes the description contents.

Parameter: <*list _name*> is the name of the prefix-list, **<*description* >**is the description contents

Default: None.

Command Mode: Global Mode

Usage Guide: This command can be used for explaining and describing a prefix-list, e.g. the application and attention matters of the prefix-list

Example:

Switch#config terminal

Switch(config)#ip prefix-list 3 description This list is used by BGP

17.2.3.2 ip prefix-list seq

Command: ip prefix-list <*list_name*> [seq <*sequence_number*>] <deny | permit> < any | *ip_addr/mask_length* [ge <*min_prefix_len*>] [le <*max_prefix_len*>]>

no ip prefix-list <*list_name*> [seq <*sequence_number*>] [<deny | permit> < any | *ip_addr/mask_length* [ge <*min_prefix_len*>] [le <*max_prefix_len*>]>]

Function: Configure the prefix-list. The "**no ip prefix-list <*list_name*> [seq <*sequence_number*>] [<deny | permit> < any | *ip_addr/mask_length* [ge <*min_prefix_len*>] [le <*max_prefix_len*>]>]**" command deletes the prefix-list.

Parameter: **<*list _name*>** is the name of prefix-list, "seq" shows the following parameters is the sequence number, **<*sequence_number*>** is the sequence number, "deny" means deny this route, "permit" means permit this route, "any" means adaptive to all packets with any prefix as well as any mask length, ***ip_addr/mask_length*** shows the prefix address (dotted decimal notation) and the length of mask, "ge" means greater than or equal to, **<*min_prefix_len*>** is the minimum length of prefix to be matched（ranging between 0～32）, "le" means less than or equal to, **<*max_prefix_len*>** is the maximum length of prefix to be matched（ranging between 0～32）.

Default: None.

Command Mode: Global Mode

Usage Guide: A prefix-list is identified by a prefix-list name. Each prefix-list may include several items each of which independently specifies a matching scope of network prefix-list type which is identified with a *sequence-number. sequence-number* specifies the sequence of matching check in the prefix-list. In the matching process the switch check in turn every items identified by "*sequence-number*" ascending. Once certain item obtains the conditions then the prefix-list filter is passed (without proceeding into the next item check)

Attentions should be paid on that at least one item match mode should be "permit" when more than one prefix-list items is defined. The deny mode items can be previously defined so to remove the unsuitable routing messages fast. However if all items are at deny mode then none of the routes would be able to pass the filter of this prefix-list. We here can define a "permit 0.0.0.0/0 ge 0 le 32" item after several defined "deny mode"

items so to grant the passage for all other routing messages.

Example:

Switch#config terminal

Switch(config)# ip prefix-list mylist seq 12345 deny 10.0.0.0/8 le 22 ge 14

17.2.3.3 match as-path

Command:match as-path <*list-name*>

no match as-path [<*list-name*>]

Function: Configure the AS path domain for matching the BGP routing messages. The "**no match as-path [<*list-name*>]**" delete this configuration.

Parameter<*list-name* > is the name of access-list

Command Mode: route-map mode

Usage Guide: This command matches the AS path domain of the BGP routing message following the rules specified in the as-path list. If the matching succeeded, then the "permit" or "deny" action in the route-map is performed.

Example:

Switch#config terminal

Switch(config)#route-map r1 permit 5

Switch(config-route-map)#match as-path 60

17.2.3.4 match community

Command: match community <*community-list-name* | *community-list-num* > [exact-match]

no match community [<*community-list-name* | *community-list-num* > [exact-match]]

Function: Configure the community attributes of BGP routing messages. The "**no match community [<*community-list-name* | *community-list-num* > [exact-match]]**" command deletes this configuration.

Parameter:<*community-list-name*> > is the name of the community-list, **<*community-list-num* >** is the community-list sequence number, ranging between 1～99（Standard ACL）or 100～199（Extended ACL）, **[exact-match]** means precise matching.

Command Mode: route-map mode

Usage Guide: This command matches the community attributes of the BGP routing message following the rules specified in the community list. If the matching succeeded, then the "permit" or "deny" action in the route-map is performed.

Example:

Switch#config terminal

Switch(config)#route-map r1 permit 5

Switch(config-route-map)#match community 100 exact-match

17.2.3.5 match interface

Command: match interface <*interface-name* >

no match interface [<*interface-name* >

Function: Configure to match the interfaces. The "**no match interface [<*interface-name* >**" deletes this configuration.

Parameter:"**<*interface-name* >**" is the name of the interface.

Command Mode: route-map mode

Usage Guide: This command matches according to the next-hop messages in the route. If the matching succeeded, then the "permit" or "deny" action in the route-map is performed. This command is only used in RIP and OSPF protocols.

Example:

Switch#config terminal

Switch(config)#route-map r1 permit 5

Switch(config-route-map)#match interface vlan1

17.2.3.6 match ip

Command: match ip <address | next-hop> <*ip-ACL-name* | *ip-ACL-num* | prefix-list *list-name*>

no match ip <address | next-hop> [<*ip-ACL-name* | *ip-ACL-num* | prefix-list *list-name*>]

Function: Configure the routing prefix or next-hop. The "**no match ip <address | next-hop> [<*ip-ACL-name* | *ip-ACL-num* | prefix-list *list-name*>]**" deletes this configuration.

Parameter: <address > means matching the routing prefix, **<next-hop>**means matching the routing next-hop, **<*ip-ACL-name* >** is the name of ip access-list, **<*ip-ACL-num* >** is the ip access-list sequence number, ranging between 1～199 or 1300～2699（extension scope）, **prefix-list** means the matching should follow the prefix-list rules, ***list-name*** is the name of prefix-list.

Command Mode: route-map mode

Usage Guide: This command matches according to the next-hop messages or routing prefix in the route. If the matching succeeded, then the "permit" or "deny" action in the route-map is performed.

Example:

Switch#config terminal

Switch(config)#route-map r1 permit 5

Switch(config-route-map)#match ip address prefix-list mylist

17.2.3.7 match metric

Command: match metric <*metric-val* >

no match metric [<*metric-val* >]

Function: Match the metric value in the routing message. The "**no match metric [<*metric-val* >]**" deletes the configuration.

Parameter: <*metric-val* > is the metric value, ranging between 0～4294967295.

Command Mode: route-map mode

Usage Guide: This command matches according to metric value in the route. If the matching succeeded, then the "permit" or "deny" action in the route-map is performed.

Example:

Switch#config terminal

Switch(config)#route-map r1 permit 5

Switch(config-route-map)#match metric 60

17.2.3.8 match origin

Command: match origin <egp | igp | incomplete >

no match origin <egp | igp | incomplete >

Function: Configure to matching with the origin of the BGP routing message. The "**no match origin <egp | igp | incomplete >**" deletes the configuration.

Parameter: egp means the route is learnt from the external gateway protocols, **IGP** means the route is learnt from the internal gateway protocols, **incomplete** means the route origin is uncertain.

Command Mode: route-map mode

Usage Guide: This command matches according to origin message in the BGP route. If the matching succeeded, then the "permit" or "deny" action in the route-map is performed.

Example:

Switch#config terminal

Switch(config)#route-map r1 permit 5

Switch(config-route-map)#match origin egp

17.2.3.9 match route-type

Command: match route-type external <type-1 | type-2 >

no match route-type external [<type-1 | type-2 >]

Function: Configure to matching with the route type of OSPF routing message. The "**no match route-type external [<type-1 | type-2 >]**" deletes the configuration.

Parameter: type-1 means match with the OSPF type 1 external route, **type-2** means

match with the OSPF type 1 external route.

Command Mode: route-map mode

Usage Guide: This command matches according to the type of OSPF routes （OSPF AS-external LSA type is either type 1or type 2）. If the matching succeeded, then the “permit” or “deny” action in the route-map is performed.

Example:

Switch#config terminal

Switch(config)#route-map r1 permit 5

Switch(config-route-map)#match route-type external type-1

17.2.3.10 match tag

Command: match tag <*tag-val* >

no match tag [<*tag-val* >]

Function: Configure to matching with the tag domain of the OSPF routing message. The “**no match tag [<*tag-val* >]**” deletes this configuration.

Parameter: <*tag-val* > is the tag value, ranging between 0～4294967295.

Command Mode: route-map mode

Usage Guide: This command matches according to the tag value in the OSPF route. If the matching succeeded, then the “permit” or “deny” action in the route-map is performed.

Example:

Switch#config terminal

Switch(config)#route-map r1 permit 5

Switch(config-route-map)#match tag 60

17.2.3.11 route-map

Command: route-map <*map_name*> {deny | permit} <*sequence_num*>

no route-map <*map_name*> [{deny | permit} <*sequence_num*>]

Function: Configure the route-map and entering the route-map mode. The “**no route-map <*map_name*> [{deny | permit} <*sequence_num*>]**” command deletes route-map.

Parameter: <*map_name*> is the name of route-map, **permit** sets route-map matching mode to permit mode, **deny** sets route-map matching mode to permit mode（**set** sub will not be executed under this mode）, **<*sequence_num*>** is the route-map sequence number, ranging between 1～65535.

Default: None

Command Mode: Global Mode

Usage Guide: A route-map may consist of several nodes each of which is a check unit.

The check sequence among nodes is identified by *sequence-number*. “permit” means the node filter will be passed if all match subs are obtained by current route and then further all the set sub of this node will be executed without entering the check in the next node; if the match subs can not be met, the proceed to the check in next node. Relation among different node should be “or”, namely one node check passed then the route filter is passed when the switch checks each node in turn in the route-map.

Attentions should be paid on that at least one node match mode should be “permit” when more than one node is defined. When a route-map is used for filtering routing messages, if certain routing message can not pass any node check, then it is considered denied by the route-map. If all nodes in the route-map are set to deny mode, then all routing message should not be able to pass that route-map.

Example:

Switch#config terminal

Switch(config)#route-map r1 permit 5

Switch(config-route-map)#match as-path 60

Switch(config-route-map)#set weight 30

17.2.3.12 set aggregator

Command: set aggregator as <*as-number*> <*ip_addr*>

no set aggregator as [<*as-number*> <*ip_addr*>]

Function: Assign an AS number for BGP aggregator. The “**no set aggregator as [<*as-number*> <*ip_addr*>]**” deletes this configuration.

Parameter: <*as-number* > is the AS number, **<*ip_addr*>** is the ip address of the aggregator shown in decimal notation.

Command Mode: route-map mode

Usage Guide: To use this command, one match clause should at first be defined.

Example:

Switch#config terminal

Switch(config)#route-map r1 permit 5

Switch(config-route-map)#set aggregator as 200 10.1.1.1

17.2.3.13 set as-path

Command: set as-path prepend <*as-num*>

no set as-path prepend [<*as-num*>]

Function: Add AS numbers in the AS path domain of the BGP routing message. The “**no set as-path prepend [<*as-num*>]**” command deletes this configuration.

Parameter: <*as-num* > is the AS number, circulating inputting several numbers is available.

Command Mode: route-map mode

Usage Guide: To add AS number in the As domain of the BGP, the AS path length should be lengthened so to affect the best neighbor path option. To use this command, one match clause should at first be defined.

Example:

Switch#config terminal

Switch(config)#route-map r1 permit 5

Switch(config-route-map)#set as-path prepend 200

17.2.3.14 set atomic-aggregate

Command: set atomic-aggregate

no set atomic-aggregate

Function: Configure the atomic aggregate attributes. The "**no set atomic-aggregate**" command deletes this configuration.

Parameter: None

Command Mode: route-map mode

Usage Guide: The BGP informs other BGP speaker by the atomic aggregate attributes. Local system selects a sub-specified route other than the more specified routes included in it. To use this command, one match clause should at first be defined.

Example:

Switch#config terminal

Switch(config)#route-map r1 permit 5

Switch(config-route-map)#set atomic-aggregate

17.2.3.15 set comm-list

Command: set comm-list <*community-list-name* | *community-list-num* > delete

no set comm-list <*community-list-name* | *community-list-num* > delete

Function: Configure to delete the community attributes from the inbound or outbound routing messages. The "**no set comm-list <*community-list-name* | *community-list-num* > delete**" command deletes the configuration.

Parameter: <*community-list-name* > is the name of community list, **<*community-list-num* >** is the sequence number of community list, ranging between 1～99（standard community list） or 100～199（extended community list）.

Command Mode: route-map mode

Usage Guide: .

Example:

Switch#config terminal

Switch(config)#route-map r1 permit 5

Switch(config-route-map)#set comm-list 100 delete

17.2.3.16 set community

Command: set community [*AA:NN*] [internet] [local-AS] [no-advertise] [no-export] [none] [additive]

no set community [*AA:NN*] [internet] [local-AS] [no-advertise] [no-export] [none] [additive]

Function: Configure the community attributes of the BGP routing message. The "**no set community [*AA:NN*] [internet] [local-AS] [no-advertise] [no-export] [none] [additive]**" command deletes this configuration.

Parameter: [*AA:NN*] is the community attribute value, **[internet]** is the internet scope, **[local-AS]** means this route do not announce outside the local AS (but can announce among the sub AS within the confederation), **[no-advertise]** means this route do not send to any neighbor, **[no-export]** means this route do not send to EBGP neighbors, **[none]** means delete the community attributes from the prefix of this route, **[additive]** means add following existing community attributes.

Command Mode: route-map mode

Usage Guide: To use this command, one match clause should at first be defined.

Example:

Switch#config terminal

Switch(config)#route-map r1 permit 5

Switch(config-route-map)#set community local-as additive

17.2.3.17 set extcommunity

Command: set extcommunity <rt | soo> <*AA:NN*>

no set extcommunity <rt | soo> [<*AA:NN*>]

Function: Configure the extended community attributes of the BGP routing message.

The "**no set extcommunity <rt | soo> [<*AA:NN*>]**" command deletes this configuration.

Parameter: *<rt>* is the route target, **<*soo*>** is the site of origin, **<*AA:NN*>** is the value of community attributes, amongst AA is AS number, NN is a random two byte number.

Command Mode: route-map mode

Usage Guide: To use this command, one match clause should at first be defined.

Example:

Switch#config terminal

Switch(config)#route-map r1 permit 5

Switch(config-route-map)#set extcommunity rt 100:10

17.2.3.18 set ip next-hop

Command: set ip next-hop <*ip_addr*>

no set ip next-hop [<*ip_addr*>]

Function: Configure the next-hop of the route. The "**no set ip next-hop [<*ip_addr*>]**" command deletes the configuration.

Parameter: <*ip_addr* > is the ip address of next-hop shown with dotted decimal notation.

Command Mode: route-map mode

Usage Guide:

Example:

Switch#config terminal

Switch(config)#route-map r1 permit 5

Switch(config-route-map)#set ip next-hop 10.2.2.2

17.2.3.19 set local-preference

Command: set local-preference <*pre_val*>

no set local-preference [<*pre_val*>]

Function: Configure the local priority of BGP route. The "**no set local-preference [<*pre_val*>]**" command deletes this configuration.

Parameter: <*pre_val* > is the value of local priority, ranging between 0～4294967295.

Command Mode: route-map mode

Usage Guide: The local priority attribute is the priority level of a route. A route with a higher local priority level when compared with other route of the same destination, will be more preferred than other route. The local priority validates only within this AS and will not be transported to EBGP neighbors. To use this command, one match clause should at first be defined.

Example:

Switch#config terminal

Switch(config)#route-map r1 permit 5

Switch(config-route-map)#set local-preference 60

17.2.3.20 set metric

Command: set metric < *+/- metric_val* | *metric_val*>

no set metric [*+/- metric_val* | *metric_val*]

Function: Configure the metric value of the route. The "**no set metric [*+/- metric_val* | *metric_val*]**" command deletes the configuration.

Parameter: <*metric_val* > is the metric value, ranging between 1～4294967295, +/- means plus or minus the set metric value.

Command Mode: route-map mode

Usage Guide: The metric value only affects the path option from external neighbors to

local AS. The less the metric value is the higher is the priority. Under normal circumstances only the path metric value of the neighbors of the same AS will be compared. To extend the comparison to the metric values of different neighbor path, the bgp always-compare-med command should be configured. To use this command, one match clause should at first be defined.

Example:

Switch#config terminal

Switch(config)#route-map r1 permit 5

Switch(config-route-map)#set metric +60

17.2.3.21 set metric-type

Command: set metric-type <type-1 | type-2>

no set metric-type [<type-1 | type-2>]

Function: Configure the metric type of the OSPF routing message. The "**no set metric-type [<type-1 | type-2>]**" command deletes this configuration.

Parameter: type-1 means matches the OSPS type 1 external route, **type-2** means matches the OSPS type 2 external route.

Command Mode: route-map mode

Usage Guide: To use this command, one match clause should at first be defined.

Example:

Switch#config terminal

Switch(config)#route-map r1 permit 5

Switch(config-route-map)#set metric-type type-1

17.2.3.22 set origin

Command: set origin <egp | igp | incomplete >

no set origin [<egp | igp | incomplete >]

Function: Configure the origin code of the BGP routing message. The "**no set origin [<egp | igp | incomplete >]**" command deletes this configuration.

Parameter: egp means the route is learnt from the external gateway protocols, **igp** means the route is learnt from the internal gateway protocols, **incomplete** means the route origin is uncertain.

Command Mode: route-map mode

Usage Guide: To use this command, one match clause should at first be defined.

Example:

Switch#config terminal

Switch(config)#route-map r1 permit 5

Switch(config-route-map)#set origin egp

17.2.3.23 set originator-id

Command: set originator-id <*ip_addr*>

no set originator-id [<*ip_addr*>]

Function: Configure the origin ip address of the BGP routing message. The "**no set originator-id [<*ip_addr*>]**" command deletes the configuration.

Parameter: <*ip_addr*> is the ip address of the route source shown by dotted decimal notation.

Command Mode: route-map mode

Usage Guide: To use this command, one match clause should at first be defined.

Example:

Switch#config terminal

Switch(config)#route-map r1 permit 5

Switch(config-route-map)#set originator-id 10.1.1.1

17.2.3.24 set tag

Command: set tag <*tag_val*>

no set tag [<*tag_val*>]

Function: Configure the tag domain of OSPF routing messages. The "**no set tag [<*tag_val*>]**" command deletes this configuration.

Parameter: <*tag-val* > is the tag value, ranging between 0～4294967295.

Command Mode: route-map mode

Usage Guide: There is a route-tag domain at the AS-external-LSA type LSA. The domain is normally identified by other routing protocols. To use this command, one match clause should at first be defined.

Example:

Switch#config terminal

Switch(config)#route-map r1 permit 5

Switch(config-route-map)#set tag 60

17.2.3.25 set vpnv4 next-hop

Command: set vpnv4 next-hop <*ip_addr*>

no set vpnv4 next-hop [<*ip_addr*>]

Function: Configure the next-hop of BGP VPNv4 routing message. The "**no set vpnv4 next-hop [<*ip_addr*>]**" command deletes the configuration.

Parameter: <*ip_addr*> is the next-hop ip address of VPNv4 route shown by dotted decimal notation.

Command Mode: route-map mode

Usage Guide: To use this command, one match clause should at first be defined.

Example:

Switch#config terminal

Switch(config)#route-map r1 permit 5

Switch(config-route-map)#set vpnv4 next-hop 10.1.1.1

17.2.3.26 set weight

Command: set weight <*weight_val*>

no set weight [<*weight_val*>]

Function: Configure the weight value of BGP routing message. The "**no set weight [<*weight_val*>]**" command deletes this configuration.

Parameter: <*weight_val*> is weight value, ranging between 0～4294967295

Command Mode: route-map mode

Usage Guide: Weight value is adopted to facilitate the best path option and validates only within the local switch. While there are several route to the same destination the one with higher priority is more preferred. To use this command, one match clause should at first be defined.

Example:

Switch#config terminal

Switch(config)#route-map r1 permit 5

Switch(config-route-map)#set weight 60

17.2.4 Configuration Examples

The figure below shows a network consisting of four Layer 3 switches. This example demonstrates how to set the BGP as-path properties through route-map. BGP protocol is applied among the Layer 3 switches. As for switchC, the network 192.68.11.0/24 can be reached through two paths in which one is AS-PATH 1 by IBGP (going through SwitchD), the other one is AS-PATH 2 by EBGP (going through SwitchB). BGP selects the shortest path, so AS-PATH 1 is the preferred path. If the path 2 is wished, which is through EBGP path, we can add two extra AS path numbers into the AS-PATH messages from SwitchA to SwitchD so as to change the determination SwitchC take to 192.68.11.0/24.

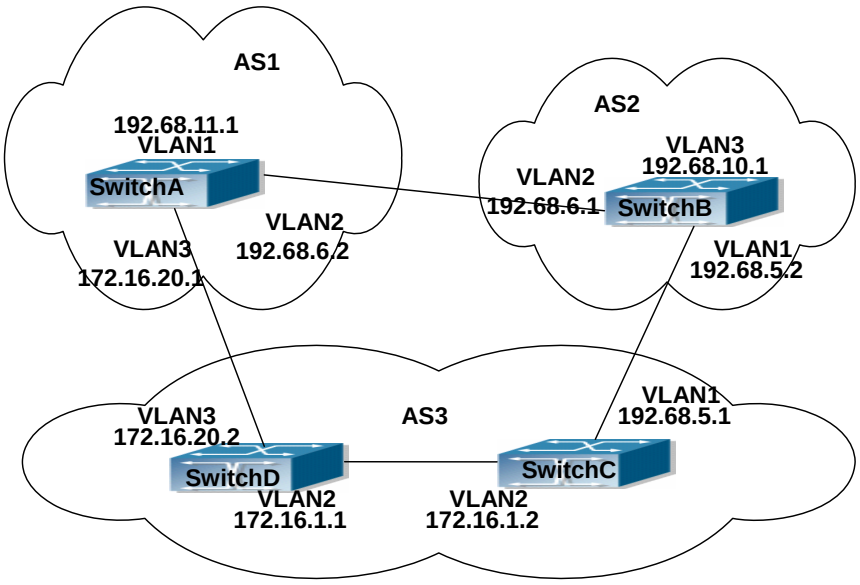


Fig 17-1 Policy routing Configuration

configuration procedure: (only SwitchA is listed,configurations for other switches are omitted.)

The configuration of Layer 3 switchA:

SwitchA#config

SwitchA (config) #router bgp 1

SwitchA (config-router)#network 192.68.11.0

SwitchA(config-router)#neighbor 172.16.20.2 remote-as 3

SwitchA(config-router)#neighbor 172.16.20.2 route-map AddAsNumbers out

SwitchA(config-router)#neighbor 192.68.6.1 remote-as 2

SwitchA(config-router)#exit

SwitchA(config)#route-map AddAsNumbers permit 10

SwitchA(config-route-map)#set as-path prepend 1 1

17.2.5 Troubleshooting

Faq: **The routing protocol could not achieve the routing messages study under normal protocol running state**

Troubleshooting: check following errors:

Each node of route-map should at least has one node is permit match mode. When the route map is used in routing messages filtering, the routing messages will be considered not pass the routing messages filtering if certain routing messages does not pass the filtering of any nodes. When all nodes are set to deny mode, all routing messages will not pass the filtering in this route-map.

Items in address prefix list should at least have one item set to permit mode. The deny mode items can be defined first to fast remove the unmatched routing messages, however if all the items are set to deny mode, any route will not be able to pass the filtering of this address prefix list. We can define a permit 0.0.0.0/0 le 32 item after several deny mode items are defined so to permit all other routing messages pass through. Only default route will be matched in less-equal 32 is not specified.

17.2.5.1 Commands for Monitor And Debug

17.2.5.1.1 show ip prefix-list <list-name>

Command: show ip prefix-list [<*list-name*> [<*ip_addr/len*> [first-match | longer] | seq <*sequence-number*>]]

Function: Show by prefix-list names.

Parameter: <*list-name*> is the name of prefix-list, **<*ip_addr/len*>** is the prefix ip address and the length of mask, **first-match** stands for the first route table matched with specified ip address, **longer** means longer prefix is required, **seq** means show by sequence number, **<*sequence-number*>** is the sequence number, ranging between 0～4294967295.

Default: None

Command Mode: all modes

Usage Guide: All prefix-list will be listed when no prefix-list name is specified.

Example:

```
Switch# #show ip prefix-list
ip prefix-list 1: 1 entries
    deny any
ip prefix-list mylist: 1 entries
    deny 1.1.1.1/8
Switch#show ip prefix-list mylist 1.1.1.1/8
    seq 5 deny 1.1.1.1/8 (hit count: 0, recount: 0)
```

Displayed information	Explanation
ip prefix-list mylist: 1 entries	Show a prefix-list named mylist which includes 1 instance.
seq 5 deny 1.1.1.1/8 (hit count: 0, recount: 0)	Show the prefix-list contents sequence numbered 5. hit count: 0 means being hit 0 time, recount: 0 means referred 0 time.

17.2.5.1.2 show ip prefix-list <detail | summary>

Command: show ip prefix-list [<detail | summary> [<*list-name*>]]

Function: Show the prefix-list contents.

Parameter: Detail means show detailed messages, **summary** means show summary messages, ***<list-name>*** is the name of prefix-list.

Default: None

Command Mode: all modes

Usage Guide: All prefix-lists will be shown if no prefix-list name is specified.

Example:

Switch#show ip prefix-list detail mylist

ip prefix-list mylist:

count: 2, range entries: 0, sequences: 5 - 10

deny 1.1.1.1/8 (hit count: 0, recount: 0)

permit 2.2.2.2/8 (hit count: 0, recount: 0)

Switch#show ip prefix-list summary mylist

ip prefix-list mylist:

count: 2, range entries: 0, sequences: 5 - 10

Displayed information	Explanation
ip prefix-list mylist:	Show the prefix-list named mylist
count: 2, range entries: 0, sequences: 5 -10	count: 2 means two prefix-list entries, sequences: 5-10 shows the sequence number, 5 is the starting sequence number, 10 is the last sequence number.
deny 1.1.1.1/8 (hit count: 0, recount: 0)	deny 1.1.1.1/8 is the detailed contents in the prefix-list entries, hit count: 0 means being hit 0 times, recount: 0 means being referred 0 times.

17.2.5.1.3 show route-map

Command: show route-map

Function: Show the content of route-map

Parameter: None

Default: None

Command Mode: all modes

Usage Guide:

Example:

Switch# show route-map

route-map a, deny, sequence 10

Match clauses:

as-path 60

Set clauses:

metric 10

Displayed information	Explanation
route-map a, deny, sequence 10	route-map a means the name of route map is a, deny means the deny mode, sequence 10 means the sequence number is 10
Match clauses:	Match sub
as-path 60	Detailed contents in the Match sub
Set clauses:	Set sub
metric 10	Detailed content in the Set clause

17.3 Static Route

17.3.1 Introduction to Static Route

As mentioned earlier, the static route is the manually specified path to a network or a host. Static route is simple and consistent, and can prevent illegal route modification, and is convenient for load balance and route backup. However, it also has its own defects. Static route, as its name indicates, is static, it won't modify the route automatically on network failure, and manual configuration is required on such occasions, therefore it is not suitable for mid and large-scale networks.

Static route is mainly used in the following two conditions: 1) in stable networks to reduce load of route selection and routing data streams. For example, static route can be used in route to STUB network. 2) For route backup, configure static route in the backup line, with a lower priority than the main line.

Static route and dynamic route can coexist; layer3 switch will choose the route with the highest priority according to the priority of routing protocols. At the same time, static route can be introduced (redistribute) in dynamic route, and change the priority of the static route introduced as required.

17.3.2 Introduction to Default Route

Default route is a kind of static route, which is used only when no matching route is found. In the route table, default route in is indicated by a destination address of 0.0.0.0 and a network mask of 0.0.0.0, too. If the route table does not have the destination of a package and has no default route configured, the package will be discarded, and an ICMP packet will be sent to the source address indicate the destination address or

network is unreachable.

17.3.3 Static Route Configuration Task List

1. Static route configuration
2. Default route configuration

1. static route configuration

Command	**Explanation**
Global mode	
ip route {<*ip-prefix*> <*mask*> | <*ip-prefix*>/<*prefix-length*>} {<*gateway-address*> | <*gateway-interface*>} [<*distance*>] **no ip route {<*ip-prefix*> <*mask*> | <*ip-prefix*>/<*prefix-length*>} [<*gateway-address*> | <*gateway-interface*>] [<*distance*>]**	Set static routing; the **no ip route {<*ip-prefix*> <*mask*> | <*ip-prefix*>/<*prefix-length*>} [<*gateway-address*> | <*gateway-interface*>] [<*distance*>]** command deletes a static route entry

2. VPN configuration

Command	**Explanation**
Global mode	
ip route vrf <*name*> {<*ip-prefix*> <*mask*>|<*ip-prefix/<prefix-length*>} {<*gateway-address*>|<*gateway-interface*>} [<*distance*>] **no ip route vrf <*name*> {<*ip-prefix*> <*mask*>|<*ip-prefix/<prefix-length*>} [<*gateway-address*>|<*gateway-interface*>] [<*distance*>]**	Configures static routing; the **no ip route vrf <*name*> {<*ip-prefix*> <*mask*>|<*ip-prefix/<prefix-length*>} [<*gateway-address*>|<*gateway-interface*>] [<*distance*>]** command deletes a static route entry

17.3.4 Commands for Static Route

17.3.4.1 ip route

Command:ip route {<*ip-prefix*> <*mask*> | <*ip-prefix*>/<*prefix-length*>} {<*gateway-address*> | <*gateway-interface*>} [<*distance*>]
no ip route {<*ip-prefix*> <*mask*> | <*ip-prefix*>/<*prefix-length*>} [<*gateway-address*> | <*gateway-interface*>] [<*distance*>]

Function: Configure the static route. The "**no ip route {*<ip-prefix>* *<mask>* | *<ip-prefix>*/*<prefix-length>*} [*<gateway-address>* | *<gateway-interface>*] [*<distance>*]**" command deletes the static route.

Parameter: The ***<ip-prefix>*** and ***<mask>*** are respectively destination IP address and subnet mask, shown in dotted decimal notation; ***<ip-prefix>*** and ***<prefix-length>*** are respectively the destination IP address and the length of prefix; ***<gateway-address>*** is the next-hop IP address shown in dotted decimal notation; ***<gateway-interface>*** is the next-hop interface, **< *distance* >** is the manage distance of route management, ranging between 1～255.

Default: The management distance of static routing is defaulted at 1.

Command Mode: Global Mode.

Usage Guide: When configuring the next-hop of static routing, both by specifying the next-hop IP address of the route data packet and the exit interface are available.

The default distance values of each route type in the layer 3 switch of our company are listed below:

Route Type	Distance Value
Direct Route	0
Static Route	1
OSPF	110
RIP	120
IBGP	200
EBGP	20

The direct route has the highest priority when each route management distance value remain unchanged and followed by static route, EBGP、OSPF、RIP、IBGP.

Example:

Example 1．Add a static route

Switch(config)#ip route 1.1.1.0 255.255.255.0 2.1.1.1

Example 2．Add default route

Switch(config)#ip route 0.0.0.0 0.0.0.0 2.2.2.1

17.3.4.2 show ip route

Command: show ip route [*<destination>*|*<destination >/<length>*|connected | static | rip| ospf | bgp | isis| kernel| statistics| database [connected | static | rip| ospf | bgp | isis| kernel] |fib [default|main|local]]

Function: Show the route table

Parameter: *<destination>* is the destination network address; ***<destination >/<length>*** is the destination network address plus the length of prefix**;** **connected** is direct route; **static** static route; **rip** is RIP route; **ospf** is OSPF route; **bgp** is BGP route; **isis** is ISIS

route; **kernel** is kernel route; **statistics** shows the number of routes; **database** route database; **fib** is kernel route table.

Command Mode: all modes

Usage Guide: Show all the contents in the route table including: route type, destination network, mask, next-hop address, interface, etc

Example:

Switch#show ip route fib

Codes: C - connected, S - static, R - RIP derived, O - OSPF derived

A - OSPF ASE, B - BGP derived

	Destination	Mask	Nexthop	Interface	Preference
C	2.2.2.0	255.255.255.0	0.0.0.0	vlan2	0
C	4.4.4.0	255.255.255.0	0.0.0.0	vlan4	0
S	6.6.6.0	255.255.255.0	9.9.9.9	vlan9	1
R	7.7.7.0	255.255.255.0	8.8.8.8	vlan8	120

Displayed information	Explanation
C –connected	Direct route, namely the segment directly connected with the layer 3 switch
S –static	Static route, the route manually configured by users
R - RIP derived	RIP route, acquired by layer 3 switch through the RIP protocol.
O - OSPF derived	OSPF route, acquired by layer 3 switch through the OSPF protocol
A- OSPF ASE	Route introduced by OSPF
B- BGP derived	BGP route, acquired by the BGP protocol.
Destination	Target network
Mask	Target network mask
Nexthop	Next-hop IP address
Interface	Next-hop pass-by layer 3 switch interfaces
Preference	Route priority. If other types of route to the target network exists, the kernel route will only shows those with high priority.

17.3.4.3 show ip route fib

Command: show ip route fib

Function: Show all the contents in the route table including: route type, destination network, mask, next-hop address, interface, etc.

Command Mode: all modes

Usage Guide: With show ip route command, contents about static route in the route table can be shown, including destination IP address, network mask and next-hop IP address or forwarding interfaces.

Example:

Switch#show ip route fib

Codes: C - connected, S - static, R - RIP derived, O - OSPF derived

A - OSPF ASE, B - BGP derived

	Destination	Mask	Nexthop	Interface	Pref
C	2.2.2.0	255.255.255.0	0.0.0.0	vlan1	0
S	6.6.6.0	255.255.255.0	2.2.2.9	vlan1	1

Among those message, S is static route with network address as 6.6.6.0、network mask as 255.255.255.0、next-hop address as 2.2.2.9 and Ethernet port vlan1 as its forwarding interface, of which the priority is 1

17.3.4.4 show ip route vrf

Command: show ip route vrf <*name*> [connected | static | rip| ospf | bgp | isis| kernel|statistics| database[connected | static | rip| ospf | bgp | isis|kernel]]

show ip route fib vrf <*name*> [default|main|local]

Function: Show the routing table

Parameter: <*name*> is the name of VPN route forwarding instances; **<*destination*>** is the destination network address; **<*destination* >/<*length*>**为 is the prefix-length plus destination network address**; connected** is direct routed; **static** is static route; **rip** is RIP route; **ospf** is OSPF route;**bgp** is BGP route; **isis** is ISIS route; **kernel** is kernel ; **statistics** shows the number of routes; **database** is the route database; **fib** is the kernel route table.

Command Mode: all modes

Usage Guide: Show VPN route table contents includingL route type, destination network, mask, next-hop, interface, etc.

17.3.4.5 ip route vrf

Command: ip route vrf <*name*> {<*ip-prefix*> <*mask*>|<*ip-prefix*/<*prefix-length*>} {<*gateway-address*>|<*gateway-interface*>} [<*distance*>]

no ip route vrf <*name*> {<*ip-prefix*> <*mask*>|<*ip-prefix*/<*prefix-length*>} [<*gateway-address*>|<*gateway-interface*>] [<*distance*>]

Function: <*name*> is the name of VPN route forwarding instances; **<*ip-prefix*>** and **<*mask*>** are respectively destination IP address and sub network mask shown in dotted decimal notation; **<*ip-prefix*>** and **<*prefix-length*>** are respectively destination IP

address and prefix length; ***<gateway-address>*** is the next-hop IP address show in dotted decimal notation; ***<gateway-interface>*** is the next-hop interface, ***< distance >*** is the route managing distance value ranging between 1～255.

Default: Default static route managing value is 1.

Command Mode: Global mode

Usage Guide: VPN route forwarding instances have to be successfully configured before using this command.

17.3.5 Configuration Examples

The figure shown below is a simple network consisting of three layer3 switches, the network mask for all switches and PC is 255.255.255.0. PC-A and PC-C are connected via the static route set in SwitchA and SwitchC; PC3 and PC-B are connected via the static route set in SwitchC to SwitchB; PC-B and PC-C is connected via the default route set in SwitchB.

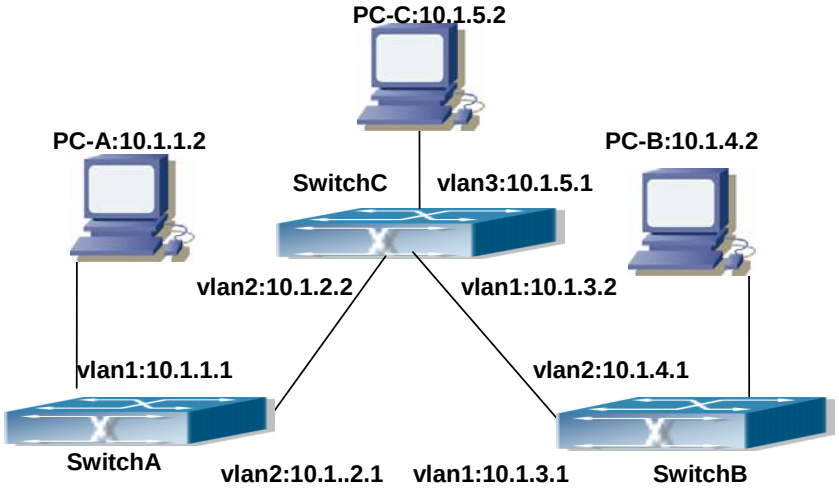


Fig 17-2 Static Route Configurations

Configuration steps:

Configuration of layer3 SwitchA

Switch#config

Switch (config) #ip route 10.1.5.0 255.255.255.0 10.1.2.2

Configuration of layer3 SwitchC

Switch#config

Next hop use the partner IP address

Switch(config)#ip route 10.1.1.0 255.255.255.0 10.1.2.1

Next hop use the partner IP address

Switch(config)#ip route 10.1.4.0 255.255.255.0 10.1.3.1
Configuration of layer3 SwitchB
Switch#config
Switch(config)#ip route 0.0.0.0 0.0.0.0 10.1.3.2
In this way, ping connectivity can be established between PC-A and PC-C, and PC-B and PC-C

17.4 RIP

17.4.1 Introduction to RIP

RIP is first introduced in ARPANET, this is a protocol dedicated to small, simple networks. RIP is a distance vector routing protocol based on the Bellman-Ford algorithm. Network devices running vector routing protocol send 2 kind of information to the neighboring devices regularly:

• Number of hops to reach the destination network, or metrics to use or number of networks to pass.

• What is the next hop, or the director (vector) to use to reach the destination network.

The distance vector Layer 3 switch send all their route selecting tables to the neighbor layer3 switches at regular interval. A layer3 switch will build their own route selecting information table based on the information received from the neighbor layer3 switches. Then, it will send this information to its own neighbor layer3 switches. As a result, the route selection table is built on second hand information, route beyond 15 hops will be deemed as unreachable.

RIP protocol is an optional routing protocol based on UDP. Hosts using RIP send and receive packets on UDP port 520. All layer3 switches running RIP send their route table to all neighbor layer3 switches every 30 seconds for update. If no information from the partner is received in 180 seconds, then the device is deemed to have failed and the network connected to that device is considered to be unreachable. However, the route of that layer3 switch will be kept in the route table for another 120 seconds before deletion.

As layer3 switches running RIP built route table with second hand information, infinite count may occur. For a network running RIP routing protocol, when an RIP route becomes unreachable, the neighboring RIP layer3 switch will not send route update packets at once, instead, it waits until the update interval timeout (every 30 seconds) and sends the update packets containing that route. If before it receives the updated packet, its neighbors send packets containing the information about the failed neighbor, “infinite

count” will be resulted. In other words, the route of unreachable layer3 switch will be selected with the metrics increasing progressively. This greatly affects the route selection and route aggregation time.

To avoid “infinite count”, RIP provides mechanism such as “split horizon” and “triggered update” to solve route loop. “Split horizon” is done by avoiding sending to a gateway routes leaned from that gateway. There are two split horizon methods: “simple split horizon” and “poison reverse split horizon”. Simple split horizon deletes from the route to be sent to the neighbor gateways the routes learnt from the neighbor gateways; poison reverse split horizon not only deletes the abovementioned routes, but set the costs of those routes to infinite. “Triggering update” mechanism defines whenever route metric changed by the gateway, the gateway advertise the update packets immediately, regardless of the 30 second update timer status.

There two versions of RIP, version 1 and version 2. RFC1058 introduces RIP-I protocol, RFC2453 introduces RIP-II, which is compatible with RFC1723 and RFC1388. RIP-I updates packets by packets broadcast, subnet mask and authentication is not supported. Some fields in the RIP-I packets are not used and are required to be all 0’s; for this reason, such all 0's fields should be checked when using RIP-I, the RIP-I packets should be discarded if such fields are non-zero. RIP-II is a more improved version than RIP-I. RIP-II sends route update packets by multicast packets (multicast address is 224.0.0.9). Subnet mask field and RIP authentication filed (simple plaintext password and MD5 password authentication are supported), and support variable length subnet mask. RIP-II used some of the zero field of RIP-I and require no zero field verification. ES4626/ES4650 switch send RIP-II packets in multicast by default, both RIP-I and RIP-II packets will be accepted.

Each layer3 switch running RIP has a route database, which contains all route entries for reachable destination, and route table is built based on this database. When a RIP layer3 switch sent route update packets to its neighbor devices, the complete route table is included in the packets. Therefore, in a large network, routing data to be transferred and processed for each layer3 switch is quite large, causing degraded network performance.

Besides the above mentioned, RIP protocol allows route information discovered by the other routing protocols to be introduced to the route table. It can also be as the protocol exchanging route messages with CE on PE routers, and supports the VPN route/transmitting examples.

The operation of RIP protocol is shown below:

Enable RIP. The switch sends request packets to the neighbor layer3 switches by broadcasting; on receiving the request, the neighbor devices reply with the packets containing their local routing information.

The Layer3 switch modifies its local route table on receiving the reply packets and sends triggered update packets to the neighbor devices to advertise route update information. On receiving the triggered update package, the neighbor lay3 switches send triggered update packages to their neighbor lay3 switches. After a sequence of triggered update package broadcast, all layer3 switches get and maintain the latest route information.

In addition, RIP layer3 switches will advertise its local route table to their neighbor devices every 30 seconds. On receiving the packets, neighbor devices maintain their local route table, select the best route and advertise the updated information to their own neighbor devices, so that the updated routes are globally valid. Moreover, RIP uses a timeout mechanism for outdated route, that is, if a switch does not receive regular update packets from a neighbor within a certain interval (invalid timer interval), it considers the route from that neighbor invalid, after holding the route fro a certain interval (holddown timer interval), it will delete that route.

17.4.2 RIP Configuration Task List

1. Enable RIP (required)
   (1) Enable/disable RIP module.
   (2) Enable interface to send/receive RIP packets
2. Configure RIP protocol parameters (optional)
   （1）Configure RIP sending mechanism
      1）Configure specified RIP packets transmission address
      2）Configure RIP interface broadcast
   （2）Configure the RIP routing parameters
      1）Configure route introduction (default route metric, configure routes of the other protocols to be introduced in RIP)
      2）Configure interface authentication mode and password
      3）Configure the route deviation
      4）Configure and apply route filter
      5）Configure horizontal segmentation
   （3）Configure other RIP protocol parameters
      1）Configure the managing distance of RIP route
      2）Configure the RIP route capacity limit in route table
      3）Configure the RIP renew, timeout, holddown and other timer.
      4）Configure the receiving buffer size of RIP UDP
3. Configure RIP-I/RIP-II switch
   （1）Configure the RIP version to be used in all interfaces

（2）Configure the RIP version to send/receive in all interfaces

（3）Configure whether to enable RIP packets sending/receiving for interfaces

4. elete the specified route in RIP route table

5. Configure the RIP VPN command.

1. Enable RIP protocol

Applying RIP route protocol with basic configuration in ES4626/ES4650 switch is simple. Normally you only have to open the RIP switch and configure the segments running RIP, namely send and receive the RIP data packet by default RIP configuration. The version of data packet sending and receiving is variable when needed, allow/deny sending, receiving RIP data packet. Refer to 3.

Command	Explanation
Global mode	
router rip **no router rip**	Enables RIP; the "**no router rip**" command disables RIP
Router and address family configuration mode	
**network <*A.B.C.D/M*	*ifname*>** **no network <*A.B.C.D/M*	*ifname*>**	Enables the segment running RIP protocol; the **no network <*A.B.C.D/M*	*ifname*>** command deletes the segment.

2. Configure RIP protocol parameters

（1）Configure RIP packet transmitting mechanism

1）Configure the RIP data packet point-transmitting

2）Configure the Rip broadcast

Command	**Explanation**
Router configuration mode	
neighbor <*A.B.C.D*> **no neighbor <*A.B.C.D*>**	Specify the IP address of the neighbor router needs point-transmitting; the **no neighbor <*A.B.C.D*>** command cancels the appointed router.
passive-interface<*ifname*> **no passive-interface<*ifname*>**	Block the RIP broadcast on specified pot and the RIP data packet is only transmittable among Layer 3 switch configured with neighbor. the **no passive-interface<*ifname*>** command cancels the function

（2）Configure RIP route parameters

1）configure route introduction (default route metric, configure routes of the other protocols to be introduced in RIP)

Command	**Explanation**

Router configuration mode	
default-metric <*value*> **no default-metric**	Sets the default route metric for route to be introduced; the "**no default-metric**" command restores the default setting.
redistribute {kernel |connected| static| ospf| isis| bgp} [metric<value>] [route-map<word>] **no redistribute {kernel |connected| static| ospf| isis| bgp} [metric<value>] [route-map<word>]**	Redistribute the routes distributed in other routing protocols into the RIP data packet; the **no redistribute {kernel |connected| static| ospf| isis| bgp} [metric<value>] [route-map<word>]** command cancels the distributed route of corresponding protocols
default-information originate **no default-information originate**	Generate a default route to the RIP protocol; the **no default-information originate** command cancels the feature.

2）Configure interface authentication mode and password

Command	**Explanation**
Interface configuration mode	
ip rip authentication mode { text| md5} **no ip rip authentication mode [text| md5]**	Sets the authentication method; the **no ip rip authentication mode [text| md5]** command cancels the authentication action
ip rip authentication string <*text*> **no ip rip authentication string**	Sets the authentication key; the **no ip rip authentication string** command means no key is needed.
ip rip authentication key <*name-of-chain*> **no ip rip authentication key** [**<*name-of-chain*>**]	Sets the key chain used in authentication, the **no ip rip authentication key** [**<*name-of-chain*>**] command means the key chain is not used
Global mode	
key chain <*name-of-chain*> **no key chain < *name-of-chain* >**	Enter keychain mode, and configure a key chain, the **no key chain < *name-of-chain* >** command deletes the key chain
Keychain mode	
key <*keyid*> **no key <*keyid*>**	Enter the keychain-key mode and configure a key of the keychain; the **no key <*keyid*>** command deletes one key.
Keychain-key mode	

key-string <*text*> **no key-string <*text*>**	Configure the password used by the key, the **no key-string <*text*>** command deletes the password
accept-lifetime <*start-time*> {<*end-time*>| duration<*seconds*>| infinite} **no accept-lifetime**	Configure a key on the key chain and accept it as an authorized time; the **no accept-lifetime** command delete it
send-lifetime <*start-time*> {<*end-time*>| duration<*seconds*>| infinite} **no send-lifetime**	Configure the transmitting period of a key on the key chain; the **no send-lifetime** command delete the send-lifetime

3）Configure the route deviation

Command	Explanation
Router configuration mode	
offset-list <access-list-number |access-list-name> {in|out }<number >[<ifname>] **no offset-list <access-list-number |access-list-name> {in|out }<number >[<ifname>]**	Configure that provide a deviation value to the route metric value when the port sends or receives RIP data packet; the **no offset-list <access-list-number |access-list-name> {in|out }<number >[<ifname>]** command removes the deviation table

4）configure and apply the route filtering

Command	Explanation
Router configuration mode	
distribute-list {< *access-list-number* |*access-list-name* >|prefix<*prefix-list-name*>}{in|out} [<*ifname*>] **no distribute-list {< *access-list-number* |*access-list-name* >|prefix<*prefix-list-name*>}{in|out} [<*ifname*>]**	Configure and apply the access table and prefix table to filter the routes. the **no distribute-list {< *access-list-number* |*access-list-name* >|prefix<*prefix-list-name*>}{in|out} [<*ifname*>]**command means do not use the access table and prefix table

5）configure the split horizon

Command	**Explanation**
Interface configuration mode	
ip rip split-horizon [poisoned] **no ip rip split-horizon**	Configure that take the split horizon when the port sends data packets; poisoned for poison reverse the **no ip rip split-horizon** command cancels the split horizon

（**3**）Configure other RIP protocol parameters

1）Configure RIP routing priority

2）Configure the RIP route capacity limit in route table

3）Configure timer for RIP update, timeout and hold-down

4）Configure RIP UDP receiving buffer size

Command	**Explanation**
Router configuration mode	
distance *<number>* [*<A.B.C.D/M>*] [*<access-list-name|access-list-number >*] **no distance [*<A.B.C.D/M>*]**	Specify the route administratively distance of RIP protocol; the **no distance [*<A.B.C.D/M>*]** command restore the default value 120
maximum-prefix *<maximum-prefix>*[*<threshold>*] **no maximum-prefix *<maximum-prefix >*** **no maximum-prefix**	Configure the maximum of RIP route; the **no maximum-prefix *<maximum-prefix >*** **no maximum-prefix** command cancels the limit
timers basic *<update>* *<invalid>* *<garbage>* **no timers basic**	Adjust the update, timeout and garbage collection time, the **no timers basic** command restore the default configuration
recv-buffer-size *<size>* **no recv-buffer-size**	The command configures the UDP receiving buffer size of the RIP; the **no recv-buffer-size** command restore the system default values

3. Configure RIP-I/RIP-II toggling

（**1**）Configure the RIP version to be used in all ports

Command	**Explanation**
RIP configuration mode	
version { 1 | 2 } **no version**	Configure the versions of all the RIP data packets transmitted/received by the Layer 3 switch port sending/receiving the **no version** command restores the default configuration, version 2.

（**2**）Configure the RIP version to send/receive in all ports**.**

（**3**）Configure whether to enable RIP packets sending/receiving for ports

Command	**Explanation**
Interface configuration mode	

ip rip send version { 1 | 1-compatible | 2 } **no ip rip send version**	Sets the version of RIP packets to send on all interfaces; the **no ip rip send version** command set the version to the one configured by the version command
ip rip receive version {1 | 2 | } **no ip rip receive version**	Sets the version of RIP packets to receive on all interfaces; the no action of this command set the version to the one configured by the version command
ip rip receive-packet **no ip rip receive-packet**	Enables receiving RIP packets on the interface; the **no ip rip receive-packet** command close data receiving on this port
ip rip send-packet **no ip rip send-packet**	Enables sending RIP packets on the interface; the "**no ip rip send-packet**" command disables sending RIP packets on the interface

4. Delete the specified route in RIP route table

Command	**Explanation**
Admin Mode	
clear ip rip route {<*A.B.C.D/M*>|kernel|static|connected |rip|ospf|isis|bgp|all}	The command deletes a specified route from the RIP route table

5. Configure the RIP VPN command.

Command	Explanation
Router configuration mode	
address-family ipv4 vrf <*vrf-name*> **no address-family ipv4 vrf <*vrf-name*>**	The command configures a RIP address family on the VRF of the PE router. the **no address-family ipv4 vrf <*vrf-name*>** command deletes the configured address family
Address family configuration mode	
exit-address-family	This command exits the address family mode

17.4.3 Commands for RIP

17.4.3.1 accept-lifetime

Command: accept-lifetime <*start-time*> {<*end-time*>| duration<*seconds*>| infinite}

no accept-lifetime

Function: Use this command to specify a key accept on the key chain as a valid time period. The "**no accept-lifetime**" command deletes this configuration.

Parameter: ***<start-time>*** parameter specifies the start time of the time period, of which the form should be:

<start-time>={<hh:mm:ss> <month> <day> <year>|<hh:mm:ss> <day> <month> <year>}

<hh:mm:ss> specify the concrete valid time of **accept-lifetime** in hours, minutes and second

<day> specifies the date of valid, ranging between 1 -31

<month> specifies the month of valid shown with the first three letters of the month, such as Jan

<year> specifies the year of valid start, ranging between 1993 - 2035

<end-time> specifies the due of the time period, of which the form should be:

<end-time>={<hh:mm:ss> <month> <day> <year>|<hh:mm:ss> <day> <month> <year>}

<hh:mm:ss> specify the concrete valid time of **accept-lifetime** in hours, minutes and second

<day> specifies the date of valid, ranging between 1 -31

<month> specifies the month of valid shown with the first three letters of the month, such as Jan

<year> specifies the year of valid start, ranging between 1993 - 2035

<seconds> the valid period of the key in seconds, ranging between 1-2147483646

Infinite means the key will never be out of date.

Default: No default configuration

Command Mode: keychain-key mode

Usage Guide: Refer to the 3.13 RIP authentication Introduction

Example: The example below shows the accept-lifetime configuration of key 1 on the keychain named mychain

Switch# config terminal

Switch(config)# key chain mychain

Switch(config-keychain)# key 1

Switch(config-keychain-key)# accept-lifetime 03:03:01 Dec 3 2004 04:04:02 Oct 6 2006

17.4.3.2 address-family ipv4

Command: address-family ipv4 vrf <*vrf-name*>

no address-family ipv4 vrf <*vrf-name*>

Function: Configure this command to enable the routing message switching among VRF and enter the address-family mode. The "**no address-family ipv4 vrf *<vrf-name>***" command deletes the RIP instances related to this VPN routing/forwarding instances

Parameter: ***<vrf-name>*** specifies the name of VPN routing/forwarding instances

Command Mode: router mode

Usage Guide: This command is only used on PE router. A VPN routing/forwarding instances must be generated with command ip vrf prior to using this command by which the VPN routing/forwarding instances can be related to RIP instances.

Example: Switch# config terminal

Switch(config)# router rip

Switch(config-router)# address-family ipv4 vrf VRF1

Switch(config-router-af)#

17.4.3.3 clear ip rip route

Command: clear ip rip route

{*<A.B.C.D/M>*|kernel|static|connected|rip|ospf|isis|bgp|all}

Function: Clear specific route in the RIP route table

Parameter: Clear the routes which match the destination address from the RIP route table. ***<A.B.C.D/M>*** specifies the IP address prefix and its length of the destination address

kernel delete kernel routes from the RIP route table

static delete static routes from the RIP route table

connected delete direct routes from the RIP route table

rip only delete RIP routes from the RIP route table

ospf only delete OSPF routes from the RIP route table

isis only delete ISIS routes from the RIP route table

bgp only delete BGP routes from the RIP route table

all delete all routes from the RIP route table

Default: No default configurations

Command Mode: Admin Mode

Usage Guide: Use this command with the all parameter will delete all learnt route in the RIP route which will be immediately recovered except for rip route. The dynamic learnt RIP route can only be recovered by studying one more time.

Example: Switch# clear ip rip route 10.0.0.0/8

Switch# clear ip rip route ospf

17.4.3.4 debug rip

Command: [no] debug rip [events| nsm| packet[recv|send][detail]| all]

Function: Open various RIP adjustment switches and show various adjustment debugging messages. The "**[no] debug rip [events| nsm| packet[recv|send][detail]| all]**" command close corresponding debugging switch.

Parameter : **events** shows the debugging messages of RIP events

nsm shows the communication messages between RIP and NSM.

packet shows the debugging messages of RIP data packets.

recv shows the messages of the received data packets

send shows the messages of the sent data packets

detail shows the messages of received or sent data packets.

Default: Debug switch closed.

Command Mode: Admin Mode

Example: Switch# debug rip packet

Switch#1970/01/01 01:01:43 IMI: SEND[Vlan1]: Send to 224.0.0.9:520

1970/01/01 01:01:43 IMI: SEND[Vlan1]: Send to 224.0.0.9:520

1970/01/01 01:01:47 IMI: RECV[Vlan1]: Receive from 20.1.1.2:520

17.4.3.5 default-information originate

Command: default-information originate

no default-information originate

Function: Allow the network 0.0.0.0 to be redistributed into the RIP. The "**no default-information originate**" disable this function.

Parameter: None

Default: Disabled

Command Mode: router mode

Example: Switch# config terminal

Switch(config)# router rip

Switch(config-router)# default-information originate

17.4.3.6 default-metric

Command: default-metric <*value*>

no default-metric

Function: Set the default metric value of the introduced route. The "**no default-metric**" command restores the default value to 1.

Parameter: <*value*> is the metric value to be set, ranging between 1~16.

Default: Default route metric value is 1

Command Mode: Router mode and address-family mode

Usage Guide: default-metric command is used for setting the default route metric value

of the routes from other routing protocols when distributed into the RIP routes. When using the **redistribute** commands for introducing routes from other protocols, the default route metric value specified by **default-metric** will be adopted if no specific route metric value is set.

Example: Set the default route metric value to 3 for introducing routes from other routing protocols into the RIP routes.

Switch(config-router)#default-metric 3

Relevant Commands: redistribute

17.4.3.7 distance

Command:distance <*number*> [<*A.B.C.D/M*>]

[<*access-list-name*|*access-list-number* >]

no distance [<*A.B.C.D/M*>]

Function: Set the managing distance with this command. The "**no distance [<*A.B.C.D/M*>]**" command restores the default value to 120

Parameter: <*number*> specifies the distance value, ranging between 1-255.**<*A.B.C.D/M*>** specifies the network prefix and its length. **<*access-list-name*|*access-list-number* >** specifies the access-list number or name applied

Default: The default managing distance of RIP is 120

Command Mode: Router mode and address-family mode

Usage Guide: In case there are routes from two different routing protocols to the same destination, the managing distance is then used for selecting routes. The less the managing distance of the route protocol is , the more reliable will be the route acquired from the protocol.

Example: Switch# config terminal

Switch(config)# router rip

Switch(config-router)# distance 8 10.0.0.0/8 mylist

17.4.3.8 distribute-list

Command: distribute-list{<*access-list-number*|*access-list-name*>

|prefix<*prefix-list-name*>} {in|out} [<*ifname*>]

no distribute-list{<*access-list-number*|

***access-list-name*> |prefix<*prefix-list-name*>} {in|out} [<*ifname*>]**

Function: This command uses access-list or prefix-list to filter the route update packets sent and received. The "**no distribute-list{<*access-list-number*|**

***access-list-name*> |prefix<*prefix-list-name*>} {in|out} [<*ifname*>]**" command cancels this route filter function.

Parameter:<*access-list-number* |*access-list-name*> is the name or access-list number to be applied. **<*prefix-list-name*>** is the name of the prefix-list to be applied. **<*ifname*>** specifies the name of interface to be applied with route filtering.

Default: The function in default situation is disabled.

Command Mode: Router mode and address-family mode

Usage Guide: The filter will be applied to all the interfaces in case no specific interface is set.

Example: Switch# config terminal

Switch(config)# router rip

Switch(config-router)# distribute-list prefix myfilter in vlan 1

17.4.3.9 exit-address-family

Command: exit-address-family

Function: Exit address-family mode

Command Mode: address-family mode

Example: Switch(config)# router rip

Switch(config-router)# address-family ipv4 vrf IPI

Switch(config-router-af)# exit-address-family

Switch(config-router)#

17.4.3.10 ip rip authentication key

Command: ip rip authentication key <*name-of-chain*>

no ip rip authentication key

Function: Use this command to enable RIPV2 authentication on an interface and further configures the adopted key chain. The "**no ip rip authentication key**" command cancels the authentication.

Parameter: <*name-of-chain*> is the name of the adopted key chain. There may be spaces in the string. The input ends with an enter and the string should not be longer than 256 bytes

Default: Not configured

Command Mode: Interface Mode

Usage Guide: If the authentication is only configured without configuring the key chain or password used by the interface, the authentication do no effect. If mode has not been configured prior to configuring this command, the mode will be set to plaintext authentication. The "no ip rip authentication key" command will cancel the authentication which only cancels the authentication process when sending or receiving data packet other than set non authentication mode.

Example: Switch# config terminal

Switch(config)# interface vlan 1
Switch(Config-if-Vlan1)# ip rip authentication key my key

17.4.3.11 ip rip authentication mode

Command:ip rip authentication mode {text|md5}
no ip rip authentication mode {ext|md5}

Function: Configure the authentication mode; the "**no ip rip authentication mode {ext|md5}**" command restores to the default authentication mode namely text authentication mode.

Parameter: text means text authentication; **md5** means MD5 authentication.

Default: Not configured authentication

Command Mode: Interface Mode

Usage Guide: RIP-I do not support authentication which the RIP-II supports two authentication modes: text authentication (i.e. Simple authentication) and data packet authentication (i.e. MD5 authentication). This command should be used associating the ip rip authentication key or ip rip authentication string. Independently configuration will not lead to authentication process.

Example: Switch# config terminal
Switch(config)# interface vlan 1
Switch(Config-if-Vlan1)# ip rip authentication mode md5

17.4.3.12 ip rip authentication string

Command: ip rip authentication string <*text*>
no ip rip authentication string

Function: Set the password used in RIP authentication. The "**no ip rip authentication string**" cancels the authentication

Parameter: <*text*> is the password used in authentication of which the length should be 1-16 characters with space available. The password should end with enter

Command Mode: Interface mode

Usage Guide: The ip rip authentication key will not be able to be configured when this command is configured, key id value is required in MD5 authentication which is 1 when use this command. The mode will be set to plaintext authentication in case no mode configuration is available. The "**no ip rip authentication string**" command will cancel the authentication which only cancels the authentication process when sending or receiving data packet other than set non authentication mode. Input ip rip authentication string aaa aaa to set the password as aaa aaa which is 7 characters.

Example: Switch# config terminal
Switch(config)# interface vlan 1

Switch(Config-if-Vlan1)# ip rip authentication string guest

17.4.3.13 ip rip authentication cisco-compatible

Command:ip rip authentication cisco-compatible

no ip rip authentication cisco-compatible

Function: After configured this command, the cisco RIP packets will be receivable by configuring the plaintext authentication or MD5 authentication.

Parameter: None

Default: Not configured

Command Mode: Interface mode

Usage Guide: After authentication is configured on the cisco router, the RIP packets will exceeds the length of the defined standard length of the protocol once the number of route items is greater than 25. By configuring this command the over-lengthen RIP packets will be receivable other than denied.

Example: Switch# config terminal

Switch(config)# interface vlan 1

Switch(Config-if-Vlan1)# ip rip authentication cisco-compatible

17.4.3.14 ip rip receive-packet

Command: ip rip receive-packet

no ip rip receive-packet

Function: Set the interface to be able to receivable RIP packets; the "**no ip rip receive-packet**" command set the interface to be unable to receivable RIP packets

Default: Interface receives RIP packets

Command Mode: Interface Mode

Example: Switch# config terminal

Switch(config)# interface vlan 1

Switch(Config-if-Vlan1)# ip rip receive-packet

17.4.3.15 ip rip receive version

Command: ip rip receive version { 1 | 2|1 2 }

no ip rip receive version

Function: Set the version information of the RIP packets the interface receives. The default version is 2; the "**no ip rip receive version**" command restores the value set by using the version command.

Parameter: 1 and 2 respectively stands for RIP version 1 and RIP version 2, 1 2 stands for the RIP versions 1, 2.

Default: Version 2

Command Mode: Interface Mode

Example: Switch# config terminal

Switch(config)# interface vlan 1

Switch(Config-if-Vlan1)# ip rip receive version 1 2

17.4.3.16 ip rip send-packet

Command: ip rip send-packet

no ip rip send-packet

Function: Set the Interface to be able to receive the RIP packets; the "**no ip rip send-packet**" set the interface to be unable to receive the RIP packets.

Default: Interface sends RIP packets

Command Mode: Interface Mode

Example: Switch# config terminal

Switch(config)# interface vlan 1

Switch(Config-if-Vlan1)# ip rip send-packet

17.4.3.17 ip rip send version

Command: ip rip send version { 1 | 2 | 1-compatible | 1 2}

no ip rip send version

Function: Set the version information of the RIP packets the interface receives. The default version is 2; the "**no ip rip send version**" command restores the value set by using the version command.

Parameter: 1 and 2 respectively stands for RIP version 1 and RIP version 2, 1 2 stands for the RIP versions 1, 2.

Default: Version 2

Command Mode: Interface Mode

Example: Switch# config terminal

Switch(config)# interface vlan 1

Switch(Config-if-Vlan1)# ip rip send version 1

17.4.3.18 ip rip split-horizon

Command: ip rip split-horizon [poisoned]

no ip rip split-horizon

Function: Enable split horizon. The "**no ip rip split-horizon**" disables the split horizon.

Parameter: [poisoned] means configure the split horizon with poison reverse.

Default: Split Horizon with poison reverse by default

Command Mode: Interface Mode

Usage Guide: The split horizon is for preventing the Routing Loops, namely preventing

the layer 3 switches from broadcasting the routes which is learnt from the same interface on which the route to be broadcasted

Example: Switch# config terminal

Switch(config)# interface vlan 1

Switch(Config-if-Vlan1)# ip rip split-horizon poisoned

17.4.3.19 key

Command:key <*keyid*>

no key <*keyid*>

Function: This command is for managing and adding keys in the key chain. The "**no key <*keyid*>**" command deletes one key.

Parameter: <*keyid*> is key ID, ranging between 0-2147483647.

Command Mode: Keychain mode

Usage Guide: The command permits entering the keychain-key mode and set the passwords corresponding to the keys.

Example: Switch# config terminal

Switch(config)# key chain mychain

Switch(config-keychain)# key 1

Switch(config-keychain-key)#

17.4.3.20 key chain

Command: key chain <*name-of-chain*>

no key chain < *name-of-chain* >

Function: This command is for entering a keychain manage mode and configure a keychain. The "**no key chain < *name-of-chain* >**" delete one keychain.

Parameter: <*name-of-chain*> is the name string of the keychain the length of which is not specifically limited.

Command Mode: Global Mode

Example: Switch# config terminal

Switch(config)# key chain mychain

Switch(config-keychain)#

17.4.3.21 key-string

Command: key-string <*text*>

no key-string <*text*>

Function: Configure a password corresponding to a key. The "**no key-string <*text*>**" command delete the corresponding password.

Parameter: <*text*> is a character string without length limit. However when referred by

RIP authentication only the first 16 characters will be used.

Command Mode: Keychain-key mode

Usage Guide: This command is for configure different passwords for keys with different ID.

Example: Switch# config terminal

Switch(config)# key chain mychain

Switch(config-keychain)# key 1

Switch(config-keychain-key)# key-string prime

17.4.3.22 maximum-prefix

Command: maximum-prefix <*maximum-prefix*>[**<*threshold*>**]

no maximum-prefix

Function: Configure the maximum number of RIP routes in the route table. The "**no maximum-prefix**" command cancels the limit.

Parameter: <*maximum-prefix*> the maximum number of RIP route, ranging between 1-65535; a warning is given when the number rate of current route exceeds **<*threshold*>** ranging between 1-100, default at 75

Command Mode: router mode

Usage Guide: The maximum RIP routes only limits the number of routes learnt through RIP but not includes direct route or the RIP static route configured by the route command. The base on which the comparison is performed is the number of route marked R in the show ip route database, and also the number of RIP routes displayed in the show ip route statistics command.

Example:

Switch# config terminal

Switch(config)# router rip

Switch(config-router)# maximum-prefix 150

17.4.3.23 neighbor

Command: neighbor <*A.B.C.D*>

no neighbor <*A.B.C.D*>

Function: Specify the destination address requires targeted-peer sending. The "**no neighbor <*A.B.C.D*>**" command cancels the specified address and restores all gateways to trustable.

Parameter: <*A.B.C.D*> is the specified destination address for the sending, shown in dotted decimal notation.

Default: Not sending to any targeted-peer destination address.

Command Mode: Router mode

Usage Guide: When used accompany with passive-interface command it can be configured to only sending routing messages to specific neighbor.

Example:

Switch# config terminal

Switch(config)# router rip

Switch(config-router)# neighbor 1.1.1.1

17.4.3.24 network

Command: [no] network <*A.B.C.C/M*|*ifname*>

Function: Configure the RIP protocol network

Parameter: <*A.B.C.C/M*|> is the IP address prefix and its length in the network

<*ifname*> is the name of a interface.

Default: Not running RIP protocol

Command Mode: Router mode and address-family mode.

Usage Guide: Use this command to configure the network for sending or receiving RIP update packets. If the network is not configured, all interfaces of the network will not be able to send or receive data packets.

Example: Switch# config terminal

Switch(config)# router rip

Switch(config-router)# network 10.0.0.0/8

Switch(config-router)# network vlan 1

17.4.3.25 offset-list

Command: offset-list <*access-list-number*|*access-list-name*> {in|out }<*number* >[<*ifname*>]

no offset-list <*access-list-number*|*access-list-name*> {in|out }<*number* >[<*ifname*>]

Function: Add an offset value to the metric value of the routes learnt by RIP. The "**no offset-list <*access-list-number*
|*access-list-name*> {in|out }<*number* >[<*ifname*>]" command disables this function

Parameter: < *access-list-number* |*access-list-name*> is the access-list or name to be applied. **<*number* >** is the added offset value, ranging between 0-16; **<*ifname*>** is the specific interface name

Default: Default offset value is the metric value defined by the system

Command Mode: Router mode and address-family mode.

Example:

Switch# config terminal

Switch(config)# router rip

Switch(config-router)# offset-list 1 in 5 vlan 1

17.4.3.26 passive-interface

Command: passive-interface <*ifname*>

no passive-interface <*ifname*>

Function: Set the RIP layer 3 switch blocks RIP broadcast on specified interface, on which the RIP data packets will only be sent to layer 3 switches configured with neighbor.

Parameter: <***ifname***> is the name of specific interface.

Default: Not configured

Command Mode: Router mode

Example:

Switch# config terminal

Switch(config)# router rip

Switch(config-router)# passive-interface vlan 1

17.4.3.27 recv-buffer-size

Command: recv-buffer-size<*size*>

no recv-buffer-size

Function: This command configures the size of UDP receiving buffer zone of RIP; the "**no recv-buffer-size**" command restores the system default.

Parameter: **<*size*>** is the buffer zone size in bytes, ranging between 8192-2147483647

Default: 8192 bytes

Command Mode: Router mode

Example:

Switch# config terminal

Switch(config)# router rip

Switch(config-router)# recv-buffer-size 23456789

17.4.3.28 redistribute

Command: redistribute {kernel |connected| static| ospf| isis| bgp} [metric<*value*>] [route-map<*word*>]

no redistribute {kernel |connected| static| ospf| isis| bgp} [metric<*value*>] [route-map<*word*>]

Function: Introduce the routes learnt from other routing protocols into RIP

Parameter:

kernel introduce from kernel routes

connected introduce from direct routes

static introduce from static routes

ospf introduce from OSPF routes

isis introduce from ISIS routes

bgp introduce from BGP routes

<*value*> is the metric value assigned to the introduced route, ranging between 0-16

<*word*> is the probe pointing to the route map for introducing routes.

Command Mode: Router mode and address-family mode.

Usage Guide: Under the address-family mode, the parameter kernel and isis is unavailable

Example:

Switch# config terminal

Switch(config)# router rip

Switch(config-router)# redistribute kernel route-map ipi

17.4.3.29 route

Command: route <*A.B.C.D/M*>

no route <*A.B.C.D/M*>

Function: This command configures a static RIP route. The "**no route <*A.B.C.D/M*>**" command deletes this route.

Parameter: Specifies this destination IP address prefix and its length.

Command Mode: **Router mode**

Usage Guide: The command add a static RIP route, and is mainly used for debugging. Routes configured by this command will not appear in kernel route table but in the RIP route database.

Example:

Switch# config terminal

Switch(config)# router rip

Switch(config-router)# route 1.0.0.0/8

17.4.3.30 router rip

Command: router rip

no router rip

Function: Enable the RIP routing process and enter the RIP mode; the "**no router rip**" command closes the RIP routing protocol

Default: Not running RIP route

Command Mode: Global mode

Usage Guide: This command is the switch for starting the RIP routing protocol which is required to be open before configuring other RIP protocol commands.

Example:

Enable the RIP protocol mode

Switch(config)#router rip

Switch(config-router)#

17.4.3.31 send-lifetime

Command: send-lifetime <*start-time*> {<*end-time*>| duration<*seconds*>| infinite}

no send-lifetime

Function: Use this command to specify a key on the keychain as the time period of sending keys. The "**no send-lifetime**" cancels this configuration.

Parameter: <*start-time*> parameter specifies the starting time of the time period, which is :

<start-time>={<hh:mm:ss> <month> <day> <year>|<hh:mm:ss> <day> <month> <year>}

<hh:mm:ss> Specify the concrete valid time of **accept-lifetime** in hours, minutes and second

<day> Specifies the date of valid, ranging between 1 -31

<month> Specifies the month of valid shown with the first three letters of the month, such as Jan

<year> Specifies the year of valid start, ranging between 1993 - 2035

<end-time>={<hh:mm:ss> <month> <day> <year>|<hh:mm:ss> <day> <month> <year>}

<end-time> Specifies the due of the time period, of which the form should be:

<end-time>={<hh:mm:ss> <month> <day> <year>|<hh:mm:ss> <day> <month> <year>}

<hh:mm:ss> Specify the concrete valid time of **accept-lifetime** in hours, minutes and second

<day> Specifies the date of valid, ranging between 1 -31

<month> Specifies the month of valid shown with the first three letters of the month, such as Jan

<year> Specifies the year of valid start, ranging between 1993 -2035

<seconds> is the valid period of the key in seconding and ranging between 1-2147483646

Default: No default configuration

Command Mode: Keychain-key mode

Usage Guide: Refer to the 3.13 RIP authentication section.

Example: The example below shows the send-lifetime configuration on the keychain named mychain for key 1.

Switch# config terminal

Switch(config)# key chain mychain
Switch(config-keychain)# key 1
Switch(config-keychain-key)# send-lifetime 03:03:01 Dec 3 2004 04:04:02 Oct 6 2006

17.4.3.32 timers basic

Command: timers basic <*update*> <*invalid*> <*garbage*>

no timers basic

Function: Adjust the RIP timer update, timeout, and garbage collecting time. The "**no timers basic**" command restores each parameters to their default values.

Parameter: <*update*> time interval of sending update packet, shown in seconds and ranging between 5-2147483647; ***<invalid>*** time period after which the RIP route is advertised dead, shown in seconds and ranging between 5-2147483647; ***<garbage>*** is the hold time in which the a route remains in the routing table after advertised dead, shown in seconds and ranging between 5-2147483647.

Default: ***<update>*** defaulted at 30; ***<invalid>*** defaulted at 180; ***<garbage>*** defaulted at120

Command Mode: Router mode

Usage Guide: The system is defaulted broadcasting RIPng update packets every 30 seconds; and the route is considered invalid after 180 seconds but still exists for another 120 seconds before it is deleted from the routing table.

Example: Set the RIP update time to 20 seconds and the timeout period to 80 second, the garbage collecting time to 60 seconds.

Switch(Config-Router)#timers basic 20 80 60

17.4.3.33 version

Command: version {1| 2}

no version

Function: Configure the version of all RIP data packets sent/received by router interfaces: the "**no version**" restores the default configuration

Parameter: 1 is version 1 rip; **2** is version 2 rip

Default: Sent and received data packet is version 2 by default

Command Mode: Router mode and address-family mode

Usage Guide: 1 refers to that each interface of the layer 3 switch only sends/receives the RIP-I data packets. 2 refers to that each interface of the layer 3 switch only sends/receives the RIP-II data packets. The RIP-II data packet is the default version.

Example: Configure the version of all RIP data packets sent/received by router interfaces to version 2.

Switch(config-router)#version 2

17.4.4 RIP Examples

17.4.4.1 Typical RIP Examples

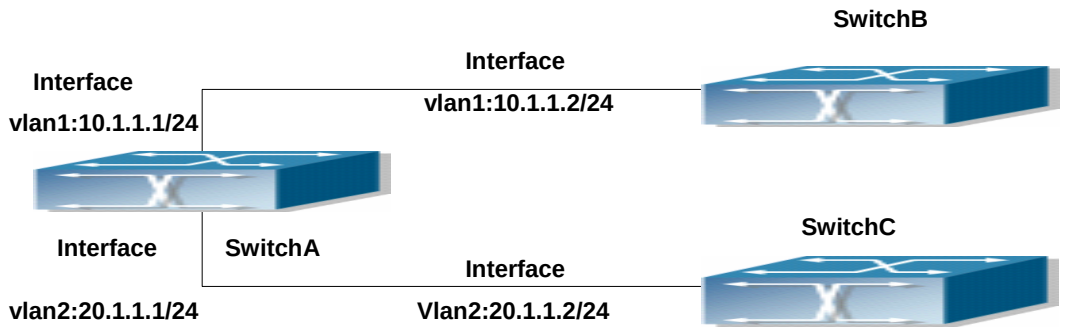


Fig 17-3 RIP example

In the figure shown above, a network consists of three Layer 3 switches, in which SwitchA connected with SwitchB and SwitchC, and RIP routing protocol is running in all of the three switches. SwitchA （interface vlan1：10.1.1.1,interface vlan2：20.1.1.1） exchanges Layer 3 switch update messages only with SwitchB（interface vlan1：10.1.1.2）, but not with SwitchC（interface vlan 2: 20.1.1.2）.

SwitchA, SwitchB, SwitchC configurations are as follows:

a) Layer 3 SwitchA：

Configure the IP address of interface vlan 1

SwitchA#config

SwitchA(config)# interface vlan 1

SwitchA(Config-if-Vlan1)# ip address 10.1.1.1 255.255.255.0

SwitchA (config-if-Vlan1)#

Configure the IP address of interface vlan 2

SwitchA (config)# vlan 2

SwitchA (Config-Vlan2)# switchport interface ethernet 1/2

Set the port Ethernet1/2 access vlan 2 successfully

SwitchA (Config-Vlan2)# exit

SwitchA (Config)# interface vlan 2

SwitchA (Config-if-Vlan2)# ip address 20.1.1.1 255.255.255.0

Initiate RIP protocol and configure the RIP segments

SwitchA(config)#router rip

SwitchA(config-router)#network vlan 1

SwitchA(config-router)#network vlan 2

SwitchA(config-router)#exit

Configure that the interface vlan 2 do not transmit RIP messages to SwitchC

SwitchA(config)#router rip

SwitchA(config-router)#passive-interface vlan 2

SwitchA(config-router)#exit

SwitchA (config) #

b) Layer 3 SwitchB

Configure the IP address of interface vlan 1

SwitchB#config

SwitchB(config)# interface vlan 1

SwitchB(Config-if-Vlan1)# ip address 10.1.1.2 255.255.255.0

SwitchB (Config-if-Vlan1)exit

Initiate RIP protocol and configure the RIP segments

SwitchB(config)#router rip

SwitchB(config-router)#network vlan 1

SwitchB(config-router)#exit

c) Layer 3 SwitchC

SwitchC#config

SwitchC(config)# interface vlan 1

Configure the IP address of interface vlan 1

SwitchC(Config-if-Vlan1)# ip address 20.1.1.2 255.255.255.0

SwitchC (Config-if-Vlan1)#exit

Initiate RIP protocol and configure the RIP segments

SwitchC(config)#router rip

SwitchC(config-router)#network vlan 1

SwitchC(config-router)#exit

17.4.4.2 Configuration Examples of RIP VPN

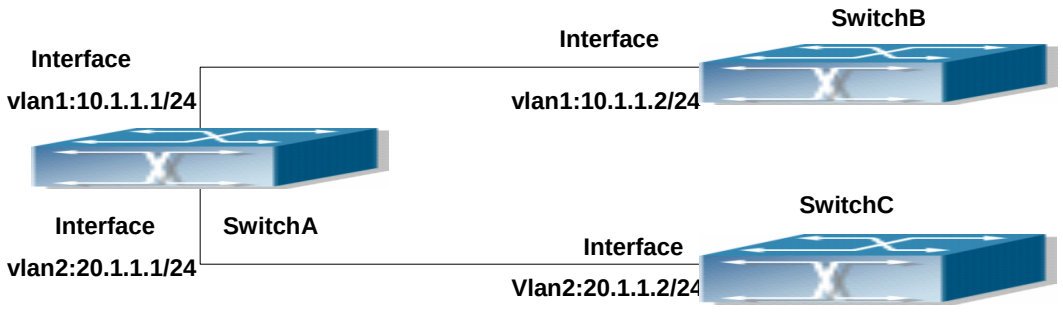


Fig 17-4 RIP VPN example

In the figure shown above, a network consists of three Layer 3 switches, in which the SwitchA as PE, SwitchB and SwitchC as CE1 and CE2. The PE is connected to CE1 and CE2 through vlan 1 and vlan 2. The routing messages are exchanged between PE and CE through RIP protocol.

a) SwitchA

Configures the VPN route/transmit example vpnb and vpnc

```
SwitchA#config
SwitchA(config)#ip vrf vpnb
SwitchA(config-vrf)#
SwitchA(config-vrf)#exit
SwitchA#(config)
SwitchA(config)#ip vrf vpnc
SwitchA(config-vrf)#
SwitchA(config-vrf)#exit
```

associate the vlan 1and vlan 2 respectively with vpnb and vpnc while configuring IP address

```
SwitchA(config)#in vlan1
SwitchA(config-if-Vlan1)#ip vrf forwarding vpnb
SwitchA(config-if-Vlan1)#ip address 10.1.1.1 255.255.255.0
SwitchA(config-if-Vlan1)#exit
SwitchA(config)#in vlan2
SwitchA(config-if-Vlan2)#ip vrf forwarding vpnc
SwitchA(config-if-Vlan2)#ip address 20.1.1.1 255.255.255.0
SwitchA(config-if-Vlan2)#exit
```

Configures the RIP examples associated with vpnb and vpnc respectively

```
SwitchA(config)#
SwitchA(config)#router rip
SwitchA(config-router)#address-family ipv4 vrf vpnb
SwitchA(config-router-af)#redistribute bgp
SwitchA(config-router-af)#network Vlan1
SwitchA(config-router-af)#exit-address-family
SwitchA(config-router)#address-family ipv4 vrf vpnc
SwitchA(config-router-af)#redistribute bgp
SwitchA(config-router-af)#network Vlan2
SwitchA(config-router-af)#exit-address-family
SwitchA(config-router)#
```

b) SwitchB

configure the IP address of Ethernet port E 1/2

```
SwitchB#config
```

SwitchB(config)# interface Vlan1

SwitchB(config-if-Vlan1)# ip address 10.1.1.2 255.255.255.0

SwitchB (config-if-Vlan1)exit

Initiate RIP protocol and configure the RIP segments

SwitchB(config)#router rip

SwitchB(config-router-rip)#network Vlan1

SwitchB(config-router-rip)#exit

c) SwitchC

Configure the IP address of Ethernet port E 1/2

SwitchC#config

SwitchC(config)# interface Vlan1

SwitchC(config-if-vlan1)# ip address 20.1.1.2 255.255.255.0

SwitchC (config-if-vlan1)#exit

Initiate RIP protocol and configure the RIP segments

SwitchC(config)#router rip

SwitchC(config-router)#network Vlan1

SwitchC(config-router)#exit

17.4.5 RIP Troubleshooting

The RIP protocol may not be working properly due to errors such as physical connection, configuration error when configuring and using the RIP protocol. So users should pay attention to following:

First ensure the physic connection is correct

Second, ensure the interface and chain protocol are UP (use show interface command)

Then initiate the RIP protocol (use router rip command) and configure the segment (use network command) and set RIP protocol parameter on corresponding interfaces, such as the option between RIP-I and RIP-II

After that, one feature of RIP protocol should be noticed ---the Layer 3 switch running RIP protocol sending route updating messages to all neighboring Layer 3 switches every 30 seconds. A Layer 3 switch is considered inaccessible if no route updating messages from the switch is received within 180 seconds, then the route to the switch will remains in the route table for 120 seconds before it is deleted. Therefore, if to delete a RIP route, this route item is assured to be deleted from route table after 300 seconds.

When exchanging routing messages with CE using RIP protocol on the PE router, we should first create corresponding VPN routing/transmitting examples to associate with

corresponding interfaces. Then enter the RIP address family mode configuring corresponding parameters.

If the RIP routing problem remains unresolved, please use debug rip command to record the debug message in three minutes, and send them to our technical service center.

17.4.5.1 Commands for Monitor And Debug

17.4.5.1.1 show debugging rip

Command: show debugging rip

Function: Show RIP event debugging, RIP packet debugging and RIP nsm debugging status

Command Mode: Any mode

Example: Switch# show debugging rip

RIP debugging status:

RIP event debugging is on

RIP packet detail debugging is on

RIP NSM debugging is on

17.4.5.1.2 show ip protocols rip

Command: show ip protocols rip

Function: Show the RIP process parameter and statistics information

Command Mode: Any mode

Example:

show ip protocols rip

Routing Protocol is "rip"

Sending updates every 30 seconds with +/-50%, next due in 8 seconds

Timeout after 180 seconds, garbage collect after 120 seconds

Outgoing update filter list for all interface is not set

Incoming update filter list for all interface is not set

Default redistribution metric is 1

Redistributing: static

Default version control: send version 2, receive version 2

Interface Send Recv Key-chain

Vlan1 2 2

Routing for Networks:

Vlan1

Vlan2

Routing Information Sources:

Gateway Distance Last Update Bad Packets Bad Routes
20.1.1.1 120 00:00:31 0 0
Distance: (default is 120)

Displayed information	Explanation
Sending updates every 30 seconds with +/-50%, next due in 8 seconds	Sending update every 30 secs
Timeout after 180 seconds, garbage collect after 120 seconds	The route time-out event period is 180 secs, the garbage collect time is 120 seconds
Outgoing update filter list for all interface is not set	Outgoing update filter list for all interface is not set
Incoming update filter list for all interface is not set	Incoming update filter list for all interface is not set
Default redistribution metric is 1	Default redistribution metric is 1
Redistributing: static	Redistributing the static route into the RIP route
Default version control: send version 2, receive version 2 Interface Send Recv Key-chain Ethernet1/8 2 2	The configuration of interface receiving and sending packets. Receive version is 2, keychain 1 not configured.
Routing for Networks: Vlan1 Vlan2	The segment running RIP is the Vlan 1 and Vlan 2
Routing Information Sources: Gateway Distance Last Update Bad Packets Bad Routes 20.1.1.1 120 00:00:31 0 0	Routing information sources The bad packetand bad routes from the gateway 20.1.1.1 are all 0. 31 seconds have passed since the last route update. The manage distance is 120
Distance: (default is 120)	Default manage distance is 120

17.4.5.1.3 show ip rip

Command: show ip rip

Function: Show the routes in the RIP route data base

Command Mode: Any mode

Example:

show ip rip

Codes: R - RIP, K - Kernel, C - Connected, S - Static, O - OSPF, I - IS-IS,

B - BGP

	Network	Next Hop	Metric	From	If	Time
R	12.1.1.0/24	20.1.1.1	2	20.1.1.1	Vlan1	02:51
R	20.1.1.0/24		1		Vlan1	

Amongst R stands for RIP route, namely a RIP route with the destination network address 12.1.1.0, the network prefix length as 24, next-hop address at 20.1.1.1. It is learnt from the Ethernet port E1/8 with a metric value of 2, and still has 2 minutes 51 seconds before time out.

17.4.5.1.4 show ip rip database

Command: show ip rip database

Function: Show the routes in the RIP route database

Command Mode: Any mode

Example: Switch# show ip rip database

Codes: R - RIP, K - Kernel, C - Connected, S - Static, O - OSPF, I - IS-IS,

B -BGP

	Network	Next Hop	Metric	From	If	Time
R	10.1.1.0/24		1		Vlan1	
R	20.1.1.0/24		1		Vlan2	

Command: show ip rip

17.4.5.1.5 show ip rip database vrf

Command: show ip rip database vrf <*vrf-name*>

Function: This command display the RIP database messages related to the VPN routing/forwarding instances.

Parameter: Specifies the name of VPN routing/forwarding instances.

Command Mode: Any mode

Example: Switch# show ip rip database vrf IPI

Codes: R - RIP, K - Kernel, C - Connected, S - Static, O - OSPF, I - IS-IS,

B - BGP

	Network	Next Hop	Metric	From	If	Time
R	10.1.1.0/24		1		Vlan1	00:46

17.4.5.1.6 show ip rip interface

Command: show ip rip interface [**<*ifname*>**]

Function: Show the RIP related messages

Parameter: <*ifname*> is the name of the interface to show the messages

Command Mode: Any mode

Example: Switch# show ip rip interface vlan 1

Vlan1 is up, line protocol is up

Routing Protocol: RIP

Receive RIP packets

Send RIP packets

Passive interface: Disabled

Split horizon: Enabled with Poisoned Reversed

IP interface address:

10.1.1.1/24

17.4.5.1.7 show ip rip interface vrf

Command: show ip rip interface vrf <*vrf-name*>[<*ifname*>]

Function: This command shows RIP interface relevant to VPN routing/forwarding instances

Parameter: Specifies the name of VPN routing/forwarding instances

<ifname> is the name of the interfaces

Command Mode: Any mode

Example: Switch# show ip rip interface vrf IPI Vlan1

Ethernet1/1 is up, line protocol is up

Routing Protocol: RIP

VPN Routing/Forwarding: vpnb

Receive RIP packets

Send RIP packets

Passive interface: Disabled

Split horizon: Enabled with Poisoned Reversed

IP interface address:11.1.1.1/24

Displayed information	Explanations
Vlan1 is up, line protocol is up	Interface is up
Routing Protocol: RIP	The protocol running on the interface is RIP
VPN Routing/Forwarding: vpnb	Interface relates to the VPN routing/forwarding instances.
Receive RIP packets	The interface can receive RIP packets
Send RIP packets	The interface can send RIP packets
Passive interface: Disabled	Passive-interface disabled
Split horizon: Enabled with Poisoned Reversed	Configure a split horizon with poison reversed
IP interface address:11.1.1.1/24	The IP address of the interface.

17.4.5.1.8 show ip vrf

Command: show ip vrf [<*vrf-name*>]

Function: This command shows the RIP instances messages related to the VPN routing/forwarding instances

Parameter: Specifies the name of the VPN routing/forwarding instances

Command Mode: Any mode

Usage Guide: The command also exist in other routing protocols, when using this command, messages of other routing protocol processes related to this VPN routing/forwarding instances will also be displayed

Example: Switch# show ip vrf IPI

VRF IPI, FIB ID 1

Router ID: 11.1.1.1 (automatic)

Interfaces:

Vlan1

!

VRF IPI; (id=1); RIP enabled Interfaces:

Ethernet1/8

Name Interfaces

IPI Vlan1

Name Default RD Interfaces

IPI Vlan1

17.5 RIPng

17.5.1 Introduction to RIPng

RIP is first introduced in ARPANET, this is a protocol dedicated to small, simple networks. RIPng is a distance vector routing protocol based on the Bellman-Ford algorithm. Network devices running vector routing protocol send 2 kind of information to the neighboring devices regularly:

• Number of hops to reach the destination network, or metrics to use or number of networks to pass.

• What is the next hop, or the director (vector) to use to reach the destination network.

Distance vector layer3 switches send all their route selecting tables to the neighbor layer3 switches at regular interval. A layer3 switch will build their own route selecting information table based on the information received from the neighbor layer3 switches.

Then, it will send this information to its own neighbor layer3 switches. As a result, the route selection table is built on second hand information, route beyond 15 hops will be deemed as unreachable.

RIPng is an optional routing protocol based on UDP. Hosts using RIPng send and receive packets on UDP port 521. All layer3 switches running RIPng send their route table to all neighbor layer3 switches every 30 seconds for update. If no information from the partner is received in 180 seconds, then the device is deemed to have failed and the network connected to that device is considered to be unreachable. However, the route of that layer3 switch will be kept in the route table for another 120 seconds before deletion.

As layer3 switches running RIPng build route table with second hand information, infinite count may occur. For a network running RIP routing protocol, when a RIPng route becomes unreachable, the neighboring RIPng layer3 switch will not send route update packets at once, instead, it waits until the update interval timeout (every 30 seconds) and sends the update packets containing that route. If before it receives the updated packet, its neighbors send packets containing the information about the failed neighbor, “infinite count” will be resulted. In other words, the route of unreachable layer3 switch will be selected with the metrics increasing progressively. This greatly affects the route selection and route aggregation time.

To avoid “infinite count”, RIPng provides mechanism such as “split horizon” and “triggered update” to solve route loop. “Split horizon” is done by avoiding sending to a gateway routes leaned from that gateway. There are two split horizon methods: “simple split horizon” and “poison reverse split horizon”. Simple split horizon deletes from the route to be sent to the neighbor gateways the routes learnt from the neighbor gateways; poison reverse split horizon not only deletes the abovementioned routes, but set the costs of those routes to infinite. “Triggering update” mechanism defines whenever route metric changed by the gateway, the gateway advertise the update packets immediately other than wait for the 30 sec timer.

So far the RIPng protocol has got only one version----Version1: RIPng protocol is introduced in RFC 2080. RIPng transmits updating data packet by multicast data packet (multicast address FF02::9)

Each layer3 switch running RIPng has a route database, which contains all route entries for reachable destination, and route table is built based on this database. When a RIPng layer3 switch sent route update packets to its neighbor devices, the complete route table is included in the packets. Therefore, in a large network, routing data to be transferred and processed for each layer3 switch is quite large, causing degraded network performance.

Besides the above mentioned, RIPng protocol allows IPv6 route information discovered by the other routing protocols to be introduced to the route table.

The operation of RIP protocol is shown below:

Enable RIPng The switch sends request packets to the neighbor layer3 switches by broadcasting; on receiving the request, the neighbor devices reply with the packets containing their local routing information.

The Layer3 switch modifies its local route table on receiving the reply packets and sends triggered update packets to the neighbor devices to advertise route update information. On receiving the triggered update package, the neighbor lay3 switches send triggered update packages to their neighbor lay3 switches. After a sequence of triggered update package broadcast, all layer3 switches get and maintain the latest route information.

In addition, RIPng layer3 switches will advertise its local route table to their neighbor devices every 30 seconds. On receiving the packets, neighbor devices maintain their local route table, select the best route and advertise the updated information to their own neighbor devices, so that the updated routes are globally valid. Moreover, RIP uses a timeout mechanism for outdated route, that is, if a switch does not receive regular update packets from a neighbor within a certain interval (invalid timer interval), it considers the route from that neighbor invalid, after holding the route fro a certain interval (garbage collect timer interval), it will delete that route.

As a result of continuous development of IPv6 network, it has the network environment of nonsupport IPv6 sometimes, so it needs to do the IPv6 operation by tunnel. Therefore, our RIPng supports configuration on configure tunnel, and passes through nonsupport IPv6 network by unicast packet of IPv4 encapsulation.

17.5.2 RIPng Configuration Task List

1. Enable RIPng protocol (required)
   （1） Enable/disable RIPng protocol
   （2） Configure the interfaces running RIPng protocol
2. Configure RIPng protocol parameters (optional)
   （1） Configure RIPng sending mechanism
      1) Configure specified RIPng packets transmission address
   （2） Configure RIP routing parameters
      1) Configure route introduction (default route metric, configure routes of the other protocols to be introduced in RIPng)
      2) Configure the route deviation
      3) Configure and apply route filter
      4) Configure split horizon
   （3） Configure other RIPng parameters
      1）Configure timer for RIPng update, timeout and hold-down

（4） Delete the specified route in RIPng route table

1. Enable RIPng protocol

Applying RIPng route protocol with basic configuration in ES4626/ES4650 switch is simple. Normally you only have to open the RIPng switch and configure the segments running RIPng, namely send and receive the RIPng data packet by default RIPng configuration.

Command	**Explanation**
Global mode	
[no] router IPv6 rip	Enables the RIPng protocol; the [no] router IPv6 rip command shuts the RIPng protocol.
Interface configuration mode	
[no] IPv6 router rip	configure the interface to run RIPng protocol; the **[no] IPv6 router rip** command set the interface not run RIPng protocol

2. Configure RIPng protocol parameters

（1）Configure RIPng sending mechanism

1）configure the RIPng data packets point-transmitting

Command	**Explanation**
Router configuration mode	
[no] neighbor *<IPv6-address> <ifname>*	Specify the IPv6 Link-local address and interface of the neighboring route needs point-transmitting; the [no] neighbor *<IPv6-address> <ifname>* command cancels the appointed router.
[no] passive-interface *<ifname>*	Block the RIPng multicast on specified port and the RIPng data packet is only transmittable among Layer 3 switch configured with neighbor. the [**no**] **passive-interface *<ifname>*** command cancels the function

（2）Configure RIP routing parameters

1）configure route introduction (default route metric, configure routes of the other protocols to be introduced in RIP)

Command	**Explanation**
Router configuration mode	

default-metric <*value*> **no default-metric**	Configure the default metric of distributed route; the **default-metric <*value*>** no default-metric command restores the default configuration 1
[no]redistribute {kernel |connected| static| ospf| isis| bgp} [metric<*value*>] [route-map<*word*>]	Redistribute the routes distributed in other route protocols into the RIPng data packet; the **[no]redistribute {kernel |connected| static| ospf| isis| bgp} [metric<*value*>] [route-map<*word*>]** command cancels the distributed route of corresponding protocols
[no]default-information originate	Generate a default route to the RIPng protocol; the **[no]default-information originate** command cancels the feature.

2）Configure the route offset

Command	**Explanation**
Router configuration mode	
[no] offset-list <*access-list-number* |*access-list-name*> {in|out} <*number* > [<*ifname*>]	Configure that provide a deviation value to the route metric value when the port sends or receives RIPng data packet; the **[no] offset-list <*access-list-number* |*access-list-name*> {in|out} <*number* > [<*ifname*>]** command removes the deviation table

c）configure and apply route filter and route aggregation

Command	**Explanation**
Router configuration mode	
[no] distribute-list {< *access-list-number* |*access-list-name* > | prefix<*prefix-list-name*>} {in|out} [<*ifname*>]	Set to filter the route when the interface sends and receives RIPng data packets. The **[no] distribute-list {< *access-list-number* |*access-list-name* > | prefix<*prefix-list-name*>} {in|out} [<*ifname*>]** command means do not set the route filter

[no]aggregate-address *<IPv6-address>*	Configure route aggregation, the **[no]aggregate-address *<IPv6-address*** command cancels the route aggregation.

3）configure split horizon

Command	**Explanation**
Interface configuration mode	
IPv6 rip split-horizon [poisoned]	Configure that take the split-horizon when the port sends data packets, poisoned means with poison reverse
no IPv6 rip split-horizon	Cancel the split-horizon.

3. Configure other RIPng protocol parameters

（1）Configure timer for RIPng update, timeout and hold-down

Command	**Explanation**
Router configuration mode	
timers basic <*update*> <*invalid*> <*garbage*> **no timers basic**	Adjust the renew, timeout and garbage recycle RIPng timer, the no timers basic command restore the default configuration

4. Delete the specified route in RIPng route table

Command	**Explanation**
Admin Mode	
clear IPv6 rip route {<*IPv6-address*>|kernel|static|connected|rip|ospf|isis|bgp|all}	the command deletes a specified route from the RIP route table

17.5.3 Commands For RIPng

17.5.3.1 aggregate-address

Command: [no] aggregate-address<*ipv6-address*>

Function: Aggregate RIPng route. The "**[no] aggregate-address<*ipv6-address*>**" command cancels the aggregation

Parameter: <*ipv6-address*> is the IPv6 network address, shown in cloned hex notation with the length of prefix.

Default: No aggregation to any address

Command Mode: Router mode

Usage Guide: none

Example: Switch# config terminal

Switch(config)# router ipv6 rip

Switch(config-router)# aggregate-address 3ffe:8088::/32

17.5.3.2 clear ipv6 route

Command: clear ipv6 rip route { *<ipv6-address >*| kernel |static | connected |rip |ospf |isis | bgp |all }

Function: Clear specific route from the RIPng route table

Parameter: Clears the route exactly match with the destination address from the RIP route table

<ipv6-address > is the destination address shown in hex notation with prefix length.

kernel delete kernel route from the RIPng route table

static delete static route from the RIPng route table

connected delete direct route from the RIPng route table

rip delete RIPng route from the RIPng route table only

ospf delete IPv6 OSPF route from the RIPng route table only

bgp delete IPv6 BGP route from the RIPng route table only

ISIS delete ivp6 isis route from the RIPng route table only

all delete all routes from the RIPng route table

Default: No default configuration

Command Mode: Admin mode

Usage Guide: All routes in the RIPng route table will be deleted by using this command with all parameters.

Example: Switch# clear ipv6 rip route 2001:1:1::/64

Switch# clear ipv6 rip route ospf

17.5.3.3 default-information originate

Command: default-information originate

no default-information originate

Function: Permit redistributing the network 0:: into RIPng. The "**no default-information originate**" disables this function

Parameter: None

Default: Disabled

Command Mode: Router mode

Example: Switch# config terminal

Switch(config)# router ipv6 rip

Switch(config-router)# default-information originate

17.5.3.4 default-metric

Command: default-metric <*value*>

no default-metric

Function: Set the default metric route value of the introduced route; the "**no default-metric**" restores the default value.

Parameter: <*value*> is the route metric value to be set, ranging between 1～16.

Default: Default route metric value is 1.

Command Mode: Router mode

Usage Guide: Default-metric command is used for setting the default route metric value of the routes from other routing protocols when distributed into the RIPng routes. When using the **redistribute** commands for introducing routes from other protocols, the default route metric value specified by **default-metric** will be adopted if no specific route metric value is set.

Example: Set the default route metric value of the routes from other routing protocols when distributed into the RIPng routes as 3.

Switch(Config-router)#default-metric 3

17.5.3.5 ipv6 rip split-horizon

Command: ipv6 rip split-horizon [poisoned]

no ipv6 rip split-horizon

Function: Permit the split horizon. The "**no ipv6 rip split-horizon**" disables the split horizon

Parameter: [poisoned] configures split horizon with poison reverse.

Default: Split horizon with poison reverse

Command Mode: Interface Mode

Usage Guide: The split horizon is for preventing the routing loops, namely preventing the layer 3 switch from broadcasting a route at the interface from which the very route is learnt. The command can configure on IPv6 tunnel interface, but it is successful configuration to only configure tunnel carefully.

Example: Switch# config terminal

Switch(config)# interface Vlan1

Switch(config-if-Vlan1)# ipv6 rip split-horizon poisoned

17.5.3.6 distribute-list

Command: [no]distribute-list{*access-list-name*> |prefix<*prefix-list-name*>} {in|out} [<*ifname*>]

Function: This command uses access-list or prefix-list to filter the route renews messages sent and received. The "**[no]distribute-list{*access-list-name*> |prefix<*prefix-list-name*>} {in|out} [<*ifname*>]**" command cancels this filter function

Parameter: ***<access-list-name>*** is the name or access-list number to be applied. ***<prefix-list-name>*** is the name of the prefix-list to be applied. ***<ifname>*** specifies the name of interface to be applied with route filtering

Default: Function disabled by RIPng by default

Command Mode: Router mode

Usage Guide: The filter will be applied to all interfaces if no specific interface is set.

Example:

Switch# config terminal

Switch(config)# router ipv6 rip

Switch(config-router)# distribute-list prefix myfilter in Vlan1

17.5.3.7 ipv6 router rip

Command: ipv6 router rip

no ipv6 router rip

Function: Enable RIPng on the interface. The "no ipv6 router rip" command disables RIPng on the interface.

Default: Not configured

Command Mode: Interface Mode

Usage Guide: The command can configure on IPv6 tunnel interface, but it is successful configuration to only configure tunnel carefully.

Example:

Switch# config terminal

Switch(config)# interface Vlan1

Switch(config-if-Vlan1)# ipv6 router rip

17.5.3.8 neighbor

Command: [no] neighbor <*ipv6-address*> <*ifname*>

Function: Specify the destination address for fixed sending. The "**[no] neighbor <*ipv6-address*> <*ifname*>**" cancels the specified address defined and restores all trusted gateways

Parameter: ***<ipv6-address>*** is the IPv6 Link-local address specified for sending and shown in colon hex notation without the prefix length. ***<ifname>*** is the name of interface.

Default: Not sending to any fixed destination address

Command Mode: Router mode

Usage Guide: When used associating passive-interface command it would be able to

send routing messages to specified neighbor only.

Example:

Switch# config terminal

Switch(config)# router ipv6 rip

Switch(config-router)# neighbor FE80:506::2 Vlan1

17.5.3.9 Offset-list

**Command: [no] offset-list <*access-list-number*
|*access-list-name*> {in|out }<*number* >[<*ifname*>]**

Function: Add an offset value on the routing metric value learnt by RIPng. The "**|*access-list-name*> {in|out }<*number* >[<*ifname*>]**" command disables this function

Parameter: < *access-list-number* |*access-list-name*> is the access-list or name to be applied. **<*number* >** is the additional offset value, ranging between 0-16; <*ifname*> is the name of specific interface

Default: The default offset value is the metric value of the interface defined by the system.

Command Mode: Router mode

Example:

Switch# config terminal

Switch(config)# router ipv6 rip

Switch(config-router)# offset-list 1 in 5 Vlan1

17.5.3.10 passive-interface

Command: [**no**] **passive-interface<*ifname*>**

Function: Set the RIP layer 3 switches to block RIP broadcast on the specified interfaces, and only send the RIP data packet to the layer 3 switch which is configured with neighbor.

Parameter: <***ifname***> is the specific interface name

Default: Not configured

Command Mode: Router mode

Example:

Switch# config terminal

Switch(config)# router ipv6 rip

Switch(config-router)# passive-interface Vlan1

17.5.3.11 redistribute

Command:[no]redistribute {kernel |connected| static| ospf| isis| bgp} [metric<*value*>] [route-map<*word*>]

Function: Introduce the routes learnt from other routing protocols into RIP

Parameter: kernel introduce from kernel routes

connected introduce from direct routes

static introduce from static routes

ospf introduce from IPv6 OSPF routes

isis introduce from IPv6 ISIS routes

bgp introduce from IPv6 BGP routes

<value> is the metric value assigned to the introduced route, ranging between 0-16

<word> is the probe pointing to the route map for introducing routes

Command Mode: **Router mode**

Example:

Switch# config terminal

Switch(config)# router ipv6 rip

Switch(config-router)# redistribute kernel route-map ipi

17.5.3.12 route

Command: route *<ipv6-address>*

no route *<ipv6-address>*

Function: This command configures a static RIP route. The "**no route *<ipv6-address>***" command deletes this route.

Parameter: **Specifies this destination IPv6 address prefix and its length show in colon hex notation.**

Usage Guide: The command add a static RIPng route, and is mainly used for debugging. Routes configured by this command will not appear in kernel route table but in the RIP route database, however it could be located by using the show ipv6 rip command.

Command Mode: Router mode

Example:

Switch# config terminal

Switch(config)# router ipv6 rip

Switch(config-router)# route 3ffe:1234:5678::1/64

17.5.3.13 router ipv6 rip

Command: router ipv6 rip

no router ipv6 rip

Function: Enable RIPng routing process and entering RIPng mode; the "**no router ipv6 rip**" of this command disables the RIPng routing protocol.

Default: RIPng routing not running

Command Mode: Global mode

Usage Guide: This command is for enabling the RIPng routing protocol, this command should be enabled before performing other global configuration of the RIPng protocol.

Example: Enable the RIPng protocol mode

Switch(Config)#router ipv6 rip

Switch(Config-Router)#

17.5.4 RIPng Configuration Examples

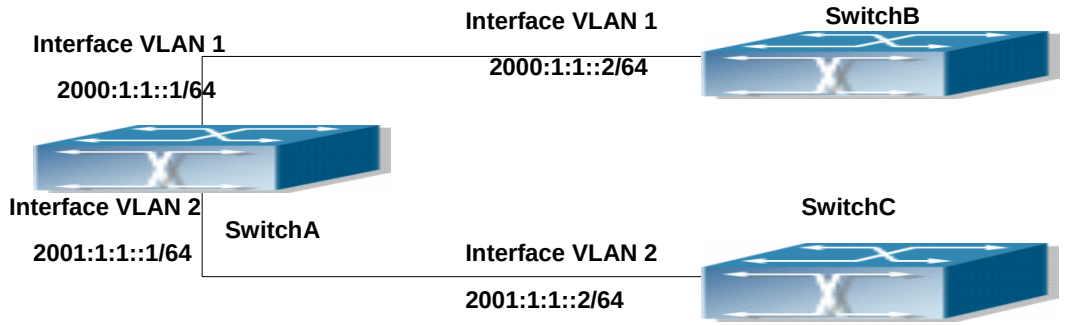


Fig 17-5 RIPng Example

As shown in the above figure, a network consists of three layer 3 switches. SwitchA and SwitchB connect to SwitchC through interface vlan1 and vlan2. All the three switches are running RIPng. Assume SwitchA（VLAN1：2001:1:1::1/64 and VLAN2：2001:1:1::1/64）exchange update information with SwitchB（VLAN1：2001:1:1::2/64） only, update information is not exchanged between SwitchA and SwitchC（VLAN1：2001:1:1::2/64）. The configuration for SwitchA, SwitchB and SwitchC is shown below:

Layer 3 SwitchA

Enable RIPng protocol

SwitchA (config)#router IPv6 rip

SwitchA (config-router)#exit

Configure the IPv6 address and interfaces of Ethernet port vlan1 to run RIPng

SwitchA#config

SwitchA (config)# interface Vlan1

SwitchA (config-if-Vlan1)# IPv6 address 2000:1:1::1/64

SwitchA (config-if-Vlan1)#IPv6 router rip

SwitchA (config-if-Vlan1)#exit

Configure the IPv6 address and interfaces of Ethernet port vlan2 to run RIPng

SwitchA (config)# interface Vlan2
SwitchA (config-if-Vlan2)# IPv6 address 2001:1:1::1/64
SwitchA (config-if-Vlan2)#IPv6 router rip
SwitchA (config-if-Vlan2)#exit

Configure the interface vlan1 do not send RIPng messages to SwitchC
SwitchA (config)#
SwitchA (config-router)#passive-interface Vlan1
SwitchA (config-router)#exit
Layer 3 SwitchB
Enable RIPng protocol
SwitchB (config)#router IPv6 rip
SwitchB (config-router-rip)#exit
Configure the IPv6 address and interfaces of Ethernet port vlan1 to run RIPng
SwitchB #config
SwitchB (config)# interface Vlan1
SwitchB (config-if)# IPv6 address 2001:1:1::2/64
SwitchB (config-if)#IPv6 router rip
SwitchB (config-if)exit

Enable RIPng protocol
SwitchC (config)#router IPv6 rip
SwitchC (config-router-rip)#exit
Configure the IPv6 address and interfaces of Ethernet port vlan1 to run RIPng
SwitchC#config
SwitchC (config)# interface Vlan1
SwitchC (config-if)# IPv6 address 2000:1:1::2/64
SwitchC (config-if)#IPv6 router rip
SwitchC (config-if)exit

17.5.5 RIPng Troubleshooting

The RIPng protocol may not be working properly due to errors such as physic connection, configuration error when configuring and using the RIPng protocol. So users should pay attention to the following:
first ensure the physic connection is correct and the IP Forwarding command is open
second, ensure the interface and link layer protocol are UP (use show interface command)

then initiate the RIPng protocol (use router IPv6 rip command) and configure the port (use IPv6 router command) ,and set RIPng protocol parameter on corresponding interfaces.

After that, a RIPng protocol feature should be noticed ---the Layer 3 switch running RIPng transmits the route updating messages every 30 seconds. A Layer 3 switch is considered inaccessible if no route updating messages from the switch are received within 180 seconds, then the route to the switch will remains in the route table for 120 seconds before it is deleted. Therefore, if to delete a RIPng route, this route item is assured to be deleted from route table after 300 seconds.

If the RIP routing problem remains unresolved, please use debug IPv6 rip command to record the debug message in three minutes, and send them to our technical service center.

17.5.5.1 Monitor And Debug Command

17.5.5.1.1 debug ipv6 rip

Command: [no] debug ipv6 rip [events| nsm| packet[recv|send][detail]| all]

Function: For opening various debugging switches of RIPng, showing various debugging messages. The "**[no] debug ipv6 rip [events| nsm| packet[recv|send][detail]| all]**" command close the corresponding debugging switch

Parameter: Events shows the debugging message of RIPng events

Nsm shows the communication messages between RIPng and NSM.

Packet shows the debugging messages of RIPng data packets

Recv shows the messages of the received data packets

Send shows the messages of the sent data packets

Detail shows the messages of the data packets received or sent.

Default: Not enabled

Command Mode: Admin mode and global mode

Example: Switch# debug ipv6 rip packet

Switch#1970/01/01 21:15:08 IMI: SEND[Ethernet1/10]: Send to [ff02::9]:521

1970/01/01 21:15:08 IMI: SEND[Ethernet1/2]: Send to [ff02::9]:521

1970/01/01 21:15:09 IMI: RECV[Ethernet1/10]: Receive from [fe80::20b:46ff:fe57:8e60]:521

1970/01/01 21:15:09 IMI: RECV[Ethernet1/10]: 3000:1:1::/64 is filtered by access-list dclist

1970/01/01 21:15:09 IMI: RECV[Ethernet1/10]: 3ffe:1:1::/64 is filtered by access-list dclist

1970/01/01 21:15:15 IMI: RECV[Ethernet1/2]: Receive from [fe80::203:fff:fe01:257c]:521

17.5.5.1.2 show debugging ipv6 rip

Command: show debugging ipv6 rip

Function: Show RIPng debugging status for following debugging options: nsm debugging, RIPng event debugging, RIPng packet debugging and RIPng nsm debugging

Command Mode: Any mode

Example: Switch# show debugging rip

RIP debugging status:

RIPng event debugging is on

RIPng packet detail debugging is on

RIPng NSM debugging is on

17.5.5.1.3 show ipv6 rip interface

Command: show ipv6 rip interface

Function: Make sure the interface and line protocols is up,.

Command Mode: Any mode

Example: Loopback is up, line protocol is up

RIPng is not enabled on this interface

Vlan1 is up, line protocol is up

Routing Protocol: RIPng

Passive interface: Disabled

Split horizon: Enabled with Poisoned Reversed

IPv6 interface address:

3000:1:1::1/64

fe80::203:fff:fe01:429e/64

Displayed information	Explanations
Vlan1 is up, line protocol is up	Interface is Up
Routing Protocol: RIP	The routing protocol running on the interface is RIPng
Passive interface: Disabled	Passive-interface disabled
Split horizon: Enabled with Poisoned Reversed	The split horizon is enabled with poisoned reversed on the interface.
IP interface address: 3000:1:1::1/64 fe80::203:fff:fe01:429e/64	IPv6 address of the interface

17.5.5.1.4 show ipv6 protocols rip

Command: show ipv6 protocols rip

Function: Show the RIPng process parameters and statistic messages

Command Mode: Any mode

Example: Routing Protocol is "RIPng"

Sending updates every 30 seconds with +/-50%, next due in 1 second

Timeout after 180 seconds, garbage collect after 120 seconds

Outgoing update filter list for all interfaces is not set

Incoming update filter list for all interfaces is not set

Ethernet1/10 filtered by dclist

Default redistribute metric is 1

Redistributing: static

Interface

Vlan10

Vlan2

Routing for Networks:

Displayed information	Explanations
Sending updates every 30 seconds with +/-50%, next due in 1 seconds	Sending updates every 30 seconds
Timeout after 180 seconds, garbage collect after 120 seconds	The route timeout time is 180 seconds, the garbage collect time is 120 seconds
Outgoing update filter list for all interface is not set	Outgoing update filter list for all interface is not set
Incoming update filter list for all interface is not set	Incoming update filter list for all interface is not set
Default redistribution metric is 1	Default redistribution metric is 1
Redistributing: static	Redistricting the static route into the RIP routes
Interface Vlan10 Vlan2	The interfaces running RIP is Vlan 10 and Vlan 2
Routing for Networks:	

17.5.5.1.5 show ipv6 rip

Command: show ipv6 rip

Function: Show RIPng Routing

Command Mode: Any mode

Example: Switch# show ipv6 rip

Codes: R - RIP, K - Kernel, C - Connected, S - Static, O - OSPF, I - IS-IS,

B - BGP, a - aggregate, s - suppressed

	Network	Next Hop	If	Met	Tag	Time
R	2000:1:1::/64	::	Vlan2	1		0
R	2001:1:1::/64	fe80::203:fff:fe01:257c	Vlan2	2		02:40
R	3000:1:1::/64	::	Vlan10	1		0
R	3010:1:1::/64	::	--	1		0

Amongst R stands for RIP route, namely a RIP route with the destination network address 2001:1:1::/64, next-hop address at fe80::203:fff:fe01:257c. It is learnt from the Ethernet port VLAN2 with a metric value of 2, and still has 2 minutes 40 seconds before time out.

17.5.5.1.6 show ipv6 rip database

Command: show ipv6 rip database

Function: Show messages related to RIPng database

Command Mode: Any mode

Example: Switch# show ipv6 rip database

17.5.5.1.7 show ipv6 rip interface

Command: show ipv6 rip interface [***<ifname>***]

Function: Show RIPng interface related messages

Parameter: *<ifname>* is the name of the interface to be displayed

Command Mode: Any mode

Example: Switch# show ip rip interface Vlan1

Loopback is up, line protocol is up

RIPng is not enabled on this interface

Ethernet1/10 is up, line protocol is up

Routing Protocol: RIPng

Passive interface: Disabled

Split horizon: Enabled with Poisoned Reversed

IPv6 interface address:

3000:1:1::1/64

fe80::203:fff:fe01:429e/64

17.6 OSPF

17.6.1 Introduction to OSPF

OSPF is abbreviation for Open Shortest Path First. It is an interior dynamic routing

protocol for autonomous system based on link-state. The protocol creates a link-state database by exchanging link-states among layer3 switches, and then uses the Shortest Path First algorithm to generate a route table basing on that database.

Autonomous system (AS) is a self-managed interconnected network. In large networks, such as the Internet, a giant interconnected network is broken down to autonomous systems. Big enterprise networks connecting to the Internet are independent AS, since the other host on the Internet are not managed by those AS and they don't share interior routing information with the layer3 switches on the Internet.

Each link-state Layer3 switch can provide information about the topology with its neighboring Layer3 switches.

- The network segment (link) connecting to the layer3 switch
- State of the connecting link

Link-state information is flooded throughout the network so that all Layer3 switches can get firsthand information. Link-state Layer3 switches will not broadcast all information contained in their route tables; instead, they only send changed link-state information. Link-state Layer3 switches establish neighborhood by sending "HELLO" to their neighbors, then link-state advertisements (LSA) will be sent among neighboring Layer3 switches. Neighboring Layer3 switch copy the LSA to their routing table and transfer the information to the rest part of the network. This process is referred to as "flooding". In this way, firsthand information is sent throughout the network to provide accurate map for creating and updating routes in the network. Link-state routing protocols use cost instead of hops to decide the route. Cost is assigned automatically or manually. According to the algorithm in link-state protocol, cost can be used to calculate the hop number for packages to pass, link bandwidth, and current load of the link.. The administrator can even add weight for better assessment of the link-state.

1) When a link-state layer3 switch enters a link-state interconnected network, it sends a HELLO package to get to know its neighbors and establish neighborhood.

2) The neighbors respond with information about the links they are connecting and the related costs.

3) The originate layer3 switch uses this information to build its own routing table

4) Then, as part of the regular update, layer3 switch send link-state advertisement (LSA) packages to its neighboring layer3 switches. The LSA include links and related costs of that layer3 switch.

5) Each neighboring layer3 switch copies the LSA package and passes it to the next neighbor (i.e. flooding).

6) Since routing database is not recalculated before layer3 switch forwards LSA flooding, the converging time is greatly reduced.

One major advantage of link-state routing protocols is the fact that infinite counting is

impossible, this is because of the way link-state routing protocols build up their routing table. The second advantage is that converging in a link-state interconnected network is very fast, once the routing topology changes, updates will be flooded throughout the network very soon. Those advantages release some layer3 switch resources, as the process ability and bandwidth used by bad route information are minor.

The features of OSPF protocol include the following: OSPF supports networks of various scales, several hundreds of layer3 switches can be supported in an OSPF network. Routing topology changes can be quickly found and updating LSAs can be sent immediately, so that routes converge quickly. Link-state information is used in shortest path algorithm for route calculation, eliminating loop route. OSPF divides the autonomous system into areas, reducing database size, bandwidth occupation and calculation load. (According to the position of layer3 switches in the autonomous system, they can be grouped as internal area switches, area edge switches, AS edge switches and backbone switches). OSPF supports load balance and multiple routes to the same destination of equal costs. OSPF supports 4 level routing mechanisms (process routing according to the order of route inside an area, route between areas, first category exterior route and second category exterior route). OSPF support IP subnet and redistribution of routes from the other routing protocols, and interface-based packet verification. OSPF supports sending packets in multicast.

Each OSPF layer3 switch maintains a database describing the topology of the whole autonomous system. Each layer3 switch gathers the local status information, such as available interface, reachable neighbors, and sends link-state advertisement (sending out link-state information) to exchange link-state information with other OSPF layer3 switches to form a link-state database describing the whole autonomous system. Each layer3 switch builds a shortest path tree rooted by itself according to the link-state database, this tree provide the routes to all nodes in an autonomous system. If two or more layer3 switches exist (i.e. multi-access network), "designated layer3 switch" and "backup designated layer3 switch" will be selected. Designated layer3 switch is responsible for spreading link-state of the network. This concept helps reducing the traffic among the Layer3 switches in multi-access network.

OSPF protocol requires the autonomous system to be divided into areas. That is to divide the autonomous system into 0 area (backbone area) and non-0 areas. Routing information between areas are further abstracted and summarized to reduce the bandwidth required in the network. OSPF uses four different kinds of routes; they are the route inside the area, route between areas, first category exterior route and second category exterior route, in the order of highest priority to lowest. The route inside an area and between areas describe the internal network structure of an autonomous system, while external routes describe how to select the routing information to destination outside

the autonomous system. The first type of exterior route corresponds to the information introduced by OSPF from the other interior routing protocols, the costs of those routes are comparable with the costs of OSPF routes; the second type of exterior route corresponds to the information introduced by OSPF from the other exterior routing protocols, but the costs of those routes are far greater than that of OSPF routes, so OSPF route cost is ignored when calculating route costs.

OSPF areas are centered with the Backbone area, identified as Area 0, all the other areas must be connected to Area 0 logically, and Area 0 must be continuous. For this reason, the concept of virtual link is introduced to the backbone area, so that physically separated areas still have logical connectivity to the backbone area. The configurations of all the layer3 switches in the same area must be the same.

In conclusion, LSA can only be transferred between neighboring Layer3 switches, OSPF protocol includes 5 types of LSA: router LSA, network LSA, summary LSA to the other areas, general LSA to AS edge switches and exterior AS LSA. They can also be called type1 LSA, type2 LSA, type3 LSA, type4 LSA, and type5 LSA. Router LSA is generated by each layer3 switch inside an OSPF area, and is sent to all the other neighboring layer3 switches in the same area; network LSA is generated by the designated layer3 switch in the OSPF area of multi-access network, and is sent to all other neighboring layer3 switches in this area. (In order to reduce traffic on layer3 switches in the multi-access network, “designated layer3 switch” and “backup designated layer3 switch” should be selected in the multi-access network, and the network link-state is broadcasted by the designated layer3 switch); summary LSA is generated by edge switches in an OSPF area , and is transferred among area edge layer3 switches; AS exterior LSA is generated by layer3 switches on exterior edge of AS, and is transferred throughout the AS.

As to autonomous systems mainly advertises exterior link-state, OSPF allow some areas to be configured as STUB areas to reduce the size of the topology database. Type4 LSA (ASBR summary LSA) and type5 LSA (AS exterior LSA) are not allowed to flood into/through STUB areas. STUB areas must use the default routes, the layer3 switches on STUB area edge advertise the default routes to STUB areas by type 3 summary LSA, those default routes only flood inside STUB area and will not get out of STUB area. Each STUB area has a corresponding default route, the route from a STUB area to AS exterior destination must rely on the default route of that area.

The following simply outlines the route calculation process of OSPF protocol:

1） Each OSPF-enabled layer3 switch maintains a database (LS database) describing the link-state of the topology structure of the whole autonomous system. Each layer3 switch generates a link-state advertisement according to its surrounding network topology structure (router LSA), and sends the LSA to other

layer3 switches through link-state update (LSU) packages. Thus each layer3 switches receives LSAs from other layer3 switches, and all LSAs combined to the link-state database.

2） Since a LSA is the description of the network topology structure around a layer3 switch, the LS database is the description of the network topology structure of the whole network. The layer3 switches can easily create a weighted vector map according to the LS database. Obviously, all layer3 switches in the same autonomous system will have the same network topology map.

3） Each layer3 switch uses the shortest path finding (SPF) algorithm to calculate a tree of shortest path rooted by itself. The tree provides the route to all the nodes in the autonomous system, leaf nodes consist of the exterior route information. The exterior route can be marked by the layer3 switch broadcast it, so that additional information about the autonomous system can be recorded. As a result, the route table of each layer3 switch is different.

OSPF protocol is developed by the IETF, the OSPF v2 widely used now is fulfilled according to the content described in RFC2328.

17.6.2 OSPF Configuration Task List

The OSPF configuration for Edge-core series switches may be different from the configuration procedure to switches of the other manufacturers. It is a two-step process:

1、Enable OSPF in the Global Mode;

2、Configure OSPF area for the interfaces.

The configuration task list is as follows:

1. Enable/disable OSPF protocol (required)

（1）Enable/disable OSPF protocol (required)

（2）Configure the ID number of the layer3 switch running OSPF (optional)

（3）Configure the network scope for running OSPF (optional)

（4）Configure the area for the interface (required)

2. Configure OSPF protocol parameters (optional)

（1）Configure OSPF package sending mechanism parameters

1）Configure OSPF package verification

2）Set the OSPF interface to receive only

3）Configure the cost for sending packages from the interface

4）Configure OSPF package sending timer parameter (timer of broadcast interface sending HELLO package to poll, timer of neighboring layer3 switch invalid timeout, timer of LSA transmission delay and timer of LSA retransmission.

（2）Configure OSPF route introduction parameters

1）Configure default parameters (default type, default tag value, default cost

2）Configure the routes of the other protocols to introduce to OSPF.

（3）Configure other OSPF protocol parameters

1）Configure OSPF routing protocol priority

2）Configure cost for OSPF STUB area and default route

3）Configure OSPF virtual link

4）Configure the priority of the interface when electing designated layer3 switch (DR).

3. Disable OSPF protocol

1. Enable OSPF protocol

Basic configuration of OSPF routing protocol on ES4626/ES4650 switch is quite simple, usually only enabling OSPF and configuration of the OSPF area for the interface are required. The OSPF protocol parameters can use the default settings. If OSPF protocol parameters need to be modified, please refer to “2. Configure OSPF protocol parameters”.

Command	**Explanation**
Global mode	
[no] router ospf [process <*id*>]	Enables OSPF protocol; the “**no router ospf**” command disables OSPF protocol (required)
OSPF protocol configuration mode	
router-id <*router_id*> **no router-id**	Configures the ID number for the layer3 switch running OSPF; the “**no router id**” command cancels the ID number. The IP address of an interface is selected to be the layer3 switch ID. (optional)
[no] network {<*network*> <*mask*> | <*network*>/<*prefix*>} area <*area_id*>	Configure certain segment to certain area, the no **[no] network {<*network*> <*mask*> | <*network*>/<*prefix*>} area <*area_id*>** command cancels this configuration. (required)
[no] passive-interface {*IFNAME* | ethernet *IFNAME* | Vlan <*ID*>}	Sets an interface to receive only, the [no] passive-interface {*IFNAME* | ethernet *IFNAME* | Vlan <*ID*>} command cancels this configuration.

2.Configure OSPF protocol parameters

（1）Configure OSPF package sending mechanism parameters

1）Configure OSPF package verification

2）Set the OSPF interface to receive only

3）Configure the cost for sending packages from the interface

Command	**Explanation**
Interface configuration mode	
ip ospf authentication **{ message-digest | null}** **no ip ospf authentication**	Configures the authentication method by the interface to accept OSPF packages; the no ip ospf authentication command restores the default settings.
ip ospf authentication-key LINE **no ip ospf authentication-key**	Configure the key of the authentication process of OSPF data packets receiving for the interfaces; the no action of this command restores the default settings.
ip ospf cost <*cost* > **no ip ospf cost**	Sets the cost for running OSPF on the interface; the "**no ip ospf cost**" command restores the default setting.

4）Configure OSPF package sending timer parameter (timer of broadcast interface sending HELLO package to poll, timer of neighboring layer3 switch invalid timeout, timer of LSA transmission delay and timer of LSA retransmission.

Command	**Explanation**
Interface configuration mode	
ip ospf hello-interval <*time*> **no ip ospf hello-interval**	Sets interval for sending HELLO packages; the "**no ip ospf hello-interval**" command restores the default setting.
ip ospf dead-interval <*time* > **no ip ospf dead-interval**	Sets the interval before regarding a neighbor layer3 switch invalid; the "**no ip ospf dead-interval**" command restores the default setting.
ip ospf transit-delay <*time*> **no ip ospf transit-delay**	Sets the delay time before sending link-state broadcast; the "**no ip ospf transmit-delay**" command restores the default setting.

ip ospf retransmit <*time*> **no ip ospf retransmit**	Sets the interval for retransmission of link-state advertisement among neighbor layer3 switches; the "**no ip ospf retransmit**" command restores the default setting.

（2）Configure OSPF route introduction parameters

Configure the routes of the other protocols to introduce to OSPF.

Command	**Explanation**
OSPF protocol configuration mode	
redistribute { bgp | connected | static | rip | kernel} [metric-type { 1 | 2 }] [tag <*tag*>] [metric <*cost_value*>] [router-map <WORD>] **no redistribute { bgp | connected | static | rip | kernel }**	Distribute other protocols to find routing and static routings as external routing messages the **no redistribute { bgp | connected | static | rip | kernel }** command cancels the distributed external messages.

（3）Configure other OSPF protocol parameters

1）configure how to calculate OSPF spf algorithm time

2）configure the LSA limit in the OSPF link state database

3）Configure various OSPF parameters

Command	**Explanation**
OSPF protocol configuration mode	
timers spf <*interval*> **no timers spf**	configure the SPF timer of OSPF; the **no timers spf** command restores the default settings
overflow database {<*max-LSA*> [hard | soft] | external <*max-LSA*> <*recover time*>} **no overflow database [external < *max-LSA* > < *recover time* >]**	Configure the LSA limit in current OSPF process database; the **no overflow database [external < *max-LSA* > < *recover time* >]** command restores the default settings.

area <id> {authentication [message-digest] | default-cost <*cost*> | filter-list {access | prefix} <*WORD*> {in | out} | nssa [default-information-originate | no-redistribution | no-summary | translator-role] | range <*range*> | shortcut {default | disable | enable} | stub [no-summary] | virtual-link <*neighbor*>} **no area <id> {authentication | default-cost | filter-list {access | prefix} <*WORD*> {in | out} | nssa [default-information-originate | no-redistribution | no-summary | translator-role] | range <*range*> | shortcut { disable | enable} | stub [no-summary] | virtual-link <*neighbor*>}**	Configure the parameters in OSPF area (STUB area, NSSA area and virtual links); the **no area <id> {authentication | default-cost | filter-list {access | prefix} <*WORD*> {in | out} | nssa [default-information-originate | no-redistribution | no-summary | translator-role] | range <*range*> | shortcut { disable | enable} | stub [no-summary] | virtual-link <*neighbor*>}** command restores the default settings.

4）Configure the priority of the interface when electing designated layer3 switch (DR).

command	**explanation**
interface configuration mode	
ip ospf priority <*priority*> **no ip ospf priority**	Sets the priority of the interface in "designated layer3 switch" election; the **no ip ospf priority** command restores the default setting.

3. Disable OSPF protocol

command	**explanation**
Global mode	
no router ospf [process <*id*>]	Disables OSPF routing protocol

17.6.3 Commands for OSPF

17.6.3.1 area authentication

Command:area <*id*> authentication [message-digest]

no area <*id*> authentication

Function: Configure the authentication mode of the OSPF area; the "**no area <*id*> authentication**" command restores the default value.

Parameter: <*id*> is the area number which could be shown in digit, ranging between 0～4294967295, or in IP address.

Default: No authentication

Command Mode: OSPF protocol mode

Usage Guide: Set the authentication mode to plaintext authentication or MD5 authentication. The authentication mode is also configurable under interface mode of which the priority is higher than those in the area. It is required to use ip ospf authentication-key to set the password while no authentication mode configured at the interface and the area is plaintext authentication., and use ip ospf message-digest. key command to configure MD5 key if is MD5 authentication. The are authentication mode could not affect the authentication mode of the interface in this area.

Example: Set the authentication mode in area 0 to MD5.

Switch(config-router)#area 0 authentication message-digest

17.6.3.2 area default cost

Command: area <*id*> default-cost <*cost*>

no area <*id*> default-cost

Function: Configure the cost of sending to the default summary route in stub or NSSA area; the "**no area <*id*> default-cost**" command restores the default value.

Parameter: <*id*> is the area number which could be shown as digits 0～4294967295, or as an IP address; **<*cost*>** ranges between <0-16777215>

Default: Default OSPF cost is 1

Command Mode: OSPF protocol mode

Usage Guide: The command is only adaptive to the ABR router connected to the stub area or NSSA area.

Example:

Set the default-cost of area 1 to 10

Switch(config-router)#area 1 default-cost 10

17.6.3.3 area filter-list

Command: [no] area <*id*> filter-list {access|prefix} {in|out}

Function: Configure the filter broadcasting summary routing on the ABR; the "**[no] area <*id*> filter-list {access|prefix} {in|out}**" command restores the default value.

Parameter: <*id*> is the area number which could be shown in digits ranging between 0～4294967295, or as an IP address; access-list is appointed for use in access, so is prefix-list for prefix; **<*name*>** is the name of the filter the length of which is between 1-256; in means from other areas to this area, out means from this area to other areas.

Default: No filter configured

Command Mode: OSPF protocol mode

Usage Guide: This command is used for restraining routes from specific area from spreading between this area and other areas.

Example: Set a filter on the area 1

Switch(config)#access-list 1 deny 172.22.0.0 0.0.0.255

Switch(config)#access-list 1 permit any-source

Switch(config)#router ospf 100

Switch(config-router)#area 1 filter-list access 1 in

17.6.3.4 area nssa

Command: area <*id*> nssa [TRANSLATOR| no-redistribution |DEFAULT-ORIGINATE |no-summary]

no area <*id*> nssa

Function: Set the area to Not-So-Stubby-Area (NSSA) area

Parameter: ***<id>*** is the area number which could be digits ranging between 0～4294967295, and also as an IP address.

TRANLATOR = translator-role {candidate|never|always}, specifies the LSA translation mode for routes: **candidate** means if the router is elected translator, Type 7 LSA can be translated to Type-5 LSA, the default is **candidate**

never means the router will never translate Type 7 LSA to Type 5 LSA

always means the route always translate Type 7 LSA to Type 5 LSA

no-redistribution means never distribute external-LSA to NSSA.

DEFAULT-ORIGINATE=default-information-originate [metric <0-16777214>] [metric-type <*1-2*>], generate the Type-7 LSA

metric <*0-16777214*> specify the metric value

metric-type <*1-2*> specifies the metric value type of external-LSA , default value is 2.

no-summary shows not injecting area route to the NSSA

Default: No NSSA area defined by default

Command Mode: OSPF protocol mode

Usage Guide: The same area can not be both NSSA and stub at the same time

Example: Set area 53 and 3 to NSSA

Switch#config terminal

Switch(config)#router ospf 100

Switch(config-router)#area 0.0.0.51 nssa

Switch(config-router)#area 3 nssa default-information-originate metric 34 metric-type 2 translator-role candidate no-redistribution

17.6.3.5 area range

Command: area <*id*> range <*address*> [advertise| not-advertise| substitute]

no area <*id*> range <*address*>

Function: Aggregate OSPF route on the area border. The "**no area <*id*> range <*address*>**" cancels this function.

Parameter: <*id*> is the area number which could be digits ranging between 0～4294967295, and also as an IP address.

<*address*>=<*A.B.C.D/M*> specifies the area network prefix and its length

advertise: Advertise this area, which is the default

not-advertise : Not advertise this area

substitute= substitute <*A.B.C.D/M*>: advertise this area as another prefix.

<*A.B.C.D/M*>: Replace the network prefix to be advertised in this area

Default: Not set

Command Mode: OSPF protocol mode

Usage Guide: Use this command to aggregate routes inside an area. If the network IDs in this area are not configured continuously, a summary route can be advertised by configuring this command on ABR. This route consists of all single networks belong to specific range.

Example:

Switch # config terminal

Switch (config)# router ospf 100

Switch (config-router)# area 1 range 192.16.0.0/24

17.6.3.6 area shortcut

Command: area <*id*> shortcut {default|enable|disable}

no area <*id*> shortcut [disable|enable]

Function: Configure shortcut mode in an area. The "**no area <*id*> shortcut [disable|enable]**" command cancels this function.

Parameter: <*id*> is the area number which could be digits ranging between 0～4294967295, and also as an IP address.

default: Set the default shortcut in this area

enable: Enable forced shortcut through area time

disable : Disable shortcut through area time.

Default: Set to **default**

Command Mode: OSPF protocol mode

Usage Guide: Whether the area border routers are connected to a backbone routes or not, enabling the area shortcut will let the flow passes through non-backbone area with lower metric values.

Example:

Switch# config terminal
Switch(config)# router ospf
Switch(config-router)# area 1 shortcut default
Switch(config-router)area 52 shortcut disable
Switch(config-router)no area 42 shortcut enable

17.6.3.7 area stub

Command: area <*id*> stub [no-summary]
no area <*id*> stub [no-summary]
Function: Define a area to a stub area. The "**no area <*id*> stub [no-summary]**" command cancels this function.
Parameter: <*id*> is the area number which could be digits ranging between 0～4294967295, and also as an IP address.
no-summary: The area border routes stop sending link summary announcement to the stub area.
Default: Not defined
Command Mode: OSPF protocol mode
Usage Guide: Configure area stub on all routes in the stub area. There are two configuration commands for the routers in the stub area: stub and default-cost. All routers connected to the stub area should be configured with area stub command. As for area border routers connected to the stub area, their introducing cost is defined with area default-cost command.
Example:
Switch # config terminal
Switch (config)# router ospf 100
Switch (config-router)# area 1 stub
Relevant Commands: area default-cost

17.6.3.8 area virtual-link

Command: area <*id*> virtual-link A.B.C.D
{AUTHENTICATION|AUTH_KEY|INTERVAL}
no area <*id*> virtual-link A.B.C.D [AUTHENTICATION|AUTH_KEY|INTERVAL]
Function: Configure a logical link between two backbone areas physically divided by non-backbone area. The "**no area <*id*> virtual-link A.B.C.D [AUTHENTICATION|AUTH_KEY|INTERVAL]**" command removes this virtual-link.
Parameter: <*id*> is the area number which could be digits ranging between 0～4294967295, and also as an IP address.
AUTHENTICATION = authentication [message-digest|null|AUTH_KEY]

authentication : Enable authentication on this virtual link

message-digest: Authentication with MD-5

null : Overwrite password or packet summary with null authentication.

AUTH_KEY= authentication-key <*key*>

<key>: A password consists of less than 8 characters

INTERVAL= [dead-interval|hello-interval|retransmit-interval|transmit-delay] <value>

***<value>*:>:** The delay or interval seconds, ranging between 1~65535

***<dead-interval>*:** A neighbor is considered offline for certain dead interval without its group messages which the default is 40 seconds.

***<hello-interval>*:** The time interval before the router sends a hello group message, default is 10 seconds

***<retransmit-interval>*:** The time interval before a router retransmitting a group message, default is 5 seconds.

***<transmit-delay>*:** The time delay before a router sending a group messages, default is 1 second

Default: None

Command Mode: OSPF protocol mode

Usage Guide: In the OSPF all non-backbone areas will be connected to a backbone area. If the connection to the backbone area is lost, virtual link will repair this connection. You can configure virtual link between any two backbone area routers connected with the public non-backbone area. The protocol treat routers connected by virtual links as a point-to-point network.

Example:

Switch#config terminal

Switch(config) #router ospf 100

Switch(config-router) #area 1 virtual-link 10.10.11.50 hello 5 dead 20

17.6.3.9 auto-cost reference-bandwidth

Command: auto-cost reference-bandwidth <bandwidth>

no auto-cost reference-bandwidth

Function: This command sets the way in which OSPF calculate the default metric value. The "**no auto-cost reference-bandwidth**" command only configures the cost to the interface by types.

Parameter: <*bandwidth*> reference bandwidth in Mbps, ranging between 1~*4294967*

Default: Default bandwidth is 100Mbps

Command Mode: OSPF protocol mode

Usage Guide: The interface metric value is acquired by divide the interface bandwidth with reference bandwidth. This command is mainly for differentiate high bandwidth links.

If several high bandwidth links exist, their cost can be assorted by configuring a larger reference bandwidth value.

Example:

Switch#config terminal

Switch(config)#router ospf 100

Switch(config-router)#auto-cost reference-bandwidth 50

17.6.3.10 capability opaque

Command: [no] capability opaque

Function: This command enables opaque-LSA. The "**[no] capability opaque**" command closes this function.

Default: Opaque-LSAs enabled

Command Mode: OSPF protocol mode

Usage Guide: Opaque-LSAs is type 9,10,11 LSA which is used for transmitting information's for the externals.

Example:

Switch#config terminal

Switch(config)#router ospf 100

Switch(config-router)#no capability opaque

17.6.3.11 compatible rfc1583

Command: [no] compatible rfc1583

Function: This command configures to rfc1583 compatible. The "**[no] compatible rfc1583**" command close the compatibility.

Default: Rfc 2328 compatible by default

Command Mode: OSPF protocol mode

Example:

Switch#config terminal

Switch(config)#router ospf 100

Switch(config-router)#compatible rfc1583

17.6.3.12 clear ip ospf process

Command: clear ip ospf [<process-id>] process

Function: Use this command to clear and restart OSPF routing processes. One certain OSPF process will be cleared by specifying the process ID, or else all OSPF processes will be cleared.

Default: No default configuration

Command Mode: Admin mode

Example: Switch#clear ip ospf process

17.6.3.13 distance

Command: distance {<value>|ROUTEPARAMETER}

no distance ospf

Function: Configure OSPF manage distance base on route type. The "**no distance ospf**" command restores the default value.

Parameter: <*value*>, OSPF routing manage distance, ranging between 1~235

ROUTEPARAMETER= ospf {ROUTE1|ROUTE2|ROUTE3}

ROUTE1= external <external-distance>, Configure the distance learnt from other routing area.

<external-distance>distance value, ranging between 1~255

ROUTE2= inter-area <inter-distance>, configure the distance value from one area to another area.

<inter-distance> manage distance value, ranging between 1~255

ROUTE3= intra-area <intra-distance> Configure all distance values in one area.

<intra-distance> Manage distance value, ranging between 1~255

Default: Default distance value is 110

Command Mode: OSPF protocol mode

Usage Guide: Manage distance shows the reliability of the routing message source. The distance value may range between 1~255. the larger the manage distance value is, the lower is its reliability.

Example:

Switch#config terminal

Switch(config)#router ospf 100

Switch(config-router)#distance ospf inter-area 20 intra-area 10 external 40

17.6.3.14 distribute-list

Command: distribute-list <access-list-name> out {kernel |connected| static| rip| isis| bgp}

[no] distribute-list out {kernel |connected| static| rip| isis| bgp}

Function: Filter network in the routing update. The "**[no] distribute-list out {kernel |connected| static| rip| isis| bgp}**" command disables this function.

Parameter: < *access-list-name*> is the access-list name to be applied

out: Filter the sent route update

kernel Kernel route

connected Direct route

static Static route

rip RIP route

isis ISIS route

bgp BGP route

Default: None

Command Mode: OSPF protocol mode

Usage Guide: When distributing route from other routing protocols into0 the OSPF routing table, we can use this command

Example: Example below is the advertisement based on the access-list list 1 of the BGP route.

Switch#config terminal

Switch(config)#access-list l1 permit 172.10.0.0 0.0.255.255

Switch(config)#router ospf 100

Switch(config-router)#distribute-list 1 out bgp

Switch(config-router)#redistribute bgp

17.6.3.15 host area

Command: [no] host <*host-address*> area <*area-id*> [cost <*cost*>]

Function: Use this command to set a stub host entire belongs to certain area. The "**[no] host <*host-address*> area <*area-id*> [cost <*cost*>]**" command cancels this configuration

Parameter: <*host-address*> is host IP address show in dotted decimal notation, **<*area-id*>** area ID shown in dotted decimal notation or integer ranging between 0~4294967295

<*cost*> specifies the entire cost, which is a integer ranging between 0~65535 and defaulted at 0

Default: No entire set

Command Mode: OSPF protocol mode

Usage Guide: With this command you can advertise certain specific host route out as stub link. Since the stub host belongs to special router in which setting host is not important.

Example:

Switch#config terminal

Switch(config)#router ospf 100

Switch(config-router)#host 172.16.10.100 area 1

Switch(config-router)#host 172.16.10.101 area 2 cost 10

17.6.3.16 ip ospf authentication

Command: ip ospf [<*ip-address*>] authentication [message-digest|null]

no ip ospf [<*ip-address*>] authentication

Function: Specify the authentication mode required in sending and receiving OSPF packets on the interfaces; the "**no ip ospf [<*ip-address*>] authentication**" command cancels the authentication

Parameter: <*ip-address*> is the interface IP address, shown in dotted decimal notation.

message-digest: Use MD5 authentication

null: no authentication applied, which resets the password or MD5 authentication applied on the interface.

Default: Authentication not required in receiving OSPF packets on the interface

Command Mode: Interface Mode

Example:

Switch#config terminal

Switch(config)#interface vlan 1

Switch(Config-if-Vlan1)#ip ospf authentication message-digest

17.6.3.17 ip ospf authentication-key

Command: ip ospf [<*ip-address*>] authentication-key <LINE>

no ip ospf [<*ip-address*>] authentication

Function: Specify the authentication key required in sending and receiving OSPF packet on the interface; the "**no ip ospf [<*ip-address*>] authentication**" cancels the authentication key.

Parameter: <*ip-address*> is the interface IP address shown in dotted decimal notation; <LINE> specifies the key required in the plaintext authentication.

Default: Authentication not required in receiving OSPF packets on the interface

Command Mode: Interface Mode

Example:

Switch#config terminal

Switch(config)#interface vlan 1

Switch(Config-if-Vlan1)#ip ospf authentication-key password

17.6.3.18 ip ospf cost

Command: ip ospf [<*ip-address*>] cost <*cost*>

no ip ospf [<*ip-address*>] cost

Function: Specify the cost required in running OSPF protocol on the interface; the "**no ip ospf [<*ip-address*>] cost**" command restores the default value.

Parameter: <*ip-address*> is the interface IP address shown in dotted decimal notation; **<*cost* >** is the cost of OSPF protocol ranging between 1~65535

Default: Default OSPF cost on the interface is 10.

Command Mode: Interface Mode

Example:

Switch#config terminal

Switch(config)#interface vlan 1

Switch(Config-if-Vlan1)#ip ospf cost 3

17.6.3.19 ip ospf database-filter

Command: ip ospf [<*ip-address*>] database-filter all out

no ip ospf [<*ip-address*>] database-filter

Function: The command opens LSA database filter switch on specific interface; the "**no ip ospf [<*ip-address*>] database-filter**" command closes the filter switch.

Parameter: **<*ip-address*>** is the interface IP address shown in dotted decimal notation;

all: All LSAs

out: Sent LSAs

Default: Filter switch Closed

Command Mode: Interface Mode

Example:

Switch#config terminal

Switch(config)#interface vlan 1

Switch(Config-if-Vlan1)#ip ospf database-filter all out

17.6.3.20 ip ospf dead-interval

Command: ip ospf [<*ip-address*>] dead-interval <*time* >

no ip ospf [<*ip-address*>] dead-interval

Function: Specify the dead interval for neighboring layer 3 switch; the "**no ip ospf [<*ip-address*>] dead-interval**" command restores the default value.

Parameter: <*ip-address*> is the interface IP address shown in dotted decimal notation;

<*time* > is the dead interval length of the neighboring layer 3 switches, shown in seconds and ranging between 1~65535

Default: The default dead interval is 40 seconds (normally 4 times of the hello-interval).

Command Mode: Interface Mode

Usage Guide: If no HELLO data packet received after the **dead-interval** period then this layer 3 switch is considered inaccessible and invalid. This command modifies the dead interval value of neighboring layer 3 switch according to the actual link state. The set **dead-interval** value is written into the Hello packet and transmitted. To ensure the normal operation of the OSPF protocol, the dead-interval between adjacent layer 3 switches should be in accordance or at least 4 times of the **hello-interval** value

Example:

Switch#config terminal

Switch(config)#interface vlan 1

Switch(Config-if-Vlan1)#ip ospf dead-interval 80

17.6.3.21 ip ospf disable all

Command: [no]ip ospf disable all

Function: Stop OSPF group process on the interface

Command Mode: Interface Mode

Usage Guide: This command resets the network area command and stops group process on specific interface.

Example:

Switch#config terminal

Switch(config)#interface vlan 1

Switch(Config-if-Vlan1)#ip ospf disable all

17.6.3.22 ip ospf hello-interval

Command: ip ospf [<*ip-address*>] hello-interval <*time*>

no ip ospf [<*ip-address*>] hello-interval

Function: Specify the hello-interval on the interface; the "**no ip ospf [<*ip-address*>] hello-interval**" restores the default value

Parameter: <*ip-address*> is the interface IP address shown in dotted decimal notation; **<*time*>** is the interval sending HELLO packet, shown in seconds and ranging between 1～65535

Default: The hello-interval on the interface is 10 seconds

Command Mode: Interface Mode

Usage Guide: HELLO data packet is the most common packet which is periodically sent to adjacent layer 3 switch to discover and maintain adjacent relationship, elect DR and BDR. The user set **hello-interval** value will be written into the HELLO packet and transmitted. The less the **hello-interval** value is, the sooner the network topological structure is discovered as well larger the cost. The ensure the normal operation of OSPF protocol the **hello-interval** parameter between the layer 3 switches adjacent to the interface must be in accordance.

Example:

Switch#config terminal

Switch(config)#interface vlan 1

Switch(Config-if-Vlan1)#ip ospf hello-interval 20

17.6.3.23 ip ospf message-digest-key

Command: ip ospf [<*ip-address*>] message-digest-key <*key_id*> MD5 <*LINE*>

no ip ospf [<*ip-address*>] message-digest-key <*key_id*>

Function: Specify the key id and value of MD5 authentication on the interface; the "**no ip ospf [<*ip-address*>] message-digest-key <*key_id*>**" restores the default value

Parameter: <*ip-address*> is the interface IP address show in dotted decimal notation; <*key_id*> ranges between 1-255; **<*LINE*>** is the OSPF key.

Default: MD5 key not configured

Command Mode: Interface Mode

Usage Guide: MD5 key encrypted authentication is used for ensure the safety between the OSPF routers on the network. Same key id and key should be configured between neighbors when using this command or else no adjacent relationship will not be created. The last configuration of this command will overwrite the previous one to prevent the system from communicating with the former key id.

Example:

Switch#config terminal

Switch(config)#interface vlan 1

Switch(Config-if-Vlan1)#ip ospf message-digest-key 2 MD5 yourpassword

17.6.3.24 ip ospf mtu

Command: ip ospf mtu <*mtu*>

no ip ospf mtu

Function: Specify the mtu value of the interface as the OSPF group structure according; the "**no ip ospf mtu**" command restores the default value.

Parameter: <*mtu* > is the interface mtu value ranging between 576~65535.

Default: Use the interface mtu acquired from the kernel.

Command Mode: Interface Mode

Usage Guide: The interface value configured by this command is only used by OSPF protocol other than updated into kernel.

Example:

Switch#config terminal

Switch(config)#interface vlan 1

Switch(Config-if-Vlan1)#ip ospf mtu 1480

17.6.3.25 ip ospf mtu-ignore

Command: ip ospf <*ip-address*> mtu-ignore

no ip ospf <*ip-address*> mtu-ignore

Function: Use this command so that the mtu size is not checked when switching DD; the "**no ip ospf <*ip-address*> mtu-ignore**" will ensure the mtu size check when performing DD switch

Parameter: <*ip-address*> is the interface IP address show in dotted decimal notation

Default: Check mtu size in DD switch

Command Mode: Interface Mode

Example:

Switch#config terminal

Switch(config)#interface vlan 1

Switch(Config-if-Vlan1)#ip ospf mtu-ignore

17.6.3.26 ip ospf network

Command: ip ospf network

{broadcast|non-broadcast|point-to-point|point-to-multipoint}

no ip ospf network

Function: This command configure the OSPF network type of the interface; the "**no ip ospf network**" command restores the default value

Parameter: broadcast: Set the OSPF network type to broadcast.

non-broadcast: Set the OSPF network type to NBMA

point-to-point: Set the OSPF network type to point-to-point

point-to-multipoint: Set the OSPF network type to point-to-multipoint

Default: The default OSPF network type is broadcast

Command Mode: Interface Mode

Example: The configuration below set the OSPF network type of the interface vlan 1 to point-to-point.

Switch#config terminal

Switch(config)#interface vlan 1

Switch(Config-if-Vlan1)#ip ospf network point-to-point

17.6.3.27 ip ospf priority

Command:ip ospf [<*ip-address*>] priority <*priority*>

no ip ospf [<*ip-address*>] priority

Function: Configure the priority when electing "Defined layer 3 switch" at the interface. The "**no ip ospf [<*ip-address*>] priority**" command restores the default value

Parameter: <*ip-address*> is the interface IP address show in dotted decimal notation

<*priority*> is the priority of which the valid value ranges between 0～255.

Default: The default priority when electing DR is 1.

Command Mode: Interface Mode

Usage Guide: When two layer 3 switches connected to the same segments both want to be the “Defined layer 3 switch”, the priority will decide which one should be chosen. Normally the one with higher priority will be elected, or the one with larger router-id number if the priorities are the same. A layer 3 switch with a priority equal to 0 will not be elected as “Defined layer 3 switch” or “Backup Defined layer 3 switch”

Example: Configure the priority of DR electing. Configure the interface vlan 1 to no election right, namely set the priority to 0.

Switch#config terminal

Switch(config)#interface vlan 1

Switch(Config-if-Vlan1)#ip ospf priority 0

17.6.3.28 ip ospf retransmit-interval

Command: ip ospf [<*ip-address*>] retransmit-interval <*time*>

no ip ospf [<*ip-address*>] retransmit-interval

Function: Specify the retransmit interval of link state announcements between the interface and adjacent layer 3 switches. The “**no ip ospf [<*ip-address*>] retransmit-interval**” command restores the default value

Parameter: <*ip-address*> is the interface IP address show in dotted decimal notation

<*time*> is the retransmit interval of link state announcements between the interface and adjacent layer 3 switches, shown in seconds and raning between 1～65535

Default: Default retransmit interval is 5 seconds

Command Mode: Interface Mode

Usage Guide: When a layer 3 switch transmits LSA to its neighbor, it will maintain the link state announcements till confirm from the object side is received. If the confirm packet is not received within the interval, the LSA will be retransmitted. The retransmit interval must be larger than the time it takes to make a round between two layer 3 switches.

Example: Configure the LSA retransmit interval of interface vlan 1 to 10 seconds

Switch#config terminal

Switch(config)#interface vlan 1

Switch(Config-if-Vlan1)#ip ospf retransmit-interval 10

17.6.3.29 ip ospf transmit-delay

Command: ip ospf [<*ip-address*>] transmit-delay <*time*>

no ip ospf [<*ip-address*>] transmit-delay

Function: Set the transmit delay value of LSA transmitting; the “**no ip ospf [<*ip-address*>] transmit-delay**” restores the default value.

Parameter: <*ip-address*> is the interface IP address show in dotted decimal notation **<*time*>** is the transmit delay value of link state announcements between the interface and adjacent layer 3 switches, shown in seconds and raning between 1～65535

Default: Default transmit delay value of link state announcements is 1 second

Command Mode: Interface Mode

Usage Guide: The LSA ages with time in the layer 3 switches, but not in the network transmitting process. By adding the **transit-delay** prior to sending the LSA, the LSA will be sent before aged

Example: Set the LSA transmit delay of interface vlan1 to 3 seconds.

Switch#config terminal

Switch(config)#interface vlan 1

Switch(Config-if-Vlan1)#ip ospf transmit-delay 3

17.6.3.30 max-concurrent-dd

Command: max-concurrent-dd <value>

no max-concurrent-dd

Function: This command set the maximum concurrent number of dd in the OSPF process; the "**no max-concurrent-dd**" command restores the default

Parameter: <*value*> ranges between ***<1-65535>***, which is the capacity of processing the concurrent dd data packet

Default: Not set, no concurrent dd limit

Command Mode: OSPF protocol mode

Usage Guide: Specify the max concurrent number of dd in the OSPF process

Example: Set the max concurrent dd to 20

Switch#config terminal

Switch(config)#router ospf 100

Switch(config-router)#max-concurrent-dd 20

17.6.3.31 neighbor

Command: neighbor A.B.C.D [<*COST*>| priority <*value*> | poll-interval <*value*>]

no neighbor A.B.C.D [<*COST*>| priority <*value*> | poll-interval <*value*>]

Function: This command configures the OSPF router connecting NBMA network. the "**no neighbor A.B.C.D [<*COST*>| priority <*value*> | poll-interval <*value*>]**" command removes this configuration fs

Parameter: <*COST*>, OSPF neighbor cost value ranging between 1-65535; **priority <*value*>** , neighbor priority defaulted at 0 and ranges between 0-255; **poll-interval <*value*>**, 120s by default, which the polling time before neighbor relationship come into shape , ranging between 1-65535

Default: No default configuration

Command Mode: OSPF protocol mode

Usage Guide: Use this command on NBMA network to configure neighbor manually. Every known non-broadcasting neighbor router should be configured with a neighbor entry. The configured neighbor address should be the main address of the interface. The poll-interval should be much larger than the hello-interval

Example:

Switch#config terminal

Switch(config)#router ospf 100

Switch(config-router)#neighbor 1.2.3.4 priority 1 poll-interval 90

Switch(config-router)#neighbor 1.2.3.4 cost 15

17.6.3.32 network area

Command: network NETWORKADDRESS area <*area-id*>

no network NETWORKADDRESS area <*area-id*>

Function: This command enables OSPF routing function one the interface with IP address matched with the network address. The "**no network NETWORKADDRESS area <*area-id*>**" command removes the configuration and stop OSPF on corresponding interface.

Parameter: NETWORKADDRESS = A.B.C.D/M | A.B.C.D X.Y.Z.W, Shown with the network address prefix or the mask. Wildcast mask if shown in mask; **<*area-id*>** is the ip address or area number shown in point divided demcial system, if shown in demcial integer, it ranges between 0~4294967295

Default: No default

Command Mode: OSPF protocol mode

Usage Guide: When certain segment belongs to certain area, interface the segment belongs will be in this area, starting hello and database interaction with the connected neighbor.

Example:

Switch#config terminal

Switch(config)#router ospf 100

Switch(config-router)#network 10.1.1.0/24 area 1

17.6.3.33 ospf abr-type

Command: ospf abr-type {cisco|ibm|shortcut|standard}

no ospf abr-type

Function: Use this command to configure a OSPF ABR type. The "**no ospf abr-type**" command restores the default value.

Parameter: cisco, Realize through cisco ABR; **ibm**, Realize through ibm ABR; **shortcut**, Specify a shortcut-ABR; **standard**, Realize with standard（RFC2328）ABR.

Default: Cisco by default

Command Mode: OSPF protocol mode

Usage Guide: For Specifying the realizing type of abr. This command is good for interactive operation among different OSPF realizing method and is especially useful in the multiple host environment.

Example: Configure abr as standard

Switch#config terminal

Switch(config)#router ospf 100

Switch(config-router)#ospf abr-type standard

17.6.3.34 ospf router-id

Command: ospf router-id <*address*>

no ospf router-id

Function: Specify a router ID for the OSPF process. The "**no ospf router-id**" command cancels the ID number

Parameter: <*address*>, IPv4 address format of router-id

Default: No default configuration

Command Mode: OSPF protocol mode

Usage Guide: The new router-id takes effect immediately

Example: Configure router-id of ospf 100 to 2.3.4.5

Switch#config terminal

Switch(config)#router ospf 100

Switch(config-router)#ospf router-id 2.3.4.5

17.6.3.35 overflow database

Command:overflow database <*maxdbsize* > [{hard|soft}]

no overflow database

Function: This command is for configuring the max LSA number. The "**no overflow database**" command cancels the limit

Default: Not configured

Parameter: < ***maxdbsize*** >Max LSA numbers, ranging between 0~4294967294

soft: Soft limit, warns when border exceeded

hard: Hard limit, directly close ospf instance when border exceeded

If there is not soft or hard configured, the configuration is taken as hard limit

Command Mode: interface mode

Example: Switch#config terminal

Switch(config)#router ospf
Switch(config-router)#overflow database 10000 soft

17.6.3.36 overflow database external

Command: [no]overflow database external [<*maxdbsize* > <*maxtime*>]
Function: The command is for configuring the size of external link database and the waiting time before the route exits overflow state. The "**[no]overflow database external [<*maxdbsize* > <*maxtime*>]**" restores the default value
Parameter: < ***maxdbsize*** > size of external link database, ranging between 0~4294967294 , defaulted at 4294967294
< *maxtime* > the seconds the router has to wait before exiting the database overflow, ranging between 0~65535
Command Mode: OSPF protocol mode
Example: Switch#config terminal
Switch(config)#router ospf
Switch(config-router)#overflow database external 5 3

17.6.3.37 passive-interface

Command: [no] passive-interface<*ifname*>
Function: Configure that the hello group not sent on specific interfaces. The "[**no**] **passive-interface<*ifname*>**" command cancels this function
Parameter: <***ifname***> is the specific name of interface
<ip-address> IP address of the interface, shown in dotted decimal notation
Default: Not configured
Command Mode: OSPF protocol mode
Example: Switch#config terminal
Switch(config)#router ospf
Switch(config-router)#passive-interface vlan1

17.6.3.38 redistribute

Command: [no]redistribute {kernel |connected| static| rip| isis| bgp} [metric<*value*>] [metric-type {1|2}][route-map<*word*>][tag<*tag-value*>]
Function: Introduce route learnt from other routing protocols into OSPF
Parameter: kernel introduce from kernel route
connected introduce from direct route
static introduce from static route
rip introduce from the RIP route
isis introduce from ISIS route

bgp introduce from BGP route

metric <*value*> is the introduced metric value, ranging between 0-16777214

metric-type {1|2} is the metric value type of the introduced external route, which can be 1 or 2, and it is 2 by default

route-map <*word*> point to the probe of the route map for introducing route

tag<*tag-value*> external identification number of the external route, ranging between 0~4294967295, defaulted at 0

Command Mode: **OSPF mode**

Usage Guide: Learn and introduce other routing protocol into OSPF area to generate AS-external_LSAs

Example: Switch#config terminal

Switch(config)#router ospf

Switch(config-router)#redistribute bgp metric 12

17.6.3.39 router ospf

Command: [no] router ospf <process_id> <*vrf-name*>

Function: This command is for relating the OSPF process and a specific VPN. All configuration commands will be related to this VPN after the configuration succeeded. The "**[no] router ospf <process_id> <*vrf-name*>**" command deletes the VPN routing/forwarding instance related OSPF instances.

Parameter: **<*process_id*>** specifies the id of the OSPF process to be created. **<*vrf-name*>** specifies the name of VPN routing/forwarding instance

Command Mode: Global mode

Usage Guide: This command is only used for PE router. A VPN routing/forwarding instance should be generated with ip vrf command before using this command, then with this command you can relate OSPF instances to this VPN routing/forwarding instance

Example: Switch# config terminal

Switch(config)# router ospf 100 VRF1

Switch(config-router)#network 10.1.1.0/24 area 0

17.6.3.40 default-information originate

Command: default-information originate

[always|METRIC|METRICTYPE|ROUTEMAP]

no default-information originate

Function: This command create a default external route to OSPF route area; the "**no default-information originate**" closes this feature

Parameter: **always:** Whether default route exist in the software or not, the default route is always advertised.

METRIC = metric <*value*>: **METRIC = metric <*value*>:** Set the metric value for creating default route, **<*value*>** ranges between 0~*16777214* , default metric value is 0

METRICTYPE = metric-type {1|2} set the OSPF external link type of default route.

1 Set the OSPF external type 1 metric value

2 Set the OSPF external type 2 metric value

ROUTEMAP = route-map <*WORD*>

<WORD> specifies the route map name to be applied.

Default: Default metric value is 10, default OSPF external link type is 2.

Command Mode: OSPF protocol mode

Usage Guide: When introducing route into OSPF route area with this command , the system will behaves like an ASBR

Example:

Switch#config terminal

Switch(config)#router ospf 100

Switch(config-router)#default-information originate always metric 23 metric-type 2 route-map myinfo

17.6.3.41 default-metric

Command: default-metric <*value*>

no default-metric

Function: The command set the default metric value of OSPF routing protocol; the "**no default-metric**" returns to the default state.

Parameter: <*value*>, metric value, ranging between 0~*16777214*

Default: Built-in, metric value auto translating

Command Mode: OSPF protocol mode

Usage Guide: When the default metric value makes the metric value not compatible, the route introducing still goes through. If the metric value can not be translated, the default value provides alternative option to carry the route introducing on. This command will result in that all introduced route will use the same metric value. This command should be used associating redistribute.

Example:

Switch#config terminal

Switch(config)#router ospf 100

Switch(config-router)#default-metric 100

17.6.3.42 summary-address

Command: summary-address <*A.B.C.D/M*> [{not-advertise|tag<*tag-value*>}]

Function: Summarize or restrain external route with specific address scope.

Parameter: <*A.B.C.D/M*> address scope, shown in dotted decimal notation IPv4 address plus mask length

not-advertised restrain the external routes

tag<*tag-value*> is the identification label of the external routes, which ranges between 0~4294967295, and is defaulted at 0

Command Mode: OSPF protocol mode

Usage Guide: When routes are introduced into OSPF from other routing protocols, it is required to advertise every route in a external LSA. This command is for advertise one summary route for those introduced routes contained in specific network address and masks, which could greatly reduces the size of the link state database.

Example: Switch#config terminal

Switch(config)#router ospf

Switch(config-router)#summary-address 172.16.0.0/16 tag 3

17.6.3.43 timers spf

Command: timers spf <*spf-delay*> <*spf-holdtime*>

no timers spf

Function: Adjust the value of the route calculating timer. The "**no timers spf**" command restores relevant values to default

Parameter: <*spf-delay*> 5 seconds by default

<*spf-holdtime*> 10 seconds by default

Command Mode: OSPF protocol mode

Usage Guide: This command configures the delay time between receiving topology change and SPF calculation, further configured the hold item between two discontinuous SPF calculation

Example: Switch#config terminal

Switch(config)#router ospf

Switch(config-router)#timers spf 5 10

17.6.4 OSPF Example

17.6.4.1 Configuration Example of OSPF

Scenario 1: OSPF autonomous system.

This scenario takes an OSPF autonomous system consists of five ES4626/ES4650 switch for example, where layer3 SwitchA and SwitchE make up OSPF area 0, layer3 SwitchB and SwitchC form OSPF area 1 (assume vlan1 interface of layer3 SwitchA belongs to area 0), layer3 SwitchD forms OSPF area 2 (assume vlan2 interface of layer3

SwitchE belongs to area 0). Switch1 and SwitchE are backbone layer3 switches, Switch2 and SwitchD are area edge layer3 switches, and SwitchC is the inside-area layer3 switch.

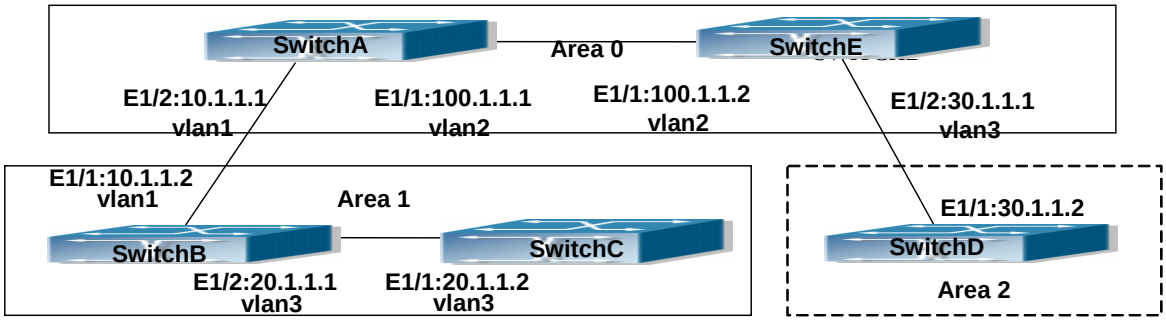


Fig 17-6 Network topology of OSPF autonomous system.

The configuration for layer3 SwitchA and SwitchE is shown below:

Layer 3 SwitchA

Configuration of the IP address for interface vlan1

SwitchA#config

SwitchA(config)# interface vlan 1

SwitchA(config-if-vlan1)# ip address 10.1.1.1 255.255.255.0

SwitchA(config-if-vlan1)#no shut-down

SwitchA(config-if-vlan1)#exit

Configuration of the IP address for interface vlan2

Configure the IP address of interface vlan2

SwitchA(config)# interface vlan 2

SwitchA(config-if-vlan2)# ip address 100.1.1.1 255.255.255.0

SwitchA (config-if-vlan2)#exit

Enable OSPF protocol, configure the area number for interface vlan1 and vlan2.

SwitchA(config)#router ospf

SwitchA(config-router)#network 10.1.1.0/24 area 0

SwitchA(config-router)#network 100.1.1.0/24 area 0

SwitchA(config-router)#exit

SwitchA(config)#exit

Layer 3 SwitchB

Configure the IP address for interface vlan1 and vlan2Configure the IP address of interface vlan1 and vlan2

SwitchB#config

SwitchB(config)# interface vlan 1

SwitchB(config-if-vlan1)# ip address 10.1.1.2 255.255.255.0

SwitchB(config-if-vlan1)#no shut-down

SwitchB(config-if-vlan1)#exit

SwitchB(config)# interface vlan 3

SwitchB(config-if-vlan3)# ip address 20.1.1.1 255.255.255.0

SwitchB(config-if-vlan3)#no shut-down

SwitchB(config-if-vlan3)#exit

Enable OSPF protocol, configure the OSPF area interfaces vlan1 and vlan3 in

SwitchB(config)#router ospf

SwitchB(config-router)# network 10.1.1.0/24 area 0

SwitchB(config-router)# network 20.1.1.0/24 area 1

SwitchB(config-router)#exit

SwitchB(config)#exit

Layer 3 SwitchC

Configuration of the IP address for interface vlan3

SwitchC#config

SwitchC(config)# interface vlan 3

SwitchC(config-if-vlan1)# ip address 20.1.1.2 255.255.255.0

SwitchC(config-if-vlan3)#no shut-down

SwitchC(config-if-vlan3)#exit

Enable OSPF protocol, configure the OSPF area interfaces vlan3 resides in.

Initiate the OSPF protocol, configure the OSPF area to which interface vlan3 belongs

SwitchC(config)#router ospf

SwitchC(config-router)# network 20.1.1.0/24 area 1

SwitchC(config-router)#exit

SwitchC(config)#exit

Layer 3 SwitchD

Configuration of the IP address for interface vlan3

SwitchD#config

SwitchD(config)# interface vlan 3

SwitchD(config-if-vlan3)# ip address30.1.1.2 255.255.255.0

SwitchD(config-if-vlan3)#no shut-down

SwitchD(config-if-vlan3)#exit

Enable OSPF protocol, configure the OSPF area interfaces vlan3 resides in. SwitchD(config)#router ospf

SwitchD(config-router)# network 30.1.1.0/24 area 0

SwitchD(config-router)#exit

SwitchD(config)#exit

Layer 3 SwitchE

Configuration of the IP address for interface vlan2

SwitchE#config

SwitchE(config)# interface vlan 2

SwitchE(config-if-vlan2)# ip address 100.1.1.2 255.255.255.0

SwitchE(config-if-vlan2)#no shut-down

SwitchE(config-if-vlan2)#exit

Configuration of the IP address for interface vlan3

SwitchE(config)# interface vlan 3

SwitchE(config-if-vlan3)# ip address 30.1.1.1 255.255.255.0

SwitchE(config-if-vlan3)#no shut-down

SwitchE(config-if-vlan3)#exit

Enable OSPF protocol, configure the number of the area in which interface vlan2 and vlan3 reside in.

SwitchE(config)#router ospf

SwitchE(config-router)# network 30.1.1.0/24 area 0

SwitchE(config-router)# network 100.1.1.0/24 area 0

SwitchE(config-router)#exit

SwitchE(config)#exit

Scenario 2：Typical OSPF protocol complex topology.

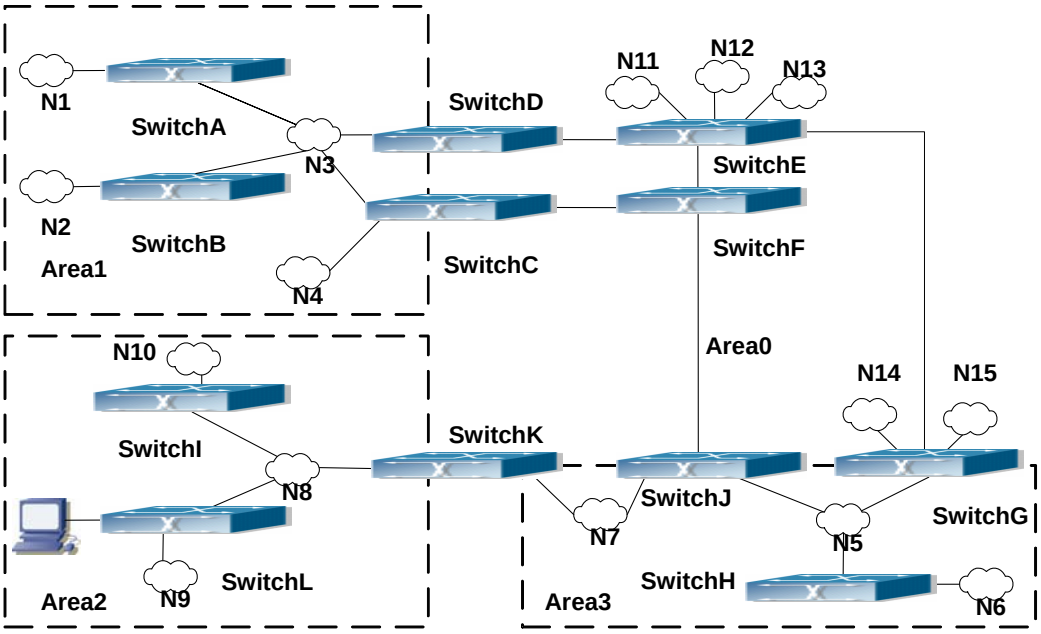


Fig 17-7 Typical complex OSPF autonomous system.

This scenario is a typical complex OSPF autonomous system network topology. Area1 include network N1-N4 and layer3 SwitchA-SwitchD, area2 include network N8-N10, host H1 and layer3 SwitchI, area3 include N5-N7 and layer3 SwitchG, SwitchH

SwitchJ and SwitchK, and network N8-N10 share a summary route with host H1(i.e. area3 is defined as a STUB area). Layer3 SwitchA, SwitchB, SwitchE, SwitchF, SwitchH, SwitchI, SwitchL are in-area layer3 switches, SwitchC, SwitchD, SwitchG, SwitchJ and SwitchK are edge layer3 switches of the area, SwitchE and SwitchG are edge layer3 switches of the autonomous system.

To area1, layer3 switches SwitchA and SwitchB are both in-area switches, area edge switches SwitchC and SwitchD are responsible for reporting distance cost to all destination outside the area, while they are also responsible for reporting the position of the AS edge layer3 switches SwitchE and SwitchG, AS exterior link-state advertisement from SwitchE and SwitchG are flooded throughout the whole autonomous system. When ASE LSA floods in area 1, those LSAs are included in the area 1 database to get the routes to network N11 and N15.

In addition, layer3 SwitchC and SwitchD must summary the topology of area 1 to the backbone area (area 0, all non-0 areas must be connected via area 0, direct connections are not allowed), and advertise the networks in area 1 (N1-N4) and the costs from SwitchC and SwitchD to those networks. As the backbone area is required to keep connected, there must be a virtual link between backbone layer3 SwitchJ and SwitchK. The area edge layer3 switches exchange summary information via the backbone layer3 switch, each area edge layer3 switch listens to the summary information from the other edge layer3 switches.

Virtual link can not only maintain the connectivity of the backbone area, but also strengthen the backbone area. For example, if the connection between backbone layer3 SwitchH and SwitchJ is cut down, the backbone area will become incontinuous. The backbone area can become more robust by establishing a virtual link between backbone layer3 switches SwitchG and SwitchJ. In addition, the virtual link between SwitchG and SwitchJ provide a short path from area 3 to layer3 SwitchG.

Take area 1 as an example. Assume the IP address of layer3 SwitchA is 10.1.1.1, IP address of layer3 SwitchB interface VLAN2 is 10.1.1.2, IP address of layer3 SwitchC interface VLAN2 is 10.1.1.3, IP address of layer3 SwitchD interface VLAN2 is 10.1.1.4. SwitchA is connecting to network N1 through Ethernet interface VLAN1 (IP address 20.1.1.1); SwitchB is connecting to network N2 through Ethernet interface VLAN1 (IP address 20.1.2.1); SwitchC is connecting to network N4 through Ethernet interface VLAN3 (IP address 20.1.3.1). All the three addresses belong to area 1. SwitchC is connecting to layer3 SwitchF through Ethernet interface VLAN1 (IP address 10.1.5.1); SwitchD is connecting to layer3 SwitchE through Ethernet interface VLAN1 (IP address 10.1.6.1); both two addresses belong to area 1. Simple authentication is implemented among layer3 switches in area1, edge layer3 switches of area 1 authenticate with the area 0 backbone layer3 switches by MD5 authentication..

The followings are just configurations for all layer3 switches in area 1, configurations for layer3 switches of the other areas are omitted. The following are the configurations of SwitchA SwitchB.SwitchC and SwitchD:

1)SwitchA：

Configure IP address for interface vlan2

SwitchA#config

SwitchA(config)# interface vlan 2

SwitchA(config-If-Vlan2)# ip address 10.1.1.1 255.255.255.0

SwitchA(config-If-Vlan2)#exit

Enable OSPF protocol, configure the area number for interface vlan2.

SwitchA(config)#router ospf

SwitchA(config-router)#network 10.1.1.0/24 area 1

SwitchA(config-router)#exit

Configure simple key authentication.

SwitchA(config)#interface vlan 2

SwitchA(config-If-Vlan2)#ip ospf authentication

SwitchA(config-If-Vlan2)#ip ospf authentication-key DCS

SwitchA(config-If-Vlan2)exit

Configure IP address and area number for interface vlan1.

SwitchA(config)# interface vlan 1

SwitchA(config-If-Vlan1)#ip address 20.1.1.1 255.255.255.0

SwitchA(config-If-Vlan1)#exit

SwitchA(config)#router ospf

SwitchA(config-router)#network 20.1.1.0/24 area 1

SwitchA(config-router)#exit

2)SwitchB：

Configure IP address for interface vlan2

SwitchB#config

SwitchB(config)# interface vlan 2

SwitchB(config-If-Vlan2)# ip address 10.1.1.2 255.255.255.0

SwitchB(config-If-Vlan2)#exit

Enable OSPF protocol, configure the area number for interface vlan2.

SwitchB(config)#router ospf

SwitchB(config-router)#network 10.1.1.0/24 area 1

SwitchB(config-router)#exit

SwitchB(config)#interface vlan 2

Configure simple key authentication.

SwitchB(config)#interface vlan 2

SwitchB(config-If-Vlan2)#ip ospf authentication
SwitchB(config-If-Vlan2)#ip ospf authentication-key DCS
SwitchB(config-If-Vlan2)#exit
Configure IP address and area number for interface vlan1.
SwitchB(config)# interface vlan 1
SwitchB(config-If-Vlan1)#ip address 20.1.2.1 255.255.255.0
SwitchB(config-If-Vlan1)#exit
SwitchB(config)#router ospf
SwitchB(config-router)#network 20.1.2.0/24 area 1
SwitchB(config-router)#exit
SwitchB(config)#exit
SwitchB#
3)SwitchC：
Configure IP address for interface vlan2
SwitchC#config
SwitchC(config)# interface vlan 2
SwitchC(config-If-Vlan2)# ip address 10.1.1.3 255.255.255.0
SwitchC(config-If-Vlan2)#exit
Enable OSPF protocol, configure the area number for interface vlan2
SwitchC(config)#router ospf
SwitchC(config-router)#network 10.1.1.0/24 area 1
SwitchC(config-router)#exit
Configure simple key authentication
SwitchC(config)#interface vlan 2
SwitchC(config-If-Vlan2)#ip ospf authentication
SwitchC(config-If-Vlan2)#ip ospf authentication-key DCS
SwitchC(config-If-Vlan2)#exit
Configure IP address and area number for interface vlan3
SwitchC(config)# interface vlan 3
SwitchC(config-If-Vlan3)#ip address 20.1.3.1 255.255.255.0
SwitchC(config-If-Vlan3)#exit
SwitchC(config)#router ospf
SwitchC(config-router)#network 20.1.3.0/24 area 1
SwitchC(config-router)#exit
Configure IP address and area number for interface vlan 1
SwitchC(config)# interface vlan 1
SwitchC(config-If-Vlan1)#ip address 10.1.5.1 255.255.255.0
SwitchC(config-If-Vlan1)#exit

SwitchC(config)#router ospf
SwitchC(config-router)#network 10.1.5.0/24 area 0
SwitchC(config-router)#exit
Configure MD5 key authentication.
SwitchC(config)#interface vlan 1
SwitchC (config-If-Vlan1)#ip ospf authentication message-digest
SwitchC (config-If-Vlan1)#ip ospf authentication-key DCS
SwitchC (config-If-Vlan1)#exit
SwitchC(config)#exit
SwitchC#
4)SwitchD：
Configure IP address for interface vlan2
SwitchD#config
SwitchD(config)# interface vlan 2
SwitchD(config-If-Vlan2)# ip address 10.1.1.4 255.255.255.0
SwitchD(config-If-Vlan2)#exit
Enable OSPF protocol, configure the area number for interface vlan2.
SwitchD(config)#router ospf
SwitchD(config-router)#network 10.1.1.0/24 area 1
SwitchD(config-router)#exit
Configure simple key authentication.
SwitchD(config)#interface vlan 2
SwitchD(config-If-Vlan2)#ip ospf authentication
SwitchD(config-If-Vlan2)#ip ospf authentication-key DCS
SwitchD(config-If-Vlan2)#exit
Configure the IP address and the area number for the interface vlan 1
SwitchD(config)# interface vlan 1
SwitchD(config-If-Vlan1)# ip address 10.1.6.1 255.255.255.0
SwitchD(config-If-Vlan1)exit
SwitchD(config)#router ospf
SwitchD(config-router)#network 10.1.6.0/24 area 0
SwitchD(config-router)#exit
Configure MD5 key authentication
SwitchD(config)#interface vlan 1
SwitchD(config-If-Vlan1)#ip ospf authentication message-digest
SwitchD(config-If-Vlan1)#ip ospf authentication-key DCS
SwitchD(config-If-Vlan1)exit
SwitchD(config)#exit

SwitchD#

17.6.4.2 Configuration Examples of OSPF VPN

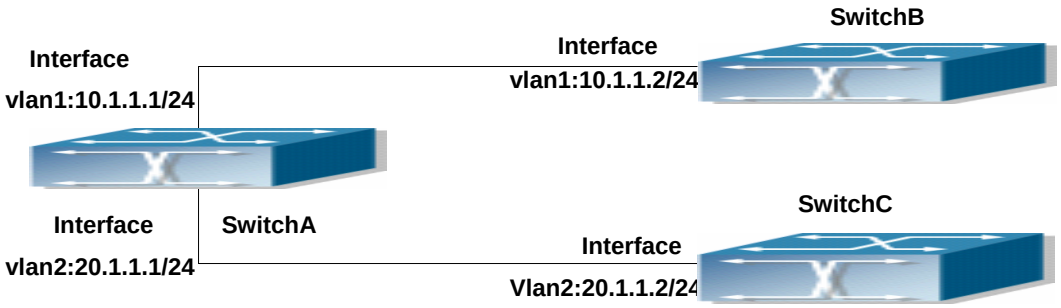


Fig 17-8 OSPF VPN Example

The above figure shows that a network consists of three Layer 3 switches in which the switchA as PE, SwitchB and SwitchC as CE1 and CE2. The PE is connected to CE1 and CE2 through vlan1 and vlan2. The routing messages are exchanged between PE and CE through OSPF protocol.

a) SwitchA, the Layer 3 switch as PE

Configure VPN route/transmitting examples vpnb and vpnc

SwitchA#config

SwitchA(config)#ip vrf vpnb

SwitchA(config-vrf)#

SwitchA(config-vrf)#exit

SwitchA#(config)

SwitchA(config)#ip vrf vpnc

SwitchA(config-vrf)#

SwitchA(config-vrf)#exit

Associate the vlan 1 and vlan 2 respectively with vpnb and vpnc while configuring IP address

SwitchA(config)#in vlan1

SwitchA(config-if-Vlan1)#ip vrf forwarding vpnb

SwitchA(config-if-Vlan1)#ip address 10.1.1.1 255.255.255.0

SwitchA(config-if-Vlan1)#exit

SwitchA(config)#in vlan2

SwitchA(config-if-Vlan2)#ip vrf forwarding vpnc

SwitchA(config-if-Vlan2)#ip address 20.1.1.1 255.255.255.0

SwitchA(config-if-Vlan2)#exit

Configure OSPF examples associated with vpnb and vpnc respectively

SwitchA(config)#

SwitchA(config)#router ospf 100 vpnb

SwitchA(config-router)#network 10.1.1.0/24 area 0

SwitchA(config-router)#redistribute bgp

SwitchA(config-router)#exit

SwitchA(config)#router ospf 200 vpnc

SwitchA(config-router)#network 20.1.1.0/24 area 0

SwitchA(config-router)#redistribute bgp

b) The Layer 3 SwitchB of CE1：

Configure the IP address of Ethernet E 1/2

SwitchB#config

SwitchB(config)# interface Vlan1

SwitchB(config-if-vlan1)# ip address 10.1.1.2 255.255.255.0

SwitchB (config-if-vlan1)exit

Enable OSPF protocol and configuring OSPF segments

SwitchB(config)#router ospf

SwitchB(config-router-rip)#network 10.1.1.0/24 area 0

SwitchB(config-router-rip)#exit

c) The Layer 3 SwitchC of CE2

Configure the IP address of Ethernet E 1/2

SwitchC#config

SwitchC(config)# interface Vlan1

SwitchC(config-if-vlan1)# ip address 20.1.1.2 255.255.255.0

SwitchC (config-if-vlan1)#exit

Initiate OSPF protocol and configuring OSPF segments

SwitchC(config)#router ospf

SwitchC(config-router)#network 20.1.1.0/24 area 0

SwitchC(config-router)#exit

17.6.5 OSPF Troubleshooting

The OSPF protocol may not be working properly due to errors such as physic connection, configuration error when configuring and using the OSPF protocol. So users should pay attention to following:

First ensure the physic connection is correct

Second, ensure the interface and link protocol are UP (use show interface command)

Configure different IP address from different segment on each interface

Then initiate OSPF protocol (use router-ospf command) and configure the OSPF

area on corresponding interface

After that, a OSPF protocol feature should be checked---the OSPF backbone area should be continuous and apply virtual link to ensure it is continuous. if not; all non 0 areas should only be connected to other non 0 area through 0 area; a border Layer 3 switch means that one part of the interfaces of this switch belongs to 0 area, the other part belongs to non 0 area; Layer 3 switch DR should be specified for multi-access network such as broadcast network.

If the OSPF routing problem remains unresolved after checking and debugging, please use debug ospf packet/events commands and record the debug messages in three minutes ,then send it to our technical service center.

17.6.5.1 Commands for Monitor And Debug

17.6.5.1.1 debug ospf events

Command: [no]debug ospf events [abr|asbr|lsa|nssa|os|router|vlink]

Function: Open debugging switches showing various OSPF events messages; the "**[no]debug ospf events [abr|asbr|lsa|nssa|os|router|vlink]**" command closes the debugging switch.

Default: Closed

Command Mode: Admin and global mode

Example:

Switch#debug ospf events router

17.6.5.1.2 debug ospf ifsm

Command: [no]debug ospf ifsm [status|events|timers]

Function: Open debugging switches showing the OSPF interface states; the "**[no]debug ospf ifsm [status|events|timers]**" command closes this debugging switches.

Default: Closed

Command Mode: Admin mode and global mode

Example:

Switch#debug ospf ifsm events

17.6.5.1.3 debug ospf lsa

Command: [no]debug ospf lsa [generate|flooding|install|maxage|refresh]

Function: Open debugging switches showing link state announcements; the "**[no]debug ospf lsa [generate|flooding|install|maxage|refresh]**" closes the debugging switches.

Default: Closed

Command Mode: Admin mode and global mode

Example:

Switch#debug ospf lsa generate

17.6.5.1.4 debug ospf nfsm

Command: [no]debug ospf nfsm [status|events|timers]

Function: Open debugging switches showing OSPF neighbor state machine; the "**[no]debug ospf nfsm [status|events|timers]**"command closes this debugging switch

Default: Closed

Command Mode: Admin mode and global mode

Example: Switch#debug ospf nfsm events

17.6.5.1.5 debug ospf nsm

Command: [no]debug ospf nsm [interface|redistribute]

Function: Open debugging switches showing OSPF NSM, the "**[no]debug ospf nsm [interface|redistribute]**" command closes this debugging switch

Default: Closed

Command Mode: Admin mode and global mode

Example:

Switch#debug ospf nsm interface

17.6.5.1.6 debug ospf packet

Command: [no]debug ospf packet

[dd|detail|hello|ls-ack|ls-request|ls-update|recv|detail]

Function: Open debugging switches showing OSPF packet messages; the "**[no]debug ospf packet [dd|detail|hello|ls-ack|ls-request|ls-update|recv|detail]**" command closes this debugging switch

Default: Closed

Command Mode: Admin mode and global mode

Example: Switch#debug ospf packet hello

17.6.5.1.7 debug ospf route

Command: [no]debug ospf route [ase|ia|install|spf]

Function: Open debugging switches showing OSPF related routes; the "**[no]debug ospf route [ase|ia|install|spf]**" command closes this debugging switch

Default: Closed

Command Mode: Admin mode and global mode

Example: Switch#debug ospf route spf

17.6.5.1.8 show ip ospf

Command: show ip ospf [<*process-id*>]

Function: Display OSPF main messages

Parameter: <*process-id*> is the process ID, ranging between 0~65535

Default: Not displayed

Command Mode: All modes

Example:

```
Switch#show ip ospf
Routing Process "ospf 0" with ID 192.168.1.1
 Process bound to VRF default
 Process uptime is 2 days 0 hour 30 minutes
 Conforms to RFC2328, and RFC1583Compatibility flag is disabled
 Supports only single TOS(TOS0) routes
 Supports opaque LSA
 SPF schedule delay 5 secs, Hold time between two SPFs 10 secs
 Refresh timer 10 secs
 Number of external LSA 0. Checksum Sum 0x000000
 Number of opaque AS LSA 0. Checksum Sum 0x000000
 Number of non-default external LSA 0
 External LSA database is unlimited.
 Number of LSA originated 0
 Number of LSA received 0
 Number of areas attached to this router: 1
     Area 0 (BACKBONE) (Inactive)
         Number of interfaces in this area is 0(0)
         Number of fully adjacent neighbors in this area is 0
         Area has message digest authentication
         SPF algorithm executed 0 times
         Number of LSA 0. Checksum Sum 0x000000
Routing Process "ospf 10" with ID 0.0.0.0
 Process bound to VRF DC1
 Process uptime is 4 days 23 hours 51 minutes
 Conforms to RFC2328, and RFC1583Compatibility flag is disabled
 Supports only single TOS(TOS0) routes
 Supports opaque LSA
 SPF schedule delay 5 secs, Hold time between two SPFs 10 secs
 Refresh timer 10 secs
 Number of external LSA 0. Checksum Sum 0x000000
 Number of opaque AS LSA 0. Checksum Sum 0x000000
 Number of non-default external LSA 0
 External LSA database is unlimited.
 Number of LSA originated 0
 Number of LSA received 0
```

Number of areas attached to this router: 1

Area 0 (BACKBONE) (Inactive)

Number of interfaces in this area is 0(0)

Number of fully adjacent neighbors in this area is 0

Area has no authentication

SPF algorithm executed 0 times

Number of LSA 0. Checksum Sum 0x000000

17.6.5.1.9 show ip ospf border-routers

Command: show ip ospf [<*process-id*>] border-routers

Function: Display ABR and ASBR under all OSPF instances

Parameter: <*process-id*> is the process ID, ranging between 0~65535

Default: Not displayed

Command Mode: All modes

Example:

Switch#show ip ospf border-routers

OSPF process 0 internal Routing Table

Codes: i - Intra-area route, I - Inter-area route

i 10.15.0.1 [10] via 10.10.0.1, Vlan1, ASBR, Area 0.0.0.0

i 172.16.10.1 [10] via 10.10.11.50, Vlan2, ABR, ASBR, Area 0.0.0.0

17.6.5.1.10 show ip ospf database

Command: show ip ospf [<*process-id*>] database[{

[<*linkstate_id*>]asbr-summary[{self-originate |adv-router <*advertiser_router*>}]

| [<*linkstate_id*>]externel [{self-originate |adv-router <*advertiser_router*>}]

| [<*linkstate_id*>]network [{self-originate |adv-router <*advertiser_router*>}]

| [<*linkstate_id*>]nssa-external [{self-originate |adv-router <*advertiser_router*>}]

| [<*linkstate_id*>]opaque-area [{self-originate |adv-router <*advertiser_router*>}]

| [<*linkstate_id*>]opaque-as [{self-originate |adv-router <*advertiser_router*>}]

| [<*linkstate_id*>]opaque-link [{self-originate |adv-router <*advertiser_router*>}]

| [<*linkstate_id*>]router [{self-originate |adv-router <*advertiser_router*>}]

| [<*linkstate_id*>]summary [{self-originate |adv-router <*advertiser_router*>}]

|self-originate | max-age }]

Function: Display the OSPF link state data base messages

Parameter: <*process-id*> is the process ID, ranging between 0~65535

<*linkstate_id*> Link state ID, shown in point divided demcial system

<*advertiser_router*> is the ID of Advertising router, shown in point divided demcial IP address format

Default: Not displayed

Command Mode: All modes

Usage Guide: According to the output messages of this command, we can view the OSPF link state database messages

Example:

Switch#show ip ospf database

Router Link States (Area 0.0.0.2)

Link ID	ADV Router	Age	Seq#	CkSum	Link count
192.168.1.2	192.168.1.2	254	0x80000031	0xec21	1
192.168.1.3	192.168.1.3	236	0x80000033	0x0521	2

Net Link States (Area 0.0.0.2)

Link ID	ADV Router	Age	Seq#	CkSum
20.1.1.2	192.168.1.2	254	0x8000002b	0xece4

Summary Link States (Area 0.0.0.2)

Link ID	ADV Router	Age	Seq#	CkSum	Route
6.1.0.0	192.168.1.2	68	0x8000002b	0x5757	6.1.0.0/22
6.1.1.0	192.168.1.2	879	0x8000002a	0xf8bc	6.1.1.0/24
22.1.1.0	192.168.1.2	308	0x8000000c	0xc8f0	22.1.1.0/24

ASBR-Summary Link States (Area 0.0.0.2)

Link ID	ADV Router	Age	Seq#	CkSum
192.168.1.1	192.168.1.2	1702	0x8000002a	0x89c7

AS External Link States

Link ID	ADV Router	Age	Seq#	CkSum	Route
2.2.2.0	192.168.1.1	1499	0x80000056	0x3a63	E2 2.2.2.0/24 [0x0]
2.2.3.0	192.168.1.1	1103	0x8000002b	0x0ec3	E2 2.2.3.0/24 [0x0]

17.6.5.1.11 show ip ospf interface

Command: show ip ospf interface <*interface*>

Function: Display the OSPF interface messages

Parameter: <*interface*> *is the* name of interface

Default: Not displayed

Command Mode: All modes

Example:

Switch#show ip ospf interface

Loopback is up, line protocol is up

OSPF not enabled on this interface

Vlan1 is up, line protocol is up

Internet Address 10.10.10.50/24, Area 0.0.0.0

Router ID 10.10.11.50, Network Type BROADCAST, Cost: 10

Transmit Delay is 5 sec, State Waiting, Priority 1

No designated router on this network

No backup designated router on this network

Timer intervals configured, Hello 35, Dead 35, Wait 35, Retransmit 5

Hello due in 00:00:16

Neighbor Count is 0, Adjacent neighbor count is 0

17.6.5.1.12 show ip ospf neighbor

Command: show ip ospf [<*process-id*>] neighbor [{<*neighbor_id*> |all |detail [all] |interface<*ifaddress*>}]

Function: Display the OSPF adjacent point messages

Parameter: **<*process-id*>** is the process ID ranging between 0~65535

<*neighbor_id*> is the dotted decimal notation neighbor ID

all: Display messages of all neighbors

detail: Display detailed messages of all neighbors

<*ifaddress*> Interface IP address

Default: Not displayed

Command Mode: All modes

Usage Guide: OSPF neighbor state can be checked by viewing the output of this command

Example:

Switch#show ip ospf neighbor

OSPF process 0:

Neighbor ID	Pri	State	Dead Time	Address	Interface
192.168.1.1	1	Full/Backup	00:00:32	6.1.1.1	Vlan1
192.168.1.3	1	Full/DR	00:00:36	20.1.1.3	Vlan2
192.168.1.3	1	Full/ -	00:00:30	20.1.1.3	VLINK2

Displayed information	Explanation
Neighbor ID	ID Neighbor ID
Priority	Priority
State	Neighbor relation state
Dead time	Neighbor dead time
Address	Interface Address
Interface	Interface name

17.6.5.1.13 show ip ospf route

Command: show ip ospf [<*process-id*>] route

Function: Display the OSPF routing table messages

Parameter: <*process-id*> is the process ID ranging between 0~65535

Default: Not displayed

Command Mode: All modes

Example:

Switch#show ip ospf route

O 10.1.1.0/24 [10] is directly connected, Vlan1, Area 0.0.0.0

O 10.1.1.4/32 [10] via 10.1.1.4, Vlan1, Area 0.0.0.0

IA 11.1.1.0/24 [20] via 10.1.1.1, Vlan1, Area 0.0.0.0

IA 11.1.1.2/32 [20] via 10.1.1.1, Vlan1, Area 0.0.0.0

IA 12.1.1.0/24 [20] via 10.1.1.2, Vlan1, Area 0.0.0.0

IA 12.1.1.2/32 [20] via 10.1.1.2, Vlan1, Area 0.0.0.0

O 13.1.1.0/24 [10] is directly connected, Vlan4, Area 0.0.0.3

O 14.1.1.0/24 [10] is directly connected, Vlan5, Area 0.0.0.4

IA 15.1.1.0/24 [20] via 13.1.1.2, Vlan4, Area 0.0.0.3

IA 15.1.1.2/32 [20] via 13.1.1.2, Vlan4, Area 0.0.0.3

E1 100.1.0.0/16 [21] via 10.1.1.1, Vlan1

E1 100.2.0.0/16 [21] via 10.1.1.1, Vlan1

17.6.5.1.14 show ip ospf virtual-links

Command: show ip ospf [<*process-id*>] virtual-links

Function: Display the OSPF virtual link message

Parameter: <*process-id*> is the process ID ranging between 0~65535

Default: Not displayed

Command Mode: All modes

Example:

Switch#show ip ospf virtual-links

Virtual Link VLINK0 to router 10.10.0.9 is up

Transit area 0.0.0.1 via interface Vlan1

Transmit Delay is 1 sec, State Point-To-Point,

Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5

Hello due in 00:00:02

Adjacency state Full

Virtual Link VLINK1 to router 10.10.0.123 is down

Transit area 0.0.0.1 via interface Vlan1

Transmit Delay is 1 sec, State Down,

Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5

Hello due in inactive

Adjacency state Down

17.6.5.1.15 show ip protocols

Command: show ip protocols

Function: Display the running routing protocol messages

Default: None

Command Mode: All modes

Example:

show ip protocols

Use show ip protocol command will show the messages of the routing protocol running on current layer 3 switch

For example, the displayed messages are:

Routing Protocol is "ospf 0"

Invalid after 0 seconds, hold down 0, flushed after 0

Outgoing update filter list for all interfaces is

Incoming update filter list for all interfaces is

Redistributing:

Routing for Networks:

10.1.1.0/24

12.1.1.0/24

Routing Information Sources:

Gateway Distance Last Update

Distance: (default is 110)

Address Mask Distance List

Routing Protocol is "bgp 0"

Outgoing update filter list for all interfaces is

Incoming update filter list for all interfaces is

IGP synchronization is disabled

Automatic route summarization is disabled

Neighbor(s):

Address FiltIn FiltOut DistIn DistOut Weight RouteMap

Incoming Route Filter:

17.7 OSPFv3

17.7.1 Introduction to OSPFv3

OSPFv3（Open Shortest Path First）is the third version for Open Shortest Path First, and it is the IPv6 version of OSPF Protocol. It is an interior dynamic routing protocol for

autonomous system based on link-state. The protocol creates a link-state database by exchanging link-states among layer3 switches, then uses the Shortest Path First algorithm to generate a route table basing on that database.

Autonomous system (AS) is a self-managed interconnected network. In large networks, such as the Internet, a giant interconnected network is broken down to autonomous systems. Big enterprise networks connecting to the Internet are independent AS, since the other host on the Internet are not managed by those AS and they don't share interior routing information with the layer3 switches on the Internet.

Each link-state layer3 switch can provide information about the topology with its neighboring layer3 switches.

• The network segment (link) connecting to the layer3 switch

• State of the connecting link

Link-state information is flooded throughout the network so that all layer3 switches can get first hand information. Link-state layer3 switches will not broadcast all information contained in their route tables; instead, they only send changed link-state information. Link-state layer3 switches establish neighborhood by sending "HELLO" to their neighbors, then link-state advertisements (LSA) will be sent among neighboring layer3 switches. Neighboring layer3 switch copy the LSA to their routing table and transfer the information to the rest part of the network. This process is referred to as "flooding". In this way, firsthand information is sent throughout the network to provide accurate map for creating and updating routes in the network. Link-state routing protocols use cost instead of hops to decide the route. Cost is assigned automatically or manually. According to the algorithm in link-state protocol, cost can be used to calculate the hop number for packages to pass, link bandwidth, and current load of the link, The administrator can even add weight for better assessment of the link-state.

1) When a link-state layer3 switch enters a link-state interconnected network, it sends a HELLO package to get to know its neighbors and establish neighborhood.

2) The neighbors respond with information about the links they are connecting and the related costs.

3) The originate layer3 switch uses this information to build its own routing table.

4) Then, as part of the regular update, layer3 switch send link-state advertisement (LSA) packages to its neighboring layer3 switches. The LSA include links and related costs of that layer3 switch.

5) Each neighboring layer3 switch copies the LSA package and passes it to the next neighbor (i.e. flooding).

6) Since routing database is not recalculated before layer3 switch forwards LSA flooding, the converging time is greatly reduced.

One major advantage of link-state routing protocols is the fact that infinite counting is

impossible, this is because of the way link-state routing protocols build up their routing table. The second advantage is that converging in a link-state interconnected network is very fast, once the routing topology changes, updates will be flooded throughout the network very soon. Those advantages release some layer3 switch resources, as the process ability and bandwidth used by bad route information are minor.

The features of OSPFv3 protocol include the following: OSPFv3 supports networks of various scales, several hundreds of layer3 switches can be supported in an OSPFv3 network. Routing topology changes can be quickly found and updating LSAs can be sent immediately, so that routes converge quickly. Link-state information is used in shortest path algorithm for route calculation, eliminating loop route. OSPFv3 divides the autonomous system intro areas, reducing database size, bandwidth occupation and calculation load. (According to the position of layer3 switches in the autonomous system, they can be grouped as internal area switches, area edge switches, AS edge switches and backbone switches). OSPFv3 supports load balance and multiple routes to the same destination of equal costs. OSPFv3 supports 4 level routing mechanisms (process routing according to the order of route inside an area, route between areas, first category exterior route and second category exterior route). OSPFv3 support IP subnet and redistribution of routes from the other routing protocols, and interface-based packet verification. OSPFv3 supports sending packets in multicast.

Each OSPFV3 layer3 switch maintains a database describing the topology of the whole autonomous system. Each layer3 switch gathers the local status information, such as available interface, reachable neighbors, and sends link-state advertisement (sending out link-state information) to exchange link-state information with other OSPFv3 layer3 switches to form a link-state database describing the whole autonomous system. Each layer3 switch builds a shortest path tree rooted by itself according to the link-state database, this tree provide the routes to all nodes in an autonomous system. If two or more layer3 switches exist (i.e. multi-access network), "designated layer3 switch” and “backup designated layer3 switch” will be selected. Designated layer3 switch is responsible for spreading link-state of the network. This concept helps reducing the traffic among the Layer3 switches in multi-access network.

OSPFv3 protocol requires the autonomous system to be divided into areas. That is to divide the autonomous system into 0 area (backbone area) and non-0 areas. Routing information between areas are further abstracted and summarized to reduce the bandwidth required in the network. OSPFv3 uses four different kinds of routes: they are the route inside the area, route between areas, first category exterior route and second category exterior route, in the order of highest priority to lowest. The route inside an area and between areas describe the internal network structure of an autonomous system, while external routes describe external routes describe how to select the routing

information to destination outside the autonomous system. The first type of exterior route corresponds to the information introduced by OSPFv3 from the other interior routing protocols, the costs of those routes are comparable with the costs of OSPFv3 routes; the second type of exterior route corresponds to the information introduced by OSPFv3 from the other exterior routing protocols, but the costs of those routes are far greater than that of OSPFv3 routes, so OSPFv3 route cost is ignored when calculating route costs.

OSPFv3 areas are centered with the Backbone area, identified as the Area 0, all the other areas must be connected to Area 0 logically, and Area 0 must be continuous. For this reason, the concept of virtual link is introduced to the backbone area, so that physically separated areas still have logical connectivity to the backbone area. The configurations of all the layer3 switches in the same area must be the same.

In one word, LSA can only be transferred between neighboring Layer3 switches, and OSPFv3 protocol includes seven kinds of LSA: link LSA, internal-area prefix LSA, router LSA, network LSA, inter-area prefix LSA, inter-area router LSA and autonomic system exterior LSA. Router LSA is generated by each Layer 3 switch in an OSPF area, and is sent to all other neighboring Layer 3 switch in this area; network LSA is generated by designated Layer 3 switch in the OSPF area of multi-access network and is sent to all other neighboring layer3 switches in this area.(To reduce data traffic among each Layer 3 switches in the multi-access network, “designated layer3 switch” and “backup designated layer3 switch” should be selected in the multi-access network, and the network link-state is broadcasted by designated Layer 3 switch); the inter-area prefix LSA and inter-area router LSA are generated by OSPF area border Layer 3 switches and transferred among those switches. The autonomic system exterior LSA is generated by autonomic system exterior border Layer 3 switches and transferred in the whole autonomic system. Link LSA is generated by Layer 3 switch on the link and sent to other Layer 3 switches on the link. Internal-area prefix LSA is generated by designated layer3 switch of each link in this area, and flooded to the whole area.

For autonomous system focused on exterior link-state announcement, OSPFv3 allow some areas to be configured as STUB areas in order to reduce the size of topological database. Router LSA, network LSA, inter-area prefix LSA, link LSA, internal-area prefix LSA are permitted to advertise to STUB area. Default route must be used in STUB area, Layer 3 switches on the area border of STUB area announces to default routes of STUB area by inter-area prefix LSA; these default routes only flood in STUB area, not outside of STUB area. Each STUB area has a corresponding default route, the route from STUB area to AS exterior destination depends only on default route of this area.

The following simply outlines the route calculation process of OSPFv3 protocol:

1）Each OSPF-enabled layer3 switch maintains a database (LS database) describing the link-state of the topology structure of the whole autonomous system. Each layer3 switch

generates a link-state advertisement according to its surrounding network topology structure (router LSA), and sends the LSA to other layer3 switches through link-state update (LSU) packages. Thus, each layer3 switches receives LSAs from other layer3 switches, and all LSAs combined to the link-state database.

2）Since a LSA is the description of the network topology structure around a layer3 switch, the LS database is the description of the network topology structure of the whole network. The layer3 switches can easily create a weighted vector map according to the LS database. Obviously, all layer3 switches in the same autonomous system will have the same network topology map.

3）Each layer3 switch uses the shortest path finding (SPF) algorithm to calculate a tree of shortest path rooted by itself. The tree provides the route to all the nodes in the autonomous system, leaf nodes consist of the exterior route information. The exterior route can be marked by the layer3 switch broadcast it, so that additional information about the autonomous system can be recorded. As a result, the route table of each layer3 switch is different.

OSPFv3 protocol is developed by the IETF, the OSPF v3 used now is fulfilled according to the content described in RFC2328 and RFC2740.

As a result of continuous development of IPv6 network, it has the network environment of nonsupport IPv6 sometimes, so it needs to do the IPv6 operation by tunnel. Therefore, our OSPFv3 supports configuration on configure tunnel, and passes through nonsupport IPv6 network by unicast packet of IPv4 encapsulation.

17.7.2 OSPFv3 Configuration Task List

1. Enable OSPFv3 (required)
   （1） Enable/disable OSPFv3(required)
   （2） Configure the router-id number of the layer3 switch running OSPFv3 (optional)
   （3） Configure the network scope for running OSPFv3 (optional)
   （4） enable OSPFv3 on the interface (required)
2. Configure OSPFv3 auxiliary parameters (optional)
   （1） Configure OSPFv3 package sending mechanism parameters
      1) Set the OSPFv3 interface to receive only
      2) Configure the cost for sending packages from the interface
      3) Configure OSPF package sending timer parameter (timer of broadcast interface sending HELLO package to poll, timer of neighboring layer3 switch invalid timeout, timer of LSA transmission delay and timer of LSA retransmission.

（2） Configure OSPFv3 route introduction parameters

1) Configure default parameters (default type, default tag value, default cost)

2) Configure the routes of the other protocols to introduce to OSPFv3

（3） Configure other OSPF protocol parameters

1) Configure OSPF routing protocol priority

2) Configure cost for OSPF STUB area and default route

3) Configure OSPF virtual link

4) Configure the priority of the interface when electing designated layer3 switch

3. Close OSPFv3 Protocol

1. Enable OSPFv3 Protocol

It is very simple to run the basic configurations of OSPFv3 routing protocol on the Layer 3 switch of ES4626/ES4650 switch, normally only enabling OSPFv3, implement OSPFv3 interface, the default value is defined to OSPFv3 protocol parameters. Refer to 2. Configure OSPF auxiliary parameters, if the OSPFv3 protocol parameters need to be modified.

Commands	Explanation
Global mode	
[no] router IPv6 ospf <*tag*>	The command initializes ospfv3 routing process and enter ospfv3 mode to configure ospfv3 routing process. The **[no] router IPv6 ospf <*tag*>** command stops relative process. (required)
OSPFv3 Protocol Configure Mode	
router-id <*router_id*> **no router-id**	Configure router for ospfv3 process. The **no router-id** command returns ID to 0.0.0.0 (required)
[**no**] **passive-interface<*ifname*>**	Configure an interface receiving without sending. The [**no**] **passive-interface<*ifname*>**command cancels configuration.
Interface Configuration Mode	

[no] IPv6 router ospf {area <*area-id*> [instance-id <*instance-id*> | tag <*tag*> [instance-id <*instance-id*>]] | tag <*tag*> area <*area-id*> [instance-id <*instance-id*>]}	Implement ospfv3 routing on the interface. The **[no] IPv6 router ospf {area <*area-id*> [instance-id <*instance-id*> | tag <*tag*> [instance-id <*instance-id*>]] | tag <*tag*> area <*area-id*> [instance-id <*instance-id*>]}** command cancels configuration.

2. Configure OSPFv3 parameters

（1）Configure OSPFv3 package sending mechanism parameters

1）Set the OSPF interface to receive only

2）Configure the cost for sending packages from the interface

Commands	Explanation
Interface Configuration Mode	
IPv6 ospf cost <*cost*> [instance-id <*id*>] **no IPv6 ospf cost [instance-id <*id*>]**	Appoint interface to implement required cost of OSPFv3 protocol. The **no IPv6 ospf cost** [**instance-id <*id*>**] restores the default setting

3）Configure OSPFv3 package sending timer parameter (timer of broadcast interface sending HELLO package to poll, timer of neighboring layer3 switch invalid timeout, timer of LSA transmission delay and timer of LSA retransmission.

Commands	Explanation
Interface Configuration Mode	
IPv6 ospf hello-interval <*time*> [instance-id <*id*>] **no IPv6 ospf hello-interval [instance-id <*id*>]**	Sets interval for sending HELLO packages; the "**no IPv6 ospf hello-interval [instance-id <*id*>]**" command restores the default setting.
IPv6 ospf dead-interval <*time*> [instance-id <*id*>] **no IPv6 ospf dead-interval [instance-id <*id*>]**	Sets the interval before regarding a neighbor layer3 switch invalid; the "**no IPv6 ospf dead-interval [instance-id <*id*>]**" command restores the default setting.
IPv6 ospf transit-delay <*time*> [instance-id <*id*>] **no IPv6 ospf transit-delay [instance-id <*id*>]**	Sets the delay time before sending link-state broadcast; the "**no IPv6 ospf transit-delay [instance-id <*id*>]**" command restores the default setting.

IPv6 ospf retransmit <*time*> [instance-id <*id*>] **no IPv6 ospf retransmit [instance-id <*id*>]**	.Sets the interval for retransmission of link-state advertisement among neighbor layer3 switches; the "**no IPv6 ospf retransmit [instance-id <*id*>]**" command restores the default setting.

（2）Configure OSPFv3 route introduction parameters

Configure OSPFv3 route introduction parameters

Commands	Explanation
OSPF Protocol Configuration Mode	
[no]redistribute {kernel |connected| static| rip| isis| bgp} [metric<*value*>] [metric-type {1|2}][route-map<*word*>]	Introduces other protocol discovery routing and static routing regarded as external routing message. The **[no]redistribute {kernel |connected| static| rip| isis| bgp} [metric<*value*>] [metric-type {1|2}][route-map<*word*>]** command cancels imported external routing message.

（3） Configure Other Parameters of OSPFv3 Protocol

1） Configure OSPFv3 STUB Area & Default Routing Cost

2） Configure OSPFv3 Virtual Link

Commands	Explanation
OSPFv3 Protocol Configuration Mode	
timers spf <*spf-delay*> <*spf-holdtime*> **no timers spf**	Configure OSPFv3 SPF timer. The **no timers spf** command recovers default value.
area <*id*> stub [no-summary] **no area <*id*> stub [no-summary]** **area <*id*> default-cost <*cost*>** **no area <*id*> default-cost** **area <*id*> virtual-link A.B.C.D [instance-id <*instance-id*> INTERVAL]** **no area <*id*> virtual-link A.B.C.D [|INTERVAL]**	Configure parameters in OSPFv3 area (STUB area, Virtual link). The no command restores default value.

4）Configure the priority of the interface when electing designated layer3 switch (DR).

Commands	Explanation

Interface Configuration Mode	
IPv6 ospf priority <*priority*> [instance-id <*id*>] **no IPv6 ospf priority [instance-id <*id*>]**	Sets the priority of the interface in "designated layer3 switch" election; the "**no IPv6 ospf priority [instance-id <*id*>]**" command restores the default setting.

3. Disable OSPFv3 Protocol

Commands	Explanation
Global mode	
no router IPv6 ospf [<*tag*>]	Disable OSPFv3 Routing Protocol

17.7.3 Commands for OSPFV3

17.7.3.1 area default cost

Command: area <*id*> default-cost <*cost*>

no area <*id*> default-cost

Function: Configure the cost of sending to the default summary route in stub or NSSA area; the "**no area <*id*> default-cost**" command restores the default value.

Parameter: <*id*> is the area number which could be shown as digits 0～4294967295, or as an IP address; **<*cost*>** ranges between <0-16777215>

Default: Default OSPFv3 cost is 1

Command Mode: OSPFv3 protocol mode

Usage Guide: The command is only adaptive to the ABR router connected to the stub area or NSSA area

Example: Set the default-cost of area 1 to 10

Switch(config-router)#area 1 default-cost 10

17.7.3.2 area range

Command: area <*id*> range <ipv6*address*> [advertise| not-advertise|]

no area <*id*> range <ipv6*address*>

Function: Aggregate OSPF route on the area border. The "**no area <*id*> range <*address*>**" cancels this function

Parameter: <*id*> is the area number which could be digits ranging between 0～4294967295, and also as an IP address.

<ipv6*address*>=<*X:X::X:X/M*>,Specifies the area ipv6 network prefix and its length

advertise: Advertise this area

not-advertise: Not advertise this area

If both are not set, this area is defaulted for advertising

Default: Function not configured

Command Mode: OSPFv3 protocol mode

Usage Guide: Use this command to aggregate routes inside an area. If the network IDs in this area are not configured continuously, a summary route can be advertised by configuring this command on ABR. This route consists of all single networks belong to specific range.

Example:

Switch # config terminal

Switch (config)# router ipv6 ospf

Switch (config-router)# area 1 range 2000::/3

17.7.3.3 area stub

Command: area <*id*> stub [no-summary]

no area <*id*> stub [no-summary]

Function: Define a area to a stub area. The "**no area <*id*> stub [no-summary]**" command cancels this function

Parameter: <*id*> is the area number which could be digits ranging between 0～4294967295, and also as an IPv4 address.

no-summary: The area border routes stop sending link summary announcement to the stub area

Default: Not defined

Command Mode: OSPFv3 protocol mode

Usage Guide: Configure area stub on all routes in the stub area. There are two configuration commands for the routers in the stub area: stub and default-cost. All routers connected to the stub area should be configured with area stub command. As for area border routers connected to the stub area, their introducing cost is defined with area default-cost command.

Example:

Switch # config terminal

Switch (config)# router ipv6 ospf

Switch (config-router)# area 1 stub

17.7.3.4 area virtual-link

Command: area <*id*> virtual-link A.B.C.D [instance-id <*instance-id*> | INTERVAL <*value*>]

no area <*id*> virtual-link A.B.C.D [instance-id <*instance-id*> | |INTERVAL]

Function: Configure a logical link between two backbone areas physically divided by non-backbone area. The "**no area <*id*> virtual-link A.B.C.D [instance-id <*instance-id*> | |INTERVAL]**" command removes this virtual-link.

Parameter: <*id*> is the area number which could be digits ranging between 0～4294967295, and also as an IP address.

<***instance-id***> is the interface instance ID ranging between 0~255 and defaulted at 0

***INTERVAL*= [*dead-interval*|*hello-interval*|*retransmit-interval*|*transmit-delay*]**

<*value*>: The delay or interval seconds, ranging between 1~65535

<*dead-interval*>: A neighbor is considered offline for certain dead interval without its group messages which the default is 40 seconds.

<*hello-interval*>: The time interval before the router sends a hello group message, default is 10 seconds

<*retransmit-interval*>: The time interval before a router retransmitting a group message, default is 5 seconds

<*transmit-delay*>: The time delay before a router sending a group messages, 1 second by default

Default: No default configuration.

Command Mode: OSPFv3 protocol mode

Usage Guide: In the OSPF all non-backbone areas will be connected to a backbone area. If the connection to the backbone area is lost, virtual link will repair this connection. You can configure virtual link between any two backbone areas routers connected with the public non-backbone area. The protocol treat routers connected by virtual links as a point-to-point network

Example:

Switch#config terminal

Switch(config) #router ipv6 ospf

Switch(config-router) #area 1 virtual-link 10.10.11.50 hello 5 dead 20

Switch(config-router) #area 1 virtual-link 10.10.11.50 instance-id 1

17.7.3.5 abr-type

Command: abr-type {cisco|ibm| standard}

no abr-type [cisco|ibm| standard]

Function: Configure an OSPF ABR type with this command. The "**no abr-type [cisco|ibm| standard]**" command restores the default

Parameter: cisco, realize by cisco ABR; **ibm**, realize by ibm ABR; **shortcut**, specify a shortcut-ABR; **standard**, realize with standard（RFC2328）ABR.

Default: Cisco configured by default

Command Mode: OSPFv3 protocol mode

Usage Guide: For Specifying the realizing type of abr. This command is good for interactive operation among different OSPF realizing method and is especially useful in the multiple host environment.

Example: Configure abr as standard

Switch#config terminal

Switch(config)#router ipv6 ospf

Switch(config-router)#abr-type standard

17.7.3.6 default-metric

Command: default-metric <*value*>

no default-metric

Function: The command set the default metric value of OSPF routing protocol; the "**no default-metric**" returns to the default state.

Parameter: <*value*>, metric value, ranging between 0~*16777214*

Default: Built-in, metric value auto translating

Command Mode: OSPF protocol mode

Usage Guide: When the default metric value makes the metric value not compatible, the route introducing still goes through. If the metric value can not be translated, the default value provides alternative option to carry the route introducing on. This command will result in that all introduced route will use the same metric value. This command should be used associating redistribute.

Example:

Switch#config terminal

Switch(config)#router ipv6 ospf

Switch(config-router)#default-metric 100

17.7.3.7 ipv6 ospf cost

Command: ipv6 ospf cost <*cost*> [instance-id <*id*>]

no ipv6 ospf cost [instance-id <*id*>]

Function: Specify the cost required in running OSPF protocol on the interface; the "**no ipv6 ospf cost [instance-id <*id*>]**" command restores the default value

Parameter: <*id*> is the interface instance ID, ranging between 0~255, defaulted at 0

<*cost* > is the cost of OSPF protocol ranging between 1~65535

Default: Default OSPF cost on the interface is 10

Command Mode: Interface Mode

Usage Guide: The command can configure on IPv6 tunnel interface, but it is successful configuration to only configure tunnel carefully.

Example:

Switch#config terminal
Switch(config)#interface vlan 1
Switch(Config-if-Vlan1)#ipv6 ospf cost 3

17.7.3.8 ipv6 ospf dead-interval

Command: ipv6 ospf dead-interval <*time* > [instance-id <*id*>]
no ipv6 ospf dead-interval [instance-id <*id*>]
Function: Specify the dead interval for neighboring layer 3 switch; the "**no ipv6 ospf dead-interval [instance-id <*id*>]**" command restores the default value.
Parameter: <*id*> is the interface instance ID, ranging between 0~255, defaulted at 0
<*time* > is the length of the adjacent layer 3 switch, in seconds, ranging between 1～65535
Default: The default dead interval is 40 seconds (normally 4 times of the hello-interval).
Command Mode: Interface Mode
Usage Guide: If no HELLO data packet received after the **dead-interval** period then this layer 3 switch is considered inaccessible and invalid. This command modifies the dead interval value of neighboring layer 3 switch according to the actual link state. The set **dead-interval** value is written into the Hello packet and transmitted. To ensure the normal operation of the OSPF protocol, the dead-interval between adjacent layer 3 switches should be in accordance or at least 4 times of the **hello-interval** value. The command can configure on IPv6 tunnel interface, but it is successful configuration to only configure tunnel carefully.
Example:
Switch#config terminal
Switch(config)#interface vlan 1
Switch(Config-if-Vlan1)#ipv6 ospf dead-interval 80

17.7.3.9 ipv6 ospf display route single-line

Command: [no] ipv6 ospf display route single-line
Function: show ipv6 ospf route change the display results of show ipv6 ospf route command. The "**[no] ipv6 ospf display route single-line**" restores to default display mode
Default: Not configured
Command Mode: Global Mode
Usage Guide: The show ipv6 ospf route command displays the same route in several lines. This command will strict that one route will be displayed in one line
Example:
Switch#config terminal

Switch(config)#ipv6 ospf display route single-line

17.7.3.10 ipv6 ospf hello-interval

Command: ipv6 ospf hello-interval <*time*> [instance-id <*id*>]

no ipv6 ospf hello-interval [instance-id <*id*>]

Function: Specify the hello-interval on the interface; the "**no ipv6 ospf hello-interval [instance-id <*id*>]**" restores the default value

Parameter: <*id*> is the interface instance ID, ranging between 0~255, defaulted at 0

<*time* > is the length of the adjacent layer 3 switch, in seconds, ranging between 1～65535

Default: Default HELLO packet sending interval is 10 seconds.

Command Mode: Interface Mode

Usage Guide: HELLO data packet is the most common packet which is periodically sent to adjacent layer 3 switch to discover and maintain adjacent relationship, elect DR and BDR. The user set **hello-interval** value will be written into the HELLO packet and transmitted. The less the **hello-interval** value is, the sooner the network topological structure is discovered as well larger the cost. The ensure the normal operation of OSPF protocol the **hello-interval** parameter between the layer 3 switches adjacent to the interface must be in accordance. The command can configure on IPv6 tunnel interface, but it is successful configuration to only configure tunnel carefully.

Example:

Switch#config terminal

Switch(config)#interface vlan 1

Switch(Config-if-Vlan1)#ipv6 ospf hello-interval 20

17.7.3.11 ipv6 ospf priority

Command: ipv6 ospf priority <*priority*> [instance-id <*id*>]

no ipv6 ospf priority[instance-id <*id*>]

Function: Configure the priority when electing "Defined layer 3 switch" at the interface. The "**no ipv6 ospf [<*ip-address*>] priority**" command restores the default value

Parameter: <id> is the interface instance ID, ranging between 0~255, and defaulted at 0**<*priority*>** is the priority of which the valid value ranges between 0～255.

Default: The default priority when electing DR is 1.

Command Mode: Interface Mode

Usage Guide: When two layer 3 switches connected to the same segments both want to be the "Defined layer 3 switch", the priority will decide which one should be chosen. Normally the one with higher priority will be elected, or the one with larger router-id number if the priorities are the same. A layer 3 switch with a priority equal to 0 will not be

elected as “Defined layer 3 switch” or “Backup Defined layer 3 switch”. The command can configure on IPv6 tunnel interface, but it is successful configuration to only configure tunnel carefully.

Example: Configure the priority of DR electing. Configure the interface vlan 1 to no election right, namely set the priority to 0.

Switch#config terminal

Switch(config)#interface vlan 1

Switch(Config-if-Vlan1)#ipv6 ospf priority 0

17.7.3.12 ipv6 ospf retransmit-interval

Command: ipv6 ospf retransmit-interval <*time*> [instance-id <*id*>]

no ipv6 ospf retransmit-interval [instance-id <*id*>]

Function: Specify the retransmit interval of link state announcements between the interface and adjacent layer 3 switches. The “**no ipv6 ospf retransmit-interval [instance-id <*id*>]**” command restores the default value

Parameter: <*id*> is the interface instance ID, ranging between 0~255, defaulted at 0

<*time*> is the retransmit interval of link state announcements between the interface and adjacent layer 3 switches, shown in seconds and raning between 1～65535

Default: Default retransmit interval is 5 seconds

Command Mode: Interface Mode

Usage Guide: When a layer 3 switch transmits LSA to its neighbor, it will maintain the link state announcements till confirm from the object side is received. If the confirm packet is not received within the interval, the LSA will be retransmitted. The retransmit interval must be larger than the time it takes to make a round between two layer 3 switches. The command can configure on IPv6 tunnel interface, but it is successful configuration to only configure tunnel carefully.

Example: Configure the LSA retransmit interval of interface vlan 1 to 10 seconds

Switch#config terminal

Switch(config)#interface vlan 1

Switch(Config-if-Vlan1)#ipv6 ospf retransmit-interval 10

17.7.3.13 ipv6 ospf transmit-delay

Command: ipv6 ospf transmit-delay <*time*> [instance-id <*id*>]

no ipv6 ospf transmit-delay [instance-id <*id*>]

Function: Configure the LSA sending delay time on the interface. The “**no ipv6 ospf transmit-delay [instance-id <*id*>]**” command restores to the default

Parameter: <*id*> is the instance ID ranging between 0~255 and defaulted at 0

<*time*> is the delay time of sending LSA on the interface, which is shown in seconds and

ranged between 1～65535.

Default: The default delay time of send LSA on the interface is 1 second by default.

Command Mode: Interface Mode

Usage Guide:

The LSA ages by time in the layer 3 switches but not in the transmission process. So by increasing the **transmit-delay** before sending LSA so that it will be sent out. The command can configure on IPv6 tunnel interface, but it is successful configuration to only configure tunnel carefully.

Example: Set the interface vlan 1 LSA sending delay to 3 seconds.

Switch#config terminal

Switch(config)#interface vlan 1

Switch(Config-if-Vlan1)#ipv6 ospf transmit-delay 3

17.7.3.14 ipv6 router ospf

Command: [no] ipv6 router ospf {area <*area-id*> [instance-id <*instance-id*>|tag <*tag*> [instance-id <*instance-id*>]]| tag <*tag*> area <*area-id*> [instance-id <*instance-id*>]}

Function: Enable ospf route on the interface; the "**[no] ipv6 router ospf {area <*area-id*> [instance-id <*instance-id*>|tag <*tag*> [instance-id <*instance-id*>]]| tag <*tag*> area <*area-id*> [instance-id <*instance-id*>]}**" command cancels this configuration

Parameter: <*area-id*> is an area ID which could be shown in digits ranging between 0～4294967295, or an IPv4 address

<*instance-id*> is the interface instance ID ranging between 0~255 and defaulted at 0.

<*tag*> ospfv3 process identifier

Default: Not configured

Command Mode: Interface Mode

Usage Guide: To enable this command on the interface, the area id must be configured. The instance ID and instance tag are optional. The ospfv3 process allows one routing instance for each instance ID. The route can be enabled on a interface with a instance ID. If the instance IDs are different, several OSPF process can be run on one interface. However different OSPF process should not use the same instance ID The command can configure on IPv6 tunnel interface, but it is successful configuration to only configure tunnel carefully.

Example:

Switch#config terminal

Switch(config)#interface vlan 1

Switch(Config-if-Vlan1)#ipv6 router ospf area 1 tag IPI instance-id 1

17.7.3.15 max-concurrent-dd

Command:max-concurrent-dd <*value*>

no max-concurrent-dd

Function: Configure with this command the current dd max concurrent number in the OSPF processing. The "**no max-concurrent-dd**" command restores the default

Parameter: <*value*> ranges between ***<1-65535>,*** the capacity of concurrent dd data packet processing.

Default: No default configuration. No dd concurrent limit

Command Mode: OSPFv3 protocol mode

Usage Guide: Specify the current dd max concurrent number in the OSPF processing

Example: Set the max concurrent dd to 20

Switch#config terminal

Switch(config)#router ipv6 ospf

Switch(config-router)#max-concurrent-dd 20

17.7.3.16 passive-interface

Command: [no] passive-interface<*ifname*>

Function: Configure that the hello group not sent on specific interfaces. The "[**no**] **passive-interface<*ifname*>**" command cancels this function

Parameter: <***ifname***> is the specific name of interface

Default: Not configured

Command Mode: OSPFv3 protocol mode

Example: Switch#config terminal

Switch(config)#router ipv6 ospf

Switch(config-router)#passive-interface vlan1

17.7.3.17 redistribute

Command: [no]redistribute {kernel |connected| static| rip| isis| bgp} [metric<*value*>] [metric-type {1|2}][route-map<*word*>]

Function: Introduce route learnt from other routing protocols into OSPF

Parameter: kernel Introduce from kernel route

connected Introduce from direct route

static Introduce from static route

rip Introduce from the RIP route

isis Introduce from ISIS route

bgp Introduce from BGP route

metric <*value*> is the introduced metric value, ranging between 0-16777214

metric-type {1|2} is the metric value type of the introduced external route, which can be 1 or 2, and it is 2 by default

route-map <*word*> targets to the probe of the route map for introducing route

Command Mode: OSPFv3 protocol mode

Usage Guide: Learn and introduce other routing protocol into OSPF area to generate AS-external_LSAs

Example: Switch#config terminal

Switch(config)#router ipv6 ospf

Switch(config-router)#redistribute bgp metric 12 metric-type 1

17.7.3.18 router-id

Command:router-id<*router-id*>

no router-id

Function: Configure router ID for ospfv3 process. The "**no router-id**" restores ID to 0.0.0.0

Parameter: <*router-id*>> is the router ID shown in IPv4 format

Default: 0.0.0.0 by default

Usage Guide: If the router-id is 0.0.0.0, the ospfv3 process can not be normally enabled. It is required to configure a router-id for ospfv3

Command Mode: OSPFv3 protocol mode

Example: Switch#config terminal

Switch(config)#router ipv6 ospf

Switch(config-router)#router-id 192.168.2.1

17.7.3.19 router ipv6 ospf

Command: [no] router ipv6 ospf [<*tag*>]

Function: This command initializes the ospfv3 routing process and enters ospfv3 mode for configuring the ospfv3 routing process. The "**[no] router ipv6 ospf [<*tag*>]**" command stops relevant process

Parameter: <*tag*> ospfv3 is the process mark which could be random strings made up of characters and digits

Command Mode: **Global mode**

Usage Guide: To let he ospfv3 routing process work properly, this command must be configured and ospfv3 must at least be enabled on one interface. When the tag configured by the ipv6 router ospf area command under interface mode matches with the tag of ospf process, the ospfv3 process is enabled on this interface.

Example: Switch#config terminal

Switch(config)#router ipv6 ospf IPI

17.7.3.20 timers spf

Command: timers spf *<spf-delay>* *<spf-holdtime>*

no timers spf

Function: Adjust route calculation timer value.The "**no timers spf**" restores the relevant value to default

Parameter: *<spf-delay>* 5 seconds by default

<spf-holdtime> 10 seconds by default

Command Mode: OSPFv3 protocol mode

Usage Guide: In this command the delay time between receiving topology change and SPF calculation, and further configured the hold time between two discontinuous SPF calculations.

Example: Switch#config terminal

Switch(config)#router ipv6 ospf

Switch(config-router)#timers spf 5 10

17.7.4 OSPFv3 Examples

Examples 1:OSPF autonomous system.

This scenario takes an OSPF autonomous system consists of five ES4626/ES4650 switch for example, where layer3 SwitchA and SwitchE make up OSPF area 0, layer3 SwitchB and SwitchC form OSPF area 1 (assume vlan1 interface of layer3 SwitchA belongs to area 0), layer3 SwitchD forms OSPF area2 (assume vlan2 interface of layer3 SwitchE belongs to area 0). SwitchA and SwitchE are backbone layer3 switches, SwitchB and SwitchD are area edge layer3 switches, and SwitchC is the in-area layer3 switch.

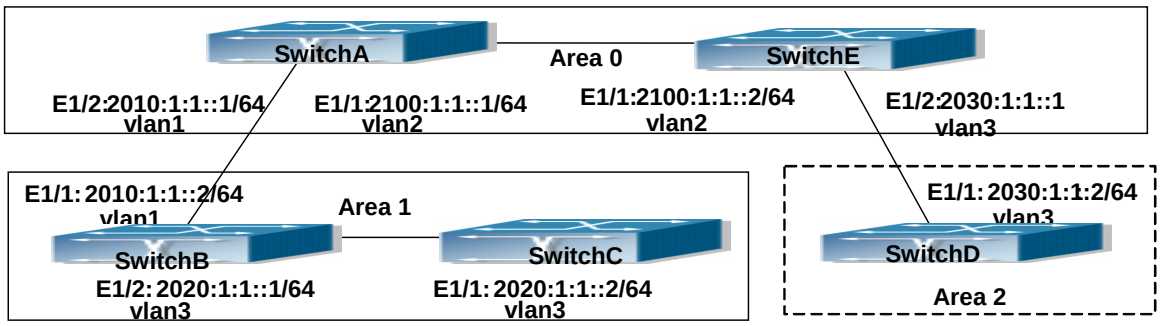


Fig 17-9 Network topology of OSPF autonomous system.

The configuration for layer3 SwitchA and SwitchE is shown below:

Layer3 SwitchA:

! Enable OSPFv3 protocol, configure router ID

SwitchA(config)#router IPv6 ospf

SwitchA (config-router)#router-id 192.168.2.1

Configure interface vlan1 IPv6 address and affiliated OSPFv3 area

SwitchA #config

SwitchA (config)# interface vlan 1

SwitchA (config-if-vlan1)# IPv6 address 2010:1:1::1/64

SwitchA (config-if-vlan1)# IPv6 router ospf area 0

SwitchA (config-if-vlan1)#exit

Configure interface vlan2 IP address and affiliated OSPFv3 area

SwitchA (config)# interface vlan 2

SwitchA (config-if-vlan2)# IPv6 address 2100:1:1::1/64

SwitchA (config-if-vlan2)# IPv6 router ospf area 0

SwitchA (config-if-vlan2)#exit

SwitchA (config)#exit

Layer 3 SwitchB :

Enable OSPFv3 protocol, configure router ID

SwitchB (config)#router IPv6 ospf

SwitchB (config-router)#router-id 192.168.2.2

Configure interface vlan1 address, vlan2 IPv6 address and affiliated OSPFv3 area

SwitchB #config

SwitchB (config)# interface vlan 1

SwitchB (config-if-vlan1)# IPv6 address 2010:1:1::2/64

SwitchB (config-if-vlan1)# IPv6 router ospf area 0

SwitchB (config-if-vlan1)#exit

SwitchB (config)# interface vlan 3

SwitchB (config-if-vlan3)# IPv6 address 2020:1:1::1/64

SwitchB (config-if-vlan3)# IPv6 router ospf area 1

SwitchB (config-if-vlan3)#exit

SwitchB (config)#exit

Layer 3 SwitchC :

! Enable OSPFv3 protocol, configure router ID

SwitchC (config)#router IPv6 ospf

SwitchC (config-router)#router-id 192.168.2.3

Configure interface vlan3 IPv6 address and affiliated OSPFv3 area

SwitchC #config

SwitchC (config)# interface vlan 3

SwitchC (config-if-vlan3)# IPv6 address 2020:1:1::2/64

SwitchC (config-if-vlan3)# IPv6 router ospf area 1

SwitchC (config-if-vlan3)#exit

SwitchC (config)#exit

Layer 3 SwitchD:

! Enable OSPFv3 protocol, configure router ID

SwitchD(config)#router IPv6 ospf

SwitchD(config-router)#router-id 192.168.2.4

Configure interface vlan3 IPv6 address and affiliated OSPFv3 area

SwitchD#config

SwitchD(config)# interface vlan 3

SwitchD(config-if-vlan3)# IPv6 address 2030:1:1::2/64

SwitchD(config-if-vlan3)# IPv6 router ospf area 0

SwitchD(config-if-vlan3)#exit

SwitchD(config)#exit

Layer 3 SwitchE:

Startup OSPFv3 protocol, configure router ID

SwitchE(config)#router IPv6 ospf

SwitchE(config-router)#router-id 192.168.2.5

Configure interface IPv6 address and affiliated OSPFv3 area

SwitchE#config

SwitchE(config)# interface vlan 2

SwitchE(config-if-vlan2)# IPv6 address 2100:1:1::2/64

SwitchE(config-if-vlan2)# IPv6 router ospf area 0

SwitchE(config-if-vlan2)#exit

Configure interface vlan3 IPv6 address and affiliated area

SwitchE(config)# interface vlan 3

SwitchE(config-if-vlan3)# IPv6 address 2030:1:1::1/64

SwitchE(config-if-vlan3)# IPv6 router ospf area 0

SwitchE(config-if-vlan3)#exit

SwitchE(config)#exit

17.7.5 OSPFv3 Troubleshooting

In the process of configuring and implementing OSPFv3, physical connection, configuration false probably leads to OSPFv3 protocol doesn't work. Therefore, the customers should give their attention to it.

First of all, to ensure correct physical connection, firstly;

Secondly, to ensure interface and link protocol are UP (execute show interface instruction);

And configure IPv6 address of the different net segment on every interface.

To startup OSPFv3 protocol (execute router IPv6 OSPF instruction), and configure affiliated OSPFv3 area on relative interface.

And then, consider OSPFv3 protocol characteristic —— OSPFv3 backbone area (area 0) must be continuous. If it doesn't ensure that virtual link is implemented continuously, all of not area 0 only can be connected by area 0 and other not area 0, not directly connected by not area 0; The border Layer 3 switch is a part of this Layer 3 switch interface belongs to area 0, and another part of interface belongs to not area 0; for multi-access net etc like broadcast, Layer 3 switch DR needs vote and appoint; for each OSPFv3 process must not configure router ID of 0.0.0.0 address.

If OSPFv3 routing problem still can't be solved by debugging, please use debug instructions like debug IPv6 OSPF packet/events etc, and copy DEBUG information in 3 minutes, then send them to our technical service center.

17.7.5.1 Monitor And Debug Command

17.7.5.1.1 debug ipv6 ospf ifsm

Command: [no]debug ipv6 ospf ifsm [status|events|timers]

Function: Open debugging switches showing the OSPF interface states; the "**[no]debug ospf ifsm [status|events|timers]**" command closes this debugging switches.

Default: Closed

Command Mode: Admin mode and global mode

Example:

Switch#debug ipv6 ospf ifsm

1970/01/01 01:11:44 IMI: IFSM[Vlan1]: Hello timer expire

1970/01/01 01:11:44 IMI: IFSM[Vlan2]: Hello timer expire

17.7.5.1.2 debug ipv6 ospf lsa

Command: [no]debug ipv6 ospf lsa [generate|flooding|install|maxage|refresh]

Function: Open debugging switches showing showing link state announcements; the "**[no]debug ospf lsa [generate|flooding|install|maxage|refresh]**" closes the debugging switches

Default: Closed

Command Mode: Admin mode and global mode

17.7.5.1.3 debug ipv6 ospf nfsm

Command: [no]debug ipv6 ospf nfsm [status|events|timers]

Function: Open debugging switches showing showing OSPF neighbor state machine; the "**[no]debug ipv6 ospf nfsm [status|events|timers]**"command closes this debugging switch

Default: Closed

Command Mode: Admin mode and global mod

Switch#debug ipv6 ospf nfsm

1970/01/01 01:14:07 IMI: NFSM[192.168.2.3-000007d4]: LS update timer expire

1970/01/01 01:14:07 IMI: NFSM[192.168.2.1-000007d3]: LS update timer expire

1970/01/01 01:14:08 IMI: NFSM[192.168.2.1-000007d3]: Full (HelloReceived)

1970/01/01 01:14:08 IMI: NFSM[192.168.2.1-000007d3]: nfsm_ignore called

1970/01/01 01:14:08 IMI: NFSM[192.168.2.1-000007d3]: Full (2-WayReceived)

17.7.5.1.4 debug ipv6 ospf nsm

Command: [no]debug ipv6 ospf nsm [interface|redistribute]

Function: Open debugging switches showing showing OSPF NSM, the "**[no]debug ipv6 ospf nsm [interface|redistribute]**" command closes this debugging switch

Default: Closed

Command Mode: Admin mode and global mode

17.7.5.1.5 debug ipv6 ospf packet

Command: [no]debug ipv6 ospf packet [dd|detail|hello|ls-ack|ls-request|ls-update|recv|detail]

Function: Open debugging switches showing OSPF packet messages; the "**[no]debug ipv6 ospf packet [dd|detail|hello|ls-ack|ls-request|ls-update|recv|detail]**" command closes this debugging switch

Default: Closed

Command Mode: Admin mode and global mode

17.7.5.1.6 debug ipv6 ospf route

Command: [no]debug ipv6 ospf route [ase|ia|install|spf]

Function: Open debugging switches showing OSPF related routes; the "**[no]debug ipv6 ospf route [ase|ia|install|spf]**" command closes this debugging switch

Default: Closed

Command Mode: Admin mode and global mode

17.7.5.1.7 show ipv6 ospf

Command: show ipv6 ospf [<*tag*>]

Function: Display OSPF global and area messages

Parameter: <*tag*> is the process tag which is a character string

Default: Not displayed

Command Mode: All modes

Example:

Routing Process "OSPFv3 (*null*)" with ID 192.168.2.2

SPF schedule delay 5 secs, Hold time between SPFs 10 secs

Minimum LSA interval 5 secs, Minimum LSA arrival 1 secs

Number of external LSA 0. Checksum Sum 0x0000

Number of AS-Scoped Unknown LSA 0

Number of LSA originated 6

Number of LSA received 14

Number of areas in this router is 1

Area BACKBONE(0)

Number of interfaces in this area is 2

SPF algorithm executed 6 times

Number of LSA 8. Checksum Sum 0x43D52

Number of Unknown LSA 0

17.7.5.1.8 show ipv6 ospf database

Command: show ipv6 ospf [<*tag*>] database

[router [adv-router <*advertiser_router*>]

|network [adv-router <*advertiser_router*>]

| intra-prefix [adv-router <*advertiser_router*>]

| link [adv-router <*advertiser_router*>]

| external [adv-router <*advertiser_router*>]

| inter-prefix [adv-router <*advertiser_router*>]

| inter-router [adv-router <*advertiser_router*>]]

Function: Display the OSPF link state data base message

Parameter: <*tag*> is the process tag which is a character string

<*advertiser_router*> is the ID of Advertising router, shown in IPv4 address format

Default: Not displayed

Command Mode: All modes

Example: According to the output messages of this command, we can view the OSPF link state database messages

Use show ipv6 ospf database command will be able to show LSA messages of the OSPF routing protocol

For Example, the displayed messages are:

OSPFv3 Router with ID (192.168.2.2) (Process *null*)

Link-LSA (Interface Vlan1)

Link State ID	ADV Router	Age	Seq#	CkSum	Prefix
0.0.7.211	192.168.2.2	1409	0x80000001	0x6dda	1
0.0.7.212	192.168.2.3	1357	0x80000001	0x248e	1

Link-LSA (Interface Vlan2)

Link State ID	ADV Router	Age	Seq#	CkSum	Prefix
0.0.7.211	192.168.2.1	1450	0x80000001	0xa565	1
0.0.7.212	192.168.2.2	1399	0x80000001	0x4305	1

Router-LSA (Area 0.0.0.0)

Link State ID	ADV Router	Age	Seq#	CkSum	Link
0.0.0.0	192.168.2.1	1390	0x80000006	0x9fe2	1
0.0.0.0	192.168.2.2	1354	0x80000007	0x4af5	2
0.0.0.0	192.168.2.3	1308	0x80000004	0xbbc4	1

Network-LSA (Area 0.0.0.0)

Link State ID	ADV Router	Age	Seq#	CkSum
0.0.7.211	192.168.2.1	1390	0x80000001	0x897e
0.0.7.211	192.168.2.2	1354	0x80000001	0x9b69

Intra-Area-Prefix-LSA (Area 0.0.0.0)

Link State ID	ADV Router	Age	Seq#	CkSum	Prefix	Reference
0.0.0.1	192.168.2.1	1389	0x80000005	0x7e2e	1	Router-LSA
0.0.0.2	192.168.2.1	1389	0x80000001	0x22cb	1	Network-LSA
0.0.0.1	192.168.2.3	1306	0x80000002	0xd0d7	1	Router-LSA

Displayed information's	Explanations
Link-LSA (Interface Vlan1)	Link LSA messages of interface Vlan1
Router-LSA (Area 0.0.0.0)	Router LSA messages in Area 0
Network-LSA (Area 0.0.0.0)	Network LSA in Area 0
Intra-Area-Prefix-LSA (Area 0.0.0.0)	Intra-domain Prefix LSA in Area 0

17.7.5.1.9 show ipv6 ospf interface

Command: show ipv6 ospf interface [*interface*]

Function: Display the OSPF interface messages

Parameter: ***<interface> is the*** name of the interface

Default: Not displayed

Command Mode: All modes

Example:

```
Loopback is up, line protocol is up
  OSPFv3 not enabled on this interface
Vlan1 is up, line protocol is up
  Interface ID 2003
  IPv6 Prefixes
    fe80::203:fff:fe01:257c/64 (Link-Local Address)
    2001:1:1::1/64
  OSPFv3 Process (*null*), Area 0.0.0.0, Instance ID 0
    Router ID 192.168.2.2, Network Type BROADCAST, Cost: 10
    Transmit Delay is 1 sec, State DR, Priority 1
    Designated Router (ID) 192.168.2.2
      Interface Address fe80::203:fff:fe01:257c
```

Backup Designated Router (ID) 192.168.2.3
Interface Address fe80::203:fff:fe01:d28
Timer interval configured, Hello 10, Dead 40, Wait 40, Retransmit 5
Hello due in 00:00:10
Neighbor Count is 1, Adjacent neighbor count is 1
Vlan2 is up, line protocol is up
Interface ID 2004
IPv6 Prefixes
fe80::203:fff:fe01:257c/64 (Link-Local Address)
2000:1:1::1/64
OSPFv3 Process (*null*), Area 0.0.0.0, Instance ID 0
Router ID 192.168.2.2, Network Type BROADCAST, Cost: 10
Transmit Delay is 1 sec, State Backup, Priority 1
Designated Router (ID) 192.168.2.1
Interface Address fe80::203:fff:fe01:429e
Backup Designated Router (ID) 192.168.2.2
Interface Address fe80::203:fff:fe01:257c
Timer interval configured, Hello 10, Dead 40, Wait 40, Retransmit 5
Hello due in 00:00:10
Neighbor Count is 1, Adjacent neighbor count is 1

Displayed information	Explanations
Vlan1 is up, line protocol is up	Let the interface up both logically and physically
IPv6 Prefixes fe80::203:fff:fe01:257c/64 (Link-Local Address) 2001:1:1::1/64	IPv6 address of the interface and the length of the prefix
OSPFv3 Process (*null*)	Ospfv3 process the interface belongs
Area 0.0.0.1	Area the interface belongs
Instance ID 0	Instance ID is 0
Router ID 192.168.2.2, Network Type BROADCAST, Cost: 10	Process ID; Router ID; Network Type; Cost
Transmit Delay is 1 sec, State DR, Priority 1	LAS transmission delay on the interface; state; electing the priority of the layer 3 switch.
Designated Router (ID) 192.168.2.2 Interface Address fe80::203:fff:fe01:257c	Specifying layer 3 switch
Backup Designated Router (ID)	Back up designated layer 3 switch

192.168.2.3 Interface Address fe80::203:fff:fe01:d28	
Timer interval configured, Hello 10, Dead 40, Wait 40, Retransmit 5 Hello due in 00:00:10	OSPF protocol timer; including hello packet, poll interval packets, router dead, router retransmission.
Neighbor Count is 1, Adjacent neighbor count is 1	Numbers of the adjacent layer 3 switch; number of the layer 3 switches established with neighbor relation

17.7.5.1.10 show ipv6 ospf neighbor

Command: show ipv6 ospf [<*tag*>] neighbor [<*neighbor_id*> | <ifname> detail | detail]

Function: Show OSPF adjacent point messages

Parameter: <*tag*> is process tag, which is a character string

<*neighbor_id*> is the neighbor ID shown in IPv4 address format

detail: Show neighbor details

<*ifname*> name of the interface

Default: Not displayed

Command Mode: All modes

Usage Guide: OSPF neighbor state can be checked by viewing the output of this command

Example:

OSPFv3 Process (*null*)

Neighbor ID	Pri	State	Dead Time	Interface	Instance ID	
192.168.2.3	1	Full/Backup	00:00:29	Vlan1	0	
192.168.2.1	1	Full/DR	00:00:38	Vlan2	0	Vlan1

Displayed information	Explanation
Neighbor ID	Neighbor ID
Instance ID	Instance ID
Address	IP address of neighboring layer 3 switch
Interface	Interface the neighbor belongs
State	Neighbor relationship state
Pri	Priority

17.7.5.1.11 show ipv6 ospf route

Command: show ipv6 ospf [<*tag*>] route

Function: Show the OSPF route table messages

Parameter: <*tag*> is the processes tag, which is a character string

Default: Not displayed

Command Mode: All modes

Example:

```
Switch#show ipv6 ospf route
Codes: C - connected, D - Discard, O - OSPF, IA - OSPF inter area
       E1 - OSPF external type 1, E2 - OSPF external type 2
   Destination                                    Metric
     Next-hop
O  2000:1:1::/64                                  10
     directly connected, Vlan2
O  2001:1:1::/64                                  10
     directly connected, Vlan1
O  3000:1:1::/64                                  20
     via fe80::203:fff:fe01:429e, Vlan2
O  3003:1:1::/64                                  20
     via fe80::203:fff:fe01:d28, Vlan1
```

17.7.5.1.12 show ipv6 ospf topology

Command: show ipv6 ospf [<*tag*>] topology [area <*area-id*>]

Function: Show messages of OSPF topology

Parameter: <*tag*> is the processes tag, which is a character string

<*area-id*> is an area ID which could be shown in digits ranging between 0～4294967295, or an IPv4 address

Default: Not displayed

Command Mode: All modes

Example:

```
Switch#show ipv6 ospf topology
OSPFv3 Process (*null*)
OSPFv3 paths to Area (0.0.0.0) routers
Router ID          Bits  Metric     Next-Hop          Interface
192.168.2.1              10         192.168.2.1       Vlan2
192.168.2.2              --
192.168.2.3              10         192.168.2.3       Vlan1
```

17.7.5.1.13 show ipv6 ospf virtual-links

Command: show ipv6 ospf [<*tag*>] virtual-links

Function: Show OSPF virtual link messages

Parameter: <*tag*> is the processes tag, which is a character string

Default: Not displayed

Command Mode: All modes

Example:

Switch#show ipv6 ospf virtual-links

Virtual Link VLINK1 to router 5.6.7.8 is up

Transit area 0.0.0.1 via interface Vlan1, instance ID 0

Local address 3ffe:1234:1::1/128

Remote address 3ffe:5678:3::1/128

Transmit Delay is 1 sec, State Point-To-Point,

Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5

Hello due in 00:00:01

Adjacency state Up

17.8 BGP

17.8.1 BGP Introduction

BGP stands for a Border Gateway Protocol.It's a dynamic routing protocol inter-autonomous system. Its basic function is automatically exchanging routing information without loops. By exchanging routing reachable information with autonomous number of AS sequence attributes, BGP could create autonomous topological map to eliminate routing loop and implement policies configured by users. Generally, the switches in an AS may use several IGPs (Interior Gateway Protocol) in order to exchange routing information in the AS, such as RIP and OSPF which are IGPs; and exchange information among ASes with EGP (Exterior Gateway Protocol). For example, BGP is one kind of EGP. The AS is usually established on a single administrative department. BGP is often used on the switches among ISPs or the departments of Multi-national Corporation.

BGP has been used since1989, its earliest three versions are RFC1105（BGP-1）、RFC1163（BGP-2）and RFC1267（BGP-3）.Currently, the most popular one is RFC1771（BGP-4）. The ES4626/ES4650 switch supports BGP-4.

1. Characteristics of BGP-4

BGP-4 is suitable for the distributed structure and supports Classless InterDomain Routing (CIDR). BGP-4 is becoming the virtual exterior routing protocol standard used for the global Internet. The features of BGP-4 are as follows.

BGP is an exterior routing protocol, unlike interior routing protocol, such as OSPF and RIP, BGP can't discovery and calculate routes, but it can control the transmission of routes and select the best route.

By carrying AS routing information in the updating route, the problem of Routing Loops can be resolved

BGP uses TCP on port 179 as its transport protocol, this could enhance the reliability of the protocol.

BGP-4 supports CIDR (Classless InterDomain Routing), which is an important improvement to BGP-3. CIDR has a brand new way to look on IP address; it doesn't distinguish class A , Class B and class C network. For instance, an illegal class C address 192.213.0.0 255.255.0.0 can be represented as 192.213.0.0/16 by CIDR which is a legal super network. /16 represents that the network number is formed by 16 bits from the beginning left of the address. The introduction of CIDR abbreviates the route aggregation. The route aggregation is the process of combining several different routes. So notifying several routes can be changed to notify only one route which decreases the route table.

When updating route, BGP send only incremental route. The bandwidth occupied by BGP transmission is reduced greatly and it is suitable for the mass routing information transmitted on the internet

For political and economical reasons, each AS expects to filter and control the route, BGP-4 provides abundant route policies which make BGP-4 more extendable to encourage the internet development.

2. The Overview of BGP-4 operation

Unlike RIP and OSPF protocols, BGP protocol is connection oriented. BGP switches must establish connection to exchange routing information. The operation of BGP protocol is driven by messages and the messages can be divided into four kinds:

Open message----It's the first message which is sent after a TCP connection is established. It is used to create BGP connecting relation among BGP peers. Some parameters in Open Message are used to negotiate if a connection could be established among BGP peers.

Keepalive Message ----- it's the message to check connection availability. It's usually sent periodically to keep BGP connection. If this message or Update message is not received within holdtime time, BGP connection is closed.

Update Message----- it's the most important message in the BGP system. It's used to exchange routing information among peers. The switches exchange not only updated routing information, but also unavailable or canceled routing information. It consists of three parts: unreachable route, NLRI(Network Layer Reach ability Information) and Path Attributes.

Notification Message------it's the mistake notification message. When a BGP speaker receives this message, it shutdowns the BGP connections with its neighbors

BGP-4 is connection oriented. BGP acts as higher protocol and runs on the

particular equipments. When detecting a neighbor, a TCP session is established and maintained. Then the exchanging and synchronization of the route table will be carried out. By sending the whole BGP route table the routing information is exchanged only when the system initiates. After that, the routing information is exchanged only when the updated routing information is available. Only incremental update message is exchanged. BGP-4 maintains links and sessions periodically through keep alive message. That is sending and receiving keep alive message periodically to check if the connections are normal.

The switches that participate the BGP session are called BGP speaker. It continuously receives or generates new routing information and advertises it to other BGP speakers. When a BGP speaker receives a new routing notification from other AS, if this route is better than the presently known route or there is no acceptable route, it sends this route to all the other BGP speakers of the AS. A BGP speaker calls other speakers that exchange route information with it as neighbors or peers. Several relevant neighbors can constitute a peer group. BGP operates on the switches in the following two manners:

- IBGP：Internal BGP
- EBGP：External BGP

When BGP runs in the same AS, it's called IBGP. When in the different AS, it's called EBGP. Generally, the outer neighbors are connected physically and the inner neighbors can be in any place of the AS. The difference is finally shown in the dealing manner of BGP to routing information. The equipments may check the AS numbers of the Open Message from neighbors to decide treating the neighbor switches as the exterior neighbor or as the interior neighbor.

IBGP are used in the AS. It sends message to all the BGP neighbors in the AS. IBGP exchanges AS routing information in a big organization. Attention, the switches in the AS needn't be connected physically. Only if the switches are in the same AS, they can be neighbors each other. Because BGP can't detect route, the route tables of other inner route protocols (such as static route, direct route, OSPF and RIP) need contain neighbor IP addresses and these routes are used to exchange information among BGPs. In order to avoid routing loops, when a BGP speaker receives a route notification from inner neighbor, it would not notify this route to other inner neighbors.

EBGP is used among the AS, and it transmits routing information to the BGP neighbors of outer ASes. EBGP need physical connection and share the same medium. Because EBGP need physical connection, the boundary equipments between two AS are usually running EBGP. When a BGP speaker receives routing information from outer neighbors, it notifies these routes to other inner neighbors.

3．Route attribute

BGP-4 can share and query inner IP route table through relevant mechanisms, but it has its own route table. In the BGP route table, each route has a network number, AS listing information (also called AS path) that it passed and some routing attributes (such as origin). The routing attribute that BGP-4 used is very complex, this attribute can be used as metrics to select path.

4. Route-selecting policy of BGP

When receiving BGP notification about a same route from several neighbors, selecting the best route need to be take into account after routing filtering. This process is called BGP route selecting process. BGP route selecting process will start only when the following conditions are fulfilled:

- The switch's route must be next hop reachable. That is in the route table there is the route that can reach the next hop.
- BGP must be synchronized with IGP (unless asynchronism is configured; only restricted to IBGP)

BGP route selecting process is based on the BGP attribute. When there are several routes that indicate the same destination, BGP need select the best route to the destination. The decision-making process is as the following:

1. Select the route with the most weight first;

2. If the weights are the same, select the route with the most local preference;

3. If the local preferences are the same, select the route generated by local switch.

4. If the local preferences are the same and there is no route generated by local switch, select the route with the shortest AS path;

5. If the AS paths are the same, select the route with the lowest "origin" type （IGP<EGP<INCOMPLETE）;

6. If the "origin" types are the same, select the route with the lowest MED attribute. Unless activating command "bgp always-compare-med", this comparison is only available among the routes from the same neighbor AS.

7. If the MED attributes are the same, EBGP is preferable to outer confederation and outer confederation is preferable to IBGP.

8. If it's still the same by now, BGP router ID（router ID）is used to break the balance. The best route is the one from the least router ID.

17.8.2 BGP Configuration Task List

The BGP configuration tasks include basic and advanced tasks. Basic BGP configuration tasks include the following:

1. Enable BGP Routing (required)
2. Configure BGP Neighbors (required)

3. Administrate the change of routing policy
4. Configure BGP Weights
5. Configure BGP Route Filtering policy basing on Neighbors
6. Configure Next-Hop of BGP
7. Configure Multi-Hop of EGBP
8. Configure BGP Session Identifier
9. Configure BGP Version

Advanced BGP configuration tasks include the following:

1. Use Route Maps to Modify Route
2. Configure Route Aggregation
3. Configure BGP Community Filtering
4. Configure BGP Confederation
5. Configure a Route Reflector
6. Configure Peer Groups
7. Configure Neighbors and Peer Groups' Parameters
8. Adjust BGP Timers
9. Adjust BGP Announcement Interval
10. Configure the default Local Priority
11. Allow to Transfer Default Route
12. Configure BGP's MED Value
13. Configure BGP Routing Redistribution
14. Configure BGP Route Dampening
15. Configure BGP capability Negotiation
16. Configure Routing Server
17. Configure Path-Selected Rule

Ⅰ. Basic BGP configuration tasks

1.Enable BGP Routing

Command	Explanation
Global mode	
router bgp *<as-id>* **no router bgp *<as-id>***	Enable BGP, the **"no router bgp *<as-id>"*** command disenable BGP process.
Router configuration mode	
network *<ip-address/M>* **no network *<ip-address/M>***	Set the network that BGP will announce, the **no network *<ip-address/M>*** command cancels the network that will be announced.

2. Configure BGP Neighbors

Command	Explanation
Router configuration mode	
neighbor {*<ip-address>*|*<TAG>*} remote-as *<as-id>* **no neighbor {*<ip-address>*|*<TAG>*} [remote-as *<as-id>*]**	Specify a BGP neighbor, the **no neighbor {*<ip-address>*|*<TAG>*} [remote-as *<as-id>*]** command deletes the neighbor.

3. Administrate the change of routing policy

（1）Configure hard reconfiguration.

Command	Explanation
Admin Mode	
clear ip bgp {<*>|*<as-id>*| external|peer-group *<NAME>*|*<ip-address>*}	Configure hard reconfiguration.

（2） Configure outbound soft reconfiguration.

Command	Explanation
Admin Mode	
clear ip bgp {<*>|*<as-id>*| external|peer-group <NAME>|*<ip-address>*} soft out	Configure outbound soft reconfiguration.

（3）Configure inbound soft reconfiguration.

Command	Explanation
Router configuration mode	
neighbor { *<ip-address>* | *<TAG>* } soft-reconfiguration inbound **no neighbor { *<ip-address>* | *<TAG>* } soft-reconfiguration inbound**	This command can store routing information from neighbors and peers; the **no neighbor { *<ip-address>* | *<TAG>* } soft-reconfiguration inbound** command cancels the storage of routing information.
Admin Mode	
Clear ip bgp {<*>|*<as-id>*| external|peer-group *<NAME>*|*<ip-address>*} soft in	Configure BGP inbound soft reconfiguration.

4. Configure BGP Weights

Command	Explanation

Router configuration mode	
neighbor { *<ip-address>* | *<TAG>* } weight *<weight>* **no neighbor { <ip-address> | <TAG> }**	Configure BGP neighbor weights; the **no neighbor { <ip-address> | <TAG> }** command recovers default weights.

5．Configure BGP Route Filtering policy based on neighbor

Command	Explanation
Router configuration mode	
neighbor {*<ip-address>*|*<TAG>*} distribute-list {*<1-199>*|*<1300-2699>*|*<WORD>*} {in|out} **no neighbor {*<ip-address>*|*<TAG>*} distribute-list {*<1-199>*|*<1300-2699>*|*<WORD>*} {in|out}**	Filter neighbor routing updating information. The **no neighbor {*<ip-address>*|*<TAG>*} distribute-list {*<1-199>*|*<1300-2699>*|*<WORD>*} {in|out}** command cancels routing filter.

6．Configure Next-Hop

1）Set Next-Hop as the switch's address

Command	Explanation
BGP configuration mode	
neighbor { *<ip-address>* | *<TAG>* } next-hop-self **no neighbor { *<ip-address>* | *<TAG>* } next-hop-self**	While sending route Next-Hop set Next-Hop as the switch's address; the **no neighbor { *<ip-address>* | *<TAG>* } next-hop-self** command cancels the setting.

2）Cancel default Next-Hop through route map

Command	Explanation
Route mapped configuration command	
set ip next-hop *<ip-address>* **no set ip next-hop**	Set the Next-Hop attribute of outbound route. The **no set ip next-hop** command cancels this setting.

7．Configure EGBP Multi-Hop

If the connections with outer neighbors are not direct, the following command can configure neighbor Multi-Hop.

Command	Explanation

BGP configuration mode	
neighbor {<*ip-address*>|<*TAG*>} ebgp-multihop [<*1-255*>] **no neighbor {<*ip-address*>|<*TAG*>} ebgp-multihop [<*1-255*>]**	Configure the allowance of EBGP connection with other networks that are not connected directly; the **no neighbor {<*ip-address*>|<*TAG*>} ebgp-multihop [<*1-255*>]** command cancels the setting.

8. Configure BGP session identifier

Command	Explanation
BGP configuration mode	
bgp router-id <*ip-address*> **no bgp router-id**	Configure the router-id value; the **no bgp router-id** command recovers the default value.

9. Configure the BGP Version

Command	Explanation
BGP configuration mode	
neighbor {<*ip-address*> | <*TAG*>} version <value> **no neighbor {<*ip-address*> | <*TAG*>} version**	Set the version used by BGP neighbors; the **no neighbor {<*ip-address*> | <*TAG*>} version** command recovers default setting. Presently only supporting version 4th .

Ⅱ. Advanced BGP configuration tasks

1. Use Route Maps to Modify Route

Command	Explanation
BGP configuration mode	
neighbor { <*ip-address*> | <*TAG*> } route-map <*map-name* > {in | out} **no neighbor { <*ip-address*> | <*TAG*> } route-map <*map-name* > {in | out}**	Apply a route map to incoming or outgoing routes; the **no neighbor { <*ip-address*> | <*TAG*> } route-map <*map-name* > {in | out}** command cancels the settings of routing maps.

2. Configure Route Aggregation

Command	Explanation

BGP configuration mode	
aggregate-address *<ip-address/M>* [summary-only] [as-set] **no aggregate-address *<ip-address/M>* [summary-only] [as-set]**	Create an aggregate entry in the BGP routing table; the **no aggregate-address *<ip-address/M>* [summary-only] [as-set]** command cancels the aggregate entry.

3. Configure BGP Community Filtering

Command	Explanation
BGP configuration mode	
neighbor {*<ip-address>* | *<TAG>*} send-community **no neighbor {*<ip-address>* | *<TAG>*} send-community**	Allow the routing updates with community attributes sending to BGP neighbors; the **no neighbor {*<ip-address>* | *<TAG>*} send-community** command enables the route without community attributes.

4. Configure BGP Confederation

Command	Explanation
BGP configuration mode	
bgp confederation identifier *<as-id>* **no bgp confederation identifier *<as-id>***	Configure a BGP AS confederation identifier; the **no bgp confederation identifier *<as-id>*** command deletes the BGP AS confederation identifier
bgp confederation peers *<as-id>* [*<as-id>..*] **no bgp confederation peers *<as-id>* [*<as-id>..*]**	Configure the AS affiliated to the AS confederation; the **no bgp confederation peers *<as-id>* [*<as-id>..*]**command deletes the AS from the AS confederation.

5. Configure a Route Reflector

（1） The following commands can be used to configure route reflector and its clients.

Command	Explanation
BGP configuration mode	

neighbor <*ip-address*> route-reflector-client **no neighbor <*ip-address*> route-reflector-client**	Configure the current switch as route reflector and specify a client. the **no neighbor <*ip-address*> route-reflector-client** commands format deletes a client.

（2） If there are more than one route reflectors in the cluster, the following commands can configure cluster-id

Command	Explanation
BGP configuration mode	
bgp cluster-id <*cluster-id*> **no bgp cluster-id**	Configure cluster id; format “no” of the **no bgp cluster-id** command cancels the cluster id configuration.

（3） If the route reflector from clients to clients is needed, the following commands can be used.

Command	Explanation
BGP configuration mode	
bgp client-to-client reflection no bgp client-to-client reflection	Configure the allowance of the route reflector from clients to clients; the no bgp client-to-client reflection commands forbids this allowance.

6．Configure Peer Groups

（1） Create peer groups

Command	Explanation
BGP configuration mode	
neighbor <*TAG*> peer-group **no neighbor <*TAG*> peer-group**	Create peer groups; the **no neighbor <*TAG*> peer-group** command deletes peer groups.

（2） Add neighbors to peers groups

Command	Explanation
BGP configuration mode	

neighbor <*ip-address*> peer-group <*TAG*> **no neighbor <*ip-address*> peer-group <*TAG*>**	Make a neighbor a member of the peer group. the **no neighbor <*ip-address*> peer-group <*TAG*>** command cancels the specified member.

7. Configure neighbors and peer Groups' parameters

Command	Explanation
BGP configuration mode	
neighbor {<*ip-address*> | <*TAG*>} remote-as <*as-id*> **no neighbor {<*ip-address*> | <*TAG*>} remote-as <*as-id*>**	Specify a BGP neighbor; format "no" of the **no neighbor {<*ip-address*> | <*TAG*>} remote-as <*as-id*>** command deletes the neighbor.
neighbor { <*ip-address*> | <*TAG*> } description <*.LINE*> **no neighbor { <*ip-address*> | <*TAG*> } description**	Associate a description with a neighbor; the **no neighbor { <*ip-address*> | <*TAG*> } description** command deletes this description.
neighbor { <*ip-address*> | <*TAG*> } default-originate [route-map <*NAME*>] **no neighbor { <*ip-address*> | <*TAG*> } default-originate [route-map <*NAME*>]**	Permit to send the default route 0.0.0.0; the **no neighbor { <*ip-address*> | <*TAG*> } default-originate [route-map <*NAME*>]** command cancels sending default route.
neighbor { <*ip-address*> | <*TAG*> } send-community **no neighbor { <*ip-address*> | <*TAG*> } send-community**	Configure the community attributes sent to the neighbor .
neighbor { <*ip-address*> | <*TAG*> } timers <*keep alive*> <*holdtime*> **no neighbor { <*ip-address*> | <*TAG*> } timers**	Configure a particular neighbor's keep-alive and hold-time timer; the **no neighbor { <*ip-address*> | <*TAG*> } timers** command recovers the default value.
neighbor {<*ip-address*> | <*TAG*>} advertisement-interval <*seconds*> **no neighbor {<*ip-address*> | <*TAG*>} advertisement-interval**	Configure the min interval of sending BGP routing information; the **no neighbor {<*ip-address*> | <*TAG*>} advertisement-interval** command recovers the default value.

neighbor {*<ip-address>* | *<TAG>*} ebgp-multihop [*<1-255>*] **no neighbor {*<ip-address>* | *<TAG>*} ebgp-multihop**	Configure the allowance of EBGP connections with networks connected indirectly; the **no neighbor {*<ip-address>* | *<TAG>*} ebgp-multihop** command cancels this setting.
neighbor { *<ip-address>* | *<TAG>* } weight <weight> **no neighbor { *<ip-address>* | *<TAG>* } weight**	Configure BGP neighbor weights; the **no neighbor { *<ip-address>* | *<TAG>* } weight** command recovers the default weights.
neighbor { *<ip-address>* | *<TAG>* } distribute-list { *<access-list-number>* | *<name>* } { in | out } **no neighbor { *<ip-address>* | *<TAG>* } distribute-list { *<access-list-number>* | *<name>* } { *in* | *out* }**	Filter neighbor route update; format "no" of the **no neighbor { *<ip-address>* | *<TAG>* } distribute-list { *<access-list-number>* | *<name>* } { *in* | *out* }** command cancels route filtering.
neighbor { *<ip-address>* | *<TAG>* } route-reflector-client **no neighbor { *<ip-address>* | *<TAG>* } route-reflector-client**	Configure the current switch as route reflector and specify a client; the **no neighbor { *<ip-address>* | *<TAG>* } route-reflector-client** command deletes a client.
neighbor { *<ip-address>* | *<TAG>* } next-hop-self **no neighbor { *<ip-address>* | *<TAG>* } next-hop-self**	When sending route, configure Next-Hop as its address; the **no neighbor { *<ip-address>* | *<TAG>* } next-hop-self** command cancels the setting.
neighbor { *<ip-address>* | *<TAG>* } version *<value>* **no neighbor { *<ip-address>* | *<TAG>* } version**	Specify the BGP version communicating with BGP neighbors; the **no neighbor { *<ip-address>* | *<TAG>* } version** command recovers default setting.
neighbor { *<ip-address>* | *<TAG>* } route-map *<map-name>* {in | out} **no neighbor { *<ip-address>* | *<TAG>* } route-map *<map-name>* {in | out}**	Apply a route map to incoming or outgoing routes; the **no neighbor { *<ip-address>* | *<TAG>* } route-map *<map-name>* {in | out}** command cancels the setting of route reflector.

neighbor { *<ip-address>* | *<TAG>* } soft-reconfiguration inbound **no neighbor { *<ip-address>* | *<TAG>* } soft-reconfiguration inbound**	Store the route information from neighbor or peers; the **no neighbor { *<ip-address>* | *<TAG>* } soft-reconfiguration inbound** command cancels the storage.
neighbor { *<ip-address>* | *<TAG>* } shutdown **no neighbor { *<ip-address>* | *<TAG>* } shutdown**	Shutdown BGP neighbor or peers; the **no neighbor { *<ip-address>* | *<TAG>* } shutdown** command activates the closed BGP neighbor or peers.

8．Adjust BGP Timers

（1） Configure the BGP timer of all the neighbors

Command	Explanation
BGP configuration mode	
timers bgp *<keep alive>* *<holdtime>* **no timers bgp**	Configure the BGP timers of all the neighbors; the no timers bgp command recovers the default value.

（2） Configure the timer value of a particular neighbor

Command	Explanation
BGP configuration mode	
neighbor { *<ip-address>* | *<TAG>* } timers *<keep alive>* *<holdtime>* **no neighbor { *<ip-address>* | *<TAG>* } timers**	Configure the keep alive and holdtime timer of a particular neighbor; the **no neighbor { *<ip-address>* | *<TAG>* } timers** command recovers the default value.

9．Adjust BGP announcement Interval

Command	Explanation
BGP configuration mode	
neighbor {*<ip-address>* | *<TAG>*} advertisement-interval <seconds> **no neighbor {*<ip-address>* | *<TAG>*} advertisement-interval**	Configure the minimum interval among BGP routes update information; the **no neighbor {*<ip-address>* | *<TAG>*} advertisement-interval** command recovers the default setting.

10. Configure the Local Preference Value

Command	Explanation
BGP configuration mode	
bgp default local-preference <*value*> **no bgp default local-preference**	Change default local preference; the **no bgp default local-preference** command recovers the default value.

11. Enable sending default route

Command	Explanation
BGP configuration mode	
neighbor { <*ip-address*> | <*TAG*> } default-originate **no neighbor { <*ip-address*> | <*TAG*> } default-originate**	Permit sending default route 0.0.0.0; the **no neighbor { <*ip-address*> | <*TAG*> } default-originate** command cancels sending default route.

12. Configure BGP's MED Value

（1） Configure MED value

Command	Explanation
Route map configuration command	
set metric <*metric-value*> **no set metric**	Configure metric value; the **no set metric** command recovers the default value.

（2） Apply route selection based on MED according to the path from different AS

Command	Explanation
BGP configuration mode	
bgp always-compare-med **no bgp always-compare-med**	Permit the MED comparison from different AS; the **no bgp always-compare-med** commands forbids the comparison.

13. Configure BGP routing redistribution

Command	Explanation
BGP configuration mode	

redistribute { connected | static | rip | ospf} [metric <*metric*>] [route-map <*NAME*>] **no redistribute { connected | static | rip | ospf}**	Redistribute IGP routes to BGP and may specify the redistributed metric and route reflector; the **no redistribute { connected | static | rip | ospf}** command cancels the redistribution.

14. Configure Route Dampening

Command	Explanation
BGP configuration mode	
bgp dampening [<*1-45*>] [<*1-20000*> <*1-20000*> <*1-255*>] [<*1-45*>] **no bgp dampening [<*1-45*>] [<*1-20000*> <*1-20000*> <*1-255*>] [<*1-45*>]**	Enable BGP route dampening and apply the specified parameters; the **no bgp dampening [<*1-45*>] [<*1-20000*> <*1-20000*> <*1-255*>] [<*1-45*>]**command stops route dampening

15. Configure BGP capability Negotiation

Command	Explanation
BGP configuration mode	

neighbor {<*ip-address*>|<*TAG*>} capability {dynamic | route-refresh} **no neighbor {<*ip-address*>|<*TAG*>} capability {dynamic | route-refresh}** **neighbor {<*ip-address*>|<*TAG*>} capability orf prefix-list {<*both*>|<*send*>|<*receive*>}** **no neighbor {<*ip-address*>|<*TAG*>} capability orf prefix-list {<*both*>|<*send*>|<*receive*>}** **neighbor {<*ip-address*>|<*TAG*>} dont-capability-negotiate** **no neighbor {<*ip-address*>|<*TAG*>} dont-capability-negotiate** **neighbor {<*ip-address*>|<*TAG*>} override-capability** **no neighbor {<*ip-address*>|<*TAG*>} override-capability** **neighbor {<*ip-address*>|<*TAG*>} strict-capability-match** **no neighbor {<*ip-address*>|<*TAG*>} strict-capability-match**	BGP provides capability negotiation regulation and carry out this capability match while establishing connection. The currently supported capabilities include route update, dynamic capability, outgoing route filtering capability and the address family's capability of supporting the negotiation. Use these command to enable these capabilities, its format "no" close these capabilities .It can also be configured by commands to not do capability negotiation, do strict capability negotiation or not care about the negotiation results

16. Configure Routing Server

Command	Explanation
BGP configuration mode	
neighbor {<*ip-address*>|<*TAG*>} route-server-client **no neighbor {<*ip-address*>|<*TAG*>} route-server-client**	Route server may configure BGP neighbors under EBGP environment to reduce the number of peers that every client has configured; format "no" of the command configures this router as route server and specify the clients it serves, the **no neighbor {<*ip-address*>|<*TAG*>} route-server-client** command can delete clients.

17. Configure Path-selected rules

Command	Explanation
BGP configuration mode	

bgp always-compare-med **no bgp always-compare-med** **bgp bestpath as-path ignore** **no bgp bestpath as-path ignore** **bgp bestpath compare-confed-aspath** **no bgp bestpath compare-confed-aspath** **bgp bestpath compare-routerid** **no bgp bestpath compare-routerid** **bgp bestpath med {[confed] [missing-is-worst]}** **no bgp bestpath med {[confed] [missing-is-worst]}**	BGP may change some path-select rules by configuration to change the best selection and compare MED under EBGP environment through these command, ignore the AS-PATH length, compare the confederation as-path length, compare the route identifier and compare the confederation MED etc. Its format "no" recovers the default route path-selected rules.

17.8.3 Commands for BGP

17.8.3.1 address-family

Command: address-family *<AFI> <SAFI>*

Function: Enter address-family mode

Parameter: *<AFI>* : address-family, such as IPv4、IPv6、VPNv4, etc

<SAFI>: sub address-family, such as unicast 、multicast.

Default: None

Command Mode: BGP routing mode

Usage Guide: Since the BGP-4 supports multi-protocol, it is available to get different configuration for each address-family. Actually the configuration outside address-family mode is configuring the default address-family (normally IPv4 unicast). To configure non default mode, enter this address-family mode

Example: Switch(config-router)# address-family ipv4 unicast

17.8.3.2 address-family ipv4

Command: address-family ipv4 {multicast | unicast | **vrf<vrf-name>}**

no address-family ipv4 vrf *<vrf-name>*

Function: Enter BGP VRF address-family mode. The "**no address-family ipv4 vrf *<vrf-name>***" command deletes the configuration of the address-family

Parameter: *<vrf-name>* specifies the name of VPN routing/forwarding instances.

Command Mode: BGP mode

Usage Guide: To support VPN, VRF has to be enabled on the border routers; to realize

VPN, create neighbors for BGP with the VRF address family on the private network, and with VPNv4 address-family on the public network. Configuration performed with this command to specific VRF, is independent from IPv4 unicast address-family. The VRF configuration is performed by using ip vrf <NAME> command under global mode. The address-family configuration is only available after the VRF RD is set.

Example: In the example below a VRF name DC1 is created with RD at 100: :10, and then enter the BGP address-family for its configuration.

Switch(config)#ip vrf DC1
Switch(config-vrf)#rd 100:10
Switch(config-vrf)#exit
Switch(config)#router bgp 100
Switch(config-router)#address-family ipv4 vrf DC1
Switch(config-router-af)#

17.8.3.3 address-family vpnv4

Command: address-family vpnv4

Function: Enter the BGP VPNv4 address family mode

Parameter: None

Command Mode: BGP mode

Usage Guide: To support VPN, VRF has to be enabled on the border routers; to realize VPN, create neighbors for BGP with the VRF address family on the private network, and with VPNv4 address-family on the public network. When configuring VPNv4 address-family with this command, IPv4 unicast address connection is available. Its neighbor configuration could be the same with IPv4 unicast only by using neighbor A.B.C.D activate on this neighbor to enable this address-family

Example:

Switch(config)#router bgp 100
Switch(config-router)#address-family vpnv4
Switch(config-router-af)#

17.8.3.4 aggregate-address

Command: aggregate-address <*ip-address/M*> [summary-only] [as-set]
no aggregate-address <*ip-address/M*> [summary-only] [as-set]

Function: Configure the aggregate-address. The "**no aggregate-address <*ip-address/M*> [summary-only] [as-set]**" command deletes the aggregate-address

Parameter: <*ip-address/M*>: IP address, length of mask

[summary-only]: Send summary only ignoring specific route

[as-set]: Show AS on the path in list, each AS is shown once.

Default: No aggregate configuration

Command Mode:BGP route mode

Usage Guide: Address aggregation reduces spreading routing messages outside. Use summary-only option so to spread aggregate route to the neighbors without spreading specific route. as-set option will list AS from each route covered by the aggregation only once without repeat.

Example:

Switch(config-router)# aggregate-address 100.1.0.0/16 summary-only

Switch(config-router)# aggregate-address 100.2.0.0/16 summary-only as-set

Switch(config-router)# aggregate-address 100.3.0.0/16 as-set

17.8.3.5 bgp aggregate-nexthop-check

Command:bgp aggregate-nexthop-check

no bgp aggregate-nexthop-check

Function: Configures whether BGP checks all the route next-hop in aggregating. The "**no bgp aggregate-nexthop-check**" command cancels this configuration, namely not check the next-hop accordance of aggregate route

Parameter: None

Default: No nexthop checked during aggregating

Command Mode: Global mode

Usage Guide: When check is enabled, the aggregate will not be performed if the next-hop of the covered routes are not in accordance. When checking is disabled, all covered route will be aggregated into the aggregate route.

Example:

Switch(config)#bgp aggregate-nexthop-check

Relevant Command: aggregate-address, no aggregate-address

17.8.3.6 bgp always-compare-med

Command: bgp always-compare-med

no bgp always-compare-med

Function: Configures If MED comparison is always performed. The "**no bgp always-compare-med**" command cancels this configuration.

Parameter: None

Default: Not configured.

Command Mode: BGP route mode

Usage Guide: Normally the BGP compares the MED only when the AS is the same. By using this configuration, MED of routes from different AS source will also be compared.

Example:

Announce the same route prefix through the two AS (100 and 300) to the same AS (200) while carrying different MED;
Configure on the route 10.1.1.64
Switch(config-router)#bgp always-compare-med

17.8.3.7 bgp bestpath as-path ignore

Command: bgp bestpath as-path ignore
no bgp bestpath as-path ignore
Function: Set to ignore the AS-PATH length. The "**no bgp bestpath as-path ignore**" command cancels this configuration
Parameter: None
Default: Not set
Command Mode: BGP route mode
Usage Guide: Length of AS-PATH will be compared in BGP pathing, and its length can be ignored by using this configuration.
Example:
Add this setting on B:
Switch(config)#router bgp 200
Switch(config-router)#bgp bestpath as-path ignore

17.8.3.8 bgp bestpath compare-confed-aspath

Command:bgp bestpath compare-confed-aspath
no bgp bestpath compare-confed-aspath
Function: Set to concern the confederation AS-PATH length. The "**no bgp bestpath compare-confed-aspath**" command cancels this configuration.
Parameter: None
Default: Not configured
Command Mode: BGP route mode
Usage Guide: Normally only the length of external AS-PATH will be compared in BGP pathing. By using this configuration, lengths of AS inner union AS-PATH will be compared at the same time.
Example:
Switch(config-router)#bgp bestpath compare-confed-aspath

17.8.3.9 bgp bestpath compare-routerid

Command: bgp bestpath compare-routerid
no bgp bestpath compare-routerid
Function: Compare route ID; the "**no bgp bestpath compare-routerid**" command

cancels this configuration

Parameter: None

Default: Not configured

Command Mode: BGP route mode

Usage Guide: Normally the first arrived route from the same AS (with other conditions equal) will be chosen as the best route. By using this command, source router ID will also be compared.

Example:

Announce the same route prefix through two devices （10.1.1.64 and 10.1.1.68）from the same AS (100) to another device（10.1.1.66, AS200）

Switch(config-router)#bgp bestpath compare-routerid

17.8.3.10 bgp bestpath med

Command: bgp bestpath med {[confed] [missing-as-worst]}

no bgp bestpath med {[confed] [missing-as-worst]}

Function: Configure whether the MED attributes should be compared in the confederation path and the treatment when MED is unavailable. The "**no bgp bestpath med {[confed] [missing-as-worst]}**" command cancels this configuration

Parameter: [confed]: Compare MED in the confederation path

[missing-is-worst]: Consider as max MED value when missing.

Default: Not configured

Command Mode: BGP route mode

Usage Guide: Choose whether MED is compared among confederations by this command. If MED is missing. It is considered max when missing-is-worst or else 0

Example:

Switch(config-router)#bgp bestpath med confed missing-as-worst

17.8.3.11 bgp client-to-client reflection

Command: bgp client-to-client reflection

no bgp client-to-client reflection

Function: Configures whether the route reflection is performed. The "**no bgp client-to-client reflection**" cancels this configuration

Parameter: None

Default: Reflection defaulted when client is configured.

Command Mode: BGP route mode

Usage Guide: After configured reflection client with neighbor {<ip-address>|<TAG>} route-reflector-client, the router performs routing reflection in default condition. The NO form of this command cancels the route reflection among CLIENT, (reflection among

Clients and non-CLIENT is not disturbed.)

Example: Switch(config-router)#no bgp client-to-client reflection

17.8.3.12 bgp cluster-id

Command: bgp cluster-id {<*ip-address*>|<*01-4294967295*>}

no bgp cluster-id {<[<*ip-address*>]|<*0-4294967295*>}

Function: Configure the route reflection ID during the route reflection. The "**no bgp cluster-id {<[<*ip-address*>]|<*0-4294967295*>}**" command cancels this configuration

Parameter: **<*ip-address*>|<*1-4294967295*>**: **>**: cluster-id which is shown in dotted decimal notation or a 32 digit number.

Default: Not configured

Command Mode: BGP route mode

Usage Guide: A CLUSTER consists of routing reflectors and its clients in an area. However in order to increase the redundancy level, sometime more than one routing reflectors may be deployed in one area. Router-id is for identifying the router exclusively in an area, and cluster-id is required for two or more reflector identification.

Example: Switch(config-router)#bgp cluster-id 1.1.1.1

17.8.3.13 bgp confederation identifier

Command: bgp confederation identifier <*as-id*>

no bgp confederation identifier [<*as-id*>]

Function: Create/delete a confederation configuration. The "**no bgp confederation identifier [<*as-id*>]**" command deletes a confederation

Parameter: ID number of the confederation AS

Default: No confederation

Command Mode: BGP route mode

Usage Guide: Confederation is for divide large AS into several smaller AS, while still identified as the large AS. Create large AS number with this command

Example: Switch(config-router)# bgp confederation identifier 600

17.8.3.14 bgp confederation peers

Command: bgp confederation peers <*as-id*> [<*as-id*>..]

no bgp confederation peers <*as-id*> [<*as-id*>..]

Function: Add/delete one or several AS to a confederation

Parameter: ID numbers of the AS included in the confederation, which could be multiple.

Default: No members

Command Mode: BGP route mode.

Usage Guide: Confederation is for divide large AS into several smaller AS, while still

identified as the large AS. Use this command to add/delete confederation members

Example:

Switch(config-router)# bgp confederation identifier 600

Switch(config-router)#bgp confederation peers 100 200

17.8.3.15 bgp dampening

Command: bgp dampening [<*1-45*>] [<*1-20000*> <*1-20000*> <*1-255*>] [<*1-45*>]

no bgp dampening [<*1-45*>] [<*1-20000*> <*1-20000*> <*1-255*>] [<*1-45*>]

Function: Configure the route dampening. The "**no bgp dampening [<*1-45*>] [<*1-20000*> <*1-20000*> <*1-255*>] [<*1-45*>]**" command cancels the route dampening function

Parameter: <*1-45*>: Respectively the penalty half-lives of accessible and inaccessible route, namely the penalty value is reduced to half of the previous value, in minutes.

<*1-20000*>: Respectively the penalty reuse border and restrain border

<*1-255*>: Maximum restrain route time, in minutes

Default: Half-life of accessible route is 15 minutes, 5 minutes for inaccessible. The restrain border is 2000, reuse border is 750, and maximum restrain time is 60 minutes

Command Mode: BGP route mode.

Usage Guide: Abundant route update due to unstable route could be reduced with route dampening technology, of which the algorithm is lay penalty on the route when the route fluctuates, and when penalty exceeds the restrain border this route will no longer be advertised. The penalty value will be reduced by time by the half-life index regulation if the route keeps stable and finally be advertised again when the penalty falls below the border or the restrain time exceeds the maximum restrain time. This command is for enabling/disabling the route dampening and configuring its parameters

Example:

Switch(config-router)# bgp dampening

17.8.3.16 bgp default

Command:bgp default {ipv4-unicast|local-preference <*0-4294967295*>}

no bgp default {ipv4-unicast|local-preference [<*0-4294967295*>]}

Function: Set the BGP defaults, the "**no bgp default {ipv4-unicast|local-preference [<*0-4294967295*>]}**" command cancels this configuration

Parameter: <*0-4294967295*>: Default local priority

Default: The IPv4 unicast is default enabled when BGP is enabled. The default priority is 100.

Command Mode: BGP route mode.

Usage Guide: IPv4 unicast address-family is default enabled in BGP. Cancel this setting

with no bgp default ipv4-unicast command so to not enable this address-family in default. Default local priority can be configured through bgp default local-preference command.

Example:

Configure on 10.1.1.66

Switch(config)#router bgp 200

Switch(config-router)# bgp default local-preference 500

17.8.3.17 bgp deterministic-med

Command: bgp deterministic-med

no bgp deterministic-med

Function: Use the best MED for the same prefix in the AS to compare with other AS. The "**no bgp deterministic-med**" cancels this configuration

Parameter: None

Default: Not configured

Command Mode: BGP route mode.

Usage Guide: Normally if same prefix routes from several paths, each path will be compared. With this configuration, the system will only use the path with the smallest MED in the AS (when other main attributes equal) to compare with other AS. After the best one is elected, select the path among AS with no regard to MED value.

Example: Switch(config-router)#bgp deterministic-med

17.8.3.18 bgp enforce-first-as

Command: bgp enforce-first-as

no bgp enforce-first-as

Function: Enforces the first AS position of the route AS-PATH contain the neighbor AS number or else disconnect this peer when the BGP is reviving the external routes. The "**no bgp enforce-first-as**" command cancels this configuration

Parameter: None

Default: Not configured

Command Mode: BGP route mode.

Usage Guide: This command is usually for avoiding unsafe or unauthenticated routes.

Example: Switch(config-router)#bgp enforce-first-as

17.8.3.19 bgp fast-external-failover

Command: bgp fast-external-failover

no bgp fast-external-failover

Function: Fast reset when the BGP neighbor connection varies at the interface other than wait for TCP timeout. The "**no bgp fast-external-failover**" command cancels this

configuration

Parameter: None

Default: Configured

Command Mode: BGP route mode.

Usage Guide: This command is for immediately cutting of the neighbor connection when the interface is DOWN.

Example: Switch(config-router)# bgp fast-external-failover

17.8.3.20 bgp inbound-route-filter

Command: bgp inbound-route-filter

no bgp inbound-route-filter

Function: The bgp do not install the RD routing message which does not exist locally. The "**no bgp inbound-route-filter**" command means the RD will be installed with no regard to the local existence of the RD.

Parameter: None

Command Mode: BGP mode

Usage Guide: Normally when the switch plays as PE, whether the route bgp acquired from VPN is saved in BGP depends on if the VRF configured in this PE has got matched information. With the "**no bgp inbound-route-filter**" command the BGP will save the routing message with no regard to the matched information

Example:

Switch(config)#router bgp 100

Switch(config-router)#no bgp inbound-route-filter

17.8.3.21 bgp log-neighbor-changes

Command: bgp log-neighbor-changes

no bgp log-neighbor-changes

Function: Output log message when BGP neighbor changes. The "**no bgp log-neighbor-changes**" command cancels this configuration.

Parameter: None

Default: Not configured

Command Mode: BGP route mode.

Usage Guide: Can display neighbor change messages on the monitor

Example:

Switch(config-router)# bgp log-neighbor-changes

17.8.3.22 bgp multiple-instance

Command: bgp multiple-instance

no bgp multiple-instance

Function: Set that whether BGP supports multiple BGP instance or not; the "**no bgp multiple-instance**" command mean multiple BGP instance not supported

Parameter: None

Default: Multiple instance not supported

Command Mode: Global mode

Usage Guide: Set that whether BGP supports multiple BGP instance or not; this configuration should be set before the BGP instance configuration

Example: Switch(config)#bgp multiple-instance

17.8.3.23 bgp network import-check

Command: bgp network import-check

no bgp network import-check

Function: Set whether check the IGP accessibility of the BGP network route or not. The "**no bgp network import-check**" command sets to not checking the IGP accessibility

Parameter: None

Default: Not configured

Command Mode: BGP route mode.

Usage Guide: Checking the IGP accessibility of the route advertised by BGP is to check the existence of next-hop and its IGP accessibility

Example: Switch(config-router)# bgp network import-check

17.8.3.24 bgp rfc1771-path-select

Command:bgp rfc1771-path-select

no bgp rfc1771-path-select

Parameter: None

Default: Not following

Command Mode: Global mode

Usage Guide: After this attribute is set, path selecting will follow the way defined in rfc 1771, namely not checking the AS internal METRIC,when different AS exist, which should be perform without this attribute set.

Example:

Switch(config)# bgp rfc1771-path-select

Switch(config)# no bgp rfc1771-path-select

17.8.3.25 bgp rfc1771-strict

Command: bgp rfc1771-strict

no bgp rfc1771-strict

Function: Set wither strictly follows the rfc1771 restrictions. The "**no bgp rfc1771-strict**" command set to not strictly following

Parameter: None

Default: Not following rfc 1771 restrictions

Command Mode: Global mode

Usage Guide: With this attribute set, generation types of routes from protocols such as RIP, OSPF, ISIS, etc will be regarded as IGP (internal generated), or else as INCOMPLETE

Example:

Switch(config)# bgp rfc1771-strict

Switch(config)# no bgp rfc1771-strict

17.8.3.26 bgp router-id

Command: bgp router-id <*ip-address*>

no bgp router-id [<IP-ADDRESS>]

Function: Configure the router ID manually. The "**no bgp router-id [<IP-ADDRESS>]**" cancels this configuration

Parameter: <*ip-address*>: Router ID

Default: Automatically acquire router ID

Command Mode: BGP route mode.

Usage Guide: Manually set the router ID with this command

Example: Switch(config-router)# bgp router-id 1.1.1.1

17.8.3.27 bgp scan-time

Command: bgp scan-time <*0-60*>

no bgp scan-time [<*0-60*>]

Function: Set the time interval of the periodical next-hop validation; the "**no bgp scan-time [<*0-60*>]**" command restores to the default value

Parameter: <*0-60*>: Validation time interval

Default: Default interval is 60s

Command Mode: BGP route mode.

Usage Guide: Validate the next-hop of BGP route, this command is for configuring the interval of this check. Set the parameter to 0 if you don't want to check

Example:

Switch(config-router)# bgp scan-time 30

17.8.3.28 clear ip bgp

Command: clear ip bgp [view <*NAME*>] {<*>|<*as-id*>| external|peer-group <*NAME*>|<*ip-address*>} [<*ADDRESS-FAMILY*>] [in [prefix-filter] |out|soft [in|out]]

Function: Clear up BGP links or states

Parameter: all

<as-id>: AS number;

<NAME>: Respectively BGP instance name and peer group name.

<ip-address>: IP address

<ADDRESS-FAMILY>: “ipv4 unicast”.” Address family

Default: None

Command Mode: Admin mode

Usage Guide: Clearing up BGP state in different parameters (such as AS number, peer group name, IPv4 address, address-family, external neighbor), or the inbound or outbound messages. Also it is optional to use the saved ORF as soft reconfiguration, or use the soft in|out commands for in or out soft reconfiguration if it is already set.

Example:

Switch# clear ip bgp * soft in

When soft reconfiguration is set, use this commands for soft reconfiguration

Switch# clear ip bgp *

Will clear up all established connections

Relevant Commands: None

17.8.3.29 clear ip bgp dampening

Command: clear ip bgp [<ADDRESS-FAMILY>] dampening [<ip-address>|<ip-address/M>]

Function: Used for resetting BGP routing dampening

Parameter: <*ADDRESS-FAMILY*>: address-family, such as “ipv4 unicast”

<ip-address>: IP address

<ip-address/M>: IP address and mask

Default: None

Command Mode: Admin mode

Usage Guide: It is possible to clear BGP routing dampening messages and state by different parameters (such as address-family or IPv4 address)

Example:

Switch# clear ip bgp ipv4 unicast dampening

17.8.3.30 clear ip bgp flap-statistics

Command: clear ip bgp [<*ADDRESS-FAMILY*>] flap-statistics [<*ip-address*>|<*ip-address/M*>]

Function: For resetting BGP routing dampening statistics messages.

Parameter: <*ADDRESS-FAMILY*>: address-family such as “ipv4 unicast”

<*ip-address/M*>: IP address and mask

Default: None

Command Mode: Admin mode

Usage Guide: It is possible to clear BGP routing dampening statistic messages and state by different parameters (such as address-family or IPv4 address)

Example:

Switch#clear ip bgp ipv4 unicast flap-statistics

17.8.3.31 distance

Command: distance <*1-255*> <*ip-address/M*> [<*WORD*>]

no distance <*1-255*> <*ip-address/M*> [<*WORD*>]

Function: Set the manage distance of the routing prefix. The “**no distance <*1-255*> <*ip-address/M*> [<*WORD*>]**” command restores to the default value

Parameter: <*1-255*>: Manage distance

<*ip-address/M*>: Routing prefix

<*WORD*>: Access-list name

Default: Not set

Command Mode: BGP route mode

Usage Guide: Set the manage distance for specified BGP route as the path selecting basis

Example: Switch(config-router)# distance 90 10.1.1.64/32

17.8.3.32 distance bgp

Command: distance bgp <*1-255*> <*1-255*> <*1-255*>

no distance bgp [<*1-255*> <*1-255*> <*1-255*>]

Function: Set the BGP protocol manage distance. The “**no distance bgp [<*1-255*> <*1-255*> <*1-255*>]**” command restores the manage distance to default value

Parameter: Respectively the EBGP, IBGP and LOCAL manage distance of the BGP

Default: Default EBGP is 20, others are 200

Command Mode: BGP route mode.

Usage Guide: Set the manage distance for BGP routing as the NSM path selecting basis

Example: Switch(config-router)# distance bgp 15 150 150

17.8.3.33 exit-address-family

Command: exit-address-family

Function: Exit the BGP address-family mode

Parameter: None

Default: None

Command Mode: BGP address-family mode

Usage Guide: Use this command to exit the mode so to end the address-family configuration when configuring address-family under BGP

Example:

```
Switch(config)#router bgp 100
Switch(config-router)#address-family ipv4 unicast
Switch(config-router-af)# exit-address-family
Switch(config-router)#
```

17.8.3.34 import map

Command: import map <*map-name*>

no import map <*map-name*>

Function: Use this command to configure the route-map regulations when introducing routes into VRF

Parameter: <*map-name*> is the route-map name used

Command Mode: vrf mode

Usage Guide: Use the route map command route-map NAME permit|deny <1-65535> to create the route-map and establish the regulations. Using this command will apply regulations to the route introducing of this VRF

Example:

```
Switch(config)#route-map map1 permit 15
Switch(config-map)#match interface Vlan1
Switch(config-map)#set weight 655
Reconfiguring VRF DC1 with this route-map
Switch(config-map)#exit
Switch(config)#ip vrf DC1
Switch(config-af)#rd 100:10
Switch(config-af)#route-target both 100:10
Switch(config-af)#import map map1
Switch#show ip bgp vpn all
    Network          Next Hop            Metric LocPrf Weight Path
Route Distinguisher: 100:10 (Default for VRF DC1)
*> 11.1.1.0/24      11.1.1.64                0             0 200 ?
*>i15.1.1.0/24      10.1.1.68                0    100      655 300 ?
*> 20.1.1.0/24      11.1.1.64                0             0 200 ?
```

*>i100.1.1.0/24 10.1.1.68 0 100 655 300 ?

Route Distinguisher: 100:10

*>i15.1.1.0/24 10.1.1.68 0 100 0 300 ?

*>i100.1.1.0/24 10.1.1.68 0 100 0 300 ?

As we can see, the weight of the route from the VPN changes to 655 after introduced into VRF DC1.

17.8.3.35 ip as-path access-list

Command: ip as-path access-list <*.LINE*> {<*permit*>|<*deny*>} <*LINE*>

no ip as-path access-list <*.LINE*> {<*permit*>|<*deny*>} <*LINE*>

Function: Configure the AS-PATH access-list. The "**no ip as-path access-list <*.LINE*> {<*permit*>|<*deny*>} <*LINE*>**" command deletes this access-list

Parameter: <*.LINE*>: name of access-list

<*LINE*>: matched strings in the AS-PATH

Default: None

Command Mode: Global mode

Usage Guide: Use this command to configure the access-list related to AS-PATH, so to supply the conditions for pass/filter.

Example: Switch(config)#ip as-path access-list ASPF deny ^100$

17.8.3.36 ip community-list

Command: ip community-list {<*LISTNAME*>|<*1-199*>|[expanded <*WORD*>]|[standard <*WORD*>]} {deny|permit} <*.COMMUNITY*>

no ip community-list {<*LISTNAME*>|<*1-199*>|[expanded <*WORD*>]|[standard <*WORD*>]} [{deny|permit} <*.COMMUNITY*>]

Function: Configure the community-list. The "**no ip community-list {<*LISTNAME*>|<*1-199*>|[expanded <*WORD*>]|[standard <*WORD*>]} [{deny|permit} <*.COMMUNITY*>]**" command deletes the community list

Parameter: <*LISTNAME*>: name of community list

<*1-199*>: Standard or extended community number

<*WORD*>: Standard or extended community number

<*.COMMUNITY* >: Members of the community list, which may be the combination of aa:nn, or internet, local-AS, no-advertise, and no-export. It can be shown in regular expressions under extended conditions

Default: None

Command Mode: Global mode

Usage Guide: With this command we can configure the community-list so to supply terms for the pass/filter/search

Example:

Switch(config)# ip community-list LN permit 100:10

17.8.3.37 ip extcommunity-list

Command: i**p extcommunity-list {<*LISTNAME*>|<*1-199*>|[expanded <*WORD*>]|[standard <*WORD*>]} {deny|permit} <*.COMMUNITY*>**

no ip extcommunity-list {<*LISTNAME*>|<*1-199*>|[expanded <*WORD*>]|[standard <*WORD*>]} {deny|permit} <*.COMMUNITY*>

Function: Configure the extended community-list. The "**no ip extcommunity-list {<*LISTNAME*>|<*1-199*>|[expanded <*WORD*>]|[standard <*WORD*>]} {deny|permit} <*.COMMUNITY*>**" command is for deleting the extended community list

Parameter: <*LISTNAME*>: name of community-list

<*1-199*>: Standard or extended community number

<*WORD*>: Standard or extended community number

<*.COMMUNITY* >: Members of the community list, which may be the combination of aa:nn, or internet, local-AS, no-advertise, and no-export. It can be shown in regular expressions under extended conditions

Default: None

Command Mode: Global mode

Usage Guide: With this command we can configure the community-list so to supply terms for the pass/filter/search

Example: Switch(config)#ip extcommunity-list LN permit 100:10

17.8.3.38 neighbor activate

Command:neighbor {<*ip-address*>|<*TAG*>} activate

no neighbor {<*ip-address*>|<*TAG*>} activate

Function: Configure the address family routing which do or do not switch specific address-family with BGP neighbors. The "**no neighbor {<*ip-address*>|<*TAG*>} activate**" command is for setting the route which do not switch the specified address family

Parameter: <*ip-address*>: IP address of the neighbor

<*TAG*>: Name of peer group

Default: Enable the routing switch of IP unicast address-family, and disable other address-families

Command Mode: BGP route mode and address-family mode

Usage Guide: IP unicast is configured under BGP route mode. Configure whether specific address-family is switched under address-family mode. If this option on any side between local side and partner is not enabled, the address-family route will not be acquired by the partner even if the corresponding address family routes acquired before

will be cancelled after this option is disabled.

Example:

Switch(config-router)#neighbor 10.1.1.64 activate

Switch(config-router)#address-family ipv4

Switch(config-router-af)#no neighbor 10.1.1.64 activate

Switch(config-router-af)#

17.8.3.39 neighbor advertisement-interval

Command: neighbor {<*ip-address*>|<*TAG*>} advertisement-interval <*0-600*>

no neighbor {<*ip-address*>|<*TAG*>} advertisement-interval [<*0-600*>]

Function: Configure the update interval of specific neighbor route. the "**no neighbor {<*ip-address*>|<*TAG*>} advertisement-interval [<*0-600*>]**" command restores to default

Parameter: **<*ip-address*>**: IP address of the neighbor

<*TAG*>: Name of the peer group

<*0-600*>: Advertise interval, in seconds

Default: EBGP 30s.

Default IBGP is 5s, default EBGP is 30s

Command Mode: BGP route mode and address-family mode

Usage Guide: Reduce this value will improve the route updating speed while also consumes more bandwidth.

Example:

Switch(config-router)#neighbor 10.1.1.64 advertisement-interval 20

Switch(config-router)#no neighbor 10.1.1.64 advertisement-interval

Switch(config-router)#

17.8.3.40 neighbor allowas-in

Command:neighbor {<*ip-address*>|<*TAG*>} allowas-in [<*1-10*>]

no neighbor {<*ip-address*>|<*TAG*>} allowas-in

Function: Configure the counts same AS is allowed to appear in the neighbor route AS table. The "**no neighbor {<*ip-address*>|<*TAG*>} allowas-in**" restores to not allow any repeat

Parameter: <*ip-address*>: IP address of the neighbor

<*TAG*>: Name of the peer group

<*1-10*>: Allowed count of same AS number

Default: In default conditions AS is not allowed repeating in the same route, and when set the repeat count it is defaulted at 3 when <1-10> parameters not set.

Command Mode: BGP route mode and address family mode

Usage Guide: Normally BGP will not allow same AS number appears in the route more

than one time. The system will deny a route when its AS number appears in the AS-PATH. However to support some special needs, especially the VPN support, the extended BGP allows the AS re-appear counts by configuration. This command is for configure the re-appear counts

Example:

Switch(config-router)#neighbor 10.1.1.66 allowas-in

17.8.3.41 neighbor attribute-unchanged

Command: neighbor {<*ip-address*>|<*TAG*>} attribute-unchanged [as-path][med][next-hop]

***no* neighbor {<*ip-address*>|<*TAG*>} attribute-unchanged [as-path] [med] [next-hop]**

Function: Configure certain attributes which is kept unchanged for transmitting, namely the attribute transparent transmission. The "***no* neighbor {<*ip-address*>|<*TAG*>} attribute-unchanged [as-path] [med] [next-hop]**" command means the attribute transparent transmission is not performed.

Parameter: <*ip-address*>: IP address of the neighbor

<*TAG*>: Name of the peer group

Default: No attribute transparent defined

Command Mode: BGP route mode and address-family mode

Usage Guide: With this configuration specified route attributes will not change when transmitted to the specified neighbor. The BGP route mode is the IPv4 unicast configuration. No parameter refers to above three parameter are configured together.

Example:

Switch(config-router)#neighbor 10.1.1.64 attribute-unchanged

Switch(config-router)# no neighbor 10.1.1.64 attribute-unchanged as-path med

17.8.3.42 neighbor as-override

Command: [no] neighbor <*ip-addr*> as-override

Function: Use this command to replace the previous AS number with its own AS number when transmitting the BGP route in the VRF.

Parameter: IP address of neighbors, shown in dotted decimal notation

Command Mode: vrf mode

Usage Guide: When BGP receives remote routing messages, it will check the AS path whether its AS number exists, if yes, the route will be considered as circuit and cleared. However in VPN environment there may be two or more CE with the same AS number on the PE link. As the EBGP is required between private network and public network, routes step across public network will be considered circuit and unable to reach the partner.

Under this circumstance we can configure the as-override attribute of the CE neighbor on the VRF address-family of BGP on PE, replacing the remote as number with the global as number, so that CE will not filter this route due to discovering its own as number.

Example:

In CE1-PE1-P-PE2-CE2 environments, as numbers of two CE are all 200, as number of area P is 100.

After typical environment is configured, the CE1 route will be restrained on CE 2 due to as number, the debugging messages shows:

Prefix 11.1.1.0/24 denied due to as-path contains our own AS.

Prefix 20.1.1.0/24 denied due to as-path contains our own AS

Now configure on PE2 as follows

Switch(config)# router bgp 100

Switch(config)#address-family ipv4 vrf DC1

Switch(config-router-af)#neighbor 15.1.1.70 as-override

Switch(config-router-af)#exit-address-family

The route is successfully transmitted to CE2 after refresh, on CE2 shown:

Switch#show ip bgp

BGP table version is 5, local router ID is 100.1.1.70

Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,

S Stale

Origin codes: i - IGP, e - EGP, ? - incomplete

Network	Next Hop	Metric	LocPrf	Weight	Path
*> 11.1.1.0/24	15.1.1.68			0	100 100 ?
*> 15.1.1.0/24	0.0.0.0	0		32768	?
*> 20.1.1.0/24	15.1.1.68			0	100 100 ?
*> 100.1.1.0/24	0.0.0.0	0		32768	?

Total number of prefixes 4

17.8.3.43 neighbor capability

Command: neighbor {*<ip-address>*|*<TAG>*} capability {dynamic | route-refresh}

no neighbor {*<ip-address>*|*<TAG>*} capability {dynamic | route-refresh}

Function: Configure dynamic update between neighbors and the route refresh capability negotiation. The "**no neighbor {*<ip-address>*|*<TAG>*} capability {dynamic | route-refresh}**" command do not enable the specific capability negotiation

Parameter: <ip-address>: Neighbor IP address

<TAG>: Name of peer group

Default: Not configure the dynamic update capability but the route refresh capability.

Command Mode: BGP route mode and address family mode

Usage Guide: This is an extended BGP capability. With this configuration supported capabilities by both side will be negotiated in the OPEN messages, and the partner will respond if this capability is supported by the partner and send NOTIFICATION if not. The originating side will then send an OPEN excluded the capability to reestablish the connection. The dynamic capability refers to when the address family negotiation changes, the connection don't have to be restarted. Route refresh refers to sending refresh request when configuring some soft reconfigurable attributes and the partner will retransmit the existing route to the originating side. With route refresh attribute, the connection will not have to be restarted but be refreshed with the clear ip bgp * soft in command.

Example:

Switch(config-router)#neighbor 10.1.1.64 capability dynamic

Switch(config-router)# no neighbor 10.1.1.64 capability route-refresh

17.8.3.44 neighbor capability orf prefix-list

Command: neighbor {<*ip-address*>|<*TAG*>} capability orf prefix-list {<*both*>|<*send*>|<*receive*>}

no neighbor {<*ip-address*>|<*TAG*>} capability orf prefix-list {<*both*>|<*send*>|<*receive*>}

Function: Configure the out route filter capability negotiation between neighbors. The "**no neighbor {<*ip-address*>|<*TAG*>} capability orf prefix-list {<*both*>|<*send*>|<*receive*>}**" command set to not perform the negotiation

Parameter: <*ip-address*>:Neighbor IP address

<*TAG*>: Name of peer group

Default: ORF capability not configured

Command Mode: BGP route mode and address-family mode

Usage Guide: This is an extended BGP capability. With this configuration supported capabilities by both side will be negotiated in the OPEN messages, and the partner will respond if this capability is supported by the partner and send NOTIFICATION if not. The originating side will then send an OPEN excluded the capability to reestablish the connection. With this capability, the side configured with in prefix-list filter rules will transmit its own filter rules to the peer, the peer group will apply this rule as its own out rules, so to avoid sending route which will be denied by the partner.

Example:

Switch(config-router)#neighbor 10.1.1.66 capability orf prefix-list both

17.8.3.45 neighbor collide-established

Command: neighbor {<*ip-address*>|<*TAG*>} collide-established

no neighbor {<*ip-address*>|<*TAG*>} collide-established

Function: Enable the collision check and settlement in the TCP connection collision. The "**no neighbor {<*ip-address*>|<*TAG*>} collide-established**" command disables the TCP connection collision settlement

Parameter: <*ip-address*>: Neighbor IP address

<*TAG*>: Name of the peer

Usage Guide: This command is for settling the problem that multi-connection among peers due to TCP connection collision. Connections created with this option on will always be check even at established state. And it will be checked if local side IP is larger than partner IP when collides. If yes, the original connection will be deleted, and if not the option will be configured to only checks when the connection originated from local side at open sent and open confirm state.

Command Mode: route mode and address family mode

Default: Disabled and Unavailable

Example: Switch(config-router)#neighbor 10.1.1.64 collide-established

17.8.3.46 neighbor default-originate

Command: neighbor {<*ip-address*>|<*TAG*>} default-originate [route-map <*WORD*>]

no neighbor {<*ip-address*>|<*TAG*>} default-originate [route-map <*WORD*>]

Function: Configures whether enables transmitting default route to the specific neighbor. The "**no neighbor {<*ip-address*>|<*TAG*>} default-originate [route-map <*WORD*>]**" command configures not sending default route to neighbors

Parameter: <*ip-address*>: IP address of the neighbor

<*TAG*>: Name of the peer

<*WORD*> : Name of route mirror

Default: Not sending default route

Command Mode: BGP route mode and address-family mode

Usage Guide: With this option, the default route of local side will be transmitted to partner, or else not. It supplies with options of which one to supply the default route. if several neighbors of the partner supply default route, the best one will be elected according to path selecting principles. According to route mirror, it can be chosen when to send the default route.

Example:

Switch(config-router)#neighbor 10.1.1.64 default-originate

Switch(config-router)#

Now the route table of the partner will generate default route from BGP.

17.8.3.47 neighbor description

Command: neighbor {<*ip-address*>|<*TAG*>} description <*.LINE*>

no neighbor {<*ip-address*>|<*TAG*>} description

Function: Configure the description string of the peer or peer group. The "**no neighbor {<*ip-address*>|<*TAG*>} description**" command deletes the configurations of this string

Parameter: **<*ip-address*>**: Neighbor IP address

<*TAG*>: Name of peer group

<*.LINE*>: Description string consists of displayable characters less than 80

Usage Guide: Configure the introduction of the peer or peer group

Command Mode: BGP mode and address-family mode

Default: Description string is empty

Example:

Switch(config-router)#neighbor 10.1.1.64 description s64down

Switch(config-router)#

17.8.3.48 neighbor distribute-list

Command: neighbor {<*ip-address*>|<*TAG*>} distribute-list {<*1-199*>|<*1300-2699*>|<*WORD*>} {in|out}

no neighbor {<*ip-address*>|<*TAG*>} distribute-list {<*1-199*>|<*1300-2699*>|<*WORD*>} {in|out}

Function: Configure the policy applied in partner route update transmission. The "**no neighbor {<*ip-address*>|<*TAG*>} distribute-list {<*1-199*>|<*1300-2699*>|<*WORD*>} {in|out}**" command cancels the policy configuration

Parameter: <*ip-address*>: Neighbor IP address

<*TAG*>: Name of peer group

<*1-199*>|<*1300-2699*>|<*WORD*>: Number or name of the access-list

Default: Policy not applied

Command Mode: BGP route mode and address-family mode

Usage Guide: Configure the policies with access-list command and apply this command on route sending and receiving. It will filter the update route from partner when use in mode, and will filter the route from local side to partner with out mode.

Example:

Configure the access-list

Switch(config)#access-list 101 deny ip 100.1.0.0 0.0.1.255 any

Switch(config)#access-list 101 permit ip any any

Switch(config)#router bgp 100

Switch(config-router)# neighbor 10.1.1.66 distribute-list 101 out

17.8.3.49 neighbor dont-capability-negotiate

Command: neighbor {<*ip-address*>|<*TAG*>} dont-capability-negotiate

no neighbor {<*ip-address*>|<*TAG*>} dont-capability-negotiate

Function: Set to not perform capability negotiate in creating connections. The "**no neighbor {<*ip-address*>|<*TAG*>} dont-capability-negotiate**" command cancels this configuration.

Parameter: <*ip-address*>: Neighbor IP address

<*TAG*>: Name of the peer group

Default: Capability negotiation performed

Command Mode: BGP route mode and address-family mode

Usage Guide: As the negotiation is the default, it can be disabled with this configuration when it is known that the partner BGP version is old which don't support capability negotiation.

Example: Last addition capability negotiation will not be realized in the connection by configuring as follows.

Switch(config-router)#neighbor 10.1.1.64 dont-capability-negotiate

17.8.3.50 neighbor ebgp-multihop

Command: neighbor {<*ip-address*>|<*TAG*>} ebgp-multihop [<*1-255*>]

no neighbor {<*ip-address*>|<*TAG*>} ebgp-multihop [<*1-255*>]

Function: Configures the EBGP neighbors can existing in different segment as well as its hop count (TTL). The "**no neighbor {<*ip-address*>|<*TAG*>} ebgp-multihop [<*1-255*>]**" set that the EBGP neighbors must be in the same segment

Parameter: <*ip-address*>: Neighbor IP address

<*TAG*>: Name of the peer group

<*1-255*>: Allowed hop count

Default: Must be in the same segment

Command Mode: BGP route mode and address-family mode

Usage Guide: Without this command, EBGP peers are required to be in the same segment and after this command is configured, peer addresses may from different segments. The allowed hop count can be configured and will be 255 if not.

Example:

Three device 10.1.1.64(AS100) and 11.1.1.120(AS300) connected respectively to the two interface 10.1.1.66 and 10.1.1.100 of another device. IGP accessibilities of 10.1.1.64 and 11.1.1.120 on both side routes are ensured through static configuration. The neighbor relationship is established only after both side are configured as follows:

on 10.1.1.64

Switch(config-router)#neighbor 11.1.1.120 ebgp-multihop

on 11.1.1.120

Switch(config-router)#neighbor 10.1.1.64 ebgp-multihop

After this, switches in different segments will be able to create BGP neighbor relationship

17.8.3.51 neighbor enforce-multihop

Command: neighbor {<*ip-address*>|<*TAG*>} enforce-multihop

no neighbor {<*ip-address*>|<*TAG*>} enforce-multihop

Function: Enforce the multihop connection to the neighbor. The "**no neighbor {<*ip-address*>|<*TAG*>} enforce-multihop**" command cancels this configuration

Parameter: <*ip-address*>: Neighbor IP address

<*TAG*>: Name of peer group

Default: Not enforced

Command Mode: BGP mode and address-family mode

Usage Guide: In fact the direct route can not be enforced to multihop, however will be treated as a multihop connection with this configuration, namely the check originally only performed on IBGP and EBGP of non-direct routes will be performed on all after this attribute set. The nexthop direct connected check will not be performed at exit in enforce multihop conditions.

Example:

Switch(config-router)#neighbor 10.1.1.66 enforce-multihop

17.8.3.52 neighbor filter-list

Command: neighbor {<*ip-address*>|<*TAG*>} filter-list <*.LINE*> {<*in*>|<*out*>}

no neighbor {<*ip-address*>|<*TAG*>} filter-list <*.LINE*> {<*in*>|<*out*>}

Function: Access-list control for AS-PATH. The "**no neighbor {<*ip-address*>|<*TAG*>} filter-list <*.LINE*> {<*in*>|<*out*>}**" cancels the AS-PATH access-list control.

Parameter: <*ip-address*>: Neighbor IP address

<*TAG*>: Name of peer group

<*.LINE*>: AS-PATH access-list name configured through ip as-path access-list *<.LINE> <permit|deny> <LINE>.*

Default: Not configured

Command Mode: BGP route mode and address list mode

Usage Guide: After first configured the IP AS-PATH access-list, apply this option to specified neighbor will be able to send/receive routes with specified AS numbers in the AS list. Accepting or denying depends on the configuration of the access-list, while sending and receiving are configured by this command.

Example:

Configure the AS-PATH access control list, "ASPF" is the name of the access-list. The

route with AS number of 100 will not be able to update to the partner due to the filter table control.

Switch(config)#ip as-path access-list ASPF deny 100

Switch(config)#router bgp 100

Switch(config-router)# redistribute static

Switch(config-router)neighbor 10.1.1.66 filter-list aspf out

17.8.3.53 neighbor interface

Command: neighbor <*ip-address*> interface <*IFNAM*>

no neighbor <*ip-address*> interface <*IFNAM*>

Function: Specify the interface to the neighbor. The "**no neighbor <*ip-address*> interface <*IFNAM*>**" of the command cancels this configuration

Parameter: <*ip-address*>: Neighbor IP address

<*IFNAME*>: Interface name, e.g. "Vlan 2"

Default: Not configured

Command Mode: BGP route mode and address-family mode

Usage Guide: Specifies the exit interface to the neighbor with this command. Interface destination accessibility should be ensured

Example: Switch(config-router)# neighbor 10.1.1.64 interface Vlan2

17.8.3.54 neighbor maximum-prefix

Command: neighbor {<*ip-address*>|<*TAG*>} maximum-prefix <*1-4294967295*> [<*1-100*> <*warning-only*>]

no neighbor {<*ip-address*>|<*TAG*>} maximum-prefix <*1-4294967295*> [<*1-100*> <*warning-only*>]

Function: Control the number of route prefix from the neighbor. The "**no neighbor {<*ip-address*>|<*TAG*>} maximum-prefix <*1-4294967295*> [<*1-100*> <*warning-only*>]**" command cancels this configuration

Parameter: <*ip-address*>: Neighbor IP address

<*TAG*>: Name of the peer

<*1-4294967295*>: Max prefix value allowed

<*1-100*>: Percentage of the max value at which it warns

<*warning-only*>: Warning only or not

Default: Not limited

Command Mode: BGP route mode and address-family mode

Usage Guide: Due to concerns of too much route updates from neighbors (e.g. attack), the max number of prefix acquired from a neighbor is limited, and will warns when the number hits certain rate. If the warning-only option is set, then there will be warning only,

if not, the connection to the neighbor will be cut till clear the records with clear ip bgp command.

Example:

Switch(config-router)#neighbor 10.1.1.64 maximum-prefix 12 50

In above configuration, it warns when the number of route prefix reaches 6, and the connection will be cut when the number hit 13.

17.8.3.55 neighbor next-hop-self

Command: neighbor {<*ip-address*>|<*TAG*>} next-hop-self

no neighbor {<*ip-address*>|<*TAG*>} next-hop-self

Function: Ask the neighbor to point the route nexthop sent by the local side to local side. The "**no neighbor {<*ip-address*>|<*TAG*>} next-hop-self**" command cancels this configuration.

Parameter: <*ip-address*>: Neighbor IP address

<*TAG*>: Name of peer group

Default: Not configured by default

Command Mode: BGP mode and address-family mode.

Usage Guide: In the EBGP environment, the nexthop will automatically point to the source neighbor. However in IBGP environment, the nexthop remains the same for route in the same segment. If it is not broadcast network, errors will be encountered. This command is for force self as the nexthop of the neighbor under IBGP.

Example: Switch(config-router)#neighbor 10.1.1.66 next-hop-self

17.8.3.56 neighbor override-capability

Command: neighbor {<*ip-address*>|<*TAG*>} override-capability

no neighbor {<*ip-address*>|<*TAG*>} override-capability

Function: Whether enable overriding capability negotiation. The "**no neighbor {<*ip-address*>|<*TAG*>} override-capability**" command restores the capability negotiation

Parameter: <*ip-address*>: Neighbor IP address

<*TAG*>: Name of the peer group

Default: Disabled

Command Mode: EBG route mode

Usage Guide: With this attribute, error notify due to unsupported capability negotiation the neighbors required will not be sent.

Example: Switch(config-router)#neighbor 10.1.1.64 override-capability

17.8.3.57 neighbor passive

Command: neighbor {<*ip-address*>|<*TAG*>} passive

no neighbor {<*ip-address*>|<*TAG*>} passive

Function: Configure whether the connecting request is positively sent in the connection with specified neighbor; the "**no neighbor {<*ip-address*>|<*TAG*>} passive**" command restores to positively send the connecting request

Parameter: <*ip-address*>: Neighbor IP address

<*TAG*>: Name of peer group

Default: Positively send the connecting request

Command Mode: BGP mode and address-family mode

Usage Guide: With this attribute set, the local side will not positively send the TCP connecting request after the neighbors are configured, but stays in listening mode waiting for the connecting request from partners

Example:

Switch(config-router)#neighbor 10.1.1.64 passive

After configured with this attribute and reestablishing the connection , the local side do not attempt to create connection but stays in ACTIVE state waiting for the TCP connection request from the partner

17.8.3.58 neighbor peer-group

Command: neighbor < *TAG*> peer-group

no neighbor < *TAG*> peer-group

Function: Create/delete a peer group. The "**no neighbor < *TAG*> peer-group**" command deletes a peer group

Parameter: <*TAG*>: Name of the peer group of which the largest length contains 256 characters

Default: No peer group

Command Mode: BGP mode and address-family mode

Usage Guide: By configuring the peer group, a group of peers with the same attributes will be configured at the same time so to reduce the configuration staff labor. Assign members to the peer group with neighbor <ip-address> peer-group <TAG> command

Example:

Switch(config-router)#neighbor pg peer-group

Switch(config-router)#neighbor 10.1.1.64 peer-group pg

Switch(config-router)#neighbor pg remote-as 100

17.8.3.59 neighbor peer-group （Configuring group members）

Command: neighbor <*ip-address*> peer-group <*TAG*>

no neighbor <*ip-address*> peer-group <*TAG*>

Function: Assign/delete peers in the group. The "**no neighbor <*ip-address*> peer-group <*TAG*>**" command deletes the peers from the peer group

Parameter: <*ip-address*>: Neighbor IP address

<*TAG*>: Name of peer group

Default: No peer group

Command Mode: BGP mode and address-family mode

Usage Guide: By configuring the peer group, a group of peers with the same attributes will be configured at the same time so to reduce the configuration staff labor. Create peer group with above command and assign members into the group with this command

Example: Refer to above examples

17.8.3.60 neighbor port

Command: neighbor <*ip-address*> port <*0-65535*>

no neighbor <*ip-address*> port [<*0-65535*>]

Function: Specify the TCP port number of the partner through which the communication carries. The "**no neighbor <*ip-address*> port [<*0-65535*>]**" command restore the port number to default value

Parameter: <*ip-address*>: Neighbor IP address

<*TAG*>: Name of the peer group

<*0-65535*>: TCP port number

Default: Default port number is 179

Command Mode: BGP mode and address-family mode

Usage Guide: This is a configuration when the partner may connect through ports not specified by BGP

Example: Switch(config-router)#neighbor 10.1.1.64 port 1023

17.8.3.61 neighbor prefix-list

Command: neighbor {<*ip-address*>|<*TAG*>} prefix-list <*LISTNAME*|*number*> {<*in*|*out*>}

no neighbor {<*ip-address*>|<*TAG*>} prefix-list <*LISTNAME*|*number*> {<*in*>|<*out*>}

Function: Configure the prefix restrictions applied in sending or receiving routes from specified neighbors. The "**no neighbor {<*ip-address*>|<*TAG*>} prefix-list <*LISTNAME*|*number*> {<*in*>|<*out*>}**" command cancels this configuration

Parameter: <*ip-address*>:Neighbor IP address

<*TAG*>: Name of the peer group

<*LISTNAME*|*number*>:Name or sequence number of the prefix-list

<*in*|*out*>:Direction on which the restrictions applied

Default: No prefix restrictions applied

Command Mode: BGP mode and address-family mode

Usage Guide: Specify the prefix and its scope by configuring ip prefix-list and determines whether this scope is permitted or denied. Only the route with permitted prefix will be sent or received

Example:

Switch(config)#ip prefix-list prw permit 100.1.0.0/22 ge 23 le 25

Switch(config)#router bgp 200

Switch(config-router)#redistribute static

Switch(config-router)neighbor 10.1.1.66 prefix-list prw out

17.8.3.62 neighbor remote-as

Command: neighbor {<*ip-address*>|<*TAG*>} remote-as <*as-id*>

no neighbor {<*ip-address*>|<*TAG*>} [remote-as <*as-id*>]

Function: Configure the BGP neighbor. The "**no neighbor {<*ip-address*>|<*TAG*>} [remote-as <*as-id*>]**" command is used for deleting BGP neighbors.

Parameter: <*ip-address*>: Neighbor IP address

<*TAG*>: Name of peer group

<*as-id*>: Neighbor AS number ranging between 1-65535

Default: No neighbors

Command Mode: BGP mode and address-family mode

Usage Guide: The BGP neighbors are completely generated through command configurations. A neighbor relationship can only be really established by mutual configuring. Partner AS number should be specified in configuration. The neighbor relationship can not be established when the AS number is incorrect. The partner AS number is the same with that of local side inside the AS

Example:

Switch(config)#router bgp 200

Switch(config-router)# neighbor 10.1.1.64 remote-as 100

17.8.3.63 neighbor remove-private-AS

Command: neighbor {<*ip-address*>|<*TAG*>} remove-private-AS

no neighbor {<*ip-address*>|<*TAG*>} remove-private-AS

Function: Configures whether remove the private AS number when sending to the neighbor. The "**no neighbor {<*ip-address*>|<*TAG*>} remove-private-AS**" command cancels this configuration.

Parameter: <*ip-address*>: Neighbor IP address

<*TAG*>: Name of peer group

Default: Not configured

Command Mode: BGP mode and address-family mode.

Usage Guide: Configure this attribute to avoid assigning the internal AS number to the external AS sometimes. The internal AS number ranges between 64512-65535, which the AS number could not be sent to the INTERNET since it is not a valid external AS number. What removed here is private AS numbers of the totally private AS routes. Those who have private AS numbers while also have public AS numbers are not processed.

Example: Switch(config-router)#neighbor 10.1.1.64 remove-private-AS

17.8.3.64 neighbor route-map

Command: neighbor {*<ip-address>*|*<TAG>*} route-map *<NAME>* {*<in*|*out>*}

no neighbor {*<ip-address>*|*<TAG>*} route-map *<NAME>* {*<in*|*out>*}

Function: Configure the route mapping policy when sending or receiving route. the "**no neighbor {*<ip-address>*|*<TAG>*} route-map *<NAME>* {*<in*|*out>*}**" command cancels this configuration

Parameter: *<ip-address>*: Neighbor IP address

<TAG>: Name of peer group

<NAME>: Name of route mapping

<in*|*out>: Direction of route mapping

Default: Not set

Command Mode: BGP mode and address-family mode.

Usage Guide: First it has to configure route mapping under global mode by creating a route map with route-map command and configure the match condition and actions, then the command can be applied.

Example:

Switch(config)#route-map test permit 5

Switch(config-route-map)#match interface Vlan1

Switch(config-route-map)#set as-path prepend 65532

Switch(config-route-map)#exit

Switch(config)#router bgp 200

Switch(config-router)#neighbor 10.1.1.64 route-map test out

17.8.3.65 neighbor route-reflector-client

Command: neighbor {*<ip-address>*|*<TAG>*} route-reflector-client

no neighbor {*<ip-address>*|*<TAG>*} route-reflector-client

Function: Configure the route reflector client. The "**no neighbor {*<ip-address>*|*<TAG>*} route-reflector-client**" command cancels this configuration

Parameter: *<ip-address>*: Neighbor IP address

<*TAG*>: Name of peer group

Default: Not configured

Command Mode: BGP mode and address-family mode.

Usage Guide: The route reflection is used for reducing the peers when the internal IBGP routers inside AS are too much. The client only exchanges messages with route reflector while the reflector deals with message exchange among each client and other IBGP, EBGP routers. This command configures itself as the route reflector, while specific peer group is as its client. Note: this configuration is only available inside AS

Example:

Switch(config)#router bgp 100

Switch(config-router)#neighbor 10.1.1.66 remote 100

Switch(config-router)#neighbor 10.1.1.66 route-reflector-client

Switch(config-router)#neighbor 10.1.1.68 remote 100

Switch(config-router)#neighbor 10.1.1.68 route-reflector-client

17.8.3.66 neighbor route-server-client

Command:neighbor {<*ip-address*>|<*TAG*>} route-server-client

no neighbor {<*ip-address*>|<*TAG*>} route-server-client

Function: Configure the route server client. The "**no neighbor {<*ip-address*>|<*TAG*>} route-server-client**" command cancels this configuration

Parameter: <*ip-address*>:Neighbor IP address

<*TAG*>: Name of peer group

Default: Not configured

Command Mode: BGP mode and address-family mode.

Usage Guide: The route service is for reducing the peers when the router between AS is too much under EBGP environment. The server transparently transforms the routing messages to other clients with its client exchanges messages through route server

Example:

Three routers : 10.1.1.64（AS100） and 10.1.1.68（AS300） respectively creates neighbor relationship with the connected 10.1.1.66（AS200）, the configuration is as follows

Switch(config)#router bgp 200

Switch(config-router)#neighbor 10.1.1.64 remote-as 100

Switch(config-router)#neighbor 10.1.1.64 route-server-client

Switch(config-router)# neighbor 10.1.1.68 remote-as 300

Switch(config-router)# neighbor 10.1.1.68 route-server-client

17.8.3.67 neighbor send-community

Command: neighbor {<*ip-address*>|<*TAG*>} send-community

[both|extended|standard]

no neighbor {<*ip-address*>|<*TAG*>} send-community [both|extended|standard]

Function: Configures whether sending the community attribute to the neighbors. The "**no neighbor {<*ip-address*>|<*TAG*>} send-community [both|extended|standard]**" command set to not sending.

Parameter: <*ip-address*>: IP address of the neighbor

<*TAG*>: Name of peer group

[both|extended|standard]: Standard community only, extended community or both.

Default: Sending the community attributes

Command Mode: BGP mode and address-family mode.

Usage Guide: The community attributes can be sent to the outside or not. By default of our company we set to sending while the default in standard protocol is not sending. By configuring this attribute community attributes will be carried when sending routing information's to the neighbors, or else not. Omission of the following choice will be equal to standard.

Example:

Switch(config-router)#no neighbor 10.1.1.66 send-community

Switch(config-router)#neighbor 10.1.1.66 send-community

17.8.3.68 neighbor shutdown

Command: neighbor {<*ip-address*>|<*TAG*>} shutdown

no neighbor {<*ip-address*>|<*TAG*>} shutdown

Function: Disconnect the neighbor connection. The "**no neighbor {<*ip-address*>|<*TAG*>} shutdown**" cancels this configuration

Parameter: <*ip-address*>: Neighbor IP address

<*TAG*>: Name of peer group

Default: Not disconnecting

Command Mode: BGP mode and address-family mode

Usage Guide: Directly disconnect/connect to a peer (group) without canceling the neighbor configuration

Example: Switch(config-router)#neighbor 10.1.1.64 shutdown

17.8.3.69 neighbor soft-reconfiguration inbound

Command: neighbor {<*ip-address*>|<*TAG*>} soft-reconfiguration inbound

no neighbor {<*ip-address*>|<*TAG*>} soft-reconfiguration inbound

Function: Configures whether perform inbound soft reconfiguration; the "**no neighbor**

{<*ip-address*>|<*TAG*>} soft-reconfiguration inbound" command set to not perform the inbound soft reconfiguration

Parameter: <*ip-address*>: Neighbor IP address

<*TAG*>: Name of peer group

Default: Not perform inbound soft reconfiguration

Command Mode: The system saves the inbound messages in the buffer after the soft reconfiguration is set, will applies as soon as it restarts so to reduce consumptions of switching with other routers. The command is only available when the route refresh capability is not enabled

Example: Switch(config-router)#neighbor 11.1.1.120 soft-reconfiguration inbound

17.8.3.70 neighbor soo

Command: [no] neighbor <*ip-addr*> soo <*soo-val*>

Function: Configure the origin source from the neighbor route

Parameter: The neighbor IP address show in dotted decimal notation

<*soo-val*> is the origin source ,which the format is the same with RD

Command Mode: vrf mode

Usage Guide: If the user AS connects with several ISP devices, to avoid the user route returns to itself through P area, this attribute can be set. Once this attribute is set, it spreads with route. routes carrying SOO attributes will not be spreader to a neighbor configured with the attribute

Example:

Switch(config)#ROUTER BGP 100

Switch(config-router)#address-family ipv4 vrf DC1

Switch(config-router-af)# neighbor 11.1.1.64 remote 200

Switch(config-router-af)# neighbor 11.1.1.64 soo 100:10

After this attribute set, the switch will no longer spreads the route with 100:10 rt attribute to 11.1.1.64. (what have to be mentioned here is that the soo attribute will be judged together with other rt attributes, which means if the rt is configured with the same attribute, it will be regarded as the origin neighbor even if it's not the real origin source. As a matter of fact, the normal configured soo are a single configuration which is different from rt/rd and unique within the accessible scope. In this way can only the origin concept be exactly expressed)

17.8.3.71 neighbor strict-capability-match

Command: neighbor {<*ip-address*>|<*TAG*>} strict-capability-match

no neighbor {<*ip-address*>|<*TAG*>} strict-capability-match

Function: Configure whether strict capability match is required when establishing

connections. The "**no neighbor {<*ip-address*>|<*TAG*>} strict-capability-match**" command set to not requiring strict match.

Parameter: <*ip-address*>: Neighbor IP address

<*TAG*>: Name of peer group

Default: No strict capability match configured

Command Mode: BGP mode and address-family mode.

Usage Guide: With this command, the connection can only be established when the both side are perfectly matched on capabilities.

Example: Switch(config-router)#neighbor 10.1.1.64 strict-capability-match

17.8.3.72 neighbor timers

Command: neighbor {<*ip-address*>|<*TAG*>} timers <*0-65535*> <*0-65535*>

no neighbor {<*ip-address*>|<*TAG*>} timers <*0-65535*> <*0-65535*>

Function: Configure the KEEPALIVE interval and hold time; the "**no neighbor {<*ip-address*>|<*TAG*>} timers <*0-65535*> <*0-65535*>**" command restores the defaults

Parameter: Neighbor IP address

<*TAG*>: Name of peer group

<*0-65535*>: Respectively the KEEPALIVE and HOLD TIME

Default: Default KEEPALIVE time is 60s, while HOLD TIME is 240s

Command Mode: BGP mode and address-family mode

Usage Guide: Send KEEPALIVE interval and HOLD TIME intervals sent in the peer connection. The hold time is the time period for maintain the connection when no message is received from the partner (such as KEEPALIVE). And the connection will be closed after this hold time.

Example: Switch(config-router)#neighbor 10.1.1.64 timers 50 200

17.8.3.73 neighbor timers connect

Command: neighbor {<*ip-address*>|<*TAG*>} timers connect <*0-65535*>

no neighbor {<*ip-address*>|<*TAG*>} timers connect [<*0-65535*>]

Function: Configure the connecting retry time interval. The "**no neighbor {<*ip-address*>|<*TAG*>} timers connect [<*0-65535*>]**" command restores the default value

Parameter: <*ip-address*>: Neighbor IP address

<*TAG*>: Name of peer group

<*0-65535*>: Retry interval

Default: 120s.

Command Mode: BGP mode and address-family mode

Usage Guide: Configure the connecting time interval when connecting a peer. The NO

form restores the default value.

Example: Switch(config-router)#neighbor 10.1.1.64 timers connect 100

17.8.3.74 neighbor unsuppress-map

Command: neighbor *{<ip-address>|<TAG>}* unsuppress-map <*WORD*>

no neighbor {<*ip-address*>|<*TAG*>} unsuppress-map <*WORD*>

Function: Configure or cancel the unsurprising to conditions meet the specified route map. The "**no neighbor {<*ip-address*>|<*TAG*>} unsuppress-map <*WORD*>**" command cancels this configuration

Parameter: <*ip-address*>: Neighbor IP address

<*TAG*>: Name of peer group

<*WORD*>: Name of route-map

Default: Not set

Command Mode: BGP route mode.

Usage Guide: This command is generally for route suppressed by the aggregated and summary-only conditions. Routs meet the route map conditions will still be send separately other than suppressed

Example:

Switch(config-router)#neighbor 10.1.1.66 unsuppress-map rmp

Switch(config)#access-list 10 permit 10.1.1.100 0.0.0.255

Switch(config)#route-map rmp permit 5

Switch(config-route-map)#match ip next-hop 10

Route with nexthop as 10.1.1.100 will not be restrained

17.8.3.75 neighbor update-source

Command: neighbor {<*ip-address*>|<*TAG*>} update-source <*IFNAME*>

no neighbor {<*ip-address*>|<*TAG*>} update-source <*IFNAME*>

Function: Configure the update source. The "**no neighbor {<*ip-address*>|<*TAG*>} update-source <*IFNAME*>**" cancels this configuration

Parameter: <*ip-address*>: Neighbor IP address

<*TAG*>: Name of peer group

<*IFNAME*>: Name or IP of the interface

Default: Not configured, namely use nearest interface

Command Mode: BGP route mode.

Usage Guide: Specified update source is allowed to connect with any available interface which normally is the loop back interface. The NO forms restores to the nearest interface update source. Improper update source use may lead to neighbor connection unavailable, while the invalid interface causes problem which is also the reasons we use

loop back interfaces. Note: the loop back interface should be maintained with its address accessibility to be able to establish connections when as the update source.

Example: Switch(config-router)#neighbor 10.1.1.66 update-source 192.168.0.1

17.8.3.76 neighbor version 4

Command: neighbor {<*ip-address*>|<*TAG*>} version 4

Function: Configure the BGP version of the partner

Parameter: <*ip-address*>: Neighbor IP address

<*TAG*>: Name of the peer group

4: Allowed BGP version, 4 only

Default: 4.

Command Mode: BGP route mode.

Usage Guide: Only version 4 is supported so far, so whatever the configuration is the version remains at 4.

Example: Switch(config-router)#neighbor 10.1.1.66 version 4

17.8.3.77 neighbor weight

Command: neighbor {<*ip-address*>|<*TAG*>} weight <*0-65535*>

no neighbor *{<ip-address>|<TAG>}* weight [<*0-65535*>]

Function: Configure the route weight sent from the partner. The "**no neighbor *{<ip-address>|<TAG>}* weight [<*0-65535*>]**" command restores the default value

Parameter: <*ip-address*>: Neighbor IP address

<*TAG*>: Name of IP address

<*0-65535*>: Weight

Default: The default weight acquired from other routers is 0. The default weight on the local static configuration is 32768

Command Mode: BGP route mode.

Default: The default weight acquired from other routers is 0. The default weight on the local static configuration is 32768

Usage Guide: The path selecting can be affected through the configuration of the weight. The weight is only relevant to the router which is not an attribute transmittable to outside.

Example: Switch(config-router)#neighbor 10.1.1.66 weight 500

17.8.3.78 network (BGP)

Command: network <*ip-address/M*> [route-map <*WORD*>] [backdoor]

no network <*ip-address/M*> [route-map <*WORD*>] [backdoor]

Function: Configure the BGP managed network, the route map specified in network application, or set the "back door" for the network. the "**no network <*ip-address/M*>**

[route-map <*WORD*>] [backdoor]" command cancels this configuration

Parameter: <*ip-address/M*>: Network prefix identifier

<*WORD*>: Name of route-map

Default: None

Command Mode: BGP route mode.

Usage Guide: As for BGP routes, specify the route through which the BGP advertisements go. With the network defined by this command, the peer will be spreader into the route map of the neighbor even if there is no route locally. Using the attribute specified in the network application through route map, when specifying the route comes from EBGP or inside the network through back door parameters, the inside route will be the optimized route even if the external route is of shorter distance.

Example: Switch(config-router)# network 172.16.0.0/16

17.8.3.79 redistribute (BGP)

Command: redistribute <*ROUTES*> [route-map <*WORD*>]

no redistribute <*ROUTES*> [route-map <*WORD*>]

Function: Set the BGP to redistribute route from other modes into BGO. The "**no redistribute <*ROUTES*> [route-map <*WORD*>]**" command cancels this configuration

Parameter: <*ROUTES*>: Route source or protocol, including: connected, isis, kernel, ospf, rip, static, etc.

<*WORD*>: Name of route map

Default: None

Command Mode: BGP route mode.

Usage Guide: Route from other ways will be distributed into the BGP route table with this command and transmitted to the neighbors

Example: The static route is introduced into BGP with this configuration and advertised to the neighbors

Switch(config-router)# redistribute static

17.8.3.80 rd

Command: rd <*rd-val*>

Function: Configure the VRF route identification label.

Parameter: **<*rd-val*>** is the route identification label, which normally should be（AS number or IP address）: digits, such as: 100:10

Command Mode: vrf mode

Usage Guide: Under VRF mode the configured RD is for identifying different VRF each of which shall have a unique RD; The BGP distinct routes with different VRF with this identification label. But attention should be paid on that once RD is configured, it will not

be changed. So there is no form command to cancel this configuration and you have to reconfigure VRF

Example:

Switch(config)#ip vrf DC1

Switch(config-vrf)#rd 100:10

Switch(config-vrf)#

Above example creates a VRF named DC1 with RD value at 100:10

17.8.3.81 router bgp

Command: router bgp <*as-id*> [view <*name*>]

no router bgp <*as-id*> [view <*name*>]

Function: Enable BGP instance. The "**no router bgp <*as-id*> [view <*name*>]**" command deletes BGP instance

Parameter: <*as-id*>: 1-65535 is AS number;

<*name*>: Character string which is the name and index for multiple BGP instance

Default: BGP Not enabled

Command Mode: Global mode

Usage Guide: Enable BGP by specified AS, and then enter the config-router state, the protocol can be configured at this prompt. In case no bgp multiple-instance is configured while a BGP is enabled, enabling new BGP instance will return with error. If bgp multiple-instance is configured, you can enable several BGP however the name of the instance has to be specified with view parameter. The NO form will cancel the configuration of this BGP instance.

Example:

Switch(config)#router bgp 200

Switch(config-router)#exit

Switch(config)#bgp multiple-instance

Switch(config)#router bgp 200

Switch(config-router)#exit

Switch(config)#router bgp 300 view as300

Switch(config)#no router bgp 300 view as300

Switch(config)#no router bgp 200

17.8.3.82 route-target

Command: route-target {import|export|both} <*rt-val*>

no route-target {import|export|both} <*rt-val*>

Function: Configure the route extended community attributes, so to determine whether

the route be spreader to specific VRF.

Parameter: *<rt-val>* is the same as RD form, standing for the extended community attributes of the routes.

Command Mode: vrf mode

Usage Guide: Under VRF mode, the configured RT attributes decides which VRF will accept the route. There are 3 RT configurations: the import RT stands for the RT value acceptable by this VRF, the export RT represents the RT value carried with this VRF when routing spreading, both refers to above two option both enabled. If the export RT carried with the received route ever matches with the import RT of this VRF, then this VRF will accept this route or else not (except for the no bgp inbound-route-filter is configured which enables RD match). Several RT can be configured on the same VRF. Normally we set one RT with the both mode so to equal the RD and RT_VALUE.

Example:

Switch(config)#ip vrf DC1

Switch(config-vrf)#rd 100:10

Switch(config-vrf)#route-target both 100:10

Switch(config-vrf)#

In above example is created a VRF named DC1 with RD value 100:10. the RT is configured bilateral. The RT-VALUE is equal to RD.

17.8.3.83 set vpnv4 next-hop

Command: set vpnv4 next-hop *<ip-addr>*

no set vpnv4 next-hop *<ip-addr>*

Function: Configure the nexthop of the VPNv4 route.

Parameter: *<ip-addr>*is nexthop of vpnv4 route

Command Mode:vrf mode

Usage Guide: Configure VPNv4 route nexthop with this command. As normal nexthop settings are only for IPv4 route, this command specially configures the VPNv4 address-family.

Example:

Configure the address-family as follows:

Switch(config)#route-map map1 permit 15

Switch(config-map)#match interface Vlan1

Switch(config-map)#set weight 655

Switch(config-map)#set vpnv4 next-hop 10.1.1.250

Switch(config-map)#exit

Switch(config)#router bgp 100

Switch(config-router)#neighbor 10.1.1.68 remote-as 100

Switch(config-router)#neighbor 10.1.1.68 route-map map1 in
Switch(config-router)#address-family vpnv4 unicast
Switch(config-router-af)#neighbor 10.1.1.68 activate
Switch(config-router-af)#exit-address-family
View the routing message after refresh
Switch#show ip bgp vpn all

Network	Next Hop	Metric	LocPrf	Weight	Path
Route Distinguisher: 100:10 (Default for VRF DC1)					
*> 11.1.1.0/24	11.1.1.64	0		0	200 ?
*>i15.1.1.0/24	10.1.1.250	0	100	655	200 ?
*> 20.1.1.0/24	11.1.1.64	0		0	200 ?
*>i100.1.1.0/24	10.1.1.250	0	100	655	200 ?
Route Distinguisher: 100:10					
*>i15.1.1.0/24	10.1.1.68	0	100	0	200 ?
*>i100.1.1.0/24	10.1.1.68	0	100	0	200 ?

We can see that the nexthop 10.1.1.68 of the VPN route is changed to 10.1.1.250 after applied with route-map

17.8.3.84 timers bgp

Command: timers bgp <*0-65535*> <*0-65535*>

no timers bgp [<*0-65535*> <*0-65535*>]

Function: Configure all neighbor time in BGP. The "**no timers bgp [<*0-65535*> <*0-65535*>]**" command restores these times to default value

Parameter: Respectively the KEEPALIVE interval and the hold time

Default: KEEPALIVE is 60s, , HOLD TIME is 240s.

Command Mode: BGP route mode.

Usage Guide: Similar to neighbor time configuration which just performed on all neighbors

Example: Switch(config-router)# timers bgp 50 200

17.8.4 Configuration Examples of BGP

17.8.4.1 Examples 1: configure BGP neighbor

SwitchB, SwitchC and SwitchD are in AS200, SwitchA is in AS100. SwitchA and SwitchB share the same network segment. SwitchB and SwitchD are not connected physically.

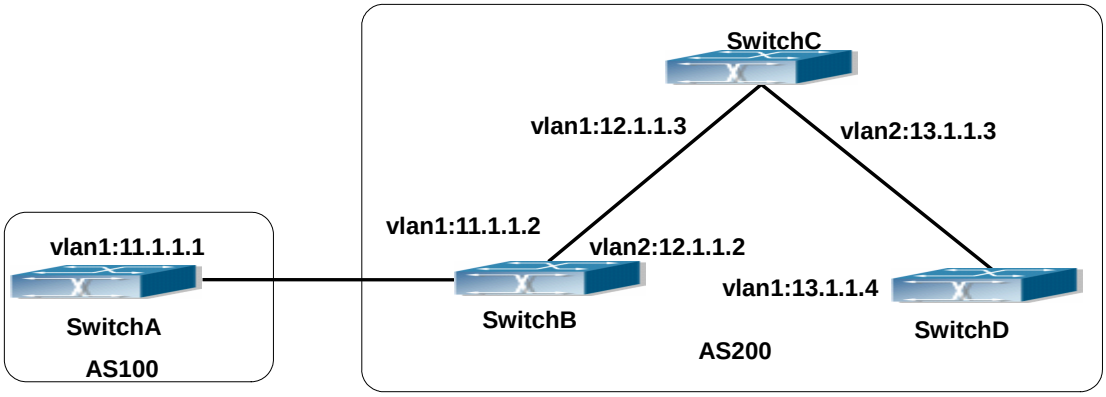


Fig 17-10BGP Network Topological Map

The configurations of SwitchA are as following:

SwitchA(config)#router bgp 100

SwitchA(config-router-bgp)#neighbor 11.1.1.2 remote-as 200

SwitchA(config-router-bgp)#exit

The configurations of SwitchB are as following:

SwitchB(config)#router bgp 200

SwitchB(config-router-bgp)#network 11.0.0.0

SwitchB(config-router-bgp)#network 12.0.0.0

SwitchB(config-router-bgp)#network 13.0.0.0

SwitchB(config-router-bgp)#neighbor 11.1.1.1 remote-as 100

SwitchB(config-router-bgp)#neighbor 12.1.1.3 remote-as 200

SwitchB(config-router-bgp)#neighbor 13.1.1.4 remote-as 200

SwitchB(config-router-bgp)#exit

The configurations of SwitchC are as following:

SwitchC(config)#router bgp 200

SwitchC(config-router-bgp)#network 12.0.0.0

SwitchC(config-router-bgp)#network 13.0.0.0

SwitchC(config-router-bgp)#neighbor 12.1.1.2 remote-as 200
SwitchC(config-router-bgp)#neighbor 13.1.1.4 remote-as 200

SwitchC(config-router-bgp)#exit

The configurations of SwitchD are as following:

SwitchD(config)#router bgp 200

SwitchD(config-router-bgp)#network 13.0.0.0
SwitchD(config-router-bgp)#neighbor 12.1.1.2 remote-as 200

SwitchD(config-router-bgp)#neighbor 13.1.1.3 remote-as 200

SwitchD(config-router-bgp)#exit

Presently, the connection between SwitchB and SwitchA is EBGP, and other connections with SwitchC and SwitchD are IBGP. SwitchB and SwitchD may have BGP connection without physical connection. But there is a precondition that these two switches must have reachable route to each other. This route can be attained through static route or IGP.

17.8.4.2 Examples 2: configure BGP aggregation

In this sample, configure route aggregation. Firstly, enable command redistribute to redistribute static route to BGP route table:

SwitchB(config)#ip route 193.0.0.0/24 11.1.12

SwitchB(config)#router bgp 100

SwitchB(config-router-bgp)#redistribute static

When there is at least one route affiliated to the specified range, the following configuration will create an aggregation route in the BGP route table. The aggregation route will be regarded as the AS from itself. More detailed route information about 193.0.0.0 will be announced.

SwitchB(config#router bgp 100

SwitchB(config-router-bgp)#aggregate 193.0.0.0/24

At the same time, the aggregation command above can be modified as following, then this switch only announce aggregation route 193.0.0.0 and forbid to announce more specified route to all the neighbors.

SwitchB(config-router-bgp)#aggregate 193.0.0.0/24 summary-only

17.8.4.3 Examples 3: configure BGP community attributes

In the following sample, “route map set-community” is used for the outgoing update to neighbor 16.1.1.6. By accessing to route in table 1 to configure special community value to “1111”, other can be announced normally.

Switch(config)#router bgp 100

Switch(config-router-bgp)#neighbor 16.1.1.6 remote-as 200

Switch(config-router-bgp)#neighbor 16.1.1.6 route-map set-community out

Switch(config-router-bgp)#exit

Switch(config)#route-map set-community permit 10

Switch(config-route-map)#match address 1

Switch(config-route-map)#set community 1111

Switch(config-route-map)#exit

```
Switch(config)#route-map set-community permit 20
Switch(config-route-map)#match address 2
Switch(config-route-map)#exit
Switch(config)#access-list 1 permit 11.1.0.0 0.0.255.255
Switch(config)#access-list 2 permit 0.0.0.0 255.255.255.255
Switch(config)#exit
Switch#clear ip bgp 16.1.1.6 soft out
```

In the following sample, configure the MED local preference of the routes from neighbor 16.1.1.6 selectively according to the route community value. All the routes that match the community list will set MED as 2000, community list com1 permits the route with community value “100 200 300”or”900 901” to pass. This route may have other community attributes. All the routes that pass community list com2 will set the local preference as 500. But the route that can’t pass both com1 and com2 will be rejected.

```
Switch(config)#router bgp 100
Switch(config-router-bgp)#neighbor 16.1.1.6 remote-as 200
Switch(config-router-bgp)#neighbor 16.1.1.6 route-map match-community in
Switch(config-router-bgp)#exit
Switch(config)#route-map match-community permit 10
Switch(config-route-map)#match community com1
Switch(config-route-map)#set metric 2000
Switch(config-route-map)#exit
Switch(config)#route-map match-community permit 20
Switch(config-route-map)#match community com2
Switch(config-route-map)#set local-preference 500
Switch(config-route-map)#exit
Switch(config)#ip community-list com1 permit 100 200 300
Switch(config)#ip community-list com1 permit 900 901
Switch(config)#ip community-list com2 permit 88
Switch(config)#ip community-list com2 permit 90
Switch(config)#exit
Switch#clear ip bgp 16.1.1.6 soft out
```

17.8.4.4 Examples 4: configure BGP confederation

The following is the configuration of an AS. As the picture illustrated, SwitchB and SwitchC establish IBGP connection. SwitchD is affiliated to AS 20.SwitchB and SwitchC establish EBGP of inner AS confederation. AS10 and AS20 form AS confederation with the AS number AS200; SwitchA belongs to AS100, SwitchB may create EBGP connection by AS200.

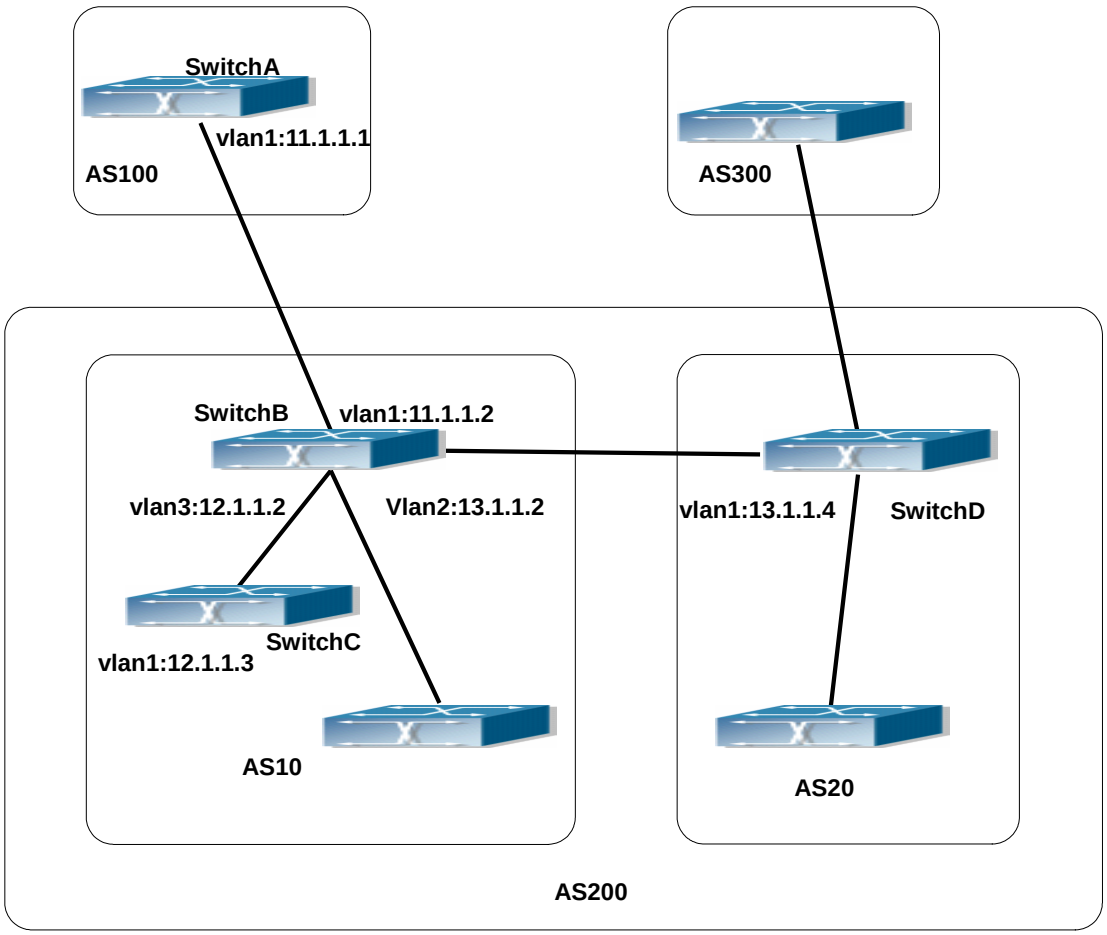


Fig 17-11 Confederation configuring topology

The configurations are as following:

SwitchA:

SwitchA(config)#router bgp 100

SwitchA(config-router-bgp)#neighbor 11.1.1.2 remote-as 200

SwitchB:

SwitchB(config)#router bgp 10

SwitchB(config-router-bgp)#bgp confederation identifier 200

SwitchB(config-router-bgp)#bgp confederation peers 20

SwitchB(config-router-bgp)#neighbor 12.1.1.3 remote-as 10

SwitchB(config-router-bgp)#neighbor 13.1.1.4 remote-as 20

SwitchB(config-router-bgp)#neighbor 11.1.1.1 remote-as 100

SwitchC:

SwitchC(config)#router bgp 10

SwitchC(config-router-bgp)#bgp confederation identifier 200

SwitchC(config-router-bgp)#bgp confederation peers 20

SwitchC(config-router-bgp)#neighbor 12.1.1.2 remote-as 10

SwitchD:

SwitchD(config)#router bgp 20
SwitchD(config-router-bgp)#bgp confederation identifier 200
SwitchD(config-router-bgp)#bgp confederation peers 10
SwitchD(config-router-bgp)#neighbor 13.1.1.2 remote-as 10

17.8.4.5 Examples 5: configure BGP route reflector

The following is the configuration of a route reflector. As the picture illustrated, SwitchA, SwitchB, SwitchC, SwitchD, SWE, SWF and SWG establish IBGP connection which is affiliated to AS100. SwitchC creates EBGP connection with AS200. SwitchA creates EBGP connection with AS300. SwitchC, SwitchD and SWG make route reflectors.

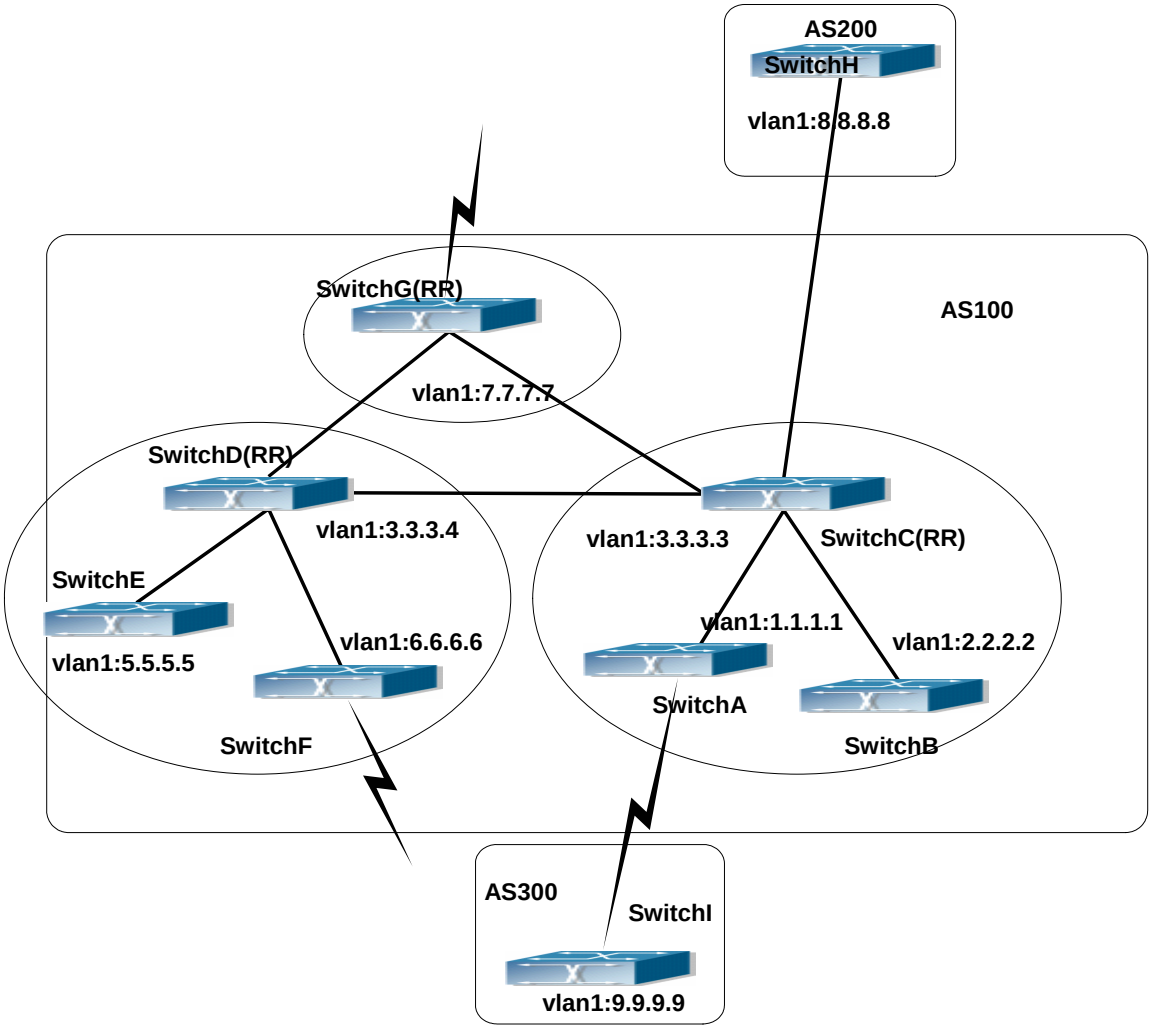


Fig 17-12 the Topological Map of Route Reflector

The configurations are as following:
The configurations of SwitchC:

SwitchC(config)#router bgp 100
SwitchC(config-router-bgp)#neighbor 1.1.1.1 remote-as 100
SwitchC(config-router-bgp)#neighbor 1.1.1.1 route-reflector-client
SwitchC(config-router-bgp)#neighbor 2.2.2.2 remote-as 100
SwitchC(config-router-bgp)#neighbor 2.2.2.2 route-reflector-client
SwitchC(config-router-bgp)#neighbor 7.7.7.7 remote-as 100
SwitchC(config-router-bgp)#neighbor 3.3.3.4 remote-as 100
SwitchC(config-router-bgp)#neighbor 8.8.8.8 remote-as 200

The configurations of SwitchD:
SwitchD(config)#router bgp 100
SwitchD(config-router-bgp)#neighbor 5.5.5.5 remote-as 100
SwitchD(config-router-bgp)#neighbor 5.5.5.5 route-reflector-client
SwitchD(config-router-bgp)#neighbor 6.6.6.6 remote-as 100
SwitchD(config-router-bgp)#neighbor 6.6.6.6 route-reflector-client
SwitchD(config-router-bgp)#neighbor 3.3.3.3 remote-as 100
SwitchD(config-router-bgp)#neighbor 7.7.7.7 remote-as 100

The configurations of SwitchA:
SwitchA(config)#router bgp 100
SwitchA(config-router-bgp)#neighbor 1.1.1.2 remote-as 100
SwitchA(config-router-bgp)#neighbor 9.9.9.9 remote-as 300

The SwitchA at this time needn’t to create IBGP connection with all the switches in the AS100 and could receive BGP route from other switches in the AS.

17.8.4.6 Examples 6: configure MED of BGP

The following is the configuration of a MED. As illustrated, SwitchA is affiliated to AS100, SwitchB is affiliated to AS400, SwitchC and SwitchD belong to AS300.

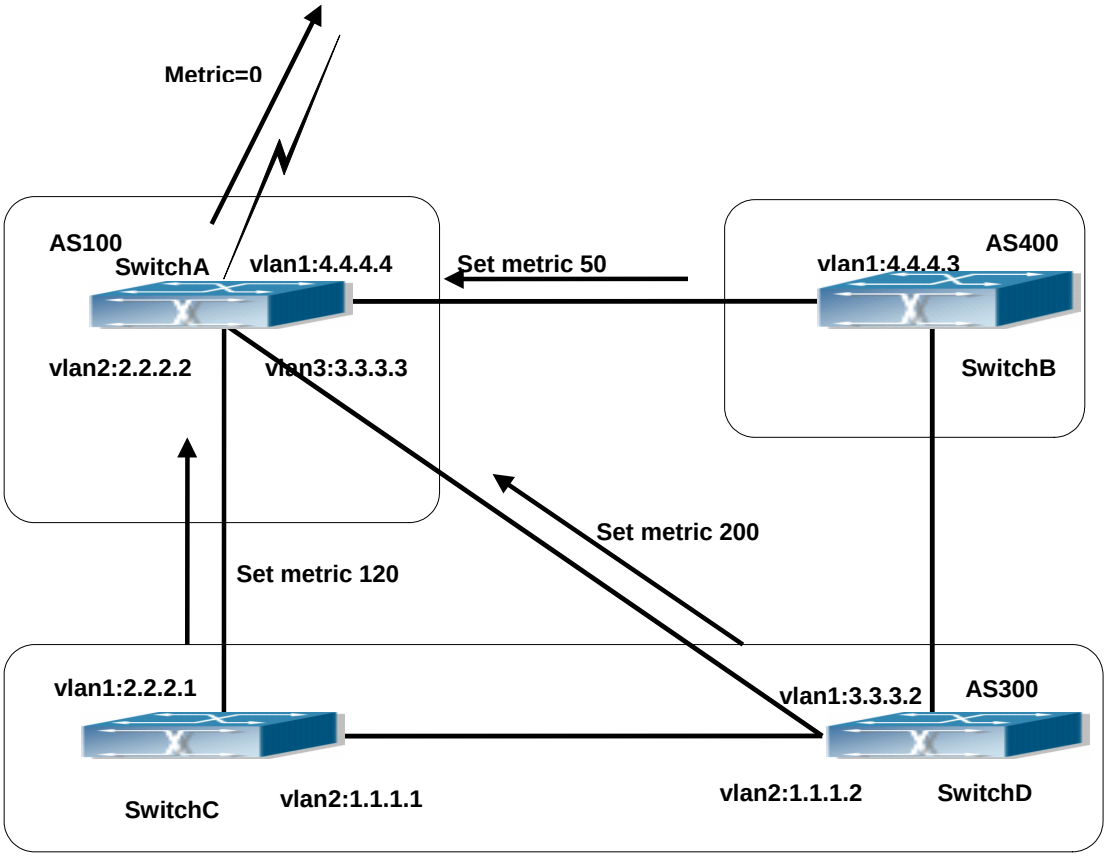


Fig 17-13 MED Configuring Topological Map

The configurations of SwitchA:

SwitchA(config)#router bgp 100

SwitchA(config-router-bgp)#neighbor 2.2.2.1 remote-as 300

SwitchA(config-router-bgp)#neighbor 3.3.3.2 remote-as 300

SwitchA(config-router-bgp)#neighbor 4.4.4.3 remote-as 400

The configurations of SwitchC:

SwitchC(config)#router bgp 300

SwitchC (config-router-bgp)#neighbor 2.2.2.2 remote-as 100

SwitchC (config-router-bgp)#neighbor 2.2.2.2 route-map set-metric out

SwitchC (config-router-bgp)#neighbor 1.1.1.2 remote-as 300

SwitchC (config-router-bgp)#exit

SwitchC (config)#route-map set-metric permit 10

SwitchC (Config-Router-RouteMap)#set metric 120

The configurations of SwitchD

SwitchD (config)#router bgp 300

SwitchD (config-router-bgp)#neighbor 3.3.3.3 remote-as 100
SwitchD (config-router-bgp)#neighbor 3.3.3.3 route-map set-metric out
SwitchD (config-router-bgp)#neighbor 1.1.1.1 remote-as 300
SwitchD (config-router-bgp)#exit
SwitchD (config)#route-map set-metric permit 10
SwitchD (Config-Router-RouteMap)#set metric 200

The configurations of SwitchB
SwitchB (config)#router bgp 400
SwitchB (config-router-bgp)#neighbor 4.4.4.4 remote-as 100
SwitchB (config-router-bgp)#neighbor 4.4.4.4 route-map set-metric out
SwitchB (config-router-bgp)#exit
SwitchB (config)#route-map set-metric permit 10
SwitchB (Config-Router-RouteMap)#set metric 50
SwitchA(config-router-bgp)# bgp always-compare-med
After the configuration above, SwitchB, SwitchC and SwitchD are assumed to send a route 12.0.0.0 to SwitchA. According to the comparison of BGP route strategy; there is an assumption that the routes sent by the three switches above have the same attribute value before the comparison of metric attribute. At this time, the route with lower value is the better route. But the comparison of metric attribute will only be done with the routes from the same AS. For SwitchA, the routes passed SwitchC are preferable to the one passed SwitchD. Because SwitchC and SwitchB are not located in the same AS, the SwitchA will not do metric comparison between the two switches. If the metric comparison between different AS is needed, the command" bgp always-compare-med" will be used. If this command is configured, the routes passed SwitchB are the best to SwitchA. At this time, the following command may be added on SwitchA: "SwitchA (config-router-bgp)# bgp always-compare-med"

17.8.5 BGP Troubleshooting

In the process of configuring and implementing BGP protocol, physical connection, configuration false probably leads to BGP protocol doesn't work. Therefore, the customers should give their attention to points as follow:

First of all, to ensure correct physical connection;

Secondly, to ensure interface and link protocol are UP (execute show interface instruction);

And startup BGP protocol (use router bgp command), configure affiliated IBGP and EBGP neighbors (use neighbor remote-as command).

Notice BGP protocol itself can't detect route, needs to import other routes to create BGP route. Only it enables these routes to announce IBGP and EBGP neighbors by importing routes. Direct-link routes, static route, and IGP route (RIP and OSPF) are included in these imported routes. Network and redistribute (BGP) command are the ways of imported routes.

For BGP, pay attention to the difference between the behaviors of IBGP and EBGP.

After configuration finishes, the command of show ip bgp summary can be used to observe neighbor's connections, so that all of the neighbors keep BGP connection situation. And use show ip bgp command to observe BGP routing table.

If BGP routing problem still can't be solved by debugging, please use debug instructions like debug ip bgp packet/events etc, and copy DEBUG information in 3 minutes, then send them to ourTechnology Service Center.

17.8.5.1 Monitor And Debug Command

17.8.5.1.1 show ip bgp

Command: show ip bgp [<*ADDRESS-FAMILY*>] [<*ip-address*>|<*ip-address/M*> [longer-prefixes]| cidr-only]

Function: For displaying the routing messages permitted by BGP

Parameter: <*ADDRESS-FAMILY*>: address-family such as "ipv4 unicast"

<*ip-address*>: IP address

<*ip-address/M*>: IP address and the mask

Default: None

Command Mode: All mode

Usage Guide: We can display BGP routing messages by different parameters (such as address-family or IPv4 address), or a route covered by a prefix, or only the routing message don't match the earliest IP address-family (namely the route is not A or B or C type address.)

Example:

```
Switch#show ip bgp
BGP table version is 147, local router ID is 10.1.1.64
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete
   Network          Next Hop            Metric LocPrf Weight Path
*> 12.0.0.0         10.1.1.121               0             32768 ?
*> 100.1.1.0/24     10.1.1.200               0             32768 ?
*> 100.1.2.0/24     10.1.1.200               0             32768 ?
*> 172.0.0.0/8      0.0.0.0                                32768 i
```

Total number of prefixes 4

17.8.5.1.2 show ip bgp attribute-info

Command: show ip bgp attribute-info

Function: Display the BGP attributes messages

Parameter: None

Default: None

Command Mode: All modes.

Usage Guide: For displaying the attribute messages permitted by BGP

Example:

Switch#sh ip bgp attribute-info

attr[1] nexthop 0.0.0.0

attr[1] nexthop 10.1.1.64

attr[3] nexthop 10.1.1.64

attr[1] nexthop 10.1.1.121

attr[2] nexthop 10.1.1.200

17.8.5.1.3 show ip bgp community

Command: show ip bgp [<*ADDRESS-FAMILY*>] community <*TYPE*> [exact-match]

Function: For displaying route permitted by BGP with community information

Parameter: <*ADDRESS-FAMILY*>: Address-family, such as “ipv4 unicast”

<*TYPE*>: Community attributes number show in AA:NN form or combination of local-AS, no-advertise, and no-export.

Default: None

Command Mode: All mode

Usage Guide: We can choose several communities at a time, exact-match shows only the perfect match entries will be displayed.

Example:

Switch#show ip bgp community

BGP table version is 10, local router ID is 10.1.1.64

Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,

S Stale

Origin codes: i - IGP, e - EGP, ? - incomplete

	Network	Next Hop	Metric	LocPrf	Weight	Path
*	100.1.1.0/24	0.0.0.0			32768	700 800 i
*>	172.0.0.0/8	0.0.0.0			32768	700 800 i

Total number of prefixes 2

17.8.5.1.4 show ip bgp community-info

Command: show ip bgp community-info

Function: For displaying the community messages permitted by BGP

Parameter: None

Default: None

Command Mode: All modes

Usage Guide: Messages in the same community multiply closable at the same time

Example:

Switch#show ip bgp community-info

Address Refcnt Community

[0x3312558] (3) 100:50

17.8.5.1.5 show ip bgp community-list

Command:show ip bgp [<*ADDRESS-FAMILY*>] community-list <*NAME*> [exact-match]

Function: For displaying the routes containing the community list messages and permitted by BGP

Parameter: <*ADDRESS-FAMILY*>: Address-family such as “ipv4 unicast”

<*NAME*>: Community list

Default: None

Command Mode: All mode

Usage Guide: Configure the community list with ip community-list command and the contained community as well. When displayed with its name, communities included in all the lists are contained

Example:

Switch(config)#ip community-list commu per 100:50

Switch#sh ip bgp community-list commu

BGP table version is 25, local router ID is 10.1.1.64

Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,

S Stale

Origin codes: i - IGP, e - EGP, ? - incomplete

	Network	Next Hop	Metric	LocPrf	Weight	Path
*	100.1.1.0/24	0.0.0.0			32768	700 800 i
*>	172.0.0.0/8	0.0.0.0			32768	700 800 i

17.8.5.1.6 show ip bgp dampening

Command: show ip bgp [<ADDRESS-FAMILY>] dampening {<dampened-paths>|<flap-statistics>|<parameters>}

Function: Display the routes permitted by BGP and relevant to the route dampening.

Parameter: <*ADDRESS-FAMILY*>: Address-family, such as “ipv4 unicast”

Default: None

Command Mode: All mode

Usage Guide: Only the surged routes will be displayed. The Parameters shows the display configuration other than specific routes. The other two options will respectively show the restrained route and the dampening (recently recovered from invalid) routing messages.

Example:

```
Switch#sh ip bgp dampening dampened-paths
BGP table version is 12, local router ID is 10.1.1.66
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete
   Network          From            Reuse     Path
*d 100.1.3.0/24     10.1.1.64       00:27:40 100 ?
Total number of prefixes 1
Switch#sh ip bgp dampening flap-statistics
BGP table version is 13, local router ID is 10.1.1.66
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete
   Network          From            Flaps  Duration  Reuse     Path
*d 100.1.3.0/24     10.1.1.64       3  00:06:05  00:27:00  100 ?
Switch#sh ip bgp dampening parameters
dampening 15 750 2000 60 15 (route-map rmp)
  Reach ability Half-Life time     : 15 min
  Reuse penalty                    : 750
  Suppress penalty                 : 2000
  Max suppress time                : 60 min
  Un-reach ability Half-Life time : 15 min
  Max penalty (ceil)               : 11999
  Min penalty (floor)              : 375
Total number of prefixes 1
```

17.8.5.1.7 show ip bgp filter-list

Command: show ip bgp [<*ADDRESS-FAMILY*>]filter-list [<*WORD* >]

Function: For displaying the routes in BGP meeting the specific AS filter list

Parameter: <*ADDRESS-FAMILY*>: address-family such as “ipv4 unicast”

<*WORD* >: AS-PATH access-list name

Default: None

Command Mode: All modes

Usage Guide: Configure AS access-list with ip as-path access-list command. This command can show the routes passed the access-list.

Example:

Switch#SH IP BGP filter-list FL

BGP table version is 2, local router ID is 11.1.1.100

Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,

S Stale

Origin codes: i - IGP, e - EGP, ? - incomplete

	Network	Next Hop	Metric	LocPrf	Weight	Path
*>	100.1.1.0/24	10.1.1.64	0		0	100 ?

Total number of prefixes 1

17.8.5.1.8 show ip bgp inconsistent-as

Command: show ip bgp [<*ADDRESS-FAMILY*>]inconsistent-as

Function: For displaying routes with inconsistent BGP AS

Parameter: <*ADDRESS-FAMILY*>: address family such as “ipv4 unicast”

Default: None

Command Mode: All modes

Usage Guide: If same prefix comes from different origin AS, the AS will be regarded as inconsistent. This command is for displaying this kind of routes.

Example:

Switch#sh ip bgp inconsistent-as

BGP table version is 2, local router ID is 11.1.1.100

Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,

S Stale

Origin codes: i - IGP, e - EGP, ? - incomplete

	Network	Next Hop	Metric	LocPrf	Weight	Path
*	100.1.1.0/24	10.1.1.68	0		0	300 ?
*>		10.1.1.64	0		0	100 ?

Total number of prefixes 1

17.8.5.1.9 show ip bgp neighbors

Command: show ip bgp [<*ADDRESS-FAMILY*>] neighbors [IP-ADDRESS] [advertised-routes|received {prefix-filter|routes}|routes]

Function: For displaying the BGP neighbor related messages

Parameter: <*ADDRESS-FAMILY*>: Address-family, such as “ipv4 unicast”

<*ip-address*>: Neighbor IP address

Default: None

Command Mode: All mode

Usage Guide: Display detailed messages of all neighbors by this command without parameters. Specifying IP address will show the detailed information of the neighbors with specified IP address. The advertised-routes、received prefix-filter、received routes、routes parameters will respectively displays the routes broadcast on local side, the received prefix filter, received routes (soft reconfiguration enabled) and the routing message from specific neighbor

Example:

```
Switch#sh ip bgp neighbor
BGP neighbor is 10.1.1.66, remote AS 200, local AS 100, external link
  BGP version 4, remote router ID 11.1.1.100
  BGP state = Established, up for 00:13:43
  Last read 00:13:43, hold time is 240, keep alive interval is 60 seconds
  Neighbor capabilities:
    Route refresh: advertised and received (old and new)
    Address family IPv4 Unicast: advertised and received
  Received 17 messages, 0 notifications, 0 in queue
  Sent 17 messages, 0 notifications, 0 in queue
  Route refresh request: received 0, sent 0
  Minimum time between advertisement runs is 30 seconds

 For address family: IPv4 Unicast
  BGP table version 2, neighbor version 2
  Index 1, Offset 0, Mask 0x2
  Community attribute sent to this neighbor (both)
  0 accepted prefixes
  1 announced prefixes
 Connections established 7; dropped 6
```

17.8.5.1.10 show ip bgp paths

Command: show ip bgp [<*ADDRESS-FAMILY*>] paths

Function: Display the path message permitted by BGP

Parameter: <*ADDRESS-FAMILY*>: Address-family such as “ipv4 unicast”

Default: None

Command Mode: All modes

Usage Guide: Display the BGP path message includes the utilization state.

Example:

```
Switch#sh ip bgp paths
Address          Refcnt Path
```

[0x331dad0:0] (1)

[0x331d850:93] (1) 600

[0x331d8d8:249] (2) 200 300

17.8.5.1.11 show ip bgp prefix-list

Command: show ip bgp [<*ADDRESS-FAMILY*>] prefix-list [<*NAME*>]

Function: For displaying the route meet the specific prefix-list in BGP.

Parameter: <*ADDRESS-FAMILY*>: Address family such as “ipv4 unicast”

<*NAME*>: Name of prefix-list

Default: None

Command Mode: All mode

Usage Guide: We can select the required BGP route by regular expression

Example:

Switch(config)#ip prefix-list PL permit any

Switch(config)#

Switch#sh ip bgp prefix-list PL

BGP table version is 1, local router ID is 10.1.1.64

Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,

S Stale

Origin codes: i - IGP, e - EGP, ? - incomplete

	Network	Next Hop	Metric	LocPrf	Weight	Path
*	100.1.1.0/24	10.1.1.66			0	200 300 ?
*>		10.1.1.100	0		32768	?

Total number of prefixes 1

17.8.5.1.12 show ip bgp quote-regexp

Command: show ip bgp [<*ADDRESS-FAMILY*>] quote-regexp [<WORD>]

Function: For displaying the BGP route meets the specific AS related regular expression.

Parameter: <ADDRESS-FAMILY>: **>**: address-family such as “ipv4 unicast”

<WORD>: Regular expression

Default: None

Command Mode: All modes

Usage Guide: Selecting the required route through regular expressions.

Example:

Switch#sh ip bgp quote-regexp ^300$

BGP table version is 2, local router ID is 11.1.1.100

Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,

S Stale

Origin codes: i - IGP, e - EGP, ? - incomplete

	Network	Next Hop	Metric	LocPrf	Weight	Path
*>	100.1.1.0/24	10.1.1.68	0		0	300 ?

Total number of prefixes 1

Switch#sh ip bgp quote-regexp 100

BGP table version is 2, local router ID is 11.1.1.100

Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,

S Stale

Origin codes: i - IGP, e - EGP, ? - incomplete

	Network	Next Hop	Metric	LocPrf	Weight	Path
*	100.1.1.0/24	10.1.1.64	0		0	500 100 600 ?

Total number of prefixes 1

Relevant Commands: None

17.8.5.1.13 show ip bgp regexp

Command: show ip bgp [<*ADDRESS-FAMILY*>] regexp [<*LINE*>]

Function: For displaying the BGP routes meets specific AS related normal expressions

Parameter: <*ADDRESS-FAMILY*>: **>**: address-family such as “ipv4 unicast”

<*LINE*>: Regular expression

Default: None

Command Mode: all modes.

Usage Guide: We can select BGP route of the required AS with normal expression

Example:

Switch#sh ip bgp regexp 100

BGP table version is 2, local router ID is 11.1.1.100

Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,

S Stale

Origin codes: i - IGP, e - EGP, ? - incomplete

	Network	Next Hop	Metric	LocPrf	Weight	Path
*	100.1.1.0/24	10.1.1.64	0		0	500 100 600 ?

Total number of prefixes 1

Relevant Commands: None

17.8.5.1.14 show ip bgp route-map

Command: show ip bgp [<*ADDRESS-FAMILY*>] route-map [<*NAME*>]

Function: For displaying the BGP routes meets the specific related route map

Parameter: <*ADDRESS-FAMILY*>: such as “ipv4 unicast”

<*NAME*>: Name of route map

Default: None

Command Mode: All modes

Usage Guide: Configure the route map with the route-map command, through which it can be displayed that process routes with route map. The command will display the routes meet specific route map

Example:

```
Switch#sh ip bgp route-map rmp
BGP table version is 2, local router ID is 11.1.1.100
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
                S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          Next Hop            Metric LocPrf Weight Path
*  100.1.1.0/24     10.1.1.64                0             0 500 100 600 ?
*>                  10.1.1.68                0             0 300 ?

Total number of prefixes 1
```

Relevant Commands: route-map, neighbor route-map

17.8.5.1.15 show ip bgp scan

Command: show ip bgp scan

Function: For displaying BGP scan messages

Parameter: None

Default: None

Command Mode: All modes.

Usage Guide: Scan regularly the nexthop messages. The command can show the current interval and related routes.

Example:

```
Switch#show ip bgp scan
BGP Instance: (Default) AS 200, router-id 11.1.1.100
BGP scan interval is 60
Current BGP nexthop cache:
```

Relevant Commands: bgp scan-time

17.8.5.1.16 show ip bgp summary

Command: show ip bgp [<*ADDRESS-FAMILY*>] summary

Function: For displaying the BGP summary information

Parameter: ***<ADDRESS-FAMILY>***: Address-family such as “ipv4 unicast”

Default: None

Command Mode: All modes

Usage Guide: Display some basic summary information of BGP

Example:

Switch#show ip bgp summary

BGP router identifier 10.1.1.66, local AS number 200

BGP table version is 1

1 BGP AS-PATH entries

0 BGP community entries

Neighbor	V	AS	MsgRcvd	MsgSent	TblVer	InQ	OutQ	Up/Down	State/PfxRcd
10.1.1.68	4	300	0	0	0	0	0	never	Active

Total number of neighbors 1

Relevant Commands: None

17.8.5.1.17 show ip bgp view

Command: show ip bgp view [<*NAME*>] [<*ip-address*>|<*ip-address/M*>|[<*ADDRESS-FAMILY*>] summary]

Function: For displaying the messages of specified BGP instance

Parameter: ***<NAME>***: Name of BGP instance

<ip-address>: IP address

<ip-address/M>: IP address and mask

<ADDRESS-FAMILY>: Address-family such as “ipv4 unicast”

Default: None

Command Mode: All modes

Usage Guide: Display messages of specified BGP instance

Example:

Switch#show ip bgp view as300 100.1.1.0/24

Relevant Commands: router bgp

17.8.5.1.18 show ip bgp view neighbors

Command: show ip bgp view [<*NAME*>] neighbors [<*ip-address*>]

Function: Display neighbor messages of specified BGP instance

Parameter: <*NAME*>: Name of BGP instance

<*ip-address*>: neighbor IP address

Default: None

Command Mode: All mode

Usage Guide: Display neighbor messages of specified BGP instance

Example:

Switch#show ip bgp view as300 neighbors

Relevant Commands: None

17.8.5.1.19 show ip bgp vpnv4

Command: show ip bgp vpnv4 {all|rd <*rd-val*>|vrf <*vrf-name*>}

Function: Display the BGP VPN routing messages

Parameter: **<*rd-val*>** is the route identification label which is normally the （AS number or IP address）: digits, such as 100:10; **<*vrf-name*>** is the name of VRF, created through if vrf <*vrf-name*> command

Command Mode: All modes

Usage Guide: Available to display by specified RD or VRF.

Example:

Switch#sh ip bgp vpn all

Network	Next Hop	Metric	LocPrf	Weight	Path
Route Distinguisher: 100:10 (Default for VRF DC1)					
*> 11.1.1.0/24	11.1.1.64	0		0	200 ?
*> 20.1.1.0/24	11.1.1.64	0		0	200 ?

17.8.5.1.20 debug bgp

Command: debug bgp [<*MODULE*>|all]

no debug bgp [<*MODULE*>|all]

Function: For BGP debugging. the "**no debug bgp [<*MODULE*>|all]**" command closes the BGP debugging messages

Parameter: **<*MODULE*>**: BGP module names, including dampening、events、filters、fsm、keepalives、nsm、updates, etc.

Default: None

Command Mode: Admin mode and global mode

Usage Guide: For monitoring BGP events and the encountered errors, warning messages.

Example: Switch#debug bgp all

17.9 MBGP4+

17.9.1 MBGP4+ Introduction

MBGP4+ is multi-protocol BGP (Multi-protocol Border Gateway Protocol) extension to IPv6, referring to BGP protocol chapter about BGP protocol introduction in this manual. Different from RIPng and OSPFv3, BGP has no corresponding independent protocol for IPv6, instead,it takes extensions to address families on the original BGP. The extensions to BGP by MBGP4+ are mostly embodied:

a. neighbor address configured can be IPv6 address;

b. Increase IPv6 unicast address family configuration.

17.9.2 MBGP4+ Configures Mission List

1. Configure IPv6 neighbor

2. Configure and enable IPv6 address family

3. Configure IPv6 neighbor

Command	Explanation
BGP Protocol Configuration Mode	
neighbor <X:X::X:X> remote-as ***<as-id>***	Configure IPv6 neighbor

4. Configure and activate IPv6 address family

Command	Explanation
BGP Protocol Configuration Mode	
address-family IPv6 unicast	Enter IPv6 unicast address family
BGP protocol address family comfiguration mode	
（no）neighbor <X:X::X:X> activate	Configure IPv6 neighbor to activate/inactivate the address family
exit-address-family	Exit address family configuration mode

17.9.3 MBGP4+ Examples

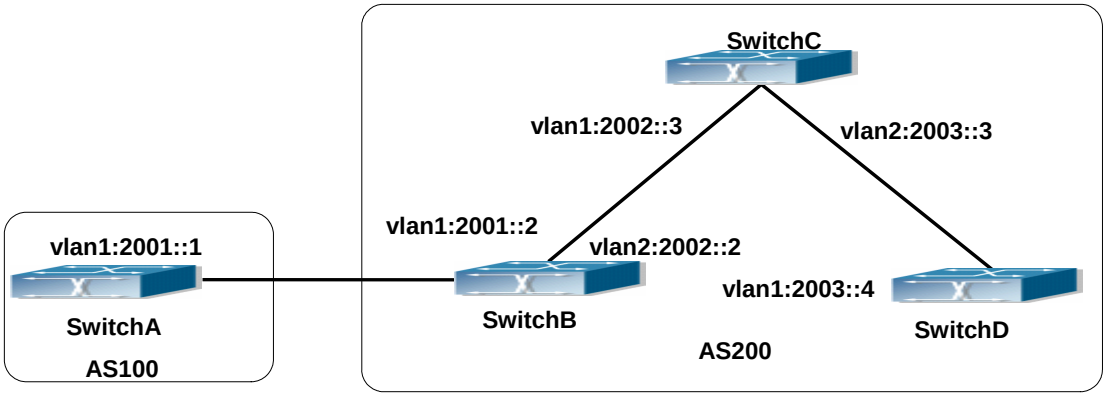


Fig 17-14 BGP Network Topological Map

Accordingly SwitchA configuration as follows:

SwitchA(config)#router bgp 100

SwitchA(config-router-bgp)#neighbor 2001::2 remote-as 200

SwitchA(config-router-bgp)#address-family IPv6 unicast

SwitchA(config-router-af)#neighbor 2001::2 activate

SwitchA(config-router-af)#exit-address-family

SwitchA(config-router-bgp)#exit

SwitchA(config)#

SwitchB configuration as follows:

SwitchB(config)#router bgp 200

SwitchB(config-router-bgp)#neighbor 2001::1 remote-as 100

SwitchB(config-router-bgp)#neighbor 2002::3 remote-as 200

SwitchB(config-router-bgp)#neighbor 2003::4 remote-as 200

SwitchB(config-router-bgp)#address-family IPv6 unicast

SwitchB(config-router-af)#neighbor 2001::1 activate

SwitchB(config-router-af)#neighbor 2002::3 activate

SwitchB(config-router-af)#neighbor 2003::4 activate

SwitchB(config-router-af)#exit-address-family

SwitchB(config-router-bgp)#exit

SwitchB(config)#

SwitchC configuration as follows:

SwitchC(config)#router bgp 200

SwitchC(config-router-bgp)#neighbor 2002::2 remote-as 200

SwitchC(config-router-bgp)#neighbor 2003::4 remote-as 200

SwitchC(config-router-bgp)#address-family IPv6 unicast

SwitchC(config-router-af)#neighbor 2002::2 activate

SwitchC(config-router-af)#neighbor 2003::4 activate
SwitchC(config-router-af)#exit-address-family
SwitchC(config-router-bgp)#exit

SwitchD configuration as follows:
SwitchD(config)#router bgp 200
SwitchD(config-router-bgp)#neighbor 2003::3 remote-as 200
SwitchD(config-router-bgp)#neighbor 2002::2 remote-as 200
SwitchD(config-router-bgp)#address-family IPv6 unicast
SwitchD(config-router-af)#neighbor 2002::2 activate
SwitchD(config-router-af)#neighbor 2003::3 activate
SwitchD(config-router-af)#exit-address-family
SwitchD(config-router-bgp)#exit
Here the connection between SwitchB and SwitchA is EBGP, and the connection between SwitchC and SwitchD is IBGP. The BGP connection can be processed between SwitchB and SwitchD without physical link, but the premise is a route which reaches from one switch to the other switch. The route can be obtained by static routing or IGP.

17.9.4 MBGP4+ Troubleshooting

It is the same as corresponding section of BGP

Chapter 18 IGMP Snooping

18.1 Introduction to IGMP Snooping

IGMP (Internet Group Management Protocol) is a protocol used in IP multicast. IGMP is used by multicast enabled network device (such as a router) for host membership query, and by hosts that are joining a multicast group to inform the router to accept packets of a certain multicast address. All those operations are done through IGMP message exchange. The router will use a multicast address (224.0.0.1) that can address to all hosts to send a IGMP host membership query message. If a host wants to join a multicast group, it will reply to the multicast address of that a multicast group with a IGMP host membership reports a message.

IGMP Snooping is also referred to as IGMP listening. The switch prevents multicast traffic from flooding through IGMP Snooping, multicast traffic is forwarded to ports associated to multicast devices only. The switch listens to the IGMP messages between the multicast router and hosts, and maintains multicast group forwarding table based on the listening result, and can then decide to forward multicast packets according to the forwarding table.

ES4626/ES4650 switch provides IGMP Snooping and is able to send a query from the switch so that the user can use ES4626/ES4650 switch in IP multicast.

18.2 IGMP Snooping Configuration Task

1. Enable IGMP Snooping
2. Configure IGMP Snooping
3. Configure sending of IGMP Query

1. Enable IGMP Snooping

Command	Explanation
Global Mode	
ip igmp snooping **no ip igmp snooping**	Enables IGMP Snooping

2. Configure IGMP Snooping

Command	Explanation
Global Mode	
ip igmp snooping vlan <*vlan-id*> **no ip igmp snooping vlan <*vlan-id*>**	Enables IGMP Snooping for specified VLAN
ip igmp snooping vlan <*vlan-id*> mrouter interface <*interface –name*> **no ip igmp snooping vlan <*vlan-id*> mrouter**	Sets the specified VLAN the port for connecting M-router
ip igmp snooping vlan <*vlan-id*> immediate-leave **no ip igmp snooping vlan <*vlan-id*> immediate-leave**	Enables IGMP Snooping in the specified VLAN to quickly leave multicast group
ip igmp snooping vlan <*vlan-id*> static <*multicast-ip-addr*> interface <*interface –name*> **no ip igmp snooping vlan <*vlan-id*> static <*multicast-ip-addr*>**	Configures a static multicast address and port member to join

3. Configure IGMP to send Query

Command	Explanation
Global Mode	
ip igmp snooping vlan <*vlan-id*> query **no ip igmp snooping vlan <*vlan-id*> query**	Enables IGMP Snooping of a specified VLAN to send a query
ip igmp snooping vlan <*vlan-id*> query robustness <*robustness-variable*> **no ip igmp snooping vlan <*vlan-id*> query robustness**	Sets the robustness parameter for IGMP Snooping Queries of a specified VLAN
ip igmp snooping vlan <*vlan-id*> query interval <*interval-value*> **no ip igmp snooping vlan <*vlan-id*> query interval**	Sets the query interval for IGMP Snooping Query of a specified VLAN
ip igmp snooping vlan <*vlan-id*> query max-response-time <*time-value*> **no ip igmp snooping vlan <*vlan-id*> query max-response-time**	Sets the maximum response time for IGMP Snooping Query of specified VLAN

18.3 Commands for IGMP Snooping

18.3.1 ip igmp snooping

Command:ip igmp snooping

no ip igmp snooping

Function: Enable the IGMP Snooping function: the " **no ip igmp snooping"** command disables this function**.**

Command mode: Global Mode

Default: IGMP Snooping is disabled by default.

Usage Guide: Use this command to enable IGMP Snooping, that is permission every vlan config the function of IGMP snooping. the " **no ip igmp snooping"** command disables this function**.**

Example: Enable IGMP Snooping.

Switch(Config)#ip igmp snooping

18.3.2 ip igmp snooping vlan

Command: ip igmp snooping vlan <*vlan-id*>

no ip igmp snooping vlan <*vlan-id*>

Function: Enable the IGMP Snooping function for the specified VLAN: the "**no ip igmp snooping vlan <vlan-id>**" command disables the IGMP Snooping function for the specified VLAN.

Parameter: <*vlan-id*> is the VLAN number.

Command mode: Global Mode

Default: IGMP Snooping is disabled by default.

Usage Guide: IGMP Snooping for the switch must be enabled first to enable IGMP Snooping for the specified VLAN. This command cannot be used with **ip igmp snooping vlan <*vlan-id*> query** command, i.e. either snooping or query can be enabled for one VLAN, but not both.

Example: Enable IGMP Snooping for VLAN 100 in Global Mode.

Switch(Config)#ip igmp snooping vlan 100

18.3.3 ip igmp snooping vlan immediate-leave

Command: ip igmp snooping vlan <*vlan-id*> immediate-leave

no ip igmp snooping vlan <*vlan-id*> immediate-leave

Function: Enable the IGMP fast leave function for the specified VLAN: the "**no ip igmp**

snooping vlan <vlan-id> immediate-leave" command disables the IGMP fast leave function.

Parameter: <*vlan-id*> is the VLAN number specified.

Command mode: Global Mode

Default: This function is disabled by default.

Usage Guide: Enabling IGMP fast leave function speeds up the process for port to leave multicast group. This command is valid only in Snooping, and is not applicable to Query.

Example: Enable the IGMP fast leave function for VLAN 100.

Switch(Config)#ip igmp snooping vlan 100 immediate-leave

18.3.4 ip igmp snooping vlan l2-general-querier

Command: ip igmp snooping vlan < *vlan-id* > l2-general-querier

no ip igmp snooping vlan < *vlan-id* > l2-general-querier

Function: Set this vlan to layer 2 general querier

Parameter: *vlan-id*: is ID number of the VLAN, ranging between <1-4094>

Command Mode: Global mode

Default: vlan is not as the IGMP Snooping layer 2 general querier

Usage Guide: It is recommended to configure a layer 2 general querier on a segment. IGMP Snooping function will be enabled by this command if not enabled on this vlan before configuring this command, IGMP Snooping function will not be disabled when disabling the layer 2 general querier function. This command is mainly for sending general queries regularly to help switches within this segment learn mrouter ports.

Comment: There are three paths igmp snooping learn mrouter

1 Port receives the IGMP query messages

2 Port receives multicast protocol packets, and supports DVMRP, PIM.

3 Static configured port

18.3.5 ip igmp snooping vlan limit

Command: ip igmp snooping vlan <*vlan-id*>

no ip igmp snooping vlan <*vlan-id*>

Function: Enable the IGMP Snooping function for the specified VLAN: the "**no ip igmp snooping vlan <vlan-id>**" command disables the IGMP Snooping function for the specified VLAN.

Parameter: <*vlan-id*> is the VLAN number.

Command mode: Global Mode

Default: IGMP Snooping is disabled by default.

Usage Guide: IGMP Snooping for the switch must be enabled first to enable IGMP Snooping for the specified VLAN. This command cannot be used with **ip igmp snooping**

vlan <*vlan-id*> query command, i.e. either snooping or query can be enabled for one VLAN, but not both.

Example: Enable IGMP Snooping for VLAN 100 in Global Mode.

Switch(Config)#ip igmp snooping vlan 100

18.3.6 ip igmp snooping vlan mrouter-port interface

Command: ip igmp snooping vlan <*vlan-id*> mrouter-port interface (<*ethernet*>|<*ifname*>|<*port-channel*>)

no ip igmp snooping vlan <*vlan-id*> mrouter-port interface (<*ethernet*>|<*ifname*>|<*port-channel*>)

Function: Configure static mrouter port of vlan. The "**no ip igmp snooping vlan <*vlan-id*> mrouter-port interface (<*ethernet*>|<*ifname*>|<*port-channel*>)**" command cancels this configuration

Parameter: *vlan-id*: ranging between <1-4094>

ethernet: Name of Ethernet port

ifname: Name of interface

***port-channel*: Port aggregation**

Command Mode: Global mode

Default: No static mrouter port on vlan by default.

Usage Guide: When a port is a static mrouter port while also a dynamic mrouter port, it should be taken as a static mrouter port. Deleting static mrouter port can only be realized by the "**no ip igmp snooping vlan <*vlan-id*> mrouter-port interface (<*ethernet*>|<*ifname*>|<*port-channel*>)**" command.

Example: Switch(config)#ip igmp snooping vlan 2 mrouter-port interface ethernet

18.3.7 ip igmp snooping vlan mrpt

Command: ip igmp snooping vlan <*vlan-id*> mrpt <*value*>

no ip igmp snooping vlan <*vlan-id*> mrpt

Function: Configure this survive time of mrouter port

Parameter: *vlan-id*: vlan id , ranging between <1-4094>

value: mrouter port survive period, ranging between <1-65535>seconds

Command Mode: Global mode

Default: 255s

Usage Guide: This command validates on dynamic mrouter ports but not on mrouter port. To use this command, IGMP Snooping of this vlan should be enabled previously.

Example: Switch(config)#ip igmp snooping vlan 2 mrpt 100

18.3.8 ip igmp snooping vlan query-interval

Command: ip igmp snooping vlan <*vlan-id*> query-interval <*value*>

no ip igmp snooping vlan <*vlan-id*> query-interval

Function: Configure this query interval

Parameter: *vlan-id*: vlan id , ranging between <1-4094>

value: query interval, ranging between <1-65535>seconds

Command Mode: Global mode

Default: 125s

Usage Guide: It is recommended to use the default settings. Please keep this configure in accordance with IGMP configuration as possible if layer 3 IGMP is running.

Example: Switch(config)#ip igmp snooping vlan 2 query-interval 130

18.3.9 ip igmp snooping vlan query-mrsp

Command: ip igmp snooping vlan <*vlan-id*> query-mrsp <*value*>

no ip igmp snooping vlan <*vlan-id*> query-mrsp

Function: Configure the maximum query response period. The "**no ip igmp snooping vlan <*vlan-id*> query-mrsp**" command restores to the default value

Parameter: *vlan-id*: vlan id , ranging between <1-4094>

value: query interval, ranging between <1-25> seconds

Command Mode: Global mode

Default: 10s

Usage Guide: It is recommended to use the default settings. Please keep this configure in accordance with IGMP configuration as possible if layer 3 IGMP is running.

Example: Switch(config)#ip igmp snooping vlan 2 query-mrsp 18

18.3.10 ip igmp snooping vlan query-robustness

Command: ip igmp snooping vlan <vlan-id> query-robustness <*value*>

no ip igmp snooping vlan <vlan-id> query-robustness

Function: Configure the query robustness. The "**no ip igmp snooping vlan <vlan-id> query-robustness**" command restores to the default value

Parameter: *vlan-id*: vlan id , ranging between <1-4094>

value: query interval, ranging between <2-10> seconds

Command Mode: Global mode

Default: 2

Usage Guide: It is recommended to use the default settings. Please keep this configure

in accordance with IGMP configuration as possible if layer 3 IGMP is running.

Example: Switch(config)#ip igmp snooping vlan 2 query- robustness 3

18.3.11 ip igmp snooping vlan suppression-query-time

Command: ip igmp snooping vlan <*vlan-id*> suppression-query-time <*value*>

no ip igmp snooping vlan <*vlan-id*> suppression-query-time

Function: Configure the suppression query time. The "**no ip igmp snooping vlan <*vlan-id*> suppression-query-time**" command restores to the default value

Parameter: *vlan-id*: vlan id , ranging between <1-4094>

value: query interval, ranging between<1-65535> seconds

Command Mode: Global mode

Default: 255s

Usage Guide: This command can only be configured on L2 general querier. The Suppression-query-time refers to the period of suppression state in which the querier enters when receives query from the layer 3 IGMP in the segments.

Example: Switch(config)#ip igmp snooping vlan 2 suppression-query-time 270

18.4 IGMP Snooping Example

Scenario 1. IGMP Snooping function

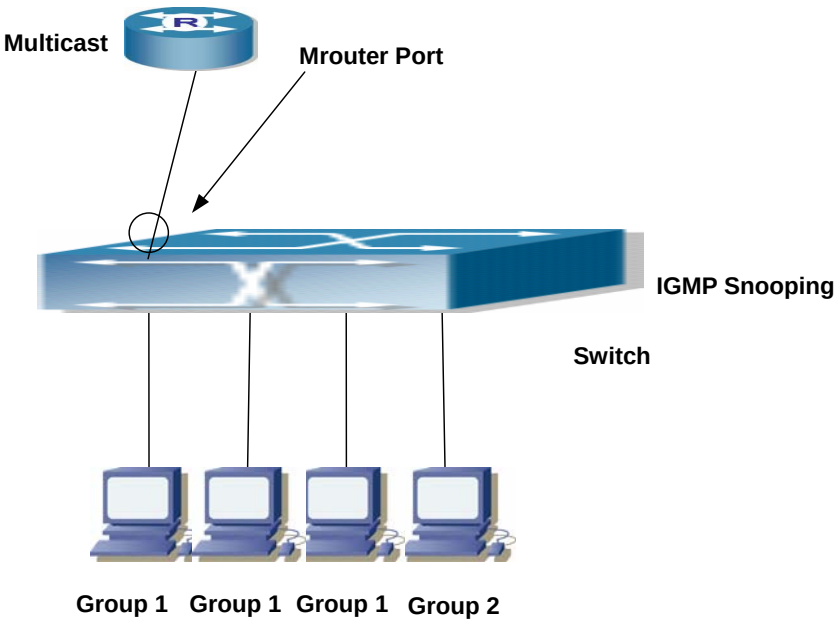


Fig 18-1 Enabling IGMP Snooping function

Example: As shown in the above figure, a VLAN 100 is configured in the switch and

includes ports 1, 2, 6, 10 and 12. Four hosts are connected to port 2, 6, 10, 12 respectively and the multicast router is connected to port 1. As IGMP Snooping is disabled by default either in the switch or in the VLANs, If IGMP Snooping should be enabled in VLAN 100, the IGMP Snooping should be first enabled for the switch in Global Mode and in VLAN 100 and set port 1 of VLAN 100 to be the M-Router port.

The configuration steps are listed below:

Switch#config
Switch(Config)#ip igmp snooping
Switch(Config)#ip igmp snooping vlan 100
Switch(Config)#ip igmp snooping vlan 100 mrouter interface ethernet 1/1

Multicast Configuration

Suppose two programs are provided in the Multicast Server using multicast address Group1 and Group2, three of four hosts running multicast applications are connected to port 2, 6, 10 plays program1, while the host is connected to port 12 plays program 2.

IGMP Snooping listening result:

The multicast table built by IGMP Snooping in VLAN 100 indicates ports 1, 2, 6, 10 in Group1 and ports 1, 12 in Group2.

All the four hosts can receive the program of their choice: ports 2, 6, 10 will not receive the traffic of program 2 and port 12 will not receive the traffic of program 1.

Scenario 2. IGMP Query

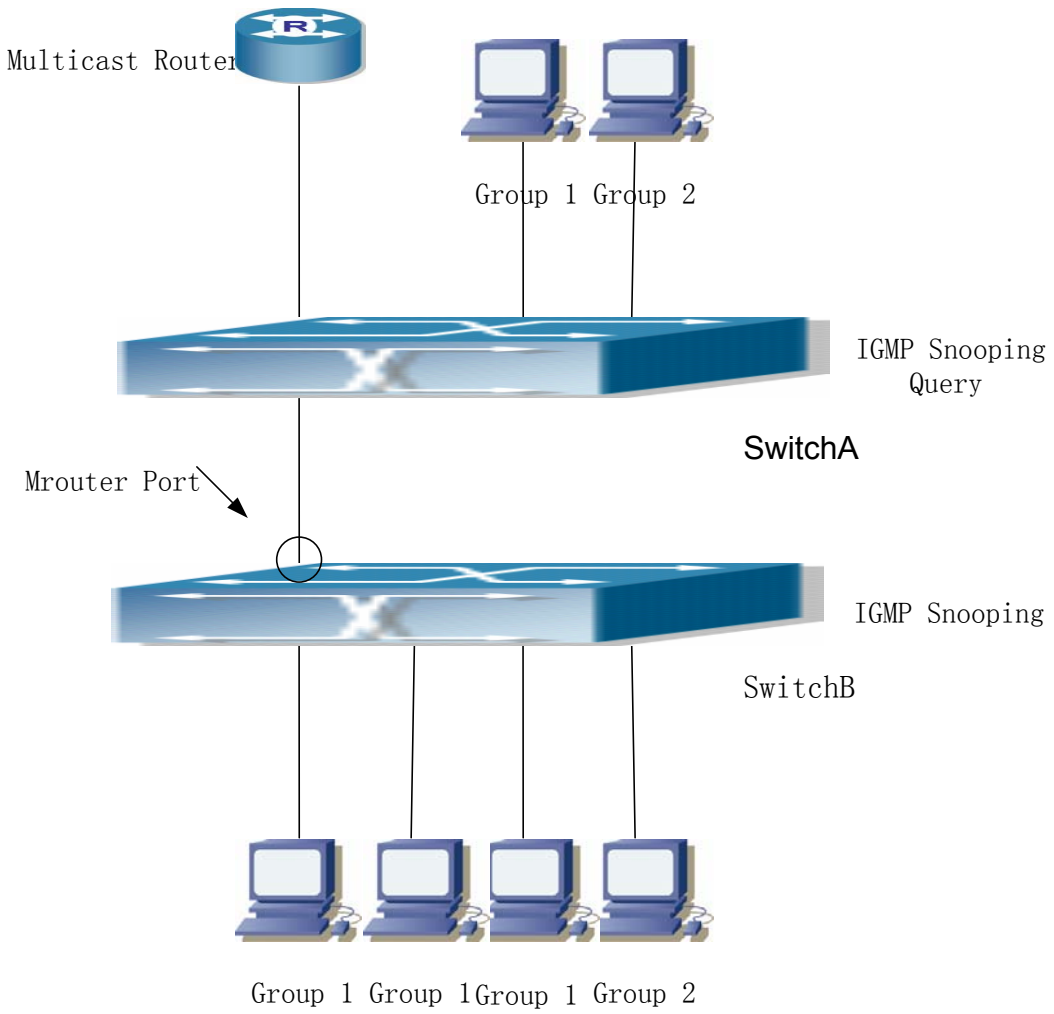


Fig 18-2 The switches as IGMP Queries

The configuration of SwitchB is the same as the switch in scenario 1, SwitchA takes the place of Multicast Router in scenario 1. Let's assume VLAN 60 is configured in SwitchA, including ports 1, 2, 6, 10 and 12. Port 1 connects to the multicast server, and port 2 connects to SwitchB. In order to send Query at regular interval, IGMP query must enabled in Global mode and in VLAN60.

The configuration steps are listed below:

SwitchA#config

SwitchA(Config)#ip igmp snooping
SwitchA(Config)#ip igmp snooping vlan 60 query

SwitchB#config

SwitchB(Config)#ip igmp snooping
SwitchB(Config)#ip igmp snooping vlan 100

SwitchB(Config)#ip igmp snooping vlan 100 mrouter interface ethernet 1/1

Multicast Configuration

The same as scenario 1.

IGMP Snooping listening result:

Similar to scenario 1.

18.5 IGMP Snooping Troubleshooting

On IGMP Snooping function configuration and usage, IGMP Snooping might not run properly because of physical connection or configuration mistakes. So the users should noted that:

- Make sure correct physical connection.
- Activate IGMP Snooping on whole config mode (use ip igmp snooping)
- Config IGMP Snooping at VLAN on whole config mode (use ip igmp snooping vlan <vlan-id>)
- Make sure one VLAN is configured as L2 common checker in same mask, or make sure configured static mrouter.
- Use show ip igmp snooping vlan <vid> command check IGMP Snooping information

If IGMP Snooping problem cannot be solve by check, then pls. use debug command like debug igmp snooping. Copy and send 3 minutes DEBUG information to our customer center.

18.5.1 Commands for Monitor And Debug

18.5.1.1 debug igmp snooping all/packet/event/timer/mfc

Command: debug igmp snooping all/packet/event/timer/mfc

no debug igmp snooping all/packet/event/timer/mfc

Function: Enable the IGMP Snooping switch of the switch; the "**no debug igmp snooping all/packet/event/timer/mfc**" disables the debugging switch

Command Mode: Admin Mode

Default: IGMP Snooping debugging switch is disabled on the switch by default

Usage Guide: The command is used for enable the IGMP Snooping debugging switch of the switch, switch IGMP data packet message can be shown with "packet" parameter, event message with "event", timer message with "time", down sending hardware entries

message with “mfc”, and all debugging messages with “all”.

show ip igmp snooping

Command: show ip igmp snooping [vlan <*vlan-id*>]

Parameter: <*vlan-id*> is the vlan number specified for displaying IGMP Snooping messages

Command Mode: Admin Mode

Usage Guide: If no vlan number is specified, it will show whether global igmp snooping switch is on, which vlan is configured with l2-general-querier function, and if a vlan number is specified, detailed IGMP messages for this vlan will be shown

Example:

1. Show IGMP Snooping summary messages of the switch

Switch(config)#show ip igmp snooping

Global igmp snooping status: Enabled

L3 multicasting: running

Igmp snooping is turned on for vlan 1(querier)

Igmp snooping is turned on for vlan 2

Displayed Information	Explanation
Global igmp snooping status	Whether the global igmp snooping switch on the switch is on
L3 multicasting	whether the layer 3 multicast protocol of the switch is running
Igmp snooping is turned on for vlan 1(querier)	which vlans on the switch is enabled with igmp snooping function, whether they are l2-general-querier

2.Display the IGMP Snooping summary messages of vlan1.

Switch#show ip igmp snooping vlan 1

Igmp snooping information for vlan 1

Igmp snooping L2 general querier :Yes(COULD_QUERY)

Igmp snooping query-interval :125(s)

Igmp snooping max response time :10(s)

Igmp snooping robustness :2

Igmp snooping mrouter port keep-alive time :255(s)

Igmp snooping query-suppression time :255(s)

IGMP Snooping Connect Group Membership

Note:*-All Source, (S)- Include Source, [S]-Exclude Source

Groups	Sources	Ports	Exptime	System Level
238.1.1.1	(192.168.0.1)	Ethernet1/8	00:04:14	V2
	(192.168.0.2)	Ethernet1/8	00:04:14	V2

Igmp snooping vlan 1 mrouter port

Note:"!"-static mrouter port

!Ethernet1/2

Displayed Information	Explanation
Igmp snooping L2 general querier	Whether the vlan enables l2-general-querier function and show whether the querier state is could-query or suppressed
Igmp snooping query-interval	Query interval of the vlan
Igmp snooping max response time	Max response time of the vlan
Igmp snooping robustness	IGMP Snooping robustness configured on the vlan
Igmp snooping mrouter port keep-alive time	keep-alive time of dynamic mrouter of the vlan
Igmp snooping query-suppression time	Suppression timeout of vlan when as l2-general-querier
IGMP Snooping Connect Group Membership	Group membership of this vlan, namely the correspondence between ports and (S,G)
Igmp snooping vlan 1 mrouter port	mrouter port of the vlan, including both static and dynamic

18.5.1.2 show mac-address-table multicast

Command: show mac-address-table multicast [vlan <*vlan-id*>]

Function: Show the multicast MAC address table messages

Parameter: <*vlan-id*> VLAN ID included in the entries to be shown

Command Mode: Admin Mode

Default: Not showing the multicast MAC address and port mapping by system default

Usage Guide: This command shows multicast MAC address table messages of current switch

Example: Show the multicast mapping in vlan 100

Switch#show mac-address-table multicast vlan 100

Vlan	Mac Address	Type	Ports
100	01-00-5e-01-01-01	MULTI	Ethernet

Chapter 19 Multicast VLAN

19.1 Introductions To Multicast VLAN

Based on current multicast order method, when orders from users in different VLAN, each VLAN will copy a multicast traffic in this VLAN, which is a great waste of the bandwidth. By configuration of the multicast VLAN, we add the switch port to the multicast VLAN, with the IGMP Snooping functions enabled, users from different VLAN will share the same multicast VLAN. The multicast traffic only exists within a multicast VLAN, so the bandwidth is saved. As the multicast VLAN is absolutely separated from the user VLAN, security and bandwidth concerns can be met at the same time, after the multicast VLAN is configured, the multicast traffic will be continuously sent to the users.

19.2 Multicast VLAN Configuration Task

1. Enable the multicast VLAN function
2. Configure the IGMP Snooping

1. Enable the multicast VLAN function

Command	Explanation
VLAN config mode	
multicast-vlan **no multicast-vlan**	Configure a VLAN and enable the multicast VLAN on it. The “**no multicast-vlan**” command disables the multicast function on the VLAN
multicast-vlan association <*vlan-list*> **no multicast-vlan association <*vlan-list*>**	Associate a multicast VLAN with several VLANs. The “no" form of this command deletes the related VLANs associated with the multicast VLAN

2. Configure the IGMP Snooping

Command	Explanation
Global Mode	
ip igmp snooping vlan <*vlan-id*> **no ip igmp snooping vlan <*vlan-id*>**	Enable the IGMP Snooping function on the multicast vlan. The "no” form of this

	command disables the IGMP Snooping on the multicast vlan
ip igmp snooping **no ip igmp snooping**	Enable the IGMP Snooping function. The "no" form of this command disables the IGMP snooping function

19.3 Commands For Multicast VLAN

19.3.1 multicast-vlan

Command:multicast-vlan

no multicast-vlan

Function: Enable multicast VLAN function on a VLAN; the "no" form of this command disables the multicast VLAN function.

Parameter: None

Command Mode: VLAN config Mode

Default: Multicast VLAN function not enabled by default

Usage Guide: The multicast VLAN function can not be enabled on private VLAN. To disabling the multicast VLAN function of the VLAN, configuration of VLANs associated with the multicast VLAN should be deleted. Note that the default vlan can not be configured with this command and only one multicast vlan is allowed on a switch

Examples:

Switch(config)#vlan 2

Switch (Config-Vlan2)# multicast-vlan

19.3.2 multicast-vlan association<*vlan-list*>

Command:multicast-vlan association <*vlan-list*>

no multicast-vlan association <*vlan-list*>

Function: Associate several VLANs with a multicast VLAN; the "no" form of this command cancels the association relations.

Parameter: <*vlan-list*> the VLAN ID list associated with multicast VLAN. Each VLAN can only be associated with one multicast VLAN and the association will only succeed when every VLAN listed in the VLAN ID table exists.

Command Mode: VLAN mode

Default: The multicast VLAN is not associated with any VLAN by default

Usage Guide: After a VLAN is associated with the multicast VLAN, when there comes the multicast order in the port of this VLAN, then the multicast data will be sent from the multicast VLAN to this port, so to reduce the data traffic. The VLAN associated with the multicast VLAN should not be a Private VLAN. A VLAN can only be associated with another VLAN after the multicast VLAN is enabled. Only one multicast VLAN can be enabled on a switch.

Examples:

Switch(config)#vlan 2

Switch (Config-Vlan2)#multicast-vlan

Switch (Config-Vlan2)# multicast-vlan association 3;4

19.4 Examples Of Multicast VLAN

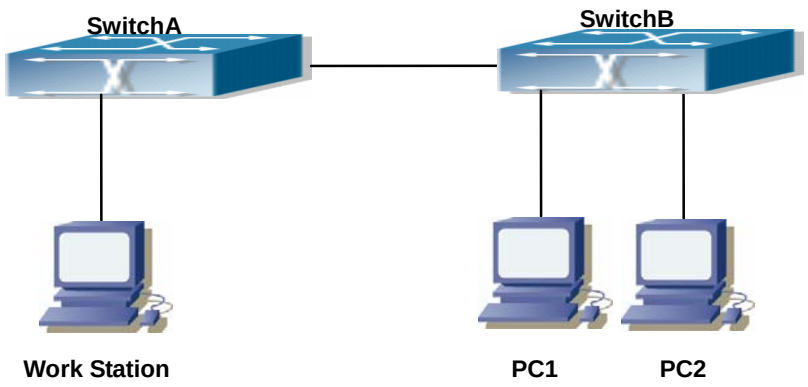


Fig 19-1 Function configuration of the Multicast VLAN

As shown in the figure, the multicast server is connected to the layer 3 switch switchA through port 1/1 which belongs to the vlan10 of the switch. The layer 3 switch switchA is connected with layer 2 switches through the port 1/10. the Vlan20 is a multicast vlan. On the switchB the vlan100 is configured set to contain port 1/15, and vlan101 to contain port 1/20. PC1 and PC2 are respectively connected to port 1/15 and 1/20. The switchB is connected with the switchA through port 1/10. vlan 20 is a multicast vlan. By configuring multicast vlan, the PC1 and PC2 will receives the multicast data from the multicast VLAN.

Following configuration is based on the IP address of the switch has been configured and all the equipment are connected correctly .

Configuration procedure

SwitchA#config

SwitchA (config)#vlan 10

SwitchA (config-vlan10)#switchport access ethernet 1/1

SwitchA (config-vlan10)exit
SwitchA (config)#interface vlan 10
Switch(Config-if-Vlan10)#ip pim dense-mode
Switch(Config-if-Vlan10)#exit
SwitchA (config)#vlan 20
SwitchA (config-vlan20)#multicast-vlan
SwitchA (config-vlan20)#exit
SwitchA (config)#ip igmp snooping
SwitchA (config)#ip igmp snooping vlan 20
SwitchA (config)#interface vlan 20
SwitchA(Config-if-Vlan20)#ip pim dense-mode
SwitchA(Config-if-Vlan20)#exit
SwitchA (config)#ip pim multicast
SwitchA (config)# interface ethernet1/10
SwitchA (Config-Ethernet1/10)switchport mode trunk

SwitchB#config
SwitchB (config)#vlan 100
SwitchB (config-vlan100)#Switchport access ethernet 1/15
SwitchB (config-vlan100)exit
SwitchB#config
SwitchB (config)#vlan 101
SwitchB (config-vlan101)#Switchport access ethernet 1/20
SwitchB (config-vlan101)exit
SwitchB (config)# interface ethernet 1/10
SwitchB (Config-Ethernet1/10)#Switchport mode trunk
SwitchB (Config-Ethernet1/10)#exit
SwitchB (config)#vlan 20
SwitchA (config-vlan20)#multicast-vlan
SwitchA (config-vlan20)#multicast-vlan association 100,101
SwitchA (config-vlan20)#exit
SwitchA (config)#ip igmp snooping
SwitchA (config)#ip igmp snooping vlan 20

Chapter 20 IPv4 Multicast Protocol

20.1 IPv4 Multicast Protocol Overview

This chapter will give an introduction to the configuration of IPv4 Multicast Protocol. All IPs in this chapter are IPv4.

20.1.1 Introduction to Multicast

Various transmission modes can be adopted when the destination of packet (including data, sound and video) transmission is the minority users in the network. One way is to use Unicast mode, i.e. to set up a separate data transmission path for each user; or, to use Broadcast mode, which is to send messages to all users in the network, and they will receive the Broadcast messages no matter they need or not. For example, if there are 200 users in a network who want to receive the same packet, then the traditional solution is to send this packet for 200 times separately via Unicast to guarantee the users who need the data can get all data wanted, or send the data in the entire domain via Broadcast. Transferring the data in the whole range of network .The users who need these data can get directly from the network. Both modes waste a great deal of valuable bandwidth resource, and furthermore, Broadcast mode goes against the security and secrecy.

The emergence of IP Multicast technology solved this problem in time. The Multicast source only sends out the message once, Multicast Routing Protocol sets up tree-routing for Multicast data package, and then the transferred packet just starts to be duplicated and distributed in the bifurcate crossing as far as possible. Thus the packet can be sent to every user who needs it accurately and effectively.

It should be noticed that it is not necessary for Multicast source to join in Multicast group. It sends data to some Multicast groups, but it is not necessarily a receiver of the group itself. There can be more than one source sending packets to a Multicast group simultaneously. There may exist routers in the network which do not support Multicast, but a Multicast router can encapsulate the Multicast packets into Unicast IP packets with tunnel mode to send them to the Multicast router next to it, which will take off the Unicast IP header and continue the Multicast transmission process, thus a big alteration of network structure is avoided. The primary advantages of Multicast are:

1) Enhance efficiency: reduce network traffic, lighten the load of server and CPU

2) Optimize performance: reduce redundant traffic

3) Distributed application: Enable Multipoint Application

20.1.2 Multicast Address

The destination address of Multicast message uses class D IP address with range from 224.0.0.0 to 239.255.255.255. D class address can not appear in the source IP address field of an IP message. In the process of Unicast data transmission, the transmission path of a data packet is from source address routing to destination address, and the transmission is performed with hop-by-hop principle. However, in IP Multicast environment, the destination addresses is a group instead of a single one, they form a group address. All message receivers will join in a group, and once they do, the data flowing to the group address will be sent to the receivers immediately and all members in the group will receive the data packets. The members in a Multicast group are dynamic, the hosts can join and leave the Multicast group at any time.

Multicast group can be permanent or temporary. Some of the Multicast group addresses are assigned officially; they are called Permanent Multicast Group. Permanent Multicast Group keeps its IP address fixed but its member structure can vary within. The member amount of Permanent Multicast Group can be arbitrary, even zero. The IP Multicast addresses which are not kept for use by Permanent Multicast Group can be utilized by temporary Multicast groups.

224.0.0. 0～224.0.0.255 are reserved Multicast addresses (Permanent Group Address), address 224.0.0.0 is reserved but not assigned, and other addresses are used by Routing Protocol; 224.0.1.0～238.255.255.255 are Multicast addresses available to users（Temporary Group Address） and are valid in the entire domain of the network; 239.0.0.0～239.255.255.255 are local management Multicast addresses, which are valid only in specific local domain. Frequently used reserved multicast address list is as follows:

Benchmark address (reserved)

224.0.0.1 Address of all hosts

224.0.0.2 Address of all Multicast Routers

224.0.0.3 Unassigned

224.0.0.4 DVMRP Router

224.0.0.5 OSPF Router

224.0.0.6 OSPF DR

224.0.0.7 ST Router

224.0.0.8 ST host

224.0.0.9 RIP-2 Router

224.0.0.10 IGRP Router

224.0.0.11 Active Agent

224.0.0.12 DHCP Server/Relay Agent

224.0.0.13 All PIM Routers

224.0.0.14 RSVP Encapsulation

224.0.0.15 All CBT Routers

224.0.0.16 Specified SBM

224.0.0.17 All SBMS

224.0.0.18 VRRP

When Ethernet transmits Unicast IP messages, the destination MAC address it uses is the receiver's MAC address. But in transmitting Multicast packets, the transmission destination is not a specific receiver any more, but a group with uncertain members, thus Multicast MAC address is used. Multicast MAC address is corresponding to Multicast IP address. It is prescribed in IANA (Internet Assigned Number Authority) that the higher 25 bits in Multicast MAC address is 0x01005e, and the lower 23bits in MAC address is the lower 23bits in Multicast IP address.

Since only 23bits out of the lower 28bits in IP Multicast address are mapped into MAC address, therefore there are 32 IP Multicast addresses which are mapped into the same MAC address.

20.1.3 IP Multicast Packet Transmission

In Multicast mode, the source host sends packets to the host group indicated by the Multicast group address in the destination address field of IP data packet. Unlike Unicast mode, Multicast data packet must be forwarded to a number of external interfaces to be sent to all receiver sites in Multicast mode, thus Multicast transmission procedure is more complicated than Unicast transmission procedure.

In order to guarantee that all Multicast packets get to the router via the shortest path, the receipt interface of the Multicast packet must be checked in some certain way based on Unicast router table; this checking mechanism is the basis for most Multicast Routing Protocol to forward in Multicast mode --- RPF (Reverse Path Forwarding) check. Multicast router makes use of the ingressed packet source address to query Unicast Router Table or independent Multicast Router Table to determine if the packet ingress interface is on the shortest path from receipt site to source address. If shortest path Tree is used, then the source address is the address of source host which sends Multicast Data Packets; if Shared Tree is used, then the source address is the address of the root of the Shared-Tree. When Multicast data packet gets to the router, if RPF check passes, then the data packet is forwarded according to Multicast forward item, and the data

packet will be discarded elsewise.

20.1.4 IP Multicast Application

IP Multicast technology has effectively solved the problem of sending in single point and receiving in multipoint. It has achieved the effective data transmission from a point to multiple points, saved a great deal of network bandwidth and reduced network load. Making use of the Multicast property of network, some new value-added operations can be supplied conveniently. In Information Service areas such as online living broadcast, network TV, remote education, remote medicine, real time video/audio meeting, the following applications may be supplied:

1) Application of Multimedia and Streaming Media
2) Data repository, finance application (stock) etc.;
3) Any data distribution application of “one point to multiple points”

In the situation of more and more multimedia operations in IP network, Multicast has tremendous market potential and Multicast operation will be generalized and popularized.

20.2 PIM-DM

20.2.1 Introduction to PIM-DM

PIM-DM（Protocol Independent Multicast, Dense Mode）is a Multicast Routing Protocol in dense mode which applies to small network. The members of multicast group are relatively dense under this kind of network environment.

The working process of PIM-DM can be summarized as: Neighbor Discovery, Flooding&Prune, and Graft.

1. Neigh hour Discovery

After PIM-DM router is enabled, Hello message is required to discover neighbors. The network nodes which run PIM-DM use Hello message to contact each other. PIM-DM Hello message is sent periodically.

2. Flooding&Prune of process

PIM-DM assumes all hosts on the network are ready to receive Multicast data. When some Multicast Source begins to send data to a Multicast Group G, after receiving the Multicast packet, the router will make RPF check first according to the Unicast table. If the check passes, the router will create a (S, G) table entry and transmit the Multicast packet to all downstream PIM-DM nodes on the network (Flooding). If the RPF check

fails, i.e. the Multicast packet is input from the incorrect interface, and then the message is discarded. After this procedure, in the PIM-DM Multicast domain, every node will create a (S, G) table entry. If there is no Multicast group member in the downstream nodes, then a Prune message is sent to upstream nodes to notify them not to transmit data of this Multicast group any more. After receiving Prune message, the upstream nodes will delete the corresponding interface from the output interface list to which their Multicast transmission table entry (S, G) corresponds. Thus a SPT（Shortest Path Tree, SPT） tree with source S as root is created. The Prune process is initiated by leaf router first.

The process above is called Flooding&Prune process. Each pruned node also provides time-out mechanics at the same time. When Prune is timed-out, the router will restart Flooding&Prune process. The PIM-DM Flooding&Prune is periodically processed.

3. RPF Check

With RPF Check, PIM-DM makes use of existing Unicast routing table to establish a Multicast transmission tree initiating from data source. When a Multicast packet arrives, the router will determine whether the coming path is correct first. If the arrival interface is the interface connected to Multicast source indicated by Unicast routing, then this Multicast packet is considered to be from the correct path. Otherwise the Multicast packet is to be discarded as redundant message. The Unicast routing message used as path judgment can root in any Unicast Routing Protocol, such as messages found by RIP, OSPF, etc. It doesn't rely on any specific Unicast Routing Protocol.

4. Assert Mechanism

If each of two Multicast routers A and B on the same LAN segment has a receiving route respectively and both will transmit the Multicast packet to the LAN after receiving the Multicast data packet sent by the Multicast Source S, then the downstream node Multicast router C will receive two exactly same Multicast packets. The router needs to choose a unique transmitter through Assert mechanism after it detects this situation. An optimal transmission path is selected through sending out Assert packet. If the priority and cost of two or more path are same, then the node with larger IP address is taken as the upstream neighbor of the (S, G) entry and in charge of the transmission of the (S, G) Multicast packet.

5. Graft

When the pruned downstream node needs to recover to transmission status, this node uses Graft Packet to notify upstream nodes to restore multicast data transmission.

20.2.2 PIM-DM Configuration Task List

1、 Setup PIM-DM (Required)

2、 Configure PIM-DM auxiliary parameters (Optional)

3、 Configure PIM-DM interface parameters

4、 Configure PIM-DM hello message interval

1. Setup PIM-DM Protocol

The basic configuration to function PIM-DM routing protocol on EDGECORE series Layer 3 switch is very simple. It is only required to turn on PIM Multicast switch in Global Mode and turn on PIM-DM switch under corresponding interface.

Command	Explanation
Global Mode	
ip pim multicast-routing	Make PIM-DM Protocol on each interface to Enable status (but the commands below are required to really enable PIM-DM protocol on the interface)

And then turn on PIM-SM switch on the interface

Command	Explanation
Interface Configuration Mode	
ip pim dense-mode	Setup PIM-DM Protocol of the interface (Required)

2. Configure PIM-DM Sub-parameters

（1）Configure PIM-DM Interface Parameters

1）Configure PIM-DM hello message interval

Command	Explanation
Interface configuration mode	
ip pim hello-interval < *interval*> **no ip pim hello-interval**	Configure interface PIM-DM hello message interval; the "**no ip pim hello-interval**" command restores the default value.

Command	Explanation
Interface configuration mode	
ip pim state-refresh origination-interval **no ip pim state-refresh origination-interval**	Configure interface PIM-DM hello message interval; the "**no ip pim state-refresh origination-interval**" command restores the default value.

3. Disable PIM-DM Protocol

Command	Explanation
Interface configuration mode	

no ip pim dense-mode	Disable PIM-DM protocol on the interface
Global Mode	
no ip pim multicast-routing	Disable PIM-DM Protocol in global mode.

20.2.3 Commands for PIM-DM

20.2.3.1 ip pim accept-register

Command: ip pim accept-register list <*list-number*>

no ip pim accept-register

Function: Filter the specified multicast group and multicast address.

Parameter: <***list-number***>: is the access-list number ,it ranges from 100 to 199.

Default: Permit the multicast registers from any sources to any groups.

Command Mode: Global Mode

Usage Guide: This command is used to configure the access-list filtering the PIM REGISTER packets.The addresses of the access-list respectively indicate the filtered multicast sources and multicast groups' information. For the source-group combinations that match DENY, PIM sends REGISTER-STOP immediately and does not create group records when receiving REGISTER packets.Unlike other access-list,when the access-list is configured ,the default value is PERMIT.

Example: Configure the filtered register message's rule to myfilter.

Switch(config)#ip pim accept-register list 120

Switch (config)#access-list 120 deny ip 10.1.0.2 0.0.0.255 239.192.1.10 0.0.0.255

20.2.3.2 ip pim cisco-register-checksum

Command: ip pim cisco-register-checksum group-list [<*simple-acl*>]

no ip pim cisco-register-checksum group-list [<*simple-acl*>]

Function: Configure the register packet's checksum of the group specified by myfilter to use the whole packet's length.

Default: Compute the checksum according to the regester packets's head length, default: 8

Parameter: <*simple-acl*>: <1-99> Simple access-list **<*simple-acl*>:** <1-99> Simple access-list

Command Mode: Global Mode

Usage Guide: This command is uesd to interact with older Cisco IOS version.

Example: Configure the register packet's ckecksum of the group specified by myfilter to use the whole packet's length.

Switch (config)#ip pim cisco-register-checksum group-list 23

20.2.3.3 ip pim dr-priority

Command: ip pim dr-priority <*priority*>

no ip pim dr-priority

Function: Configure,disable or change the interface's DR priority. The neighboring nodes in the same net segment select the DR in their net segment according to hello packets. The "**no ip pim dr-priority"** command restores the default value.

Parameter: <*priority*> is priority

Default: 1

Command Mode: Interface Configuration Mode

Usage Guide: Range from 0 to 4294967294, the higher value has more priority.

Example: Configure vlan's DR priority to 100

Switch (Config)# interface vlan 1

Switch(Config-if-Vlan1)ip pim dr-priority 100

Switch (Config -if-Vlan1)#

20.2.3.4 ip pim exclude-genid

Command: ip pim exclude-genid

no ip pim exclude-genid

Function: This command makes the Hello packets sent by PIM SM do not include GenId option. The "**no ipv6 pim exclude-genid**" command restores the default value

Parameter: None

Default: The Hello packets include GenId option.

Command Mode: Interface Configuration Mode

Usage Guide: This command is used to interact with older Cisco IOS version.

Example: Configure the Hello packets sent by the switch do not include GenId option.

Switch (Config-if-Vlan1)#ip pim exclude-genid

Switch (Config-if-Vlan1)#

20.2.3.5 ip pim hello-holdtime

Command: ip pim hello-holdtime <*value*>

no ip pim hello-holdtime

Function: Configure or disable the Holdtime option in the Hello packets,this value is to describe neighbore holdtime,if the switch hasn't received the neighbore hello packets when the holdtime is over, this neighbore is deleted. The "**no ip pim hello-holdtime**" command cancels configured holdtime value and restores default value.

Parameter: <*value*> is the value of holdtime.

Default: The default value of Holdtime is 3.5*Hello_interval, Hello_interval's default value

is 30s,so Holdtime's default value is 105s.

Command Mode: Interface Configuration Mode

Usage Guide: If this value is not configured, hellotime's default value is 3.5*Hello_interval. If the configured holdtime is less than the current hello_interval , this configuration is denyed. Every time hello_interval is updated, the Hello_holdtime will update according to the following rules: If hello_holdtime is not configured or hello_holdtime is configured but less than current hello_interval,hello_holdtime is modified to 3.5*hello_interval, otherwise the configured value is maintained.

Example: Configure vlan1's Hello Holdtime

Switch (Config)# interface vlan1

Switch (Config -if-Vlan1)#ip pim hello-holdtime 10

Switch (Config -if-Vlan1)#

20.2.3.6 ip pim dense-mode

Command: ip pim dense-mode

no ip pim dense-mode

Function: Enable PIM-DM protocol on interface; the "**no ip pim dense-mode**" command disenables PIM-DM protocol on interface.

Parameter: None.

Default: Disable PIM-DM protocol.

Command Mode: Interface Configure Mode

Usage Guide: The command will be taken effect, executing ip multicast-routing in Global Mode. Don't support multicast protocol mutual operation, namely can't synchronously enable dense mode and sparse mode in one swtich.

Example: Enable PIM-DM protocol on interface vlan1.

Switch (Config)#ip pim multicast-routing

Switch (Config)#interface vlan 1

Switch(Config-if-Vlan1)#ip pim dense-mode

20.2.3.7 ip pim hello-interval

Command: ip pim hello-interval < *interval*>

no ip pim hello-interval

Function: Configure interface PIM-DM hello message interval; the "**no ip pim hello-interval**" restores default value.

Parameter: < *interval*> is interval of periodly transmitted PIM-DM hello message, value range from 1s to 18724s.

Default: Default interval of periodly transmitted PIM-DM hello message as 30s.

Command Mode: Interface Configuration Mode.

Usage Guide: Hello message makes PIM-DM switch mutual location, and ensures neighborship. PIM-DM switch announces existence itself by periodly transmitting hello messages to neighbors. If it doesn't receive hello messages from neighbors in regulation time, it confirms that the neighbors were lost. Configuration time is not more than neighbor overtime.

Example: Configure PIM-DM hello interval on interface vlan1.

Switch (Config)#interface vlan1

Switch(Config-if-Vlan1)#ip pim hello-interval 20

20.2.3.8 ip pim multicast-routing

Command: ip pim multicast-routing

no ip pim multicast-routing

Function: Enable PIM-SM globally. The "**no ip pim multicast-routing** » command disables PIM-SM globally.

Parameter: None

Default: Disabled PIM-SM

Command Mode: Global Mode

Usage Guide: Enable PIM-SM globally.The interface must enable PIM-SM to have PIM-SM work

Example: Enable PIM-SM globally.

Switch (Config)#ip pim multicast-routing

20.2.3.9 ip pim neighbor-filter

Command: ip pim neighbor-filter{<*list-number*>}

no ip pim neighbor-filter{<*list-number*>}

Function: Configure the neighbore access-list. If filtered by the lists and connections with neighbors are created, this connections are cut off immediately. If no connection is created, this conncetion can't be created.

Parameter: <*list-number*>: <*list-number*> is the simple access-list number, it ranges from 1 to 99

Default: No neighbor filter configuration.

Command Mode: Interface Configuration Mode

Usage Guide: ACL's default is DENY. If configuring access-list 1,access-list 1's default is deny. In the following example, if "permit any-source" is not configured, deny 10.1.4.10 0.0.0.255 is the same as deny any-source.

Example: Configure vlan's filtering rules of pim neighbors.

Switch #show ip pim neighbor

Neighbor Interface Uptime/Expires Ver DR

```
Address                                                    Priority/Mode
10.1.4.10          Vlan1          02:30:30/00:01:41 v2     4294967294 / DR
Switch (Config-if-Vlan1)#ip pim neighbor-filter 2
Switch (config)#access-list 2 deny 10.1.4.10 0.0.0.255
Switch (config)#access-list 2 permit any-source
Switch (config)#show ip pim neighbor
Switch (config)#
```

20.2.3.10 ip pim state-refresh origination-interval

Command: ip pim state-refresh origination-interval <interval>

no ip pim state-refresh origination-interval

Function: Configure transmission interval of state-refresh message on interface. The "**no ip pim state-refresh origination-interval**" command restores default value.

Parameter: <*interval*> packet transmission interval value is from 4s to 100s.

Default: 60s

Usage Guide: The first-hop router periodically transmits stat-refresh messages to maintain PIM-DM list items of all the downstream routers. The command can modify origination interval of state-refresh messages. Usually do not modify relevant timer interval.

Example: Configure transmission interval of state-refresh message on interface vlan1 to 90s.

```
Switch (Config-if-Vlan1)#ip pim state-refresh origination-interval   90
```

20.2.4 PIM-DM Configuration Examples

As shown in the following figure, add the Ethernet interfaces of Switch A and Switch B to corresponding vlan, and enable PIM-DM Protocol on each vlan interface.

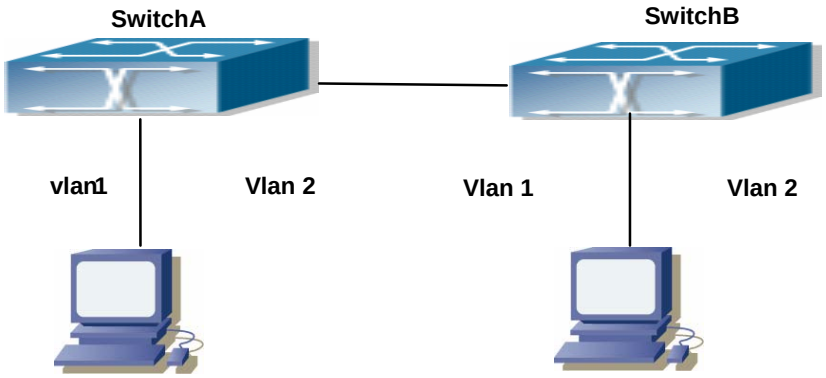


Fig 20-1PIM-DM Typical Environment

The configuration procedure for SwitchA and SwitchB is as follows:

(1) Configure SwitchA:

```
Switch (Config)#ip pim multicast-routing
Switch (Config)#interface vlan 1
Switch(Config-if-Vlan1)# ip address 10.1.1.1 255.255.255.0
Switch(Config-if-Vlan1)# ip pim dense-mode
Switch(Config-if-Vlan1)#exit
Switch (Config)#interface vlan2
Switch(Config-if-Vlan2)# ip address 12.1.1.1 255.255.255.0
Switch(Config-if-Vlan2)# ip pim dense-mode
```

(2) Configure SwitchB:

```
Switch (Config)#ip pim multicast-routing
Switch (Config)#interface vlan 1
Switch(Config-if-Vlan1)# ip address 12.1.1.2 255.255.255.0
Switch(Config-if-Vlan1)# ip pim dense-mode
Switch(Config-if-Vlan1)#exit
Switch (Config)#interface vlan 2
Switch(Config-if-Vlan2)# ip address 20.1.1.1 255.255.255.0
Switch(Config-if-Vlan2)# ip pim dense-mode
```

At the same time, you should pay attention to the configuration of Unicast Routing Protocol, assure that each device can communicate with each other in the network layer, and be able to implement dynamic routing update in virtue of Unicast Routing Protocol.

20.2.5 PIM-DM Troubleshooting

In configuring and using PIM-DM Protocol, PIM-DM Protocol might not operate normally caused by physical connection or incorrect configuration. Therefore, the user should pay attention to the following issues:

- ✧ To assure that physical connection is correct.
- ✧ To assure the Protocol of Interface and Link is UP (use show interface command);
- ✧ To assure PIM Protocol is enabled in Global Mode (use ipv6 pim multicast-routing)
- ✧ Enable PIM-DM Protocol on the interface (use ipv6 pim dense-mode command)
- ✧ Multicast Protocol requires RPF Check using Unicast routing; therefore the correctness of Unicast routing must be assured beforehand.

If all attempts including Check are made but the problems on PIM-DM can't be solved yet, then use debug commands such as debug pim please, and then copy DEBUG information in 3 minutes and send to Technology Service Center.

20.2.5.1 Monitor and debug command

20.2.5.1.1 debug pim timer sat

Command: debug pim timer sat

no debug pim timer sat

Function: Enable debug switch of PIM-DM source activity timer information in detail; the "**no debug pim timer sat**" command disenables the debug switch.

Parameter: None.

Default: Disabled.

Command Mode: Admin Mode.

Usage Guide: Enable the switch, and display source activity timer information in detail.

Example:

Switch # debug ip pim timer sat

Remark: Other debug switches in PIM-DM are common in PIM-SM, including debug pim event, debug pim packet, debug pim nexthop, debug pim nsm, debug pim mfc, debug pim timer, debug pim state, refer to PIM-SM handbook.

20.2.5.1.2 debug pim timer srt

Command: debug pim timer srt

no debug pim timer srt

Function: Enable debug switch of PIM-DM state-refresh timer information in detail; the "**no debug pim timer srt**" command disenables the debug switch.

Parameter: None.

Default: Disabled.

Command Mode: Admin Mode and Global Mode.

Usage Guide: Enable the switch, and display PIM-DM state-refresh timer information in detail.

Example: Switch # debug ip pim timer srt

Remark: Other debug switches in PIM-DM are common in PIM-SM, including debug pim event, debug pim packet, debug pim nexthop, debug pim nsm, debug pim mfc, debug pim timer, debug pim state, refer to PIM-SM manual section.

20.2.5.1.3 show ip pim interface

Command: show ip pim interface

Function: Display PIM interface information

Parameter: None

Default: None

Command Mode: Admin Mode and Global Mode

Usage Guide: Display PIM interface information

Example: testS2(config)#show ip pim interface

Address	Interface	VIFindex	Ver/ Mode	Nbr Count	DR Prior	DR
10.1.4.3	Vlan1	0	v2/S	1	1	10.1.4.3
10.1.7.1	Vlan2	2	v2/S	0	1	10.1.7.1

Displayed Information	Explanations
Address	Interface address
Interface	Interface name
VIF index	Interface index
Ver/Mode	Pim version and mode,usually v2,sparse mode displays S,dense mode displays D
Nbr Count	The interface's neighbor count
DR Prior	Dr priority
DR	The interface's DR address

20.2.5.1.4 show ip pim neighbor

Command: show ip pim neighbor

Function: Display router neighbors

Parameter: None

Default: None

Command Mode: Admin Mode and Global Mode

Usage Guide: Display multicast router neighbors maintained by the PIM

Example: s1(config)#show ip pim neighbor

Neighbor Address	Interface	Uptime/Expires	Ver	DR Priority/Mode
10.1.6.1	Vlan1	00:00:10/00:01:35	v2	1 /
10.1.6.2	Vlan1	00:00:13/00:01:32	v2	1 /
10.1.4.2	Vlan3	00:00:18/00:01:30	v2	1 /
10.1.4.3	Vlan3	00:00:17/00:01:29	v2	1 /

Displayed Information	Explanations
Neighbor Address	Neighbor address
Interface	Neighbor interface
Uptime/Expires	Running time /overtime
Ver	Pim version ,v2 usually
DR Priority/Mode	DR priority in the hello messages from the neighbor and if the neighbor is the interface's DP.

20.2.5.1.5 show ip pim nexthop

Command: show ip pim nexthop

Function: Display the PIM buffered nexthop router in the unicast route table

Parameter: None

Default: None

Command Mode: Admin Mode and Global Mode

Usage Guide: Display the PIM buffered nexthop router information.

Example:

Switch(config)#show ip pim nexthop

Flags: N = New, R = RP, S = Source, U = Unreachable

Destination	Type	Nexthop Num	Nexthop Addr	Nexthop Ifindex	Nexthop Name	Metric	Pref	Refcnt
192.168.1.1	N...	1	0.0.0.0	2006		0	1	0
192.168.1.9	..S.	1	0.0.0.0	2006		0	1	0

Displayed Information	Explanations
Destination	Destination of next item
Type	N: created nexthop,RP direction and S direction are not determined . R: RP derection S: source direction U: can't reach
Nexthop Num	Nexthop number
Nexthop Addr	Nexthop address
Nexthop Ifindex	Nexthop interface index
Nexthop Name	Nexthop name
Metric	Metric Metric to nexthop
Pref	Preference Route preference
Refcnt	Reference count

20.2.5.1.6 show ip pim mroute dense-mode

Command: show ip pim mroute dense-mode [group <*A.B.C.D*>] [source <*A.B.C.D*>]

Function: Display PIM-DM message forwarding items.

Parameter:group <A.B.C.D>: displays forwarding items relevant to this multicast address.Source <A.B.C.D>: displays forwarding items relevant to this source.

Default: Do not display (Off).

Command Mode: Admin Mode

Usage Guide: The command shows PIM-DM multicast forwarding items, namely forwarding items of forward multicast packet in system FIB table.

Example: Display all of PIM-DM message forwarding items.

Switch(config)#show ip pim mroute dense-mode
IP Multicast Routing Table

(*,G) Entries: 1
(S,G) Entries: 1

(*, 226.0.0.1)
Local ..l.....

(192.168.1.12, 226.0.0.1)
RPF nbr: 0.0.0.0
RPF idx: Vlan2
Upstream State: FORWARDING
Origin State: ORIGINATOR
Local .....
Pruned .....
Asserted .....
Outgoing ..o.....
Switch#

Displayed Information	Explanations
(*,226.0.0.1)	(*,G) Forwaridng item
(192.168.1.12, 226.0.0.1)	(S,G) Forwarding item
RPF nbr	Backward path neighbor, upstream neighbor of source direction in DM, 0.0.0.0 expresses the switch is the first hop.
RPF idx	Interface located in RPF neighbor
Upstream State	Upstream direction, including FORWARDING(forwarding upstream data), PRUNED(Upstream stops forwarding data), ACKPENDING(waiting for upstream response, forwarding upstream data)
Origin State	The two states: ORIGINATOR(on transmit state-refresh state), NON_ORIGINATOR(on non_transmit state-refresh state)
Local	Local position joins interface, the interface receives IGMP Join
Pruned	PIM prunes interface, the interface

	receives Prune messages
Asserted	Asserted state
Outgoing	Multicast data finally exported from interface is index number, index is 2 in this case. It can check interface information in detail by commanding show ip pim interface

20.2.5.1.7 show ip mroute

Command: show ip mroute [<GroupAddr> [<SourceAddr>]]

Function: show IPv4 software multicast route table.

Parameter: GroupAddr: show the multicast entries relative to this Group address.

SourceAddr：show the multicast route entries relative to this source address.

Default: None

Command Mode： Admin mode and global mode

Usage Guide:

Example: show all entries of multicast route table

Switch(config)#show ip mroute

Name: Loopback, Index: 2002, State:49

Name: null0, Index: 2003, State:49

Name: sit0, Index: 2004, State:80

Name: Vlan1, Index: 2005, State:1043

Name: Vlan2, Index: 2006, State:1002

Name: pimreg, Index: 2007, State:c1

The total matched ipmr active mfc entries is 1, unresolved ipmr entries is 0

Group	Origin	Iif	Wrong	Oif:TTL
225.1.1.1	192.168.1.136	vlan1	0	2006:1

Displayed information	Explanation
Name	the name of interface
Index	the index number of interface
State	the state of interface
The total matched ipmr active mfc entries	The total matched active IP multicast route mfc（multicast forwarding cache） entries
unresolved ipmr entries	unresolved ip multicast route entries
Group	the destination address of the entries
Origin	the source address of the entries
Iif	ingress interface of the entries
Wrong	packets received from the wrong interface

Oif	egress interface of the entries
TTL	the value of TTL

Remark: This command is common in PIM-SM and DVMRP.

20.3 PIM-SM

20.3.1 Introduction to PIM-SM

PIM-SM（Protocol Independent Multicast, Sparse Mode）is Protocol Independent Multicast Sparse Mode. It is a Multicast Routing Protocol in Sparse Mode and mainly used in big scale network with group members distributed relatively sparse and wide-spread. Unlike the Flooding&Prune of Dense Mode, PIM-SM Protocol assumes no host needs receiving Multicast data packets. PIM-SM router transmits Multicast Data Packets to a host only if it presents explicit requirement.

By setting RP (Rendezvous Point) and BSR (Bootstrap Router), PIM-SM announce Multicast packet to all PIM-SM routers and establish RPT (RP-rooted shared tree) based on RP using Join/Prune message of routers. Consequently the network bandwidth occupied by data packets and message control is cut down and the transaction cost of routers decreases. Multicast data get to the network segment where the Multicast group members are located along the shared tree flow. When the data traffic reaches a certain amount, Multicast data stream can be switched to the shortest path tree SPT based on the source to reduce network delay. PIM-SM doesn't rely on any specific Unicast Routing Protocol but make RPF Check using existing Unicast routing table.

1. PIM-SM Working Principle

The central working processes of PIM-SM are: Neighbor Discovery, Generation of RP Shared Tree (RPT), Multicast source registration, SPT Switch, etc. We won't describe the mechanism of Neighbor Discovery here since it is same as that of PIM-DM.

(1) Generation of RP Shared Tree (RPT)

When a host joins a Multicast Group G, the leaf router that is connected to this host directly finds out through IGMP message that there is a receiver of Multicast Group G, then it works out the corresponding Rendezvous Point RP for Multicast Group G, and send join message to upper lever nodes in RP direction. Every router on the way from the leaf router to RP will generate a (*, G) table entry, where a message from any source to Multicast group applies to this entry. When RP receives the message sent to Multicast Group G, the message will get to the leaf router along the set up path and reach the host. In this way the RPT with RP as root is generated.

(2) Multicast Source Registration

When a Multicast Source S sends a Multicast packet to Multicast Group G, the PIM-SM Multicast router connected to it directly will take charge of encapsulating the Multicast packet into registered message and unicast it to corresponding RP. If there are more than one PIM-SM Multicast routers on a network segment, then DR (Designated Router) takes charge of sending the Multicast packet.

(3) SPT Switch

When the Multicast router finds that the rate of the Multicast packet from RP with destination address G exceeds threshold, the Multicast router will send Join message to the next upper lever nodes in the source direction, which results in the switch from RPT to SPT.

2. Preparation before PIM-SM configuration

(1) Configuration Candidate RP

More than one RPs (candidate RP) can exist in PIM-SM network and each C-RP (Candidate RP) takes charge of transmitting Multicast packets with destination address in a certain range. To configure more than one candidate RPs can implement RP load share. No master or slave is differentiated among RPs. All Multicast routers work out the RP corresponding to some Multicast group based on the same algorithm after receiving the candidate RP message announced by BSR.

Note that one RP can serve more than one Multicast groups and all Multicast groups. Each Multicast group can only correspond to one unique RP at any moment. It can't correspond to more than one RP at the same time.

(2) Configure BSR

BSR is the management center of PIMSM network. It is in charge of collecting messages sent by candidate RPs and broadcast them.

Only one BSR can exist within a network, but more than one C-BSR (Candidate-BSR) can be configured. In this way, if some BSR goes wrong, it can switch to another. C-BSRs elect BSR automatically.

20.3.2 PIM-SM Configuration Task List

1、Enable PIM-SM (Required)

2、Configure PIM-SM sub-parameters (Optional)

（1） Configure PIM-SM interface parameters

2）Configure PIM-SM hello message interval

3）Configure interface as PIM-SM domain boundary

（1） Configure PIM-SM global parameters

1) Configure Switch as candidate BSR

2) Configure switch as candidate RP

3、Disable PIM-SM Protocol

1. Enable PIM-SM Protocol

The basic configuration to function PIM-SM Routing Protocol on EDGECORE series Layer 3 switch is very simple. It is only required to turn on PIM Multicast switch in Global Mode and turn on PIM-SM switch under corresponding interface.

Command	Explanation
Global Mode	
ip pim multicast-routing	Make PIM-SM Protocol on each interface to Enable status (but the commands below are required to really enable PIM-SM protocol on the interface) (Required)

And then turn on PIM-SM switch on the interface

Command	Explanation
Interface Configuration Mode	
ip pim sparse-mode	Enable PIM-SM Protocol of the interface. (Required)

2. Configure PIM-SM Sub-parameters

（1）Configure PIM-SM Interface Parameters

1）Configure PIM-SM hello message interval

Command	Explanation
Interface Configuration Mode	
ip pim hello-interval < *interval*> **no ip pim hello-interval**	Configure interface PIM-SM hello message interval; the "**no ip pim hello-interval**" command restores the default value.

2）Configure PIM-SM hello message holdtime

Command	Explanation
Interface Configuration Mode	
ip pim hello-holdtime <*value*> **no ip pim hello-holdtime**	Configure the value of holdtime field in interface PIM-SM hello message.

3）Configure PIM-SM Neighbor Access-list

Command	Explanation
Interface Configuration Mode	

[no] ip pim neighbor-filter{<*access-list-number*> }	Configure Neighbor Access-list. If a neighbor is filtered by the list and a connection has been set up with this neighbor, then this connection is cut off immediately; and if no connection is set up yet, then this connection can't be created.

（2） Configure PIM-SM Global Parameters

1) Configure switch to be candidate BSR

Command	Explanation
Global Mode	
ip pim bsr-candidate {vlan <*vlan-id*>| <*ifname*>}[<*mask-length*>][<*priority*>] **no ip pim bsr-candidate**	This command is the global candidate BSR configuration command, which is used to configure the information of PIM-SM candidate BSR so that it can compete for BSR router with other candidate BSRs. The "**no ip pim bsr-candidate**" command cancels the configuration of BSR.

2) Configure switch to be candidate RP

Command	Explanation
Global Mode	
ip pim rp-candidate { vlan <*vlan-id* >| <*ifname*>} **[<A.B.C.D/M>][<*priority*>]** **(no) ip pim rp-candidate**	This command is the global candidate RP configuration command, which is used to configure the information of PIM-SM candidate RP so that it can compete for RP router with other candidate RPs. The "**no ip pim rp-candidate**" command cancels the configuration of RP.

3) Configure Static RP

Command	Explanation
Global Mode	

ip pim rp-address <A.B.C.D> [<A.B.C.D/M>] **no ip pim rp-address <A.B.C.D> {<*all*>|<A.B.C.D/M>}**	This command is the global candidate RP configuration command, which is used to configure the information of PIM-SM candidate RP so that it can compete for RP router with other candidate RPs. The "**no ip pim rp-address <A.B.C.D> {<*all*>|<A.B.C.D/M>}**" command cancels the configuration of RP.

3Disable PIM-SM Protocol

Command	Explanation
Interface Configuration Mode	
no ip pim sparse-mode | no ip pim multicast-routing **no ip pim sparse-mode | no ip pim multicast-routing (Global Mode)**	Disable PIM-SM Protocol.

20.3.3 Commands for PIM-SM

20.3.3.1 ip pim accept-register

Command: ip pim accept-register list <*list-number*>

no ip pim accept-register

Function: Filter the specified multicast group and multicast address.

Parameter: <***list-number***>: **<*list-number*>** is the access-list number ,it ranges from 100 to 199.

Default: Permit the multicast registers from any sources to any groups.

Command Mode: Global Mode

Usage Guide: This command is used to configure the access-list filtering the PIM REGISTER packets.The addresses of the access-list respectively indicate the filtered multicast sources and multicast groups' information. For the source-group combinations that match DENY, PIM sends REGISTER-STOP immediately and does not create group records when receiving REGISTER packets. Unlike other access-list, when the access-list is configured ,the default value is PERMIT.

Example: Configure the filtered register message's rule to myfilter.

Switch(config)#ip pim accept-register list 120

Switch (config)#access-list 120 deny ip 10.1.0.2 0.0.0.255 239.192.1.10 0.0.0.255

20.3.3.2 ip pim bsr-candidate

Command: ip pim bsr-candidate {vlan <*vlan-id*>| <*ifname*>} [*hash-mask-length*] [*priority*]

no ip pim bsr-candidate

Function: This command is the candidate BSR configure command in global mode and is used to configure PIM-SM information about candidate BSR in order to compete the BSR router with other candidate BSRs. The command **"no ip pim bsr-candidate"** disables the candidate BSR.

Parameter: ***Ifname*** is the specified interface's name;

[*hash-mask-length*] is the specified hash mask length. It's used for the RP enable selection and ranges from 0 to 32;

[*priority*] is the candidate BSR priority and ranges from 0 to 255. If this parameter is not configured ,the default priority value is 0.

Default: This switch is not a candidate BSR router.

Command Mode: Global Mode

Usage Guide: This command is the candidate BSR configure command in global mode and is used to configure PIM-SM information about candidate BSR in order to compete the BSR router with other candidate BSRs. Only this command is configured , this switch is the BSR candidate router.

Example: Globally configure the interface vlan1 as the candidate BSR-message transmitting interface.

Switch (Config)# ip pim bsr-candidate vlan1 30 10

20.3.3.3 ip pim cisco-register-checksum

Command: ip pim cisco-register-checksum group-list [<*simple-acl*>]

no ip pim cisco-register-checksum group-list [<*simple-acl*>]

Function: Configure the register packet's checksum of the group specified by myfilter to use the whole packet's length.

Default: Compute the checksum according to the register packet's head length, default: 8

Parameter: <*simple-acl*>: <1-99> Simple access-list **<*simple-acl*>:** <1-99> Simple access-list

Command Mode: Global Mode

Usage Guide: This command is used to interact with older Cisco IOS version.

Example: Configure the register packet's checksum of the group specified by myfilter to use the whole packet's length.

Switch (config)#ip pim cisco-register-checksum group-list 23

20.3.3.4 ip pim dr-priority

Command: ip pim dr-priority <*priority*>

no ip pim dr-priority

Function: Configure, disable or change the interface's DR priority. The neighboring nodes in the same net segment select the DR in their net segment according to hello packets. The "**no ip pim dr-priority"** command restores the default value.

Parameter: <*priority*> is priority

Default: 1

Command Mode: Interface Configuration Mode

Usage Guide: Range from 0 to 4294967294, the higher value has more priority.

Example: Configure vlan's DR priority to 100

Switch (Config)# interface vlan 1

Switch(Config-if-Vlan1)ip pim dr-priority 100

Switch (Config -if-Vlan1)#

20.3.3.5 ip pim exclude-genid

Command: ip pim exclude-genid

no ip pim exclude-genid

Function: This command makes the Hello packets sent by PIM SM do not include GenId option. The "**no ipv6 pim exclude-genid**" command restores the default value

Parameter: None

Default: The Hello packets include GenId option.

Command Mode: Interface Configuration Mode

Usage Guide: This command is used to interact with older Cisco IOS version.

Example: Configure the Hello packets sent by the switch do not include GenId option.

Switch (Config-if-Vlan1)#ip pim exclude-genid

Switch (Config-if-Vlan1)#

20.3.3.6 ip pim hello-holdtime

Command: ip pim hello-holdtime <*value*>

no ip pim hello-holdtime

Function: Configure or disable the Holdtime option in the Hello packets, this value is to describe neighbor holdtime,if the switch hasn't received the neighbor hello packets when the holdtime is over, this neighbor is deleted. The "**no ip pim hello-holdtime**" command cancels configured holdtime value and restores default value.

Parameter: <*value*> is the value of holdtime.

Default: The default value of Holdtime is 3.5*Hello_interval, Hello_interval's default value

is 30s,so Hold time's default value is 105s.

Command Mode: Interface Configuration Mode

Usage Guide: If this value is not configured, hellotime's default value is 3.5*Hello_interval. If the configured holdtime is less than the current hello_interval , this configuration is denied. Every time hello_interval is updated, the Hello_holdtime will update according to the following rules: If hello_holdtime is not configured or hello_holdtime is configured but less than current hello_interval,hello_holdtime is modified to 3.5*hello_interval, otherwise the configured value is maintained.

Example: Configure vlan1's Hello Holdtime

Switch (Config)# interface vlan1

Switch (Config -if-Vlan1)#ip pim hello-holdtime 10

Switch (Config -if-Vlan1)#

20.3.3.7 ip pim hello-interval

Command: ip pim hello-interval <*interval*>

no ip pim hello-interval

Function: Configure the interface's hello_interval of pim hello packets. The "**no ip pim hello-interval**" command restores the default value.

Parameter: <*interval*> is the hello_interval of periodically transmitted pim hello packets', ranges from 1 to 18724s.

Default: The default periodically transmitted pim hello packets' hello_interval is30s.

Command Mode: Interface Configuration Mode

Usage Guide: Hello messages make pim switches oriented each other and determine neighbor relationship. Pim switch announce the existence of itself by periodically transmitting hello messages to neighbors. If no hello messages from neighbors are received in the certain time, the neighbor is considered lost. This value can't be greater than neighbor overtime.

Example: Configure vlan's pim-sm hello interval

Switch (Config)#interface vlan 1

Switch(Config-If-Vlan1)#ip pim hello-interval 20

Switch(Config-If-Vlan1)#

20.3.3.8 ip pim ignore-rp-set-priority

Command: ip pim ignore-rp-set-priority

no ip pim ignore-rp-set-priority

Function: When RP selection is carried out, this command configure the switch to enable Hashing regulation and ignore RP priority. This command is used to interact with older Cisco IOS versions.

Default: Disabled

Parameter: None

Command Mode: Global Mode

Usage Guide: When selecting RP, Pim usually will select according to RP priority. When this command is configured, pim will not select according to RP priority. Unless there are older routers in the net, this command is not recommended.

Example: Switch (config)#ip pim ignore-rp-set-priority

20.3.3.9 ip pim jp-timer

Command: ip pim jp-timer <*value*>

no ip pim jp-timer

Function: Configure to add JP timer. the "**no ip pim jp-timer**" command restores the default value.

Parameter: <*value*> ranges from 10 to 65535s

Default: 60s

Command Mode: Global Mode

Usage Guide: Configure the interval of JOIN-PRUNE packets sent by PIM periodically, the default value is 60s. The default value is recommended if no special reasons.

Example: Configure the interval of timer

Switch (config)#ip pim jp-timer 59

20.3.3.10 ip pim multicast-routing

Command: ip pim multicast-routing

no ip pim multicast-routing

Function: Enable PIM-SM globally. The "**no ip pim multicast-routing** » command disables PIM-SM globally.

Parameter: None

Default: Disabled PIM-SM

Command Mode: Global Mode

Usage Guide: Enable PIM-SM globally. The interface must enable PIM-SM to have PIM-SM work

Example: Enable PIM-SM globally.

Switch (Config)#ip pim multicast-routing

20.3.3.11 ip pim neighbor-filter

Command: ip pim neighbor-filter{<*list-number*>}

no ip pim neighbor-filter{<*list-number*>}

Function: Configure the neighbor access-list. If filtered by the lists and connections with

neighbors are created, this connections are cut off immediately. If no connection is created, this connection can't be created.

Parameter: <*list-number*>: <*list-number*> is the simple access-list number, it ranges from 1 to 99

Default: No neighbor filter configuration.

Command Mode: Interface Configuration Mode

Usage Guide: ACL's default is DENY. If configuring access-list 1,access-list 1's default is deny. In the following example, if "permit any-source" is not configured, deny 10.1.4.10 0.0.0.255 is the same as deny any-source.

Example: Configure vlan's filtering rules of pim neighbors.

```
Switch #show ip pim neighbor
Neighbor          Interface          Uptime/Expires      Ver   DR
Address                                                        Priority/Mode
10.1.4.10         Vlan1              02:30:30/00:01:41 v2     4294967294 / DR
Switch (Config-if-Vlan1)#ip pim neighbor-filter 2
Switch (config)#access-list 2 deny 10.1.4.10 0.0.0.255
Switch (config)#access-list 2 permit any-source
Switch (config)#show ip pim neighbor
```

20.3.3.12 ip pim state-refresh origination-interval

Command: ip pim state-refresh origination-interval <interval>

no ip pim state-refresh origination-interval

Function: Configure transmission interval of state-refresh message on interface. The "**no ip pim state-refresh origination-interval**" command restores default value.

Parameter: <*interval*> packet transmission interval value is from 4s to 100s.

Default: 60s

Usage Guide: The first-hop router periodically transmits stat-refresh messages to maintain PIM-DM list items of all the downstream routers. The command can modify origination interval of state-refresh messages. Usually do not modify relevant timer interval.

Example: Configure transmission interval of state-refresh message on interface vlan1 to 90s.

```
Switch (Config-if-Vlan1)#ip pim state-refresh origination-interval  90
```

20.3.3.13 ip pim register-rate-limit

Command: ip pim register-rate-limit <*limit*>

no ip pim register-rate-limit

Function: This command is used to configure the speedrate of DR sending register

packets; the unit is packet/second. The "**no ip pim Register-rate-limit**" command restores the default value. This configured speedrate is each（S, G）state's ,not the whole system's.

Parameter: *<limit>* ranges from 1 to 65535.

Default: No limit for sending speed

Command Mode: Global Mode

Usage Guide: This configuration is to prevent the attack to DR, limiting sending REGISTER packets.

Example: Configure the speedrate of DR sending register packets to 59 p/s.

Switch (config)#ip pim register-rate-limit 59

20.3.3.14 ip pim register-rp-reachability

Command: ip pim register-rp-reachability

no ip pim register-rp-reachability

Function: This command makes DR check the RP reachability in the process of registration.

Parameter: None

Default: Do not check

Command Mode: Global Mode

Usage Guide: This command configures DR whether or not to check the RP reachability.

Example: Configure DR to check the RP reachability.

Switch (config)#ip pim register-rp-reachability

20.3.3.15 ip pim register-source

Command: ip pim register-source {*<A.B.C.D>* | *<ifname>* | *<ethernet>* | vlan *<vlan-id>*}

no ip pim register-source

Function: This command is to configure the source address of register packets sent by DR to overwrite default source address. This default source address is usually the RPF neighbor of source host direction.

Parameter: *<ifname>* is the interface name,

<ethernet> is the ethernet interface,

<vlan-id> is VLAN ID;

<A.B.C.D> is the configured source IP addresses.

Default: Do not check

Command Mode: Global Mode

Usage Guide: The "**no ip pim register-source**" command restores the default value, no more parameter is needed. Configured address must be reachable to Register-Stop

messages sent by RP. It's usually a circle address, but it can be other physical addresses. This address must be announcable through unicast router protocols of DR.

Example: Configure the source address sent by DR.

Switch (config)#ip pim register-source 10.1.1.1

20.3.3.16 ip pim register-suppression

Command: ip pim register-suppression <*value*>

no ip pim register-suppression

Function: This command is to configure the value of register suppression timer, the unit is second. The "**no ip pim register-suppression**" command restores the default value.

Parameter: <***value***> is the timer's value, it ranges from 1 to 65535s.

Default: 60s

Command Mode: Global Mode

Usage Guide: If this value is configured at DR,it's the value of register suppression timer; if this value is configured at RP and ipv6 pim rp-register-kat is not used at RP, this command modifies Keepalive-period value.

Example: Configure the value of register suppression timer to 10s.

Switch (config)#ip pim register- suppression 10

20.3.3.17 ip pim rp-address

Command: ip pim rp- address <*A.B.C.D*> <*A.B.C.D/M*>

no ip pim rp-address <*A.B.C.D*> [<*A.B.C.D/M*>|<*all*>]

Function: This command is to configure static RP globally or in a multicast address range. The **"no ipv6 pim rp-address <*A.B.C.D*> [<*A.B.C.D/M*>|<*all*>]**" command cancels static RP.

Parameter: <*A.B.C.D*> is the RP address

<*A.B.C.D/M*> is the expected RP

<*all*> is all the range

Default: This switch is not a RP static router.

Command Mode: Global Mode

Usage Guide: This command is to configure static RP globally or in a multicast address range and configure PIM-SM static RP information. Attention, when computing rp, BSR RP is selected first. If it doesn't succeed, static RP is selected.

Example: Configure vlan1 as candidate RP announcing sending interface globally.

Switch (Config)# ip pim rp-address 10.1.1.1 238.0.0.0/8

20.3.3.18 ip pim rp-candidate

Command: ip pim rp-candidate { vlan < *vlan-id* >| <*ifname*>} [<*A.B.C.D/M*>]

[<priority>]

no ip pim rp-candiate

Function: This command is the candidate RP global configure command, it is used to configure PIM-SM candidate RP information in order to compete RP router with other candidate RPs. The "**no ip pim rp-candiate**" command cancels the candidate RP.

Parameter: ***vlan-id*** is**Vlan ID**;***ifname*** is the name of the specified interface;

A.B.C.D/M is the ip prefix and mask; ***<priority>*** is the RP selection priority, it ranges from 0 to 255, the default value is 192, the lower value has more priority.

Default: This switch is not a RP static router.

Command Mode: Global Mode

Usage Guide: This command is the candidate RP global configure command, it is used to configure PIM-SM candidate RP information in order to compete RP router with other candidate RPs.Only this command is configured, this switch is the RP candidate router.

Example: Configure vlan1 as the sending interface of candidate RP announcing sending messages

Switch (Config)# ip pim rp-candidate vlan1 100

20.3.3.19 ip pim rp-register-kat

Command: ip pim rp-register-kat <*vaule*>

no ip pim rp-register-kat

Function: This command is to configure the KAT（KeepAlive Timer）value of the RP（S, G）items, the unit is second. The "**no ip pim rp-register-kat**" command restores the default value.

Parameter: <*vaule*> is the timer value, it ranges from 1 to 65535s.

Default: 185s

Command Mode: Global Mode

Usage Guide: This command is to configure the RP's keep alive time, during the keep alive time RP's （S,G）item will not be deleted because it hasn't received REGISTER packets. If no new REGISTER packet is received when the keep alive time is over, this item will be obsolete.

Example: Configure the kat value of RP's (S,G) item to 180s

Switch (config)#ip pim rp-register- kat 180

20.3.3.20 ip pim sparse-mode

Command: ip pim sparse-mode [passive]

no ip pim sparse-mode [passive]

Function: Enable PIM-SM on the interface; the "**no ip pim sparse-mode [passive]**" command disables PIM-SM.

Parameter: [*passive*] means to disable PIM-SM (that's PIM-SM doesn't receive any packets) and only enable IGMP(receive and transmit IGMP packets).

Default: Do not enable PIM-SM

Command Mode: Interface Configuration Mode

Usage Guide: Enable PIM-SM on the interface.

Example: Enable PIM-SM on the interface vlan1.

Switch (Config)#interface vlan 1

Switch(Config-If-Vlan1)#ip pim sparse-mode

20.3.3.21 ip pim ssm

Command: ip pim ssm {default|range <*access-list-number* >}

no ip pim ssm

Function: Configure the range of pim ssm multicast address. The "**no ip pim ssm**" command deletes configured pim ssm multicast group.

Parameter: *default :* indicates the default range of pim ssm multicast group is 232/8.

<*access-list-number* > is the applying access-list number, it ranges from 1 to 99.

Default: Do not configure the range of pim ssm group address

Command Mode: Global Mode

Usage Guide:

1. Only this command is configured, pim ssm can be available.
2. Before configuring this command, make sure ip pim multicasting succeed. This command can't work with DVMRP.
3. Access-list can't use the lists created by ip access-list, but the lists created by access-list.
4. Users can execute this command first and then configure the corresponding acl; or delete corresponding acl in the bondage. After the bondage, only command no ip pim ssm can release the bondage.
5. If ssm is needed, this command should be configured at the related edge route. For example, the local switch with igmp(must) and multicast source DR or RP(at least one of the two) configure this command, the middle switch need only enable PIM-SM.

Example: Configure the switch to enable PIM-SSM, the group's range is what is specified by access-list 23.

Switch (config)#ip pim ssm range 23

20.3.4 PIM-SM Configuration Examples

As shown in the following figure, add the Ethernet interfaces of SwitchA, SwitchB, switchC and switchD to corresponding vlan, and enable PIM-SM Protocol on

each vlan interface.

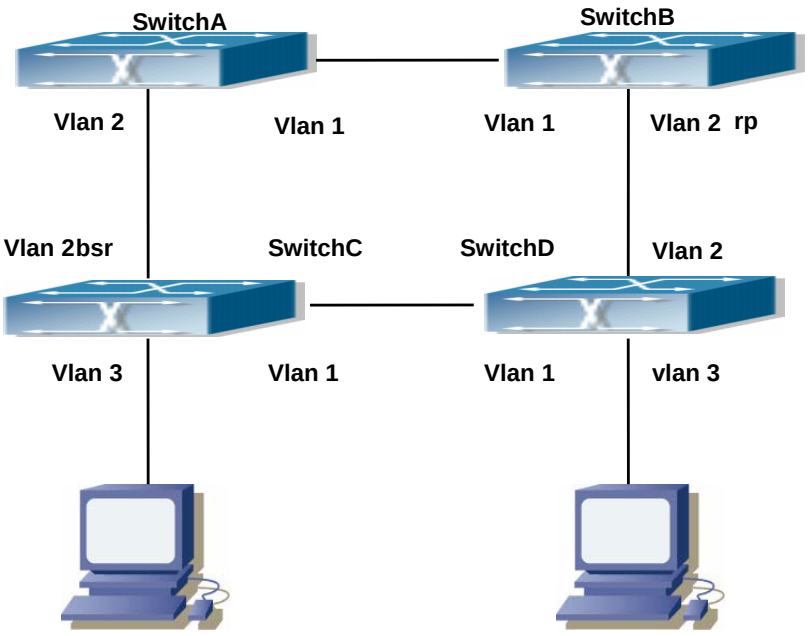


Fig 20-2 PIM-SM Typical Environment

The configuration procedure for SwitchA, SwitchB, switchC and switchD is as follows:

(1) Configure SwitchA:

Switch (Config)#ip pim multicast-routing

Switch (Config)#interface vlan 1

Switch(Config-If-Vlan1)# ip address 12.1.1.1 255.255.255.0

Switch(Config-If-Vlan1)# ip pim sparse-mode

Switch(Config-If-Vlan1)#exit

Switch (Config)#interface vlan 2

Switch(Config-If-Vlan2)# ip address 13.1.1.1 255.255.255.0

Switch(Config-If-Vlan2)# ip pim sparse-mode

(2) Configure SwitchB:

Switch (Config)#ip pim multicast-routing

Switch (Config)#interface vlan 1

Switch(Config-If-Vlan1)# ip address 12.1.1.2 255.255.255.0

Switch(Config-If-Vlan1)# ip pim sparse-mode

Switch(Config-If-Vlan1)#exit

Switch (Config)#interface vlan 2

Switch(Config-If-Vlan2)# ip address 24.1.1.2 255.255.255.0

Switch(Config-If-Vlan2)# ip pim sparse-mode

Switch(Config-If-Vlan2)# exit

```
Switch (Config)# ip pim rp-candidate vlan2
```

(3) Configure SwitchC:

```
Switch (Config)#ip pim multicast-routing
Switch (Config)#interface vlan 1
Switch(Config-If-Vlan1)# ip address 34.1.1.3 255.255.255.0
Switch(Config-If-Vlan1)# ip pim sparse-mode
Switch(Config-If-Vlan1)#exit
Switch (Config)#interface vlan 2
Switch(Config-If-Vlan2)# ip address 13.1.1.3 255.255.255.0
Switch(Config-If-Vlan2)# ip pim sparse-mode
Switch(Config-If-Vlan2)#exit
Switch (Config)#interface vlan 3
Switch(Config-If-Vlan3)# ip address 30.1.1.1 255.255.255.0
Switch(Config-If-Vlan3)# ip pim sparse-mode
Switch(Config-If-Vlan3)# exit
Switch (Config)# ip pim bsr-candidate vlan2 30 10
```

(4) Configure SwitchD:

```
Switch (Config)#ip pim multicast-routing
Switch (Config)#interface vlan 1
Switch(Config-If-Vlan1)# ip address 34.1.1.4 255.255.255.0
Switch(Config-If-Vlan1)# ip pim sparse-mode
Switch(Config-If-Vlan1)#exit
Switch (Config)#interface vlan 2
Switch(Config-If-Vlan2)# ip address 24.1.1.4 255.255.255.0
Switch(Config-If-Vlan2)# ip pim sparse-mode
Switch(Config-If-Vlan2)#exit
Switch (Config)#interface vlan 3
Switch(Config-If-Vlan3)# ip address 40.1.1.1 255.255.255.0
Switch(Config-If-Vlan3)# ip pim sparse-mode
```

At the same time, you should pay attention to the configuration of Unicast Routing Protocol, assure that each device can communicate with each other in the network layer, and be able to implement dynamic routing update in virtue of Unicast Routing Protocol.

20.3.5 PIM-SM Troubleshooting

In configuring and using PIM-SM Protocol, PIM-SM Protocol might not operate normally caused by physical connection or incorrect configuration. Therefore, the user should pay

attention to the following issues:

- ✧ Assure that physical connection is correct;
- ✧ Assure the Protocol of Interface and Link is UP (use show interface command);
- ✧ Assure that PIM Protocol is enabled in Global Mode (use ip pim multicast-routing)
- ✧ Assure that PIM-SM is configured on the interface (use ip pim sparse-mode);
- ✧ Multicast Protocol requires RPF Check using unicast routing; therefore the correctness of unicast routing must be assured beforehand.
- ✧ PIM-SM Protocol requires supports by rp and bsr, therefore you should use **show ip pim bsr-router** first to see if there is bsr information. If not, you need to check if there is unicast routing leading to bsr.
- ✧ Use **show ip pim rp-hash** command to check if rp information is correct; if there is not rp information, you still need to check unicast routing;

If all attempts including Check are made but the problems on PIM-SM can't be solved yet, then use debug commands such debug pim/debug pim bsr please, and then copy DEBUG information in 3 minutes and send to Technology Service Center.

20.3.5.1 Commands for Monitor And Debug

20.3.5.1.1 debug pim timer sat

Command: debug pim timer sat

no debug pim timer sat

Function: Enable debug switch of PIM-SM source activity timer information in detail; the "**no debug pim timer sat**" command disenables the debug switch.

Parameter: None.

Default: Disabled.

Command Mode: Admin Mode.

Usage Guide: Enable the switch, and display source activity timer information in detail.

Example:

Switch # debug ip pim timer sat

20.3.5.1.2 debug pim timer srt

Command: debug pim timer srt

no debug pim timer srt

Function: Enable debug switch of PIM-SM state-refresh timer information in detail; the "**no debug pim timer srt**" command disenables the debug switch.

Parameter: None.

Default: Disabled.

Command Mode: Admin Mode and Global Mode.

Usage Guide: Enable the switch, and display PIM-SM state-refresh timer information in

detail.

Example: Switch # debug ip pim timer srt

20.3.5.1.3 debug pim event

Command: debug pim event

no debug pim event

Function: Enable or Disable pim event debug switch

Parameter: None

Default: Disabled

Command Mode: Enable or Disable pim event debug switch

Usage Guide: Enable pim event debug switch and display events information about pim operation.

Example: Switch# debug ip pim event

20.3.5.1.4 debug pim mfc

Command: debug pim mfc

no debug pim mfc

Function: Enable or Disable pim mfc debug switch

Parameter: None

Default: Disabled

Command Mode: Admin Mode and Global Mode

Usage Guide: Enable pim mfc debug switch and display generated and transmitted multicast id's information.

Example: Switch# debug ip pim mfc

20.3.5.1.5 debug pim mib

Command: debug pim mib

no debug pim mib

Function: Enable or Disable PIM MIB debug switch

Parameter: None

Default: Disabled

Command Mode: Admin Mode and Global Mode

Usage Guide: Inspect PIM MIB information by PIM MIB debug switch. It's not available now and it's for the future extension.

Example: Switch# debug ip pim mib

20.3.5.1.6 debug pim nexthop

Command: debug pim nexthop

no debug pim nexthop

Function: Enable or Disable pim nexthop debug switch

Parameter: None

Default: Disabled

Command Mode: Admin Mode and Global Mode

Usage Guide: Inspect PIM NEXTHOP changing information by the pim nexthop switch.

Example: Switch# debug ip pim nexthop

20.3.5.1.7 debug pim nsm

Command: debug pim nsm

no debug pim nsm

Function: Enable or Disable pim debug switch communicating with Network Services

Parameter: None

Default: Disabled

Command Mode: Admin Mode and Global Mode

Usage Guide: Inspect the communicating information between PIM and Network Services by this switch.

Example: Switch# debug ip pim nsm

20.3.5.1.8 debug pim packet

Command: debug pim packet

debug pim packet in

debug pim packet out

no debug pim packet

no debug pim packet in

no debug pim packet out

Function: Enable or Disable pim debug switch

Parameter: in display only received pim packets

out display only transmitted pim packets

none display both

Default: Disabled

Command Mode: Admin Mode and Global Mode

Usage Guide: Inspect the received and transmitted pim packets by this switch.

Example: Switch# debug ip pim packet in

20.3.5.1.9 debug pim state

Command: debug pim state

no debug pim state

Function: Enable or Disable pim debug switch

Parameter: None

Default: Disabled

Command Mode: Admin Mode and Global Mode

Usage Guide: Inspect the changing information about pim state by this switch.

Example: Switch# debug ip pim state

20.3.5.1.10 debug pim timer

Command: debug pim timer

debug pim timer assert
debug pim timer assert at
debug pim timer bsr bst
debug pim timer bsr crp
debug pim timer bsr
debug pim timer hello ht
debug pim timer hello nlt
debug pim timer hello tht
debug pim timer hello
debug pim timer joinprune et
debug pim timer joinprune jt
debug pim timer joinprune kat
debug pim timer joinprune ot
debug pim timer joinprune plt
debug pim timer joinprune ppt
debug pim timer joinprune pt
debug pim timer joinprune
debug pim timer register rst
debug pim timer register
no debug pim timer
no debug pim timer assert
no debug pim timer assert at
no debug pim timer bsr bst
no debug pim timer bsr crp
no debug pim timer bsr
no debug pim timer hello ht
no debug pim timer hello nlt
no debug pim timer hello tht
no debug pim timer hello
no debug pim timer joinprune et
no debug pim timer joinprune jt
no debug pim timer joinprune kat
no debug pim timer joinprune ot
no debug pim timer joinprune plt
no debug pim timer joinprune ppt

no debug pim timer joinprune pt

no debug pim timer joinprune

no debug pim timer register rst

no debug pim timer register

Function: Enable or Disable each pim timer

Parameter: None

Default: Disabled

Command Mode: Admin Mode and Global Mode

Usage Guide: Enable the specified timer's debug information.

Example: Switch# debug ip pim timer assert

20.3.5.1.11 show ip pim bsr-router

Command: show ip pim bsr-router

Function: Display BSR address

Parameter: None

Default: None

Command Mode: Admin Mode and Global Mode

Usage Guide: Display the BSR information maintained by the PIM.

Example: show ip pim bsr-router

PIMv2 Bootstrap information

This system is the Bootstrap Router (BSR)

BSR address: 10.1.4.3 (?)

Uptime: 00:06:07, BSR Priority: 0, Hash mask length: 10

Next bootstrap message in 00:00:00

Role: Candidate BSR

State: Elected BSR

Next Cand_RP_advertisement in 00:00:58

RP: 10.1.4.3(Vlan1)

Displayed Information	Explanations
BSR address	Bsr-router Address
Priority	Bsr-router Priority
Hash mask length	Bsr-router hash mask length
State	The current state of this candidate BSR, Elected BSR is selected BSR

20.3.5.1.12 show ip pim interface

Command: show ip pim interface

Function: Display PIM interface information

Parameter: None

Default: None

Command Mode: Admin Mode and Global Mode

Usage Guide: Display PIM interface information

Example: testS2(config)#show ip pim interface

Address	Interface	VIFindex	Ver/ Mode	Nbr Count	DR Prior	DR
10.1.4.3	Vlan1	0	v2/S	1	1	10.1.4.3
10.1.7.1	Vlan2	2	v2/S	0	1	10.1.7.1

Displayed Information	Explanations
Address	Interface address
Interface	Interface name
VIF index	Interface index
Ver/Mode	Pim version and mode,usually v2,sparse mode displays S,dense mode displays D
Nbr Count	The interface's neighbor count
DR Prior	Dr priority
DR	The interface's DR address

20.3.5.1.13 show ip pim mroute sparse-mode

Command: show ip pim mroute sparse-mode [group <*A.B.C.D*>] [source <*A.B.C.D*>]

Function: Display the multicast route table of PIM-SM.

Parameter: group <A.B.C.D>: Display redistributed items that related to this multicast address

source <A.B.C.D>: Display redistributed items that related to this source

Default: None

Command Mode: Admin Mode and Global Mode

Usage Guide: Display the BSP routers in the network maintained by PIM-SM.

Example: testS2#show ip pim mroute sparse-mode

IP Multicast Routing Table

(*,*,RP) Entries: 0

(*,G) Entries: 1

(S,G) Entries: 0

(S,G,rpt) Entries: 0

(*, 239.192.1.10)

RP: 10.1.6.1

RPF nbr: 10.1.4.10

RPF idx: Vlan1

Upstream State: JOINED

Local ..I.....

Joined .....

Asserted .....

Outgoing ..o.....

Displayed Information	Explanations
Entries	The counts of each item
RP	Share tree's RP address
RPF nbr	RP direction or upneighbor of source direction.
RPF idx	RPF nbr interface
Upstream State	Upstream State, there are two state of Joined(join the tree, expect to receive data from upstream) and Not Joined(quit the tree, not expect to receive data from upstream), and more options such as RPT Not Joined, Pruned, Not Pruned are available for（S,G,rpt.）
Local	Local join interface, this interface receive IGMPJoin
Joined	PIM join interface, this interface receive J/P messages
Asserted	Asserted state
Outgoing	Final outgoing of multicast data, in this example, the index of the outgoing interface is 2. Command "show ip pim interface" can query interface information.

20.3.5.1.14 show ip pim neighbor

Command: show ip pim neighbor

Function: Display router neighbors

Parameter: None

Default: None

Command Mode: Admin Mode and Global Mode

Usage Guide: Display multicast router neighbors maintained by the PIM

Example: s1(config)#show ip pim neighbor

Neighbor Address	Interface	Uptime/Expires	Ver	DR Priority/Mode
10.1.6.1	Vlan1	00:00:10/00:01:35	v2	1 /
10.1.6.2	Vlan1	00:00:13/00:01:32	v2	1 /
10.1.4.2	Vlan3	00:00:18/00:01:30	v2	1 /
10.1.4.3	Vlan3	00:00:17/00:01:29	v2	1 /

Displayed Information	Explanations
Neighbor Address	Neighbor address
Interface	Neighbor interface
Uptime/Expires	Running time /overtime
Ver	Pim version ,v2 usually
DR Priority/Mode	DR priority in the hello messages from the neighbor and if the neighbor is the interface's DP.

20.3.5.1.15 show ip pim nexthop

Command: show ip pim nexthop

Function: Display the PIM buffered nexthop router in the unicast route table

Parameter: None

Default: None

Command Mode: Admin Mode and Global Mode

Usage Guide: Display the PIM buffered nexthop router information.

Example:

Switch(config)#show ip pim nexthop

Flags: N = New, R = RP, S = Source, U = Unreachable

Destination	Type	Nexthop Num	Nexthop Addr	Nexthop Ifindex	Nexthop Name	Metric	Pref	Refcnt
192.168.1.1	N...	1	0.0.0.0	2006		0	0	1
192.168.1.9	..S.	1	0.0.0.0	2006		0	0	1

Displayed Information	Explanations
Destination	Destination of next item
Type	N: created nexthop,RP direction and S

	direction are not determined . R: RP direction S: source direction U: can't reach
Nexthop Num	Nexthop number
Nexthop Addr	Nexthop address
Nexthop Ifindex	Nexthop interface index
Nexthop Name	Nexthop name
Metric	Metric Metric to nexthop
Pref	Preference Route preference
Refcnt	Reference count

20.3.5.1.16 show ip pim rp-hash

Command: show ip pim rp-hash <*A.B.C.D*>

Function: Display the RP address of A,B,C,D's merge point

Parameter: Group address

Default: None

Command Mode: Admin Mode and Global Mode

Usage Guide: Display the RP address corresponding to the specified group address

Example: testS2(Config-if-Vlan1)#show ip pim rp-hash 239.192.1.10

RP: 10.1.6.1

Info source: 10.1.6.1, via bootstrap

Displayed Information	Explanations
RP	Queried group'sRP
Info source	The source of Bootstrap information

20.3.5.1.17 show ip pim rp mapping

Command: show ip pim rp mapping

Function: Display Group-to-RP Mapping and RP

Parameter: None

Default: None

Command Mode: Admin Mode and Global Mode

Usage Guide: Display the current RP and mapping relationship.

Example: testS2(Config-if-Vlan1)#show ip pim rp mapping

PIM Group-to-RP Mappings

Group(s): 224.0.0.0/4

RP: 10.1.6.1

Info source: 10.1.6.1, via bootstrap, priority 6

Uptime: 00:11:04

Displayed Information	Explanations
Group(s)	Group address range of RP

Info source	Source of Bootstrap messages
Priority	Priority of Bootstrap messages

20.4 DVMRP

20.4.1 Introduction to DVMRP

DVMRP Protocol, namely, is “Distance Vector Multicast Routing Protocol”. It is a Multicast Routing Protocol in dense mode, which sets up a Forward Broadcast Tree for each source in a manner similar to RIP, and sets up a Truncation Broadcast Tree, i.e. the Shortest Path Tree to the source, for each source through dynamic Prune/Graft.

Some of the important features of DVMRP are:

1. The routing exchange used to determine reverse path checking information is based on distance vector (in a manner similar to RIP)
2. Routing exchange update occurs periodically (the default is 60 seconds)
3. TTL upper limit = 32 hops (and that RIP is 16)
4. Routing update includes net mask and supports CIDR

In comparison with Unicast routing, Multicast routing is a kind of reverse routing (that is, what you are interested in is where the packets are from but not where they go), thus the information in DVMRP routing table is used to determine if an input Multicast packet is received at the correct interface. Otherwise, the packet will be discarded to prevent Multicast circulation.

The check which determines if the packet gets to the correct interface is called RPF check. When some Multicast data packets get to some interface, it will determine the reverse path to the source network by looking up DVMRP router table. If the interface data packets get to is the one which is used to send Unicast message to the source, then the reverse path check is correct, and the data packets are forwarded out from all downstream interfaces. If not, then probably there is failure, and the Multicast packet is discarded.

Since not all switches support Multicast, DVMRP supports tunnel multicast communication, tunnel is a method to send multicast data report among DVMRP switches separated by switches which don’t support multicast routing. Multicast data packets are encapsulated in unicast data packets and directly sent to the next switch which supports multicast. DVMRP Protocol treat tunnel interface and general physical interface equally.

If two or more switches are connected to a multi-entrance network, it is likely to

transmit more than one copy of a data packet to the sub-network. Thus a specified transmitter must be appointed. DVMRP achieves this goal by making use of routing exchange mechanism; when two switches on the multi-entrance network exchange routing information, they will be aware of the routing distance from each other to the source network, thus the switch with the shortest distance to the source network will become the specified transmitter of the sub-network. If some have the same distance, then the one with the lowest IP prevails.

After some interface of the switch is configured to Function DVMRP Protocol, the switch will multicast Probe message to other DVMRP switches on this interface, which is used to find neighbors and detect the capabilities of each other. If no Probe message from the neighbor is received until the neighbor is timed out, then this neighbor is considered missing.

In DVMRP, source network routing selection message are exchanged in a basic manner same to RIP. That is, routing report message is transmitted among DVMRP neighbors periodically (the default is 60 seconds). The routing information in DVMRP routing selection table is used to set up source distribution tree, i.e. to determine by which neighbor it passes to get to the source transmitting multicast packet; the interface to this neighbor is called upstream interface. The routing report includes source network (use net mask) address and the hop entry for routing scale.

In order to finish transmission correctly, every DVMRP switch needs to know which downstream switches need to receive multicast packet from some specific source network through it. After receiving packets from some specific source, DVMRP switch firstly will broadcast these multicast packets from all downstream interfaces, i.e. the interfaces on which there are other DVMRP switches which have dependence on the specific source. After receiving Prune message from some downstream switch on the interface, it will prune this switch. DVMRP switch makes use of poison reverse to notify the upstream switch for some specific source: “I am your downstream.” By adding infinity (32) to the routing distance of some specific source it broadcasts, DVMRP switch responds to the source upstream exchange to fulfill poison reverse. This means distance correct value is 1 to 2* infinity (32) -1 or 1 to 63, 1 to 63 means it can get to source network, 32 means source network is not arrival, 33 to 63 means the switch which generates the report message will receive multicast packets from specific source depending on upstream router.

20.4.2 Configuration Task List

1、Globally enable and disable DVMRP (required)

2、Configure Enable and Disable DVMRP Protocol at the interface (optional)

3、 Configure DVMRP Sub-parameters (optional)

Configure DVMRP interface parameters

1）Configure the delay of transmitting report message on DVMRP interface and the message number each time it transmits.

2） Configure metric value of DVMRP interface

3） Configure if DVMRP is able to set up neighbors with DVMRP routers which can not Prune/Graft

4、 Configure DVMRP tunnel

1. Globally enable DVMRP Protocol

The basic configuration to function DVMRP routing protocol on EDGECORE series Layer 3 switch is very simple. Firstly it is required to turn on DVMRP switch globally.

Command	Explanation
Global Mode	
[no] ip dvmrp multicast-routing	Globally enable DVMRP Protocol, the "**no ip dvmrp multicast-routing**" command disables DVMRP Protocol globally. (Required)

2. Enable DVMRP Protocol on the interface

The basic configuration to function DVMRP routing protocol on EDGECORE series Layer 3 switch is very simple. After globally enabling DVMRP Protocol, it is required to turn on DVMRP switch under corresponding interface.

Command	Explanation
Interface Configuration Mode	
ip dvmrp **[no] ip dvmrp**	Enable DVMRP Protocol on the interface, the "**no ip dvmrp**" command disables DVMRP Protocol on the interface.

3. Configure DVMRP Sub-parameters

（1）Configure DVMRP Interface Parameters

1）Configure the delay of transmitting report message on DVMRP interface and the message number each time it transmits.

2）Configure metric value of DVMRP interface

3）Configure if DVMRP is able to set up neighbors with DVMRP routers which can not Prune/Graft

Command	Explanation
Interface Configuration Mode	

ip dvmrp output-report-delay <*delay_val*> [<*burst_size*>] **no ip dvmrp output-report-delay**	Configure the delay of transmitting DVMRP report message on interface and the message number each time it transmits, the "**no ip dvmrp output-report-delay**" command restores default value.
ip dvmrp metric <*metric_val*> **no ip dvmrp metric**	Configure interface DVMRP report message metric value; the "**no ip dvmrp metric**" command restores default value.
ip dvmrp reject-non-pruners **no ip dvmrp reject-non-pruners**	Configure the interface rejects to set up neighbor relationship with non pruning/grafting DVMRP router. The "**no ip dvmrp reject-non-pruners**" command restores to being able to set up neighbor ship.

4. Configure DVMRP Tunnel

Command	Explanation
Interface Configuration Mode	
ip dvmrp tunnel <*index*> <*src-ip*> <*dst-ip*> **no ip dvmrp tunnel {<*index*> |<*src-ip*> <*dst-ip*>}**	This command configures a DVMRP tunnel; the "**no ip dvmrp tunnel {<*index*> |<*src-ip*> <*dst-ip*>}**" command deletes a DVMRP tunnel.

20.4.3 Commands for DVMRP

20.4.3.1 ip dvmrp

Command: ip dvmrp

no ip dvmrp

Function: Configure to enable DVMRP protocol on interface; the "**no ip dvmrp**" command disenables DVMRP protocol.

Parameter: None

Default: Disable DVMRP Protocol

Command Mode: Interface Configuration Mode

Usage Guide: The interface processes DVMRP protocol messages, only executing DVMRP protocol on interface.

Example: Enable DVMRP Protocol on interface vlan1.

Switch (Config)#interface vlan 1

Switch(Config-If-vlan1)#ip dvmrp

20.4.3.2 ip dvmrp metric

Command: ip dvmrp metric <*metric_val*>

no ip dvmrp metric

Function: Configure interface DVMRP report message metric value; the "**no ip dvmrp metric**" command restores default value.

Parameter: <*metric_val*> is metric value, value range from 1 to 31

Default: Default: 1

Command Mode: Interface Configuration Mode

Usage Guide: The routing information in DVMRP report messages includes a groupsource network and metric list. After configuring interface DVMRP report message metric value, it makes all received routing entries from the interface adding configured interface metric value as new metric value of the routing. The metric value applies to calculate position reverse, namely ensuring up-downstream relations. If the metric value of some route on the switch is not less than 32, it explains the route can be reach. If it is downstream of some route after calculation and judgment, it will transmit report message included the route to upstream. The route metric increases 32 based on original value in order to indicate downstream itself.

Example: Configure interface DVMRP report message metric value: 2

Switch (Config)#interface vlan 1

Switch(Config-If-Vlan1)#ip dvmrp metric 2

20.4.3.3 ip dvmrp multicast-routing

Command: ip dvmrp multicast-routing

no ip dvmrp multicast-routing

Function: Globally enable DVMRP protocol; the "no ip dvmrp multicast-routing" command globally disenables DVMRP protocol

Parameter: None

Default: Defalut

Command Mode: Global Mode

Usage Guide: Dvmrp multicast-protocol can enable after globally execute the command

Example: Switch (Config)#ip dvmrp multicast-routing

20.4.3.4 ip dvmrp output-report-delay

Command: ip dvmrp output-report-delay <*delay_val*> [<*burst_size*>]

no ip dvmrp output-report-delay

Function: Configure the delay of DVMRP report message transmitted on interface and transmitted message quantity every time, the "**no ip dvmrp output-report-delay**"

command restores default value.

Parameter: <*delay_val*> is the delay of periodically transmitted DVMRP report message, value range from 1s to 5s. **<*burst_size*>** is a quantity of transmitted message every time, value range from 1 to 65535

Default: Default the delay of transmitted DVMRP report message as 1s, default: transmitting two messages every time.

Command Mode: Interface Configuration Mode

Usage Guide: Avoid message burst if setting an appropriate delay.

Example: Switch (Config-If-vlan1)#ip dvmrp output-report-delay 1 1024

20.4.3.5 ip dvmrp reject-non-pruners

Command: ip dvmrp reject-non-pruners

no ip dvmrp reject-non-pruners

Function: Configure to reject neighbor ship with DVMRP router of non pruning/grafting on the interface, the "**no ip dvmrp reject-non-pruners**" command restores neighbor ship can be established.

Parameter: None

Default: Default

Command Mode: Interface Configuration Mode

Usage Guide: The command determines if it will establish neighboring ship with DVMRP router of non pruning/grafting or not.

Example: Switch (Config-If-vlan1)#ip dvmrp reject-non-pruners

20.4.3.6 ip dvmrp tunnel

Command: ip dvmrp tunnel <*index*> <*src-ip*> <*dst-ip*>

no ip dvmrp tunnel {**<*index*> |<*src-ip*> <*dst-ip*>}**

Function: Configure a DVMRP tunnel; the "**no ip dvmrp tunnel** {**<*index*> |<*src-ip*> <*dst-ip*>}**" command deletes a DVDMRP tunnel.

Parameter: <*src-ip*> is source IP address,

<*dst-ip*> is remote neighbor IP address,

<*index*> is tunnel index number, value range from 1 to 65525.

Default: Default: Do not Configure DVMRP tunnel.

Command Mode: Global Mode

Usage Guide: Because not all of switches support multicast, DVMRP supports tunnel multicast communication. The tunnel is a way of transmitted multicast data packet among DVMRP switches partitioned off switches without supporting multicast routing. It acts as a virtual network between two DVMRP switches. Multicast data packages packed in unicast data packages, directly are transmitted to next supporting multicast switch.

DVMRP protocol equally deal with tunnel interface and general physical interface. After configuring no ip dv multicast-routing, all of the tunnel configurations are deleted.

Example: Switch(Config)#ip dvmrp tunnel 1 12.1.1.1 24.1.1.1

20.4.4 DVMRP Configuration Examples

As shown in the following figure, add the Ethernet interfaces of Switch A and Switch B to corresponding vlan, and enable DVMRP on each vlan interface.

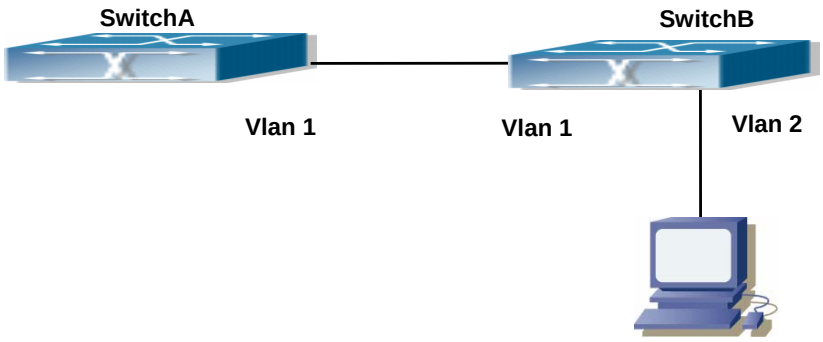


Fig 20-3DVMRP Network Topology Diagram

The configuration procedure for SwitchA and SwitchB is as follows:

(1) Configure SwitchA:

Switch (Config)#ip dvmrp multicast-routing

Switch (Config)#interface vlan 1

Switch(Config-if-Vlan1)# ip address 10.1.1.1 255.255.255.0

Switch(Config-if-Vlan1)# ip dvmrp

Switch(Config-if-Vlan1)#exit

Switch (Config)#interface vlan2

Switch(Config-if-Vlan2)# ip address 12.1.1.1 255.255.255.0

Switch(Config-if-Vlan2)# ip dvmrp

(2) Configure SwitchB:

Switch (Config)#ip dvmrp multicast-routing

Switch (Config)#interface vlan 1

Switch(Config-if-Vlan1)# ip address 12.1.1.2 255.255.255.0

Switch(Config-if-Vlan1)# ip dvmrp

Switch(Config-if-Vlan1)#exit

Switch (Config)#interface vlan 2

Switch(Config-if-Vlan2)# ip address 20.1.1.1 255.255.255.0

Switch(Config-if-Vlan2)# ip dvmrp

Since DVMRP itself does not rely on Unicast Routing Protocol, it is not necessary to

configure Unicast Routing Protocol. This is the difference from PIM-DM and PIM-SM.

20.4.5 DVMRP Troubleshooting

In configuring and using DVMRP Protocol, DVMRP Protocol might not operate normally caused by physical connection or incorrect configuration. Therefore, the user should pay attention to the following issues:

- ✧ Firstly to assure that physical connection is correct.
- ✧ Next, to assure the Protocol of Interface and Link is UP (use show interface command);
- ✧ Please check if the correct IP address is configured on the interface (use **ip address** command)
- ✧ Afterwards, enable DVMRP Protocol on the interface (use **ip dvmrp** command and **ip dv multicast-routing** command)
- ✧ Multicast Protocol requires RPF Check using unicast routing; therefore the correctness of unicast routing must be assured beforehand.(DVMRP uses its own unicast table, please use show ip dvmrp route command to look up);

If all attempts including Check are made but the problems on DVMRP can't be solved yet, then please use commands such as debug dvmrp, and then copy DEBUG information in 3 minutes and send to Technology Service Center.

20.4.5.1 Monitor And Debug Command

20.4.5.1.1 debug dvmrp

Command: debug dvmrp [events[neighbor|packet|igmp|kernel|prune [detail] |route]| nsm|mfc|mib|timer [probe[probe-timer|neigbor-expiry-timer]| prune[prune-expiry-timer|prune-retx-timer|graft-retx-timer]| route[report-timer|flash-upd-timer|route-expirytimer|route-holdown-timer|route-burst-timer]|packet[[probe [in|out] | report [in|out | prune [in|out] raft [in|out] | graft-ack [in|out] |in|out]]|all]

no debug dvmrp [events[neighbor|packet|igmp|kernel|prune [detail] |route]| nsm| mfc|mib|timer [probe[probe-timer|neigbor-expiry-timer]| prune[prune-expiry-timer|prune-retx-timer|graft-retx-timer]| route[report-timer|flash-upd-timer|route-expirytimer| route-holdown-timer|route-burst-timer]] |packet[[probe [in|out] | report [in|out | prune [in|out] raft [in|out] | graft-ack [in|out] |in|out]]| all]

Function: Display DVMRP protocol debugging message; the "**no debug dvmrp**

[events[neighbor|packet|igmp|kernel|prune [detail] |route]| nsm|
mfc|mib|timer [probe[probe-timer|neigbor-expiry-timer]|
prune[prune-expiry-timer|prune-retx-timer|graft-retx-timer]|
route[report-timer|flash-upd-timer|route-expirytimer|
route-holdown-timer|route-burst-timer]]
|packet[[probe [in|out] | report [in|out | prune [in|out] raft [in|out] | graft-ack
[in|out] |in|out]]|
all]" command disenables this debugging switch.

Parameter: None

Default: Disabled

Command Mode: Admin Mode

Usage Guide: Enable this switch, and display DVMRP protocol executed relevant messages.

20.4.5.1.2 show ip dvmrp

Command: show ip dvmrp

Function: Display DVMRP protocol information.

Parameter: None

Default: Do not display (Off)

Command Mode: Any Configuration Mode

Usage Guide: The command applies to display some total statistic information of DVMRP protocol

Example:

Switch#show ip dvmrp
DVMRP Daemon Start Time: MON JAN 01 00:00:09 2001
DVMRP Daemon Uptime: 17:37:03
DVMRP Number of Route Entries: 2
DVMRP Number of Reachable Route Entries: 2
DVMRP Number of Prune Entries: 1
DVMRP Route Report Timer: Running
DVMRP Route Report Timer Last Update: 00:00:56
DVMRP Route Report Timer Next Update: 00:00:04
DVMRP Flash Route Update Timer: Not Running

20.4.5.1.3 show ip dvmrp interface

Command: show ip dvmrp interface [<*ifname*>]

Function: Display DVMRP interface

Parameter:<*ifname*> is interface name, namely displaying configured interface information of specified interface.

Default: Do not display (Off)

Command Mode: Any Configuration Mode

Example:

Switch #show ip dv in vlan4

Address	Interface	Vif Index	Ver.	Nbr Cnt	Type	Remote Address
13.1.1.3	Vlan1	1	v3.ff	0	BCAST	N/A
10.1.35.3	Vlan2	0	v3.ff	0	BCAST	N/ASwitch #

Displayed Information	Explanations
Address	Address
Interface	Interface corresponding physical interface name
Vif Index	Virtual interface index
Ver	Interface supporting version
Nbr Cnt	Neighbor count
Type	Interface type
Remote Address	Remote address

20.4.5.1.4 show ip dvmrp neighbor

Command: show ip dvmrp neighbor [{<*ifname*> <A.B.C.D> [detail]}|{ <*ifname*>[detail]}|detail]

Function: Display DVMRP neighbor.

Parameter: ***<ifname>*** is interface name, namely displaying neighbor information of specified interface.

Default: Do not display (Off).

Command Mode: Any Configuration Mode

Example: Display interface vlan1 neighbor on Ethernet.

Switch #show ip dvmrp neighbor

Neighbor Address	Interface	Uptime/Expires	Maj Ver	Min Ver	Cap Flg
10.1.35.5	Vlan2	00:00:16/00:00:29	3	255	2e

Displayed Information	Explanations
Neighbor Address	Neighbor address
Interface	Detect the neighbor’s interface
Uptime/Expires	The neighbor uptime/expire time
Maj Ver	Major version
Min Ver	Mini version

Cap Flg	Capacity flag

20.4.5.1.5 show ip dvmrp pr

Command: show ip dvmrp pr [{group <A.B.C.D> [detail]}|{source <A.B.C.D/M> group <A.B.C.D> [detail]}|{source <A.B.C.D/M> [detail] }|detail]

Function: Display DVMRP message forwarding item.

Parameter: None

Default: Do not display

Command Mode: Any Configuration Mode

Usage Guide: This command applies to display DVMRP multicast forwarding item, namely multicast forwarding table calculated by dvmrp protocol.

Example:

Switch#show ip dv prune

Flags: P=Pruned,H=Host,D=Holddown,N=NegMFC,I=Init

Source Address	Mask Len	Group Address	State	FCR Exptime Cnt	Prune/Graft ReXmit-Time
13.1.1.0	24	239.0.0.1	 1	01:59:56	Off

Displayed Information	Explanations
Source Address	Source address
Mask Len	Mask length
Group Address	Group address
State	Table item state
FCR Exptime	FCR expire time
Prune/Graft ReXmit-Time	Prune expire time/ Graft retransmit time

20.4.5.1.6 show ip dvmrp route

Command: show ip dvmrp route [{<A.B.C.D/M>[detail]}|{nexthop <A.B.C.D>[detail]}|{best-match <A.B.C.D> [detail]}|detail]

Function: Prune expire time/ Graft retransmit time

Parameter: None

Default: Do not display

Command Mode: Any Configuration Mode

Usage Guide: The command applies to display DVMRP routing table item; DVMRP maintains individual unicast routing table to check RPF.

Example: Display DVMRP routiing.

Switch #show ip dv route

Flags: N = New, D = DirectlyConnected, H = Holddown

Network Flags Nexthop Nexthop Metric Uptime Exptime

```
                        Xface        Neighbor
10.1.35.0/24      .D.   Vlan2        Directly  Connected      1        00:11:16
00:00:00
13.1.1.0/24       .D.   Vlan1        Directly  Connected      1        00:10:22
00:00:00
```

Displayed Information	Explanations
Network	Target net segment or address and mask
Flags	Routing state flag
Nexthop Xface	Next hop interface address
Nexthop Neighbor	Next hop neighbor
Metric	Routing metric value
Uptime	Routing uptime
Exptime	Routing expire time

20.5 DCSCM

20.5.1 Introduction to DCSCM

DCSCM (Destination control and source control multicast) technology mainly includes three aspects, i.e. Multicast Packet Source Controllable, Multicast User Controllable and Service-Oriented Priority Strategy Multicast.

The Multicast Packet Source Controllable technology of Security Controllable Multicast technology is mainly processed in the following manners:

1. On the edge switch, if source under-control multicast is configured, then only multicast data from specified group of specified source can pass.
2. For RP switch in the core of PIM-SM, for REGISTER information out of specified source and specified group, REGISTER_STOP is transmitted directly and table entry is not allowed to set up. (This task is implemented in PIM-SM model).

The implement of Multicast User Controllable technology of Security Controllable Multicast technology is based on the control over IGMP report message sent out by the user, thus the model being controlled is IGMP snooping and IGMP model, of which the control logic includes the following three, i.e. to take control based on VLAN+MAC address transmitting packets, to take control based on IP address of transmitting packets and to take control based on the port where messages enter, in which IGMP snooping can use the above three methods to take control simultaneously, while since IGMP model

is located at layer 3, it only takes control over the IP address transmitting packets.

The Service-Oriented Priority Strategy Multicast of Security Controllable technology adopts the following mode: for multicast data in limit range, set the priority specified by the user at the join-in end so that data can be sent in a higher priority on TRUNK port, consequently guarantee the transmission is processed in user-specified priority in the entire network.

20.5.2 DCSCM Configuration Task List

1) Source Control Configuration
2) Destination Control Configuration
3) Multicast Strategy Configuration

1. Source Control Configuration

Source Control Configuration has three parts, of which the first is to enable source control. The command of source control is as follows:

Command:	Explanation
Global Configuration Mode	
[no] ip multicast source-control (Required)	Enable source control globally, the "**no ip multicast source-control**" command disables source control globally. It is noticeable that, after enabling source control globally, all multicast packets are discarded by default. All source control configuration can not be processed until the it is enabled globally, while source control can not be disabled until all configured rules are disabled.

The next is to configure the rule of source control. It is configured in the same manner as for ACL, and uses ACL number of 5000-5009, every rule number can be used to configure 10 rules. It is noticeable that these rules are ordered, the front one is the one which is configured the earliest. Once the configured rules are matched, the following rules won't take effect, so rules of globally allow must be put at the end. The commands are

Command	Explanation
Global Configuration Mode	

[no] access-list <5000-5099> {deny|permit} ip {{<source> <source-wildcard>}|{host-source <source-host-ip>}|any-source} {{<destination> <destination-wildcard>}|{host-destination <destination-host-ip>}|any-destination}	The rule used to configure source control. This rule does not take effect until it is applied to specified port. Using the NO form of it can delete specified rule.

The last is to configure the configured rule to specified port.

Note: If the rules being configured will occupy the table entries of hardware, configuring too many rules will result in configuration failure caused by bottom table entries being full, so we suggest user to use the simplest rules if possible. The configuration rules are as follows

Command	Explanation
Port Configuration Mode	
[no] ip multicast source-control access-group <5000-5099>	Used to configure the rules source control uses to port, the NO form cancels the configuration.

Destination Control Configuration

Like source control configuration, destination control configuration also has three steps.

First, enable destination control globally. Since destination control need to prevent unauthorized user from receiving multicast data, the switch won't broadcast the multicast data it received after configuring global destination control. Therefore, It should be avoided to connect two or more other Layer 3 switches in the same VLAN on a switch on which destination control is enabled. The configuration command are as follows

Command	Explanation
Global Configuration Mode	
[no] multicast destination-control（required）	Enable IPv4/IPv6 destination control globally, the "**no multicast destination-control**" command disables destination control globally. All other configuration do not take effect until it is globally enabled.

Next is to configure destination control rule. It is similar to source control, except to use ACL No. of 6000-7999.

Command	Explanation

Global Configuration Mode	
[no] access-list <6000-7999> {deny|permit} ip {{<source> <source-wildcard>}|{host-source <source-host-ip>}|any-source} {{<destination> <destination-wildcard>}|{host-destination <destination-host-ip>}|any-destination}	The rule used to configure source control. This rule does not take effect until it is applied to source IP or VLAN-MAC and port. Using the NO form of it can delete specified rule.

The last is to configure the rule to specified source IP, source VLAN MAC or specified port. It is noticeable that, due to the above situations, these rules can only be used globally in enabling IGMP-SNOOPING. And if IGMP-SNOOPING is not enabled, then only source IP rule can be used under IGMP Protocol. The configuration commands are as follows:

Command	Explanation
Port Configuration Mode	
[no] ip multicast destination-control access-group <6000-7999>	Used to configure the rules destination control uses to port, the NO form cancels the configuration.
Global Configuration Mode	
[no] ip multicast destination-control <1-4094> <macaddr> access-group <6000-7999>	Used to configure the rules destination control uses to specified VLAN-MAC, the NO form cancels the configuration.
[no] ip multicast destination-control <IPADDRESS/M> access-group <6000-7999>	Used to configure the rules destination control uses to specified IP address/net mask, the NO form cancels the configuration.

2. Multicast Strategy Configuration

Multicast Strategy uses the manner of specifying priority for specified multicast data to achieve and guarantee the effects the specific user requires. It is noticeable that multicast data can not get a special care all along unless the data are transmitted at TRUNK port. The configuration is very simple, it has only one command, i.e. to set priority for the specified multicast. The commands are as follows:

Command	Explanation
Global Configuration Mode	

[no] ip multicast policy <IPADDRESS/M> <IPADDRESS/M> cos <priority>	Configure multicast strategy, specify priority for sources and groups in specific range, and the range is <0-7>

20.5.3 Commands for DCSCM

20.5.3.1 access-list (Multicast Source Control)

Command: access-list <5000-5099> {deny|permit} ip {{<source> <source-wildcard>}|{host-source <source-host-ip>}|any-source} {{<destination> <destination-wildcard>}|{host-destination <destination-host-ip>}|any-destination}

no access-list <5000-5099> {deny|permit} ip {{<source> <source-wildcard>}|{host-source <source-host-ip>}|any-source} {{<destination> <destination-wildcard>}|{host-destination <destination-host-ip>}|any-destination}

Function: Configure source control multicast access-list; the "**no access-list <5000-5099> {deny|permit} ip {{<source> <source-wildcard>}|{host-source <source-host-ip>}|any-source} {{<destination> <destination-wildcard>}|{host-destination <destination-host-ip>}|any-destination}**" command deletes the access-list.

Parameter: **<5000-5099>**: source control access-list number.

{deny|permit}: deny or permit.

<source>: multicast source address..

<source-wildcard>: multicast source address wildcard character.

<source-host-ip>: multicast source host address.

<destination>: multicast destination address.

<destination-wildcard>: multicast destination address wildcard character.

<destination-host-ip>: multicast destination host address.

Default: None

Command Mode: Global Mode

Usage Guide: ACL of Multicast destination control list item is controlled by specifical ACL number from 5000 to 5099, the command applies to configure this ACL. ACL of Multicast destination control only needs to configure source IP address and destination IP address controlled (group IP address), the configuration mode is basically the same to other ACLs, and use wildcard character to configure address range, and also specify a host address

or all address. Remarkable, “all address” is 224.0.0.0/4 according to group IP address, not 0.0.0.0/0 in other access-list.

Example: Switch(config)#access-list 5000 permit ip 10.1.1.0 0.0.0.255 232.0.0.0 0.0.0.255

20.5.3.2 access-list (Multicast Destination Control)

Command: access-list <6000-7999> {deny|permit} ip {{<source> <source-wildcard>}|{host-source <source-host-ip>}|any-source} {{<destination> <destination-wildcard>}|{host-destination <destination-host-ip>}|any-destination}

no access-list <6000-7999> {deny|permit} ip {{<source> <source-wildcard>}|{host-source <source-host-ip>}|any-source} {{<destination> <destination-wildcard>}|{host-destination <destination-host-ip>}|any-destination}

Function: Configure destination control multicast access-list, the “**no access-list <6000-7999> {deny|permit} ip {{<source> <source-wildcard>}|{host-source <source-host-ip>}|any-source} {{<destination> <destination-wildcard>}|{host-destination <destination-host-ip>}|any-destination}**” command deletes the access-list.

Parameter: **<6000-7999>**: destination control access-list number.

{deny|permit}: deny or permit.

<source>: multicast source address.

<source-wildcard>: multicast source address wildcard character..

<source-host-ip>: multicast source host address.

<destination>: multicast destination address.

<destination-wildcard>: multicast destination address wildcard character.

<destination-host-ip>: multicast destination host address

Default: None

Command Mode: Global Mode

Usage Guide: ACL of Multicast destination control list item is controlled by specifical ACL number from 6000 to 7999, the command applies to configure this ACL. ACL of Multicast destination control only needs to configure source IP address and destination IP address controlled (group IP address), the configuration mode is basically the same to other ACLs, and use wildcard character to configure address range, and also specify a host address or all address. Remarkable, “all address” is 224.0.0.0/4 according to group IP address, not 0.0.0.0/0 in other access-list.

Example: Switch(config)#access-list 6000 permit ip 10.1.1.0 0.0.0.255 232.0.0.0

0.0.0.255

20.5.3.3 ip multicast destination-control access-group

Command: ip multicast destination-control access-group <6000-7999>

no ip multicast destination-control access-group <6000-7999>

Function: Configure multicast destination-control access-list used on interface, the "**no ip multicast destination-control access-group <6000-7999>**" command deletes the configuration.

Parameter: <6000-7999>: destination-control access-list number.

Default: None

Command Mode: Interface Configuration Mode

Usage Guide: The command is only working under global multicast destination-control enabled, after configuring the command, if IGMP-SPOOPING is enabled, for adding the interface to multicast group, and match configured access-list, such as matching: permit, the interface can be added, otherwise do not be add.

Example:switch(config-if-ethernet)#ip multicast destination-control access-group 6000

20.5.3.4 ip multicast destination-control access-group (vmac)

Command: ip multicast destination-control <1-4094> <macaddr >access-group <6000-7999>

no ip multicast destination-control <1-4094> <macaddr >access-group <6000-7999>

Function: Configure multicast destination-control access-list used on specified vlan-mac, the "**no ip multicast destination-control <1-4094> <macaddr >access-group <6000-7999>**" command deletes this configuration.

Parameter: <1-4094>: VLAN-ID;

<macaddr>: Transmitting source MAC address of IGMP-REPORT, the format is "xx-xx-xx-xx-xx-xx";

<6000-7999>: Destination-control access-list number.

Default: None

Command Mode: Global Mode

Usage Guide: The command is only working under global multicast destination-control enabled, after configuring the command, if IGMP-SPOOPING is enabled, for adding the members to multicast group. If configuring multicast destination-control to source MAC address of transmitted igmp-report, and match configured access-list, such as matching: permit, the interface can be added, otherwise do not be add.

Example:switch(config)#ip multicast destination-control 1 00-01-03-05-07-09 access-group 6000

20.5.3.5 ip multicast destination-control access-group (sip)

Command: ip multicast destination-control <IPADDRESS/M> access-group <6000-7999>

no ip multicast destination-control <IPADDRESS/M> access-group <6000-7999>

Function: Configure multicast destination-control access-list used on specified net segment, the "**no ip multicast destination-control <IPADDRESS/M> access-group <6000-7999>**" command deletes this configuration.

Parameter: <IPADDRESS/M>: IP address and mask length;;

<6000-7999>: Destination control access-list number.

Default: None

Command Mode: Global Mode

Usage Guide: The command is only working under global multicast destination-control enabled, after configuring the command, if IGMP-SPOOPING or IGMP is enabled, for adding the members to multicast group. If configuring multicast destination-control to source MAC address of transmitted igmp-report, and match configured access-list, such as matching: permit, the interface can be added, otherwise do not be add. The command uses the format "<IPADDRESS> <IPADDRESS>" to match on layer 2 switch, format "<IPADDRESS/M> on layer 3 switch. If relevant group or source in show ip igmp groups detail has been established before executing the command, it needs to execute clear ip igmp groups command to clear relevant groups in Admin mode.

Example: Switch(Config)#ip multicast destination-control 10.1.1.0/24 access-group 6000

20.5.3.6 multicast destination-control

Command: multicast destination-control

no multicast destination-control

Function: Configure to globally enable IPv4/IPv6 multicast destination-control, the "**no multicast destination-control**" command restores disabled global multicast group control.

Parameter: None

Default: Disabled

Command Mode: Global Mode

Usage Guide: Other destination control configurations can be taken effect with only enabling global multicast destination control, the destination control access-list applies to interface, VLAN-MAC and SIP. After configuring the command, igmp snooping and IGMP match, according to above rules, when they receive IGMP REPORT to try to add interface.

Example: Switch(config)#multicast destination-control

20.5.3.7 ip multicast policy

Command:ip multicast policy <IPADDRESS/M> <IPADDRESS/M> cos <priority>

no ip multicast policy <IPADDRESS/M> <IPADDRESS/M> cos

Function: Configure multicast policy, the "**no ip multicast policy <IPADDRESS/M> <IPADDRESS/M> cos**" command deletes it.

Parameter: <IPADDRESS>: are multicast source address, source adapter identifier, destination address, and destination adapter identifier separately.

<IPADDRESS/M>: are multicast source address, mask length, destination address, and mask length separately.

<priority>: specified priority, range from 0 to 7

Default: None

Command Mode: Global Mode

Usage Guide: The command configuration modifies to a specified value through the switch matching priority of specified range multicast data package, and the TOS is specified to the same value simultaneously. The command uses the format "<IPADDRESS> <IPADDRESS>" to match on layer 2 switch, format "<IPADDRESS/M> on layer 3 switch. Carefully, the packet transmitted in UNTAG mode does not modify its priority.

Example: switch(config)#ip multicast policy 10.1.1.0/24 225.1.1.0/24 cos 7

20.5.3.8 ip multicast source-control

Command:ip multicast source-control

no ip multicast source-control

Function: Configure to globally enable multicast source control, the "**no ip multicast source-control**" command restores global multicast source control disabled.

Parameter: None

Default: Disabled

Command Mode: Global Mode

Usage Guide: The destination control access-list applies to interface with only enabling global multicast source control, and configure to disabled global multicast source control without configuring source control access-list on every interface. After configuring the command, multicast data received from every interface does not have matching multicast source control list item, and then they will be thrown away by switches, namely only multicast data matching to PERMIT can be received and forwarded.

Example: Switch(config)#ip multicast source-control

20.5.3.9 ip multicast source-control access-group

Command: ip multicast source-control access-group <5000-5099>

no ip multicast source-control access-group <5000-5099>

Function: Configure multicast source control access-list used on interface, the “no ip multicast source-control access-group <5000-5099>“ command deletes the configuration.

Parameter: <5000-5099>: Source control access-list number**.**

Default: None

Command Mode: Interface Configuration Mode

Usage Guide: The command configures with only enabling global multicast source control. After that, it will match multicast data message imported from the interface according to configured access-list, such as matching: permit, the message will be received and forwarded; otherwise the message will be thrown away.

Example: switch(config-if-ethernet)#ip multicast source-control access-group 5000

20.5.4 DCSCM Configuration Examples

1. Source Control

In order to prevent an Edge Switch from putting out multicast data arbitrarily, we configure Edge Switch so that only the switch at port Ethernet1/5 is allowed to transmit multicast, and the data group must be 225.1.2.3. Also, switch connected up to port Ethernet1/10 can transmit multicast data without any limit, and we can make the following configuration.

Switch(config)#access-list 5000 permit ip any host 225.1.2.3

Switch(config)#access-list 5001 permit ip any any

Switch(config)#ip multicast source-control

Switch(config)#interface ethernet1/5

Switch(Config-If-Ethernet1/5)#ip multicast source-control access-group 5000

Switch(config)#interface ethernet1/10

Switch(Config-If-Ethernet1/10)#ip multicast source-control access-group 5001

2. Destination Control

We want to limit users with address in 10.0.0.0/8 network segment from entering the group of 238.0.0.0/8, so we can make the following configuration:

Firstly enable IGMP snooping in the VLAN it is located (Here it is assumed to be in VLAN2)

EC(config)#ip igmp snooping

EC(config)#ip igmp snooping vlan 2

After that, configure relative destination control access-list, and configure specified IP address to use that access-list.

Switch(config)#access-list 6000 deny ip any 238.0.0.0 0.255.255.255
Switch(config)#access-list 6000 permit ip any any
Switch(config)#multicast destination-control
Switch(config)#ip multicast destination-control 10.0.0.0/8 access-group 6000
In this way, users of this network segment can only join groups other than 238.0.0.0/8.

3. Multicast strategy

Server 210.1.1.1 is distributing important multicast data on group 239.1.2.3, we can configure on its join-in switch as follows:

Switch(config)#ip multicast policy 210.1.1.1/32 239.1.2.3/32 cos 4

In this way, the multicast stream will have a priority of value 4 (Usually this is pretty higher, the higher possible one is protocol data; if higher priority is set, when there is too many multicast data, it might cause abnormal behavior of the switch protocol) when it gets to other switches through this switch.

20.5.5 DCSCM Troubleshooting

The effect of DCSCM module itself is similar to ACL, and the problems occurred are usually related to improper configuration. Please read the descriptions above carefully. If you still can determine the cause of the problem, please send your configurations and the effects you expect to the after-sale service staff of our company.

20.5.5.1 Monitor And Debug

20.5.5.1.1 show ip multicast destination-control

Command: show multicast destination-control [detail]

show ip multicast destination-control interface <Interfacename> [detail]

show ip multicast destination-control host-address <ipaddress> [detail]

show ip multicast destination-control <vlan-id> <mac-address> [detail]

Function: Display multicast destination control

Parameter: detail: expresses if it display information in detail or not..

<Interfacename>: interface name or interface aggregation name, such as Ethernet1/1, port-channel 1 or ethernet1/1..

Default: None

Command Mode: Admin Mode and Global Mode

Usage Guide: The command displays multicast destination control rules of configuration, including detail option, and access-list information applied in detail.

Example:

switch (config)#show multicast destination-control

ip multicast destination-control is enabled

ip multicast destination-control 11.0.0.0/8 access-group 6003

ip multicast destination-control 1 00-03-05-07-09-11 access-group 6001

multicast destination-control access-group 6000 used on interface Ethernet

20.5.5.1.2 show ip multicast destination-control access-list

Command: show ip multicast destination-control access-list

show ip multicast destination-control access-list <6000-7999>

Function: Display destination control multicast access-list of configuration.

Parameter: <6000-7999>: access-list number.

Default: None

Command Mode: Admin Mode and Global Mode

Usage Guide: The command displays destination control multicast access-list of configuration.

Example:

switch# sh ip multicast destination-control acc

access-list 6000 deny ip any-source any-destination

access-list 6000 deny ip any-source host-destination 224.1.1.1

access-list 6000 deny ip host-source 2.1.1.1 any-destination

access-list 6001 deny ip host-source 2.1.1.1 225.0.0.0 0.255.255.255

access-list 6002 permit ip host-source 2.1.1.1 225.0.0.0 0.255.255.255

access-list 6003 permit ip 2.1.1.0 0.0.0.255 225.0.0.0 0.255.255.255

20.5.5.1.3 show ip multicast policy

Command: show ip multicast policy

Function: Display multicast policy of configuration

Parameter: None

Default: None

Command Mode: Admin Mode and Global Mode

Usage Guide: The command displays multicast policy of configuration

Example:

switch#show ip multicast policy

ip multicast-policy 10.1.1.0/24 225.0.0.0/8 cos 5

20.5.5.1.4 show ip multicast source-control

Command: show ip multicast source-control [detail]

show ip multicast source-control interface <Interfacename> [detail]

Function: Display multicast source control configuration

Parameter: detail: expresses if it displays information in detail.

<Interfacename>: interface name, such as Ethernet 1/1 or ethernet 1/1.

Default: None

Command Mode: Admin Mode and Global Mode

Usage Guide: The command displays multicast source control rules of configuration, including detail option, and access-list information applied in detail

Example:

Switch#show ip multicast source-control detail

ip multicast source-control is enabled Interface Ethernet use multicast source control access-list 5000

access-list 5000 permit ip 10.1.1.0 0.0.0.255 232.0.0.0 0.0.0.255

access-list 5000 deny ip 10.1.1.0 0.0.0.255 233.0.0.0 0.255.255.255

20.5.5.1.5 show ip multicast source-control access-list

Command: show ip multicast source-control access-list

show ip multicast source-control access-list <5000-5099>

Function: Display source control multicast access-list of configuration

Parameter: <5000-5099>: access-list number

Default: None

Command Mode: Admin Mode and Global Mode

Usage Guide: The command displays source control multicast access-list of configuration

Example:

Switch#sh ip multicast source-control access-list

access-list 5000 permit ip 10.1.1.0 0.0.0.255 232.0.0.0 0.0.0.255

access-list 5000 deny ip 10.1.1.0 0.0.0.255 233.0.0.0 0.255.255.255

20.6 IGMP

20.6.1 Introduction to IGMP

IGMP (Internet Group Management Protocol) is the protocol in TCP/IP protocol family which is responsible for IP multicast member management. It is used to set up and maintain multicast group member relationship between IP host and its neighbor multicast switches. IGMP does not include the spread and maintenance of relation information of group members among multicast switches, this work is accomplished by each multicast routing protocol. All hosts participating in multicast must implement IGMP protocol.

Hosts participating IP multicast can join in and exit multicast group at any location, any time and without limit of member total. Multicast switch does not need and not likely

to save all relationships of all hosts. It only gets to know if there are receivers of some multicast group, i.e. group member, on the network segment each interface connects to. And the host only needs to save which multicast groups it joined.

IGMP is asymmetric between host and router: the host needs to respond the IGMP query messages of multicast switches, i.e. to report message response in membership; the switch sends out membership query messages periodically, and then determine if there are hosts of some specific group joining in the sub-network it belongs to based on the received response message, and send out query of specific group (IGMP version2) when receiving the report of a host exiting the group to determine if there exists no member in some specific group.

Up to now, there are three versions of IGMP: IGMP version1 (defined by RFC1112), IGMP version2 (defined by RFC2236) and IGMP version3 (defined by RFC3376).

The main improvements of IGMP version2 over version1 are:

1. The election mechanism of multicast switches on the shared network segment

Shared network segment is the situation of there are more than one multicast switch on a network segment. Under this kind of situation, since all switches which runs IGMP under this network segment can get membership report message from the host, therefore, only one switch is required to transmit membership query message, so an exchange election mechanism is required to determine a switch as query machine. In IGMP version1, the selection of query machine is determined by Multicast Routing Protocol; IGMP version2 made an improvement for it, it prescribed that when there are more than one multicast switches on the same network segment, the multicast switch with the lowest IP address will be elected as the query machine.

2. IGMP version2 added Leave Group Mechanism

In IGMP version 1, the host leaves the multicast group silently without sending any notification to any multicast switch. This causes that the multicast switch can only determine the leave of multicast member by multicast group response time-out. But in version2, when a host decides to leave a multicast group, if it is the host which gives response to the latest membership query message, then it will send out a message implying it is leaving.

3. IGMP version 2 added the query to specific group

In IGMP version1, a query of multicast switch is for all multicast groups on the network segment. This query is called general group query. In IGMP version2, query of specific group is added besides general group query. The destination IP address of this kind of query message is the IP address of the very multicast group, the group address field part of the message is also the IP address of the multicast group. Thus it is prevented that hosts which are other multicast group members transmit response message.

4. IGMP version2 added the biggest response time field

IGMP version2 added the biggest response time field to dynamically adjust the response time of the host to group query message.

The main features of version3 is allowing the host to choose receiving from or rejecting a certain source, which is the basis of SSM （Source-Specific Multicast） multicast. For example, when a host is sending a report of INCLUDE{10.1.1.1, 10.1.1.2} to some group G, that means the host needs the router to forward the flux from 10.1.1.1 and 10.1.1.2; when a host is sending a report of EXCLUDE{192.168.1.1} to some group G, that means the host needs the flux from all sources of group G except 192.168.1.1. This makes a great difference from the previous IGMP.

The main improvements of IGMP version3 over IGMP version1 are:

1. The status to be maintained is group and source list, not only the groups in IGMPv2.
2. The interoperations with IGMPv1 and IGMPv2 are defined in IGMPv3 status.
3. IP service interface is modified to allow specific source list thereby.
4. The queried includes his/her Robustness Variable and Query Interval in query group to allow the synchronization with these variables of non-queries.
5. Max Response Time in Query Message has an exponential range, with maximum value from 25.5 secs of v2 to 53 mins, which can be used in links of great capacity.
6. In order to increase strength, the host retransmits State-Change message.
7. Additional data is defined to adapt future extension.
8. Report group is sent to 224.0.0.22 to help with IGMP Snooping of Layer 2 Switch.
9. Report group can include more than one group record, and it allows using small group to report complete current status.
10. The host does not restrain operation any more, which simplifies the implement and allows direct membership trace.
11. In querying messages, the new router side restraint process (S sign) modified the existing strength of IGMPv2.

20.6.2 Configuration Task List

1、Enable IGMP (Required)

2、Configure IGMP sub-parameters (Optional)

（1）Configure IGMP group parameters

1）Configure IGMP group filtering conditions

2）Configure IGMP to join in group

3）Configure IGMP to join in static group

（2）Configure IGMP query parameters

1）Configure the interval of IGMP sending query message

2）Configure the maximum response time of IGMP query

3）Configure time-out of IGMP query

（3）Configure IGMP version

3、 Disable IGMP Protocol

1. Enable IGMP Protocol

There is not specific commands for enabling IGMP Protocol on the Layer 3 switch. Enabling any multicast protocol under corresponding interface will automatically enable IGMP.

Command	Explanation
Global Mode	
ip dvmrp multicast-routing | ip pim multicast-routing	To enable global multicast protocol is the prerequisite to enable IGMP protocol, the "**no ip dvmrp multicast-routing | no ip pim multicast-routing**" commands disable multicast protocol and IGMP protocol. (Required)

Command	Explanation
Interface Configuration Mode	
ip dvmrp | ip pim dense-mode | ip pim sparse-mode	Enable IGMP Protocol, the corresponding commands "**no ip dvmrp | no ip pim dense-mode | no ip pim sparse-mode**" disable IGMP Protocol. (Required)

2. Configure IGMP Sub-parameters

（1）Configure IGMP group parameters

1）Configure IGMP group filtering conditions

2）Configure IGMP to join in group

3）Configure IGMP to join in static group

Command	Explanation
Interface Configuration Mode	
ip igmp access-group {<*acl_num* | *acl_name*>} **no ip igmp access-group**	Configure the filtering conditions of the interface to IGMP group; the "**no ip igmp access-group**" command cancels the filtering condition.
ip igmp join-group <*A.B.C.D* > **no ip igmp join-group <*A.B.C.D* >**	Configure the interface to join in some IGMP group, the "**no ip igmp join-group <*A.B.C.D* >**" command cancels the join.

ip igmp static-group <*A.B.C.D* > no ip igmp static -group <*A.B.C.D* > >	Configure the interface to join in some IGMP static group; the "**no ip igmp static -group <*A.B.C.D* >**" command cancels the join.

（2）Configure IGMP Query parameters

1）Configure interval for IGMP to send query messages

2）Configure the maximum response time of IGMP query

3）Configure the time-out of IGMP query

Command	Explanation
Interface Configuration Mode	
ip igmp query-interval <*time_val*> no ip igmp query-interval	Configure the interval of IGMP query messages sent periodically; the "**no ip igmp query-interval**" command restores default value.
ip igmp query-max-response-time <*time_val*> no ip igmp query-max-response-time	Configure the maximum response time of the interface for IGMP query; the "**no ip igmp query-max-response-time**" command restores default value.
ip igmp query-timeout <*time_val*> no ip igmp query-timeout	Configure the time-out of the interface for IGMP query; the "**no ip igmp query-timeout**" command restores default value.

（3）Config IGMP version

Command	Explanation
Global Mode	
ip igmp version <*version*> no ip igmp version	Configure IGMP version on the interface; the "**no ip igmp version**" command restores the default value.

3. Disable IGMP Protocol

Command	Explanation
Interface Configuration Mode	
no ip dvmrp | no ip pim dense-mode | no ip pim sparse-mode | no ip pim multicast-routing | no ip pim multicast-routing	Disable IGMP Protocol.

20.6.3 Commands for IGMP

20.6.3.1 ip igmp access-group

Command: ip igmp access-group {<*acl_num* | *acl_name*>}

no ip igmp access-group

Function: Configure interface to filter IGMP group; the "**no ip igmp access-group**" command cancels the filter condition

Parameter: {<acl_num | acl_name>} is SN or name of access-list, value range of **acl_name** is from 1 to 99.

Default: Default no filter condition

Command Mode: Interface Configuration Mode

Usage Guide: Configure interface to filter groups, permit or deny some group joining.

Example: Configure interface vlan1 to permit group 224.1.1.1, deny group 224.1.1.2.

Switch (Config)#access-list 1 permit 224.1.1.1 0.0.0.0

Switch (Config)#access-list 1 deny 224.1.1.2 0.0.0.0

Switch (Config)#interface vlan 1

Switch(Config-If-Vlan1)#ip igmp access-group 1

20.6.3.2 ip igmp immediate-leave

Command: ip igmp immediate-leave group-list {<number>|<name>}

no ip igmp immediate-leave

Function: Configure IGMP working in immediate-leave mode, that is, when the host transmits member identity report of equivalent to leave a group, router does not transmit query, it directly confirms there is no member of this group in subnet; the "**no ip igmp immediate-leave**" command cancels immediate-leave mode.

Parameter: <*number*> is access-list SN, value is from 1 to 99.

<*name*> is access-list name.

Default: Interface default and no immediate-leave group of configuration after finished product

Command Mode: Interface Configuration Mode

Usage Guide: The command only can apply in only one host condition in subnet.

Example: Configure immediate-leave mode on access-group list 1

Switch (Config-if-Vlan1)#ip igmp immediate-leave group-list 1

20.6.3.3 ip igmp last-member-query-interval

Command: ip igmp last-member-query-interval <interval>

no ip igmp last-member-query-interval

Function: Configure interval of specified group query transmitting on interface; the "**no ip igmp last-member-query-interval**" command cancels the value of user manual configuration, and restores default value.

Parameter: **<*interval*>** is interval of specified group query, range from 1000ms to

25000ms; the value is integer times of 1000ms, namely if input value is not integer times of 1000ms, the system automatically changes to integer times of 1000ms.

Default: Default: 1000ms

Command Mode: Interface Configuration Mode

Example: Configure interface vlan1 IGMP last-member-query-count to 2000.

Switch (Config)#int vlan 1

Switch (Config-if-vlan1)#ip igmp last-member-query-interval 2000

20.6.3.4 ip igmp limit

Command: ip igmp limit <state-count>

no ip igmp limit

Function: Configure limit IGMP state-count on interface; the "**no ip igmp limit**" command cancels the value of user manual configuration, and restores default value.

Parameter: ***<state-count>*** is maximum IGMP state reserved by interface, range from 1 to 65000

Default: Default: 0, no limit.

Command Mode: Interface Configuration Mode

Usage Guide: After configuring maximum state state-count, interface only saves states which are not more than state-count groups and sources. If it reaches upper limit of state-count, it does not deal with when receiving related new group member identity report. If it has saved some IGMP group states before configuring the command, it deletes all of the states, and then immediately transmits IGMP general query to collect the member identity report which is not more than state-count group. Static state and static source are not in the limit

Example: Configure interface vlan1 IGMP limit to 4000.

Switch (Config)#int vlan 1

Switch (Config-if-vlan1)#ip igmp limit 4000

20.6.3.5 ip igmp join-group

Command: ip igmp join-group <*A.B.C.D* >

no ip igmp join-group <*A.B.C.D* >

Function: Configure interface to join some IGMP group; the "no ip igmp join-group" command cancels this join

Parameter: ***<A.B.C.D>:*** is group address

Default: Do not join

Command Mode: Interface Configuration Mode

Usage Guide: When the switch is the HOST, the command configures HOST to join some group; that is, if configuring the interface join-group 224.1.1.1, it will transmit IGMP

member report including group 224.1.1.1 when the switch receives IGMP group query transmitted by other switches. Carefully, it is the difference between the command and **ip igmp static-group** command.

Example: Configure join-group 224.1.1.1 on interface vlan1.

Switch (Config)#interface vlan 1

Switch(Config-If-Vlan1)#ip igmp join-group 224.1.1.1

20.6.3.6 ip igmp query-interval

Command: ip igmp query-interval <*time_val*>

no ip igmp query-interval

Function: Configure interval of periodically transmitted IGMP query information; the "**no ip igmp query-interval**" command restores default value.

Parameter: **<*time_val*>** is interval of periodically transmitted IGMP query information, value range from 1s to 65535s.

Default: Default interval of periodically transmitted IGMP query information to 125s.

Command Mode: Interface Configuration Mode

Usage Guide: Periodically transmitting IGMP query information on interface when some interface enables some group multicast protocol. The command applies to configure this query period time.

Example: Configure interval of periodically transmitted IGMP query message to 10s

Switch (Config)#interface vlan 1

Switch(Config-If-Vlan1)#ip igmp query-interval 10

20.6.3.7 ip igmp query-max-response-time

Command: ip igmp query-max-response-time <*time_val*>

no ip igmp query- max-response-time

Function: Configure IGMP query-max-response-time of interface; the "**no ip igmp query-max-response-time**" command restores default value.

Parameter: <***time_val***> is IGMP query-max-response-time of interface, value range from 1s to 25s

Default: Default: 10s.

Command Mode: Interface Configuration Mode

Usage Guide: After the switch receives a query message, the host will configure a timer for its affiliated every multicast group, the value of timer is selected random from 0 to maximum response time, the host will transmit member report message of the multicast group. Reasonable configuring maximum response time, it can make host quickly response query message. The router can also quickly grasp the status of multicast group member.

Example: configure the maximum period responding to the IGMP query messages to 20s

Switch (Config)#interface vlan 1

Switch(Config-If-Vlan1)#ip igmp query- max-response-time 20

20.6.3.8 ip igmp query-timeout

Command: ip igmp query-timeout <*time_val*>

no ip igmp query-timeout

Function: Configure IGMP query timeout of interface; the "**no ip igmp query-timeout**" command restores default value.

Parameter: <***time_val***> is IGMP query-timeout, value range from 60s to 300s.

Default: Default: 265s.

Command Mode: Interface Configuration Mode

Usage Guide: When multi-running IGMP switches are exist on sharing network, a switch will be voted as query processor on the sharing network, and other switches will be a timer monitoring the state of query processor; It still does not receive query message transmitting by query processor over query time-out, thus it re-votes another switch as new query processor.

Example: Configure timeout of IGMP query message on interface to 100s.

Switch (Config)#interface vlan 1

Switch(Config-If-Vlan1)#ip igmp query-timeout 100

20.6.3.9 ip igmp static-group

Command: ip igmp static-group <*A.B.C.D* > [source <*A.B.C.D* >]

no ip igmp static -group <*A.B.C.D* > [source <*A.B.C.D* >]

Function: Configure interface to join some IGMP static group; the "no ip igmp static-group" command cancels this join.

Parameter: <*A.B.C.D*> is group address;;

Source **<*A.B.C.D*>** expresses SSM source address of configuration.

Default: Do not join static group

Command Mode: Interface Configuration Mode

Usage Guide: When configuring some interface to join some static group, it will receives about the multicast package of the static group whether the interface has a real receiver or not; that is, if configuring the interface to join static group 224.1.1.1, the interface always receives about multicast packet about group 224.1.1.1 whether the interface has a receiver or not. Carefully, it is the diffence between the command and ip igmp join-group command.

Example: Configure static-group 224.1.1.1 on interface vlan1.

Switch (Config)#interface vlan 1

Switch(Config-If-Vlan1)#ip igmp static-group 224.1.1.1

20.6.3.10 ip igmp version

Command: ip igmp version <*version*>

no ip igmp version

Function: Configure IGMP version on interface; the "**no ip igmp version**" command restores default value.

Parameter: <***version***> is IGMP version of configuration, currently supporting version 1, 2 and 3.

Default: Default: version 2.

Command Mode: Interface Configuration Mode

Usage Guide: The command mainly applies to supply upward compatibility of the different version; it is not communicated between version 1 and version 2, therefore it must configure to the same version IGMP in the same network. When other routers which are not upgraded to IGMPv3 on interface-connected subnet need to join member identity collection of subnet IGMP together, the interface is configured to corresponding version.

Example: Configure IGMP on interface to version 1.

Switch (Config)#interface vlan 1

Switch(Config-If-Vlan1)#ip igmp version 3

20.6.4 IGMP Configuration Example

As shown in the following figure, add the Ethernet ports of Switch A and Switch B to corresponding vlan, and start PIM-DM on each vlan interface.

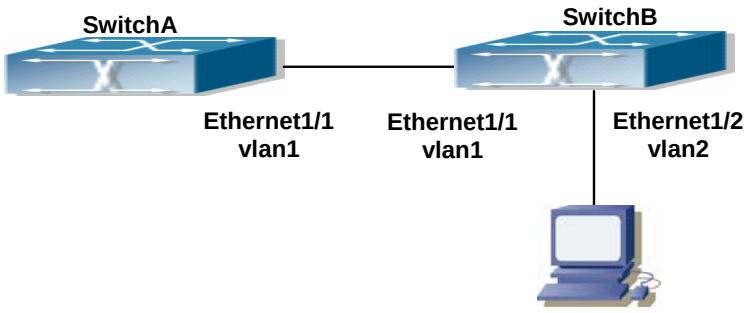


Fig 20-4 IGMP Network Topology Diagram

The configuration procedure for SwitchA and SwitchB is as follows:

(1) Configure SwitchA:

Switch(Config)#ip pim multicast-routing

Switch (Config)#interface vlan 1

Switch(Config-If-Vlan1)#ip address 12.1.1.1 255.255.255.0
Switch(Config-If-Vlan1)#ip pim dense-mode
(2) Configure SwitchB:
Switch(Config)#ip pim multicast-routing
Switch(Config)#interface vlan1
Switch(Config-If-Vlan1)#ip address 12.1.1.2 255.255.255.0
Switch(Config-If-Vlan1)#ip pim dense-mode
Switch(Config-If-Vlan1)#exit
Switch(Config)#interface vlan2
Switch(Config-If-Vlan1)#ip address 20.1.1.1 255.255.255.0
Switch(Config-If-Vlan2)#ip pim dense-mode
Switch(Config-If-Vlan2)#ip igmp version 3

20.6.5 IGMP Troubleshooting

In configuring and using IGMP Protocol, IGMP Protocol might not operate normally caused by physical connection or incorrect configuration. Therefore, user should pay attention to the following issues:

- ✧ Firstly to assure that physical connection is correct.
- ✧ Next, to assure the Protocol of Interface and Link protocol is UP (use show interface command);
- ✧ Afterwards, to assure to start a kind of multicast protocol on the interface;
- ✧ Multicast Protocol requires RPF Check using unicast routing; therefore the correctness of unicast routing must be assured beforehand.

If all attempts including Check are made but the problems on IGMP can't be solved yet, then use debug commands such debug ipv6 mld event/packet please, and then copy DEBUG information in 3 minutes and send to Technology Service Center.

20.6.5.1 Commands for Monitor and debug

20.6.5.1.1 debug igmp event

Command: debug igmp event

no debug igmp event

Function: Enable debugging switch of IGMP event; the "**no debug igmp event**" command disenables the debugging switch

Parameter: None

Default: Disabled

Command Mode: Admin Mode

Usage Guide: Enable debugging switch if querying IGMP event information

Example:

Switch# debug igmp event

igmp event debug is on

Switch# 01:04:30:56: IGMP: Group 224.1.1.1 on interface vlan1 timed out

20.6.5.1.2 debug igmp packet

Command: debug igmp packet

no debug igmp packet

Function: Enable debugging switch of IGMP message information; the "**no debug igmp packet**" command disenables the debugging switch

Parameter: None

Default: Disabled

Command Mode: Admin Mode

Usage Guide: Enable the debugging switch if querying IGMP message information.

Example:

Switch# debug igmp packet

igmp packet debug is on

Switch #02:17:38:58: IGMP: Send membership query on dvmrp2 for 0.0.0.0

02:17:38:58: IGMP: Received membership query on dvmrp2 from 192.168.1.11 for 0.0

.0.0

02:17:39:26: IGMP: Send membership query on vlan1 for 0.0.0.0

02:17:39:26: IGMP: Received membership query on dvmrp2 from 192.168.1.11 for 0.0

.0.0

20.6.5.1.3 show ip igmp groups

Command: show ip igmp groups [<*A.B.C.D*>] [*detail*]

Function: Display IGMP group information

Parameter: ***<group_addr>*** is group address, namely querying specified group information; Detail expresses group information in detail

Default: Do not display

Command Mode: Admin Mode

Example:

Switch (config)#show ip igmp groups

IGMP Connected Group Membership (2 group(s) joined)

Group Address	Interface	Uptime	Expires	Last Reporter
226.0.0.1	Vlan1	00:00:01	00:04:19	1.1.1.1
239.255.255.250	Vlan1	00:00:10	00:04:10	10.1.1.1

Switch#

Displayed Information	Explanations
Group Address	Multicast group IP address
Interface	Interface affiliated with multicast group
Uptime	Multicast group uptime
Expires	Multicast group expire time
Last Reporter	Last reporter to the host of the multicast group

Switch (config)#show ip igmp groups 234.1.1.1 detail

IGMP Connect Group Membership (2 group(s) joined)
Flags: SG - Static Group, SS - Static Source, SSM - SSM Group, V1 - V1 Host Pres
ent, V2 - V2 Host Present
Interface: Vlan1
Group: 234.1.1.1
Flags:
Uptime: 00:00:19
Group Mode: INCLUDE
Last Reporter: 10.1.1.1
Exptime: stopped
Source list: (2 members S - Static)
Source Address Uptime v3 Exp Fwd Flags
1.1.1.1 00:00:19 00:04:01 Yes
2.2.2.2 00:00:19 00:04:01 Yes

Displayed Information	Explanations
Group	Multicast group IP address
Interface	Interface affiliated with Multicast group
Flags	Group property flag
Uptime	Multicast group uptime
Group Mode	Group mode, including INCLUDE and EXCLUDE. Group V3 will be available, group V1 and group V2 are regards as EXCLUDE mode.
Exptime	Multicast group expire time
Last Reporter	Last reporter to the host of the Multicast group
Source Address	Source address of this group
V3 Exp	Source expire time

Fwd	If the data of the source is forwarded or not.
Flags	Source property flag

20.6.5.1.4 show ip igmp interface

Command: show ip igmp interface [<*ifname*>]

Function: Display related IGMP information on interface.

Parameter: **<*ifname*>** is interface name, namely displaying IGMP information of specified interface.

Default: Do not display

Command Mode: Admin Mode

Example: Display interface valn1 IGMP message on Ethernet.

```
Switch (config)#show ip igmp interface Vlan1
Interface Vlan1(2005)
 Index 2005
 Internet address is 10.1.1.2
 IGMP querier
 IGMP current version is V3, 2 group(s) joined
 IGMP query interval is 125 seconds
 IGMP querier timeout is 255 seconds
 IGMP max query response time is 10 seconds
 Last member query response interval is 1000 ms
 Group Membership interval is 260 seconds
 IGMP is enabled on interface
```

Chapter 21 IPv6 Multicast Protocol

21.1 PIM-DM6

21.1.1 Introduction to PIM-DM6

PIM-DM6（Protocol Independent Multicast, Dense Mode）is the IPv6 version of Protocol Independent Multicast Dense Mode. It is a Multicast Routing Protocol in dense mode which adapted to small network. The members of multicast group are relatively dense under this kind of network environment. There is no difference compared with the IPv4 version PIM-DM except that the addresses it uses are IPv6 addresses. Thus we don't differentiate between PIM-DM and PIM-DM6 in this chapter. All PIM-DM in the text without specific explanation refers to IPv6 version PIM-DM.

As a result of continuous development of IPv6 network, it has the network environment of nonsupport IPv6 multicast sometimes, so it needs to do the IPv6 multicast operation by tunnel. Therefore, our PIM-DM6 supports configuration on configure tunnel, and passes through nonsupport IPv6 multicast network by single cast packet of IPv4 encapsulation.

The working process of PIM-DM can be summarized as: Neighbor Discovery, Flooding-Prune, and Graft.

1. Neigh hour Discovery

When PIM-DM router is started at beginning, Hello message is required to discover neighbors. The network nodes running PIM-DM use Hello message to contact each other. PIM-DM Hello message is sent periodically.

2. Flooding-Prune

PIM-DM assumes that all hosts on the network are ready to receive multicast data. When certain multicast source S begins to send data to a multicast group G, after receiving the multicast packet, the router will make RPF examination first according to the unicast table. If the check passes, the router will create a (S, G) table item and forward the multicast packet to all downstream PIM-DM nodes (Flooding). If the RPF examination fails, i.e. the multicast packet is inputted from the incorrect interface, and then the message is discarded. After this procedure, every node will create an (S, G) item in the PIM-DM multicast domain. If there is no multicast group member in the downstream nodes, then a Prune message is sent to upstream nodes notifying not to

forward data to this multicast group any more. After receiving Prune message, the corresponding interfaces will be deleted from the output interface list corresponding with the multicast-forwarding item (S, G). Through this process, a SPT (Shortest Path Tree) is established with source S as root. Prune process is started by a sub-router.

The process above is called Flooding-Prune process. Each pruned node also provides overtime mechanism at the same time. In case of overtime of prune, the router will restart flooding-prune process. Flooding-prune of PIM-DM is conducted periodically

3. RPF examination

Adopting RPF examination, PIM-DM establishes a multicast forwarding tree initiating from data source, using existing unicast routing table. When a multicast packet arrives, the router will determine the correctness of its coming path first. If the arrival interface is the interface connected to multicast source indicated by unicast routing, then this multicast packet is considered to be from the correct path; otherwise the multicast packet will be discarded as redundant message. The unicast routing message used as path judgment can root in any Unicast Routing Protocol, such as messages found by RIP, OSPF, etc. It doesn't rely on any specific unicast routing protocol.

4. Assert Mechanism

If two multicast router A and B in the same LAN segment have their own receiving paths to multicast source S, they will respectively forward multicast data packet to LAN after receiving the packet from multicast source S. Then downstream nodes multicast router C will receive two multicast packets that are exactly the same. Once router detects such circumstance, a unique forwarder will be selected through "assert" mechanism. The optimized forwarding path is selected through "assert" packet. If the priority and costs of two or more than two paths are same, the node with a larger IP address will be selected as the upstream neighbor of item (S, G), which will be responsible for forwarding the (S, G) multicast packet.

5. Graft

When the pruned downstream node needs to recover to forwarding status, this node uses Graft Message to notify upstream nodes to resume multicast data forwarding.

21.1.2 PIM-DM Configuration Task List

1、Start PIM-DM (Required)
2、Configure PIM-DM auxiliary parameters (Optional)
3、Configure PIM-DM interface parameters
4、Configure PIM-DM hello message interval time
5、Shut down PIM-DM protocol

1. Start PIM-DM Protocol

It's easy to make basic configuration of the PIM-DM routing protocol in EdgeCore layer 3 switch, only need to turn on PIM multicast switch in Global Mode and turn on PIM-DM switch on relevant interface.

Command	**Explanation**
Global Mode	
ipv6 pim multicast-routing	Enable PIM-DM Protocol (but below commands are required to really function PIM-DM protocol)

And then turn on PIM-DM switch on the interface

Command	**Explanation**
Port Configuration Mode	
ipv6 pim dense-mode	Start PIM-DM Protocol of the interface (Required)

2. Configure PIM-DM Auxiliary Parameters

（1）Configure PIM-DM Interface Parameters

Configure PIM-DM hello message interval time

Command	**Explanation**
Port Configuration Mode	
ipv6 pim hello-interval < *interval*> **no ipv6 pim hello-interval**	Configure PIM-DM hello message interval time; the NO operation of this command restores the default value.

Configure PIM-DM state-refresh message interval time

Command	**Explanation**
Port Configuration Mode	
ipv6 pim state-refresh origination-interval **no ipv6 pim state-refresh origination-interval**	Configure PIM-DM state-refresh message interval time; the NO operation of this command restores the default value.

3. Shut down PIM-DM Protocol

Command	**Explanation**
Port Configuration Mode	
no ipv6 pim dense-mode	Turn off PIM-DM protocol of the interface
Global Mode	
no ipv6 pim multicast-routing	Shut down PIM-DM Protocol in global mode.

21.1.3 Commands for PIM-DM6

21.1.3.1 ipv6 pim accept-register

Command: ipv6 pim accept-register list <a*cess-list-name*>

no ipv6 pim accept-register

Function: Filter the specified multicast group.

Parameter: <a*cess-list-name*> is the applying access-list name

Default: Permit the multicast registers from any sources to any groups

Command Mode: Global Mode

Usage Guide: This command is used to configure the access-list filtering the PIM REGISTER packets.The addresses of the access-list respectively indicate the filtered multicast sources and multicast groups' information. For the source-group combinations that match DENY ,PIM sends REGISTER-STOP immediately and does not create group records when receiving REGISTER packets.Unlike other access-list,when the access-list is configured ,the default value is PERMIT..

Example: Configure the filtered register message's rule to myfilter.

Switch(config)#ipv6 pim accept-register list myfilter

Switch(config)#ipv6 access-list myfilter permit ff1e::10/128

21.1.3.2 ipv6 pim cisco-register-checksum

Command:ipv6 pim cisco-register-checksum [group-list *<access-list name>*|]

no ipv6 pim cisco-register-checksum [group-list *<access-list name>*|]

Function: Configure the register packet's checksum of the group specified by myfilter to use the whole packet's length.

Default: Compute the checksum according to the regester packets's head length default: 8

Parameter: <*access-list name*> is the applying simple access-list.

Command Mode: Global Mode

Usage Guide: This command is uesd to interact with older Cisco IOS version.

Example: Configure the register packet's ckecksum of the group specified by myfilter to use the whole packet's length.

Switch(config)#ipv6 pim cisco-register-checksum group-list myfilter

Switch(config)#ipv6 access-list myfilter permit ff1e::10/128

21.1.3.3 ipv6 pim dense-mode

Command: ipv6 pim dense-mode

no ipv6 pim dense-mode

Function: Enable PIM-DM protocol on interface; the "**no ipv6 pim dense-mode**" command disenables PIM-DM protocol on interface.

Parameter: None

Default: Disable PIM-DM protocol

Command Mode: Interface Configure Mode

Usage Guide: The command will be taken effect, executing ipv6 multicast-routing in Global Mode. Don't support multicast protocol mutual operation, namely can't synchronously enable dense mode and sparse mode in one switch. The command can configure on IPv6 tunnel interface, but it is successful configuration to only configure tunnel carefully.

Example: Enable PIM-DM protocol on interface vlan1.

Switch (Config)#ipv6 pim multicast-routing

Switch (Config)#interface vlan 1

Switch(Config-if-Vlan1)#ipv6 pim dense-mode

21.1.3.4 ipv6 pim dr-priority

Command: ipv6 pim dr-priority <*priority*>

no ipv6 pim dr-priority

Function: Configure, cancel and change priority value of interface DR. The same net segment border nodes vote specified router DR in this net segment through hello messages, the "no ipv6 pim dr-priority" restores default value.

Parameter: < *priority*> priority, value range from 0 to 4294967294

Default: 1

Command Mode: Interface Configuration Mode

Usage Guide: Value range is from 0 to 4294967294, the bigger value, the more priority. The command can configure on IPv6 tunnel interface, but it is successful configuration to only configure tunnel carefully.

Example: Switch (Config)# interface vlan 1

Switch(Config-if-Vlan1)ipv6 pim dr-priority 100

21.1.3.5 ipv6 pim exclude-genid

Command: **ipv6 pim exclude-genid**

no ipv6 pim exclude-genid

Function: The command make Hello message transmitted by PIM-SM exclude Genid option, the "**no ipv6 pim exclude-genid**" restores default value.

Parameter: None

Default: Hello message includes Genid option

Command Mode: Interface Configuration Mode

Usage Guide: The command is used to interactive with old Cisco IOS Version. The command can configure on IPv6 tunnel interface, but it is successful configuration to only configure tunnel carefully.

Example: Configure hello messages transmitted by switch to exclude Genid option.

Switch(Config-if-Vlan1)#ipv6 pim exclude-genid

21.1.3.6 ipv6 pim hello-holdtime

Command: ipv6 pim hello-holdtime <*value*>

no ipv6 pim hello-holdtime

Function: Configure and cancel Holdtime item value in Hello message, the value describes neighbor overtime. If it goes over the time and does not receive hello message of the neighbor, the register of the neighbor will be delete.

Parameter: <*value*> is configure time of holdtime.

Default: Define 3.5 times of Hello_interval, and default hello_interval as 30s, so default value of hello_holdtime is 105s.

Command Mode: Interface Configuration Mode

Usage Guide: If no setting, hello time will default current 3.5 times of Hello_interval. If setting hello time is less than current hello_interval, this setting will be declined. When updating hello_interval every time, hello_holdtime will be also update based on these rules below: if hello_holdtime does not be configured, or if hello_holdtime configured is less than current hello_interval, hello_holdtime will be modified to 3.5 times Hello_interval, otherwise, keeps configured value. The command can configure on IPv6 tunnel interface, but it is successful configuration to only configure tunnel carefully.

Example: Configure hello holdtime setting on interface vlan1 to 10.

Switch (Config)# interface vlan1

Switch (Config -if-Vlan1)#ipv6 pim hello-holdtime 10

21.1.3.7 ipv6 pim hello-interval

Command: ipv6 pim hello-interval < *interval*>

no ipv6 pim hello-interval

Function: Configure interface PIM-DM hello message interval; the "**no ipv6 pim hello-interval**" command restores default value.

Parameter: < *interval*> is interval of periodically transmitted PIM-DM hello message, value range from 1s to 18724s.

Default: Default interval of periodically transmitted PIM-DM hello message as 30s.

Command Mode: Interface Configuration Mode

Usage Guide: Hello message makes PIM-DM switch mutual location, and ensures

neighbor ship. PIM-DM switch announces existence itself by periodically transmitting hello messages to neighbors. If it doesn't receive hello messages from neighbors in regulation time, it confirms that the neighbors were lost. Configuration time is not more than neighbor overtime. The command can configure on IPv6 tunnel interface, but it is successful configuration to only configure tunnel carefully.

Example: Configure PIM-DM hello interval on interface vlan1

Switch (Config)#interface vlan1

Switch(Config-if-Vlan1)#ipv6 pim hello-interval 20

21.1.3.8 ipv6 pim multicast-routing

Command: ipv6 pim multicast-routing

no ipv6 pim multicast-routing

Function: Globally enable PIM-DM protocol; the "**no ipv6 pim multicast-routing**" command disenables PIM-DM protocol.

Parameter: None

Default: Disable PIM-DM protocol

Command Mode: Global Mode

Usage Guide: Ipv6 pim can enable only after executing this command.

Example: Globally enable PIM-DM protocol

Switch (Config)#ipv6 pim multicast-routing

21.1.3.9 ipv6 pim neighbor-filter

Command: ipv6 pim neighbor-filter <*access-list-name*>

no ipv6 pim neighbor-filter <*access-list-name*>

Function: Configure neighbor access-list. If filtered by list and connected the neighbor, the connection immediately was broken. If no connection, the connection can be established.

Parameter: <*access-list-name*> is an applied access-list name

Default: No neighbor filter configuration

Command Mode: Interface Configuration Mode

Usage Guide: If it is not necessary for partner to establish neighbor ship, the command can filter pim message of partner. The command can configure on IPv6 tunnel interface, but it is successful configuration to only configure tunnel carefully.

Example: Configure access-list of pim neighbor on interface vlan1

Switch (Config-if-Vlan1)#ipv6 pim neighbor-filter myfilter

Switch (Config)# ipv6 access-list myfilter deny fe80:20e:cff:fe01:facc

Switch (Config)# ipv6 access-list myfilter permit any

21.1.3.10 ipv6 pim state-refresh origination-interval

Command: ipv6 pim state-refresh origination-interval <interval>

no ipv6 pim state-refresh origination-interval

Function: Configure transmission interval of state-refresh message on interface. The “no ipv6 pim state-refresh origination-interval” command restores default value.

Parameter: <*interval*> message transmission interval value is from 4s to 100s.

Default: 60s

Usage Guide: The first-hop router periodically transmits stat-refresh messages to maintain PIM-DM list Items of all the downstream routers. The command can modify origination interval of state-refresh messages. Usually do not modify relevant timer interval. The command can configure on IPv6 tunnel interface, but it is successful configuration to only configure tunnel carefully.

Example: Configure transmission interval of state-refresh message on interface vlan1 to 90s.

Switch (Config-if-Vlan1)#ipv6 pim state-refresh origination-interval 90

21.1.4 PIM-DM Typical Application

As shown in the following figure, add the Ethernet interfaces of Switch A and Switch B to corresponding vlan, and start PIM-DM Protocol on each vlan interface.

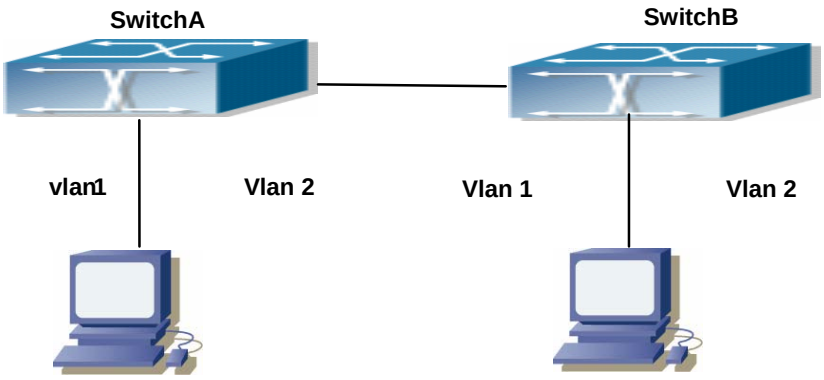


Fig 21-1 PIM-DM Typical Environment

The configuration procedure for SwitchA and SwitchB is as below:

(1) Configure SwitchA:

Switch (Config) # ipv6 pim multicast-routing

Switch (Config) # interface vlan 1

Switch (Config-if-Vlan1) # ipv6 address 2000:10:1:1::1/64

Switch (Config-if-Vlan1) # ipv6 pim dense-mode

Switch (Config-if-Vlan1) #exit

Switch (Config) # interface vlan2
Switch (Config-if-Vlan2) # ipv6 address 2000:12:1:1:: 1/64
Switch (Config-if-Vlan2) # ipv6 pim dense-mode
(2) Configure SwitchB:
Switch (Config) #ip pim multicast-routing
Switch (Config) #interface vlan 1
Switch (Config-if-Vlan1) # ipv6 address 2000:12:1:1::2/64
Switch (Config-if-Vlan1) # ipv6 pim dense-mode
Switch (Config-if-Vlan1) #exit
Switch (Config) #interface vlan 2
Switch (Config-if-Vlan2) # ipv6 address 2000:20:1:1::1/64
Switch (Config-if-Vlan2) # ipv6 pim dense-mode

21.1.5 PIM-DM Troubleshooting

When configuring and using PIM-DM protocol, PIM-DM protocol may fail to work normally due to physical connections, incorrect configuration and so on. So, users shall note the following points:

- ✧ Assure the physical connection is correct.
- ✧ Assure the Protocol of Interface and Link is UP (use show interface command);
- ✧ Assure PIM Protocol is turned on in Global Mode (use ipv6 pim multicast-routing command)
- ✧ Start PIM-DM Protocol on the interface (use ipv6 pim dense-mode command)

Unicast route shall be used to carry out RPF examination for multicast protocol. So the correctness of unicast route shall be guaranteed above all. If all attempts fail to solve the problems on PIM-DM, then use debug commands such as debug ipv6 pim, copy DEBUG information in 3 minutes and send to Technology Service Center.

21.1.5.1 Commands for Monitor and debug

21.1.5.1.1 debug ipv6 pim timer sat

Command: debug ipv6 pim timer sat
no debug ipv6 pim timer sat
Function: Enable debug switch of PIM-DM source activity timer information in detail; the "**no debug ipv6 pim timer sat**" command disenables the debug switch.
Parameter: None
Default: Disabled
Command Mode: Admin Mode

Usage Guide: Enable the switch, and display source activity timer information in detail.

Example:

Switch # debug ipv6 pim timer sat

Remark: Other debug switches in PIM-DM are common in PIM-SM.

21.1.5.1.2 debug ipv6 pim timer srt

Command: debug ipv6 pim timer srt

no debug ipv6 pim timer srt

Function: Enable debug switch of PIM-DM state-refresh timer information in detail; the "**no debug ipv6 pim timer srt**" command disenables the debug switch.

Parameter: None

Default: Disabled

Command Mode: Admin Mode

Usage Guide: Enable the switch, and display PIM-DM state-refresh timer information in detail

Example:

Switch # debug ipv6 pim timer srt

Remark: Other debug switches in PIM-DM are common in PIM-SM.

21.1.5.1.3 show ipv6 pim interface

Command: show ipv6 pim interface [detail]

Function: Display PIM interface information

Parameter: None

Default: None

Command Mode: Any Mode

Example:

```
Switch#show ipv6 pim interface
Interface VIFindex Ver/     Nbr       DR
                           Mode     Count    Prior
Vlan2         0             v2/S     0          1
      Address           : fe80::203:fff:fee3:1244
      Global Address: 2000:1:111::100
      DR                : this system
Vlan3         2             v2/S     0          1
      Address           : fe80::203:fff:fee3:1244
      Global Address: 2000:10:1:13::1
      DR                : this system
```

Displayed Information	Explanations
Address	Interface address

Interface	Interface name
VIF index	Interface index
Ver/Mode	Pim version and mode,usually v2,sparse mode displays S,dense mode displays D
Nbr Count	The interface's neighbor count
DR Prior	Dr priority
DR	The interface's DR address

21.1.5.1.4 show ipv6 pim neighbor

Command: show ipv6 pim neighbor [detail|]

Function: Display router neighbors

Parameter: None

Default: None

Command Mode: Any Mode

Usage Guide: Display multicast router neighbors maintained by the PIM

Example:

Switch(config)#show ipv6 pim neighbor

Neighbor Address	Interface	Uptime/Expires	Ver	DR Priority/Mode
Fe80::203:fff:fee3:1244	Vlan1	00:00:10/00:01:35	v2	1 /DR
fe80::20e:cff:fe01:facc	Vlan1	00:00:13/00:01:32	v2	1 /

Displayed Information	Explanations
Neighbor Address	Neighbor address
Interface	Neighbor interface
Uptime/Expires	Running time /overtime
Ver	Pim version ,v2 usually
DR Priority/Mode	DR priority in the hello messages from the neighbor and if the neighbor is the interface's DP

21.1.5.1.5 show ipv6 pim nexthop

Command: show ipv6 pim nexthop

Function: Display the PIM buffered nexthop router in the unicast route table

Parameter: None

Default: None

Command Mode: Any Mode

Usage Guide: Display the PIM buffered nexthop router information

Example:

Switch#show ipv6 pim nexthop

Flags: N = New, R = RP, S = Source, U = Unreachable ….

Destination Type Nexthop

Nexthop ..Nexthop Nexthop Metric Pref Refcnt

Num Addr

Ifindex Name

2000:1:111::11 ..S. 1 :

: 2004 0 0 2

2000:1:111::100 .RS. 1 ::

2004 0 0 2

2004 0 0 2

Displayed Information	Explanations
Destination	Destination of next item
Type	N: created nexthop,RP direction and S direction are not determined . R: RP derection S: source direction U: can't reach
Nexthop Num	Nexthop number
Nexthop Addr	Nexthop address
Nexthop Ifindex	Nexthop interface index
Nexthop Name	Nexthop name
Metric	Metric Metric to nexthop
Pref	Preference Route preference
Refcnt	Reference count

21.1.5.1.6 show ipv6 pim mroute dense-mode

Command: show ipv6 pim mroute dense-mode [group <*X:X::X:X*>] [source <*X:X::X:X*>]

Function: Display PIM-DM message forwarding items.

Parameter: group < X:X::X:X >: displays forwarding items relevant to this multicast address

Source < X:X::X:X >: displays forwarding items relevant to this source.

Default: Do not display

Command Mode: Admin Mode

Usage Guide: The command shows PIM-DM multicast forwarding items, namely forwarding items of forward multicast packet in system FIB table

Example: Display all of PIM-DM message forwarding items

Switch(config)#show ipv6 pim mroute dense-mode

IP Multicast Routing Table

(*,G) Entries: 1
(S,G) Entries: 1

(*, ff1e::15)
 Local ..l.....

(2000:10:1:12::11, ff1e::15)
RPF nbr: ::
RPF idx: Vlan12
Upstream State: FORWARDING
Origin State: ORIGINATOR
 Local .....
 Pruned .....
 Asserted .....
 Outgoing ..o.....

Switch#

Displayed Information	Explanations
(*, ff1e::15)	(*,G) Forwaridng item
(2000:10:1:12::11, ff1e::15)	(S,G) Forwarding item
RPF nbr	Backward path neighbor, upstream neighbor of source direction in DM, 0.0.0.0 expresses the switch is the first hop.
RPF idx	Interface located in RPF neighbor
Upstream State	Upstream direction, including FORWARDING(forwarding upstream data), PRUNED(Upstream stops forwarding data), ACKPENDING(waiting for upstream response, forwarding upstream data)
Origin State	The two states: ORIGINATOR(on transmit state-refresh state), NON_ORIGINATOR(on non_transmit state-refresh state)
Local	Join Local position joins interface, the interface receives IGMP Join
Pruned	PIM prunes interface, the interface receives Prune messages

Asserted	Asserted state
Outgoing	Multicast data finally exported from interface is index number, index is 2 in this case. It can check interface information in detail by commanding show ip pim interface

21.1.5.1.7 show ipv6 mroute

Command: show ipv6 mroute [<GroupAddr> [<SourceAddr>]]

Function: show IPv6 software multicast route table

Parameter: GroupAddr: show the multicast entries relative to this Group address.

SourceAddr：show the multicast route entries relative to this source address

Default: None

Command Mode：Admin mode and global mode

Usage Guide:

Example: show all entries of IPv6 multicast route table

Switch(config)# show ipv6 mroute

Name: Loopback, Index: 2002, State:49

Name: Vlan1, Index: 2006, State:1043

Name: Vlan11, Index: 2007, State:1043

Name: Vlan12, Index: 2008, State:1043

Name: Tunnel1, Index: 2009, State:d1

Name: Tunnel2, Index: 0, State:0

Name: pim6reg, Index: 2010, State:c1

Name: pimreg, Index: 2011, State:c1

The total matched ip6mr active mfc entries is 1, unresolved ip6mr entries is 1

Group	Origin	Iif	Wrong	Oif:TTL
ff2f::1	2014:1:2:3::2	Tunnel1	0	2008:1
ff3f::1	2012:1:2:3::2	NULL	4	0:0

Displayed information	Explanation
Name	the name of interface
Index	the index number of interface
State	the state of interface
The total matched ipmr active mfc entries	The total matched active IP multicast route mfc（multicast forwarding cache） entries
unresolved ipmr entries	unresolved ip multicast route entries
Group	the destination address of the entries
Origin	the source address of the entries

Iif	ingress interface of the entries
Wrong	packets received from the wrong interface
Oif	egress interface of the entries
TTL	the value of TTL

Remark: This command is common in PIM-SM6.

21.2 PIM-SM6

21.2.1 Introduction to PIM-SM6

PIM-SM6（Protocol Independent Multicast, Sparse Mode）is the IPv6 version of Protocol Independent Multicast Sparse Mode. It is a multicast routing protocol in sparse mode and mainly used in large network with group members distributed relatively sparse and wide. It is no difference from the IPv4 version PIM-SM except the addresses it uses are IPv6 addresses. Thus we don't differentiate between PIM-SM and PIM-SM6 in this chapter. All PIM-SM in the text without specific explanation is IPv6 version PIM-SM. Unlike the Flooding-Prune of Dense Mode, PIM-SM Protocol assumes no host needs receiving multicast data packets. PIM-SM router forwards multicast data packets to a host only on definite request.

By setting RP (Rendezvous Point) and BSR (Bootstrap Router), PIM-SM announce multicast packet to all PIM-SM routers and establish, using Join/Prune message of routers, RPT (RP-rooted shared tree) based on RP. Consequently the network bandwidth occupied by data packets and control messages is cut down and the transaction cost of routers is reduced. Multicast data get to the network segment where the multicast group members are located along the shared tree flow. When the data traffic reaches a certain amount, multicast data stream can be switched to source-based SPT (Shortest Path Tree) to shorten network delay. PIM-SM doesn't rely on any specific unicast routing protocol but make RPF examination using existing unicast routing table.

1. PIM-SM Working Principle

The working process of PIM-SM mainly includes neighbor discovery, creation of RPT, registration of multicast source, SPT switch and so on. The neighbor discovery mechanism is the same with the mechanism of PIM-DM. We won't introduce any more.

(1) Creation of RP Shared Tree (RPT)

When a host joins a multicast group G, the leaf router directly connected with the host finds out through IGMP message that there is a receiver of multicast group G, then it works out the corresponding Rendezvous Point RP for multicast group G, and send join

message to upper level nodes in RP direction. Every router on the way from the leaf router to RP will create a (*, G) table item, indicating the message from any source to multicast group G is suitable for this item. When RP receives the message sent to multicast group G, the message will get to the leaf router along the established path and then reach the host. In this way, the RPT with RP as root is created.

(2) Multicast Source Registration

When multicast source S sends a multicast packet to multicast group G, the PIM-SM multicast router directly connected to it will take charge of sealing the multicast packet into registered message and unicast it to corresponding RP. If there are more than one PIM-SM multicast routers on a network segment, then DR (Designated Router) takes charge of forwarding the multicast packet.

(3) SPT Switch

Once the multicast router finds that the rate of the multicast packet from RP with destination address G exceeds threshold, the multicast router will send Join message to the upper lever nodes in the source direction, which results in the switch from RPT to SPT.

2. Preparation before PIM-SM configuration

(1) Configuration Candidate RP

More than one RPs (candidate RP) are permitted in PIM-SM network and each C-RP (Candidate RP) takes charge of forwarding multicast packets with destination address in a certain range. To configure more than one candidate RPs can achieve RP load balancing. There is no master or slave difference among RPs. All multicast routers work out the RP corresponded with certain multicast group based on the same algorithm after receiving the candidate RP message announced by BSR.

Note that one RP can serve more than one multicast groups, even all multicast groups. But each multicast group can only correspond with one unique RP at any moment. It can't correspond with more RPs at the same time.

(2) BSR Configuration

As the management core of PIMSM network, BSR is in charge of collecting messages sent by candidate RPs and broadcast them.

There may be only one BSR within a network. However, there may be several candidate BSRs to be configured. With such arrangement, once a BSR fails, another may be switched to. C-BSR determines BSR through automatic selection.

As a result of continuous development of IPv6 network, it has the network environment of nonsupport IPv6 multicast sometimes, so it needs to do the IPv6 multicast operation by tunnel. Therefore, our PIM-SM6 supports configuration on configure tunnel, and passes through nonsupport IPv6 multicast network by single cast packet of IPv4 encapsulation.

21.2.2 PIM-SM Configuration Task List

1、 Start PIM-SM (Required)

2、 Configure PIM-SM auxiliary parameters (Optional）

（1） Configure PIM-SM interface parameters

1) Configure PIM-SM hello message interval time

2) Configure interface as PIM-SM domain boundary

（2） Configure PIM-SM global parameters

1) Configure switch as candidate BSR

2) Configure switch as candidate RP

3) Configure static RP

3、 Shut down PIM-SM Protocol

1. Start PIM-SM Protocol

It's easy to make basic configuration of the PIM-SM routing protocol in EDGECORE layer 3 switch, only need to turn on PIM multicast switch in Global Mode and turn on PIM-SM switch on relevant interface.

Command	**Explanation**
Global Mode	
[no] ipv6 pim multicast-routing	Enable PIM-SM Protocol on each interface (but below commands are required to really start PIM-SM protocol on the interface), and the NO operation of this command shuts PIM-SM Protocol on all interfaces. (Required)

And then turn on PIM-SM switch on the interface

Command	**Explanation**
Port Configuration Mode	
[no] ipv6 pim sparse-mode [passive]	Start PIM-SM Protocol of the interface. The NO operation of this command shuts the PIM-SM Protocol of this interface. (Required)

2. Configure PIM-SM Auxiliary Parameters

（1）Configure PIM-SM Interface Parameters

1）Configure PIM-SM hello message interval time

Command	**Explanation**
Port Configuration Mode	
Ipv6 pim hello-interval < *interval*> **no ipv6 pim hello-interval**	Configure interface PIM-SM hello message interval time; the NO operation of this command restores the default value.

2）Configure PIM-SM hello message holdtime

Command	Explanation
Port Configuration Mode	
Ipv6 pim hello-holdtime <*value*> **no ipv6 pim hello-holdtime**	Configure the value of holdtime domain in interface PIM-SM hello message; the NO operation of this command restores the default value.

3）Configure PIM-SM Neighbor Access-list

Command	Explanation
Port Configuration Mode	
(no)ipv6 pim neighbor-filter <*access-list-name*>	Configure Neighbor Access-list. If a neighbor is filtered by the list and a connection has been set up with this neighbor, then this connection will be cut off immediately; and if no connection is set up yet, then this connection can't be created.

（2）Configure PIM-SM Global Parameters

1）Configure switch to be candidate BSR

Command	Explanation
Global Mode	
Ipv6 pim bsr-candidate <*ifname*> **[*hash-mask-length*] [*priority*]** **no ipv6 pim bsr-candidate**	This command is the global candidate BSR configuration command, which is used to configure the information of PIM-SM candidate BSR so that it can compete for BSR router with other candidate BSRs. The NO operation is to cancel the configuration of BSR.

2）Configure switch to be candidate RP

Command	Explanation
Global Mode	
Ipv6 pim rp-candidate <*ifname*> **[<*group range*>] [<*priority*>]** **(no) ipv6 pim rp-candidate <*ifname*>**	This command is the global candidate RP configuration command, which is used to configure the information of PIM-SM candidate RP so that it can compete for RP router with other candidate RPs. The NO operation is to cancel the configuration of RP.

3）Configure Static RP

Command	Explanation
Global Mode	
Ipv6 pim rp-address <*rp-address*> [<*group-range*>] **no ipv6 pim rp-address <*rp-address*> {all|<*group-range*>}**	This command is the global candidate RP configuration command, which is used to configure the information of PIM-SM candidate RP so that it can compete for RP router with other candidate RPs. The NO operation is to cancel the configuration of RP.

3. Shut down PIM-SM Protocol

Command	Explanation
Port Configuration Mode	
no ipv6 pim sparse-mode	Shut down PIM-SM Protocol.
Global Mode	
no ipv6 pim multicast-routing	Shut down PIM-SM Protocol globally.

21.2.3 Commands for PIM-SM

21.2.3.1 ipv6 pim accept-register

Command: ipv6 pim accept-register list <a*cess-list-name*>

no ipv6 pim accept-register

Function: Filter the specified multicast group.

Parameter: <a*cess-list-name*> is the applying access-list name

Default: Permit the multicast registers from any sources to any groups

Command Mode: Global Mode

Usage Guide: This command is used to configure the access-list filtering the PIM REGISTER packets.The addresses of the access-list respectively indicate the filtered multicast sources and multicast groups' information. For the source-group combinations that match DENY ,PIM sends REGISTER-STOP immediately and does not create group records when receiving REGISTER packets. Unlike other access-list, when the access-list is configured ,the default value is PERMIT.

Example: Configure the filtered register message's rule to myfilter.

Switch(config)#ipv6 pim accept-register list myfilter

Switch(config)#ipv6 access-list myfilter permit ff1e::10/128

21.2.3.2 ipv6 pim bsr-candidate

Command: ipv6 pim bsr-candidate <*ifname*> [<*hash-mask-length*>] [<*priority*>]

no ipv6 pim bsr-candidate [*ifname*]

Function: This command is the candidate BSR configure command in global mode and is used to configure PIM-SM information about candidate BSR in order to compete the BSR router with other candidate BSRs. The command **"no ipv6 pim bsr-candidate [*ifname*]"** command disables the candidate BSR.

Parameter: <*ifname*> is the specified interface name;

[*hash-mask-length*] is the specified hash mask length. It's used for the RP enable selection and ranges from 0 to 32;

[*priority*] is the candidate BSR priority and ranges from 0 to 255. If this parameter is not configured ,the default priority value is 0

Default: This switch is not a candidate BSR router

Command Mode: Global Mode

Usage Guide: This command is the candidate BSR configure command in global mode and is used to configure PIM-SM information about candidate BSR in order to compete the BSR router with other candidate BSRs. Only this command is configured , this switch is the BSR candidate router.

Example: Globally configure the interface vlan1 as the candidate BSR-message transmitting interface.

Switch (Config)# ipv6 pim bsr-candidate vlan1 30 10

21.2.3.3 ipv6 pim cisco-register-checksum

Command: ipv6 pim cisco-register-checksum [group-list <*access-list name*>|]

no ipv6 pim cisco-register-checksum [group-list <*access-list name*>|]

Function: Configure the register packet's checksum of the group specified by myfilter to use the whole packet's length.

Default: Compute the checksum according to the register packet's head length default: 8

Parameter: <*access-list name*> is the applying simple access-list.

Command Mode: Global Mode

Usage Guide: This command is used to interact with older Cisco IOS version.

Example: Configure the register packet's checksum of the group specified by myfilter to use the whole packet's length.

Switch(config)#ipv6 pim cisco-register-checksum group-list myfilter

Switch(config)#ipv6 access-list myfilter permit ff1e::10/128

21.2.3.4 ipv6 pim dr-priority

Command: ipv6 pim dr-priority <*priority*>

no ipv6 pim dr-priority

Function: Configure, disable or change the interface's DR priority. The neighboring nodes in the same net segment select the DR in their net segment according to hello packets. The "**no ipv6 pim dr-priority**" command restores the default value

Parameter: <*priority*> priority, it ranges from 0 to 4294967294

Default: 1

Command Mode: Interface Configuration Mode

Usage Guide: Range from 0 to 4294967294, the higher value has more priority. The command can configure on IPv6 tunnel interface, but it is successful configuration to only configure tunnel carefully.

Example: Switch (Config)# interface vlan 1

Switch(Config-if-Vlan1)ipv6 pim dr-priority 100

21.2.3.5 ipv6 pim exclude-genid

Command: **ipv6 pim exclude-genid**

no ipv6 pim exclude-genid

Function: This command makes the Hello packets sent by PIM SM do not include GenId option, the "**no ipv6 pim exclude-genid**" command restores the default value

Parameter: None

Default: The Hello packets include GenId option.

Command Mode: Interface Configuration Mode

Usage Guide: This command is used to interact with older Cisco IOS version. The command can configure on IPv6 tunnel interface, but it is successful configuration to only configure tunnel carefully.

Example: Configure the Hello packets sent by the switch do not include GenId option

Switch(Config-if-Vlan1)#ipv6 pim exclude-genid

21.2.3.6 ipv6 pim hello-holdtime

Command: ipv6 pim hello-holdtime <*value*>

no ipv6 pim hello-holdtime

Function: Configure or disable the Holdtime option in the Hello packets, this value is to describe neighbor holdtime,if the switch hasn't received the neighbor hello packets when the holdtime is over, this neighbor is deleted.

Parameter: <*value*> is the value of holdtime.

Default: The default value of Holdtime is 3.5*Hello_interval, Hello_interval's default value is 30s,so Holdtime's default value is 105s.

Command Mode: Interface Configuration Mode

Usage Guide: If this value is not configured, hellotime's default value is 3.5*Hello_interval. If the configured holdtime is less than the current hello_interval , this

configuration is denied. Every time hello_interval is updated, the Hello_holdtime will update according to the following rules: If hello_holdtime is not configured or hello_holdtime is configured but less than current hello_interval,hello_holdtime is modified to 3.5*hello_interval, otherwise the configured value is maintained. The command can configure on IPv6 tunnel interface, but it is successful configuration to only configure tunnel carefully.

Example: Configure vlan1's Hello Holdtime to 10s

Switch (Config)# interface vlan1

Switch (Config -if-Vlan1)#ipv6 pim hello-holdtime 10

21.2.3.7 ipv6 pim hello-interval

Command: ipv6 pim hello-interval <*interval*>

no ipv6 pim hello-interval

Function: Configure the interface's hello_interval of pim hello packets. The "**no ipv6 pim hello-interval**" command restores the default value.

Parameter: <*interval*> is the hello_interval of periodically transmitted pim hello packets', ranges from 1 to 18724s

Default: The default periodically transmitted pim hello packets' hello_interval is30s.

Command Mode: Interface Configuration Mode

Usage Guide: Hello messages make pim switches oriented each other and determine neighbor relationship. Pim switch announce the existence of itself by periodically transmitting hello messages to neighbors. If no hello messages from neighbors are received in the certain time, the neighbor is considered lost. This value can't be greater than neighbor overtime.The command can configure on IPv6 tunnel interface, but it is successful configuration to only configure tunnel carefully.

Example: Configure vlan's pim-sm hello_interval.

Switch (Config)#interface vlan 1

Switch(Config-If-Vlan1)#ipv6 pim hello-interval 20

21.2.3.8 ipv6 pim ignore-rp-set-priority

Command: ipv6 pim ignore-rp-set-priority

no ipv6 pim ignore-rp-set-priority

Function: When RP selection is carried out, this command configures the switch to enable Hashing regulation and ignore RP priority. This command is used to interact with older Cisco IOS versions.

Default: None

Parameter: None

Command Mode: Global Mode

Usage Guide: When selecting RP, Pim usually will select according to RP priority. When this command is configured, pim will not select according to RP priority. Unless there are older routers in the net, this command is not recommended.

Example: Configure to ignore RP priority.

Switch(config)#ipv6 pim ignore-rp-set-priority

21.2.3.9 ipv6 pim jp-timer

Command: ipv6 pim jp-timer <*value*>

no ipv6 pim jp-timer

Function: Configure to add JP timer. **no ipv6 pim jp-timer** restores the default value.

Parameter: <*value*> ranges from 10 to 65535

Default: 60s

Command Mode: Global Mode

Usage Guide: Configure the interval of transmitting J/P messages to59s.

Example: Switch(config)#ipv6 pim jp-timer 59

21.2.3.10 ipv6 pim multicast-routing

Command: ipv6 pim multicast-routing

no ipv6 pim multicast-routing

Function: Enable PIM-SM globally. The "**no ipv6 pim multicast-routing**" command disables PIM-SM globally.

Parameter: None

Default: Disabled PIM-SM protocol

Command Mode: Global Mode

Usage Guide: Inspect the changing information about pim state by this switch..

Example: Enable PIM-SM globally.

Switch (Config)#ipv6 pim multicast-routing

21.2.3.11 ipv6 pim neighbor-filter

Command: ipv6 pim neighbor-filter <*acess-list-name*>

no ipv6 pim neighbor-filter <*acess-list-name*>

Function: Configure the neighbor access-list. If filtered by the lists and connections with neighbors are created, this connections are cut off immediately. If no connection is created, this connection can't be created.

Parameter: <*acess-list-name*> is the applying access-list' name

Default: No neighbor filter configuration

Command Mode: Interface Configuration Mode

Usage Guide: ACL's default is DENY. If configuring access-list 1,access-list 1's default is

deny. In the following example, if “permit any-source” is not configured, deny 10.1.4.10 0.0.0.255 is the same as deny any-source. The command can configure on IPv6 tunnel interface, but it is successful configuration to only configure tunnel carefully.

Example: Configure vlan’s pim neighbor access-list

Switch (Config-if-Vlan1)#ipv6 pim neighbor-filter myfilter

Switch (Config)# ipv6 access-list myfilter deny fe80:20e:cff:fe01:facc

Switch (Config)# ipv6 access-list myfilter permit any

21.2.3.12 ipv6 pim state-refresh origination-interval

Command: ipv6 pim state-refresh origination-interval <interval>

no ipv6 pim state-refresh origination-interval

Function: Configure transmission interval of state-refresh message on interface. The “no ipv6 pim state-refresh origination-interval” command restores default value.

Parameter: <*interval*> message transmission interval value is from 4s to 100s.

Default: 60s

Usage Guide: The first-hop router periodically transmits stat-refresh messages to maintain PIM-DM list Items of all the downstream routers. The command can modify origination interval of state-refresh messages. Usually do not modify relevant timer interval. The command can configure on IPv6 tunnel interface, but it is successful configuration to only configure tunnel carefully.

Example: Configure transmission interval of state-refresh message on interface vlan1 to 90s.

Switch (Config-if-Vlan1)#ipv6 pim state-refresh origination-interval 90

21.2.3.13 ipv6 pim register-rate-limit

Command: ipv6 pim Register-rate-limit <*limit*>

no ipv6 pim Register-rate-limit

Function: This command is used to configure the speedrate of DR sending register packets, the unit is packet/second. the “**no ipv6 pim Register-rate-limit**” command restores the default value. This configured speedrate is each（S, G）state’s, not the whole systems.

Parameter: <*limit*> ranges from 1 to 65535

Default: No limit for sending speed

Command Mode: Global Mode

Usage Guide: Configure the speedrate of DR sending register packets

Example: Configure the speedrate of DR sending register packets to 59 p/s

Switch(config)#ipv6 pim Register-rate-limit 59

21.2.3.14 ipv6 pim register-rp-reachability

Command: ipv6 pim Register-rp-reachability

no ipv6 pim Register-rp-reachability

Function: This command makes DR check the RP reachability in the process of registration

Parameter: None

Default: Do not check

Command Mode: Global Mode

Usage Guide: This command configures DR whether or not to check the RP reachability.

Example: Configure the router to check the RP reachability before sending register packets.

Switch(config)# ipv6 pim Register-rp-reachability

21.2.3.15 ipv6 pim register-source

Command: ipv6 pim register-source {<*source-address*> |<*ifname*>}

no ipv6 pim register-source

Function: This command is to configure the source address of register packets sent by DR to overwrite default source address. This default source address is usually the RPF neighbor of source host direction.

Parameter: <*ifname*> is the interface name that will be the register packets source.

<*source-address*> is the interface address will be the register packets source. In the format of hex without prefix length.

Default: Do not check.

Command Mode: Global Mode

Usage Guide: The "**no ipv6 pim register-source**" command restores the default value, no more parameter is needed. Configured address must be reachable to Register-Stop messages sent by RP. It's usually a circle address, but it can be other physical addresses. This address must be announcable through unicast router protocols of DR.

Example: Configure the source address of the sent register packets to vlan1's address

Switch(config)# ipv6 pim register-source Vlan1

21.2.3.16 ipv6 pim register-suppression

Command: ipv6 pim register-suppression <***value***>

no ipv6 pim register-suppression

Function: This command is to configure the value of register suppression timer, the unit is second

Parameter: <***value***> is the timer's value, it ranges from 1 to 65535s

Default: 60s

Command Mode: Global Mode

Usage Guide: If this value is configured at DR,it's the value of register suppression timer; if this value is configured at RP and ipv6 pim rp-register-kat is not used at RP, this command modifies Keepalive-period value. The "**no ipv6 pim register-suppression**" command restores the default value.

Example: Configure the value of register suppression timer to 30s

Switch(config)# ipv6 pim register-suppression 30

21.2.3.17 ipv6 pim rp-address

Command: Ipv6 pim rp-address <*rp-address*> [<*group-range*>]

no ipv6 pim rp-address <*rp-address*> [all|<*group-range*>]

Function: This command is to configure static RP globally or in a multicast address range. The "**no ipv6 pim rp-address**" command cancels static RP.

Parameter: <*rp-address*> is the RP address, the format is **X:X::X:X** ,**ipv6** address

<*group-range*> is the expected RP, the format is **X:X::X:X/M, ipv6** address and prefix length all the ranges

Default: This switch is not a RP static router

Command Mode: Global Mode

Usage Guide: This command is to configure static RP globally or in a multicast address range.

Example: Configure 2000:112::8 as RP address globally

Switch (Config)# ipv6 pim rp-address 2000:112::8 ff1e::/64

21.2.3.18 ipv6 pim rp-candidate

Command: Ipv6 pim rp-candiate <*ifname*> [<*group range*>] [<*priority*>]

no ipv6 pim rp-candiate <*ifname*>

Function: This command is the candidate RP global configure command, it is used to configure PIM-SM candidate RP information in order to compete RP router with other candidate RPs.The **"no ipv6 pim rp-candiate**" command cancels the candidate RP.

Parameter: <*ifname*> is the name of the interface; **<*group range*>** is the group range of the candidate RP,the format is **X:X::X:X/M**, **ipv6** address and prefix length; **<*priority*>** is the RP selection priority, ranges from 0 to 255, the default value is 192, the lower value has more priority

Default: This switch is not a RP static router.

Command Mode: Global Mode

Usage Guide: This command is the candidate RP global configure command, it is used to configure PIM-SM candidate RP information in order to compete RP router with other

candidate RPs.Only this command is configured, this switch is the RP candidate router

Example: Configure vlan1 as the sending interface of candidate RP announce messages

Switch (Config)# ipv6 pim rp-candidate vlan1 100

21.2.3.19 ipv6 pim rp-register-kat

Command: ipv6 pim rp-register-kat <*vaule*>

no ipv6 pim rp-register-kat

Function: This command is to configure the KAT(KeepAlive Timer)value of the RP(S,G)items, the unit is second. The "**no ipv6 pim rp-register-kat**" command restores the default value

Parameter: <*vaule*> is the timer value, ranges from 1 to 65535s

Default: 185s

Command Mode: Global Mode

Usage Guide: Configure rp-register-kat interval to 30s

Example: Switch(config)# ipv6 pim rp-register-kat 30

21.2.3.20 ipv6 pim sparse-mode

Command: ipv6 pim sparse-mode [passive]

no ipv6 pim sparse-mode [passive]

Function: Enable PIM-SM on the interface. **no ipv6 pim sparse-mode [passive]** disables PIM-SM.

Parameter: [*passive*] means to disable PIM-SM (that's PIM-SM doesn't receive any packets) and only enable IGMP(receive and transmit IGMP packets).

Default: Disabled PIM-SM

Command Mode: Interface Configuration Mode

Usage Guide: Enable PIM-SM on the interface. The command can configure on IPv6 tunnel interface, but it is successful configuration to only configure tunnel carefully.

Example: Enable PIM-SM on the interface vlan1

Switch (Config)#interface vlan 1

Switch(Config-If-Vlan1)#ipv6 pim sparse-mode

21.2.3.21 ipv6 pim ssm

Command: ipv6 pim ssm {default|range <*access-list-name* >}

no ipv6 pim ssm

Function: Configure the range of pim ssm multicast address. The "**no ipv6 pim ssm**" command deletes configured pim ssm multicast group.

Parameter: *default :* indicates the default range of pim ssm multicast group is ff3x::/32.

<access-list-number > is the name of applying access-list.

Default: Do not configure the range of pim ssm group address

Command Mode: Global Mode

Usage Guide:

1. Only this command is configured, pim ssm can be available.

2. Before configuring this command, make sure ipv6 pim multicasting succeed.

3. Access-list only can use the lists created by ipv6 access-list.

4.Users can execute this command first and then configure the corresponding acl; or delete corresponding acl in the bondage. After the bondage, only command no ipv6 pim ssm can release the bondage.

5 .If ssm is needed, this command should be configured at the related edge route. For example, the local switch with igmp(must) and multicast source DR or RP(at least one of the two) configure this command, the middle switch need only enable PIM-SM.

Example: Configure the switch to enable PIM-SSM, the group's range is what is specified by access-list 23.

Switch (config)#ipv6 pim ssm range 23

Switch (config)#ipv6 access-list dcn permit ff1e::/48

21.2.4 PIM-SM Typical Application

As shown in the following figure, add the Ethernet interfaces of SwitchA, SwitchB, switchC and switchD to corresponding vlan, and start PIM-SM Protocol on each vlan interface.

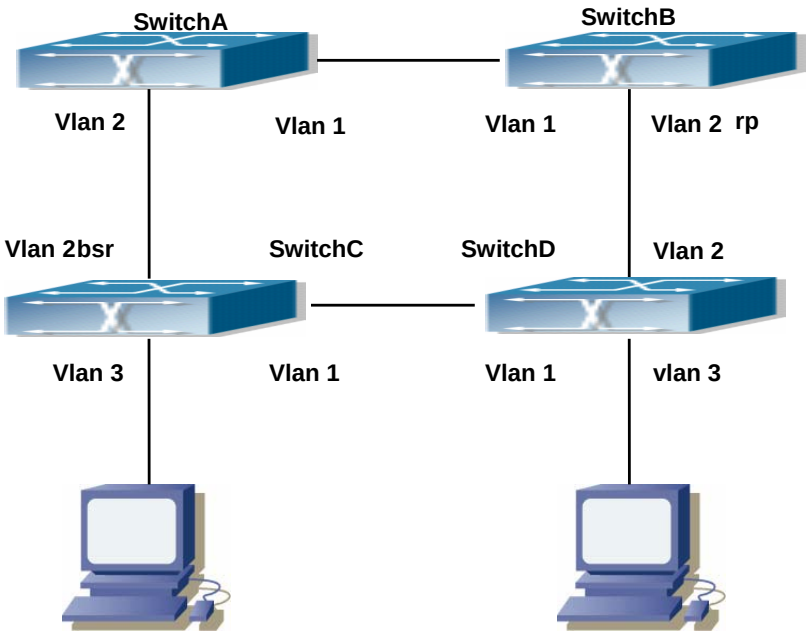


Fig 21-2 PIM-SM Typical Environment

The configuration procedure for SwitchA, SwitchB, switchC and switchD is as below:

(1) Configure SwitchA:

```
Switch (Config) #ipv6 pim multicast-routing
Switch (Config) #interface vlan 1
Switch (Config-If-Vlan1) # ipv6 address 2000:12:1:1::1/64
Switch (Config-If-Vlan1) # ipv6 pim sparse-mode
Switch (Config-If-Vlan1) #exit
Switch (Config) #interface vlan 2
Switch (Config-If-Vlan2) # ipv6 address 2000:13:1:1::1/64
Switch (Config-If-Vlan2) # ipv6 pim sparse-mode
```

(2) Configure Switch B:

```
Switch (Config) #ipv6 pim multicast-routing
Switch (Config) #interface vlan 1
Switch (Config-If-Vlan1) # ipv6 address 2000:12:1:1::2/64
Switch (Config-If-Vlan1) # ipv6 pim sparse-mode
Switch (Config-If-Vlan1) #exit
Switch (Config) #interface vlan 2
Switch (Config-If-Vlan2) # ipv6 address2000:24:1:1::2/64
Switch (Config-If-Vlan2) # ipv6 pim sparse-mode
Switch (Config-If-Vlan2) # exit
Switch (Config) # ipv6 pim rp-candidate vlan2
```

(3) Configure SwitchC:

```
Switch (Config) #ipv6 pim multicast-routing
Switch (Config) #interface vlan 1
Switch (Config-If-Vlan1) # ipv6 address 2000:34:1:1::3/64
Switch (Config-If-Vlan1) # ipv6 pim sparse-mode
Switch (Config-If-Vlan1) #exit
Switch (Config) #interface vlan 2
Switch (Config-If-Vlan2) # ipv6 address 2000:13:1:1::3/64
Switch (Config-If-Vlan2) # ipv6 pim sparse-mode
Switch (Config-If-Vlan2) #exit
Switch (Config) #interface vlan 3
Switch (Config-If-Vlan3) # ipv6 address 2000:30:1:1::1/64
Switch (Config-If-Vlan3) # ipv6 pim sparse-mode
Switch (Config-If-Vlan3) # exit
Switch (Config) # ipv6 pim bsr-candidate vlan2 30 10
```

(4) Configure SwitchD:

```
Switch (Config) #ipv6 pim multicast-routing
```

Switch (Config) #interface vlan 1
Switch (Config-If-Vlan1) # ipv6 address 2000:34:1:1::4/64
Switch (Config-If-Vlan1) # ipv6 pim sparse-mode
Switch (Config-If-Vlan1) #exit
Switch (Config) #interface vlan 2
Switch (Config-If-Vlan2) # ipv6 address 2000:24:1:1::4/64
Switch (Config-If-Vlan2) # ipv6 pim sparse-mode
Switch (Config-If-Vlan2) #exit
Switch (Config) #interface vlan 3
Switch (Config-If-Vlan3) # ipv6 address 2000:40:1:1::1/64
Switch (Config-If-Vlan3) # ipv6 pim sparse-mode

21.2.5 PIM-SM Troubleshooting

When configuring and using PIM-SM protocol, PIM-SM protocol may fail to work normally due to physical connections, incorrect configuration and so on. So, users shall note the following points:

- ✧ Assure the physical connection is correct.
- ✧ Assure the Protocol of Interface and Link is UP (use show interface command);
- ✧ Unicast route shall be used to carry out RPF examination for multicast protocol. So the correctness of unicast route shall be guaranteed above all.
- ✧ PIM-SM Protocol requires supports of RP and BSR, therefore you should use **show ipv6 pim bsr-router** first to see if there is BSR information. If not, you need to check if there is unicast routing leading to BSR.
- ✧ Use **show ipv6 pim rp-hash** command to check if RP information is correct; if there is no RP information, you still need to check unicast routing;

If all attempts fail to solve the problems on PIM-SM, then use debug commands such as debug ipv6 pim/ debug ipv6 pim bsr, copy DEBUG information in 3 minutes and send to Technology Service Center.

21.2.5.1 Commands for Monitor and debug

21.2.5.1.1 debug ipv6 pim timer sat

Command: debug ipv6 pim timer sat
no debug ipv6 pim timer sat

Function: Enable debug switch of PIM-SM source activity timer information in detail; the "**no debug ipv6 pim timer sat**" command disenables the debug switch.

Parameter: None

Default: Disabled

Command Mode: Admin Mode

Usage Guide: Enable the switch, and display source activity timer information in detail.

Example: Switch # debug ipv6 pim timer sat

21.2.5.1.2 debug ipv6 pim timer srt

Command: debug ipv6 pim timer srt

no debug ipv6 pim timer srt

Function: Enable debug switch of PIM-SM state-refresh timer information in detail; the "**no debug ipv6 pim timer srt**" command disenables the debug switch.

Parameter: None

Default: Disabled

Command Mode: Admin Mode

Usage Guide: Enable the switch, and display PIM-SM state-refresh timer information in detail

Example: Switch # debug ipv6 pim timer srt

21.2.5.1.3 debug ipv6 pim events

Command: debug ipv6 pim events

no debug ipv6 pim events

Function: Enable or Disable pim events debug switch

Parameter: None

Default: Disabled

Command Mode: Admin Mode and Global Mode

Usage Guide: Enable "pim events debug" switch and display events information about pim operation.

Example: Switch# debug ipv6 pim events

21.2.5.1.4 debug ipv6 pim mfc

Command: debug ipv6 pim mfc（in|out|）

no debug ipv6 pim mfc（in|out|）

Function: Enable or Disable pim mfc debug switch

Parameter: None

Default: Disabled

Command Mode: Admin Mode and Global Mode

Usage Guide: Enable pim mfc debug switch and display generated and transmitted multicast id's information.

Example: Switch# debug ipv6 pim mfc in

21.2.5.1.5 debug ipv6 pim mib

Command: debug ipv6 pim mib

no ipv6 debug pim mib

Function: Enable or Disable PIM MIB debug switch

Parameter: None

Default: Disabled

Command Mode: Admin Mode and Global Mode

Usage Guide: Inspect PIM MIB information by PIM MIB debug switch. It's not available now and it's for the future extension.

Example: Switch# debug ipv6 pim mib

21.2.5.1.6 debug ipv6 pim nexthop

Command: debug ipv6 pim nexthop

no debug ipv6 pim nexthop

Function: Enable or Disable pim nexthop debug switch

Parameter: None

Default: Disabled

Command Mode: Admin Mode and Global Mode

Usage Guide: Inspect PIM NEXTHOP changing information by the pim nexthop switch.

Example: Switch# debug ipv6 pim nexthop

21.2.5.1.7 debug ipv6 pim nsm

Command: debug ipv6 pim nsm

no debug ipv6 pim nsm

Function: Enable or Disable pim debug switch communicating with Network Services

Parameter: None

Default: Disabled

Command Mode: Admin Mode and Global Mode

Usage Guide: Inspect the communicating information between pim and Network Services by this switch.

Example: Switch# debug ipv6 pim nsm

21.2.5.1.8 debug ipv6 pim packet

Command: debug ipv6 pim packet [in|out|]

no debug ipv6 pim packet [in|out|]

Function: Enable or Disable pim debug switch

Parameter: in display only received pim packets

out display only transmitted pim packets

none display both

Default: Disabled

Command Mode: Admin Mode and Global Mode

Usage Guide: Inspect the received and transmitted pim packets by this switch.

Example: Switch# debug ipv6 pim packet in

21.2.5.1.9 debug ipv6 pim state

Command: debug ipv6 pim state

no debug ipv6 pim state

Function: Enable or Disable pim debug switch

Parameter: None

Default: Disabled

Command Mode: Admin Mode and Global Mode

Usage Guide: Inspect the changing information about pim state by this switch.

Example: Switch# debug ipv6 pim state

21.2.5.1.10 debug ipv6 pim timer

Command: debug ipv6 pim timer

debug ipv6 pim timer assert

debug ipv6 pim timer assert at

debug ipv6 pim timer bsr bst

debug ipv6 pim timer bsr crp

debug ipv6 pim timer bsr

debug ipv6 pim timer hello ht

debug ipv6 pim timer hello nlt

debug ipv6 pim timer hello tht

debug ipv6 pim timer hello

debug ipv6 pim timer joinprune et

debug ipv6 pim timer joinprune grt

debug ipv6 pim timer joinprune jt

debug ipv6 pim timer joinprune kat

debug ipv6 pim timer joinprune ot

debug ipv6 pim timer joinprune plt

debug ipv6 pim timer joinprune ppt

debug ipv6 pim timer joinprune pt

debug ipv6 pim timer joinprune

debug ipv6 pim timer register rst

debug ipv6 pim timer register

no debug ipv6 pim timer

no debug ipv6 pim timer assert

no debug ipv6 pim timer assert at

no debug ipv6 pim timer bsr bst

no debug ipv6 pim timer bsr crp

no debug ipv6 pim timer bsr

no debug ipv6 pim timer hello ht

no debug ipv6 pim timer hello nlt

no debug ipv6 pim timer hello tht

no debug ipv6 pim timer hello

no debug ipv6 pim timer joinprune et

no debug ipv6 pim timer joinprune grt

no debug ipv6 pim timer joinprune jt

no debug ipv6 pim timer joinprune kat

no debug ipv6 pim timer joinprune ot

no debug ipv6 pim timer joinprune plt

no debug ipv6 pim timer joinprune ppt

no debug ipv6 pim timer joinprune pt

no debug ipv6 pim timer joinprune

no debug ipv6 pim timer register rst

no debug ipv6 pim timer register

no debug ipv6 pim timer

Function: Enable or Disable each pim timer

Parameter: None

Default: Disabled

Command Mode: Admin Mode and Global Mode

Usage Guide: Enable the specified timer’s debug information

Example: Switch# debug ipv6 pim timer assert

21.2.5.1.11 show ipv6 pim bsr-router

Command: show ipv6 pim bsr-router

Function: Display BSR address

Parameter: None

Default: None

Command Mode: Admin Mode and Global Mode

Example:

Switch#show ipv6 pim bsr-router

PIMv2 Bootstrap information

This system is the Bootstrap Router (BSR)

BSR address: 2000:1:111::100 (?)

Uptime: 00:16:00, BSR Priority: 0, Hash mask length: 126

Next bootstrap message in 00:00:10

Role: Candidate BSR

State: Elected BSR

Next Cand_RP_advertisement in 00:00:10

RP: 2000:1:111::100(Vlan2)

Displayed Information	Explanations
BSR address	Bsr-router Address
Priority	Bsr-router Priority
Hash mask length	Bsr-router hash mask length
State	The current state of this candidate BSR, Elected BSR is selected BSR

21.2.5.1.12 show ipv6 pim interface

Command: show ipv6 pim interface [detail|]

Function: Display PIM interface information

Parameter: None

Default: None

Command Mode: Any Mode

Example:

```
Switch#show ipv6 pim interface
Interface VIFindex Ver/     Nbr       DR
                           Mode     Count    Prior
Vlan2        0             v2/S     0          1
     Address           : fe80::203:fff:fee3:1244
     Global Address: 2000:1:111::100
     DR                : this system
Vlan3        2             v2/S     0          1
     Address           : fe80::203:fff:fee3:1244
     Global Address: 2000:10:1:13::1
     DR                : this system
```

Displayed Information	Explanations
Address	Interface address
Interface	Interface name
VIF index	Interface index
Ver/Mode	Pim version and mode, usually v2,sparse mode displays S,dense mode displays D
Nbr Count	The interface's neighbor count
DR Prior	Dr priority
DR	The interface's DR address

21.2.5.1.13 show ipv6 pim mroute sparse-mode

Command: show ipv6 pim mroute sparse-mode

Function: Display the multicast route table of PIM-SM

Parameter: None

Default: None

Command Mode: Admin Mode and Global Mode

Usage Guide: Display the BSP routers in the network maintained by PIM-SM

Example:

Switch#show ipv6 pim mr group ff1e::15
IPv6 Multicast Routing Table
(*,*,RP) Entries: 0
(*,G) Entries: 1
(S,G) Entries: 1
(S,G,rpt) Entries: 1
FCR Entries: 0
(*, ff1e::15)
RP: 2000:1:111::100
RPF nbr: ::
RPF idx: None
Upstream State: JOINED
 Local ..I.....
 Joined .....
 Asserted .....
FCR:

(2000:1:111::11, ff1e::15)
RPF nbr: ::
RPF idx: None
SPT bit: 1
Upstream State: JOINED
 Local .....
 Joined .....
 Asserted .....
 Outgoing ..o.....

(2000:1:111::11, ff1e::15, rpt)
RP: 2000:1:111::100
RPF nbr: ::

RPF idx: None

Upstream State: NOT PRUNED

Pruned .....

Outgoing ..o.....

Displayed Information	Explanations
Entries	The counts of each item
RP	Share tree's RP address
RPF nbr	RP direction or upneighbor of source direction
RPF idx	RPF nbr interface
Upstream State	Upstream State, there are two state of Joined(join the tree, expect to receive data from upstream) and Not Joined(quit the tree, not expect to receive data from upstream), and more options such as RPT Not Joined, Pruned, Not Pruned are available for（S,G,rpt.）
Local	Local join interface, this interface receive IGMPJoin
Joined	PIM join interface, this interface receive J/P messages
Asserted	Asserted state
Outgoing	Final outgoing of multicast data

21.2.5.1.14 show ipv6 pim neighbor

Command: show ipv6 pim neighbor [detail|]

Function: Display router neighbors

Parameter: None

Default: None

Command Mode: Any Mode

Usage Guide: Display multicast router neighbors maintained by the PIM

Example:

Switch(config)#show ipv6 pim neighbor

Neighbor Address	Interface	Uptime/Expires	Ver	DR Priority/Mode
Fe80::203:fff:fee3:1244	Vlan1	00:00:10/00:01:35	v2	1 /DR
fe80::20e:cff:fe01:facc	Vlan1	00:00:13/00:01:32	v2	1 /

Displayed Information	Explanations
Neighbor Address	Neighbor address
Interface	Neighbor interface
Uptime/Expires	Running time /overtime
Ver	Pim version ,v2 usually
DR Priority/Mode	DR priority in the hello messages from the neighbor and if the neighbor is the interface's DP

21.2.5.1.15 show ipv6 pim nexthop

Command: show ipv6 pim nexthop

Function: Display the PIM buffered nexthop router in the unicast route table

Parameter: None

Default: None

Command Mode: Any Mode

Usage Guide: Display the PIM buffered nexthop router information

Example:

Switch#show ipv6 pim nexthop

Flags: N = New, R = RP, S = Source, U = Unreachable ….

Destination Type Nexthop

Nexthop ..Nexthop Nexthop Metric Pref Refcnt

Num Addr

Ifindex Name

2000:1:111::11 ..S. 1 :

: 2004 0 0 2

2000:1:111::100 .RS. 1 ::

2004 0 0 2

2004 0 0 2

Displayed Information	Explanations
Destination	Destination of next item
Type	N: created nexthop,RP direction and S direction are not determined . R: RP direction S: source direction U: can't reach
Nexthop Num	Nexthop number

Nexthop Addr	Nexthop address
Nexthop Ifindex	Nexthop interface index
Nexthop Name	Nexthop name
Metric	Metric to nexthop
Pref	Preference Route preference
Refcnt	Reference count

21.2.5.1.16 show ipv6 pim rp-hash

Command: show ipv6 pim rp-hash X:X::X:X

Function: Display the RP address of group **X:X::X:X's** merge point

Parameter: Group address

Default: None

Command Mode: Any Mode

Usage Guide: Display the RP address corresponding to the specified group address

Example:

Switch#show ipv6 pim rp-hash ff1e::15

RP: 2000:1:111::100

Info source: 2000:1:111::100, via bootstrap

Displayed Information	Explanations
RP	Queried group'sRP
Info source	The source of Bootstrap information

21.2.5.1.17 show ipv6 pim rp mapping

Command: show ipv6 pim rp mapping

Function: Display Group-to-RP Mapping and RP

Parameter: None

Default: None

Command Mode: Any Mode

Usage Guide: Display the current RP and mapping relationship

Example:

Switch#show ipv6 pim rp mapping

PIM Group-to-RP Mappings

This system is the Bootstrap Router (v2)

Group(s): ff00::/8

RP: 2000:1:111::100

Info source: 2000:1:111::100, via bootstrap, priority 192

Uptime: 00:10:24, expires: 00:02:06

Group(s): ff00::/8, Static

RP: 2000:1:111::100

Uptime: 00:11:01

Displayed Information	Explanations
Group(s)	Group address range of RP
Info source	Source of Bootstrap messages
Priority	Priority of Bootstrap messages

21.3 MLD

21.3.1 Introduction to MLD

MLD (Multicast Listener Discovery) is the multicast group member (receiver) discovery protocol serving IPv6 multicast. It is similar to IGMP Protocol in IPv4 multicast application. Correspondingly, MLD Protocol version1 is similar to IGMP Protocol version2, and MLD Protocol version2 is similar to IGMP Protocol version3. Current firmware supports MLDv1/ MLDv2.

The IPv6 multicast hosts can join or leave from multicast group at any location, any time, regardless of the total number of group members. It is unnecessary and impossible for multicast switch to store the relationship among all host members. Multicast switch simply finds out via MLD protocol if there are receivers of certain multicast group on the network segment connected to each port. The only thing host need to do is to keep the record of which multicast groups it joined.

MLD is unsymmetrical between host and switch: the host needs to respond the MLD query message of multicast switch with membership report message; the switch periodically sends membership query message and determines if there is host joining a specific group in its subnetworks according to the response message received, and after it receives the report of a host quitting from the group, it sends out the query for the group to confirm if there is no member left in it.

There are three types of protocol messages of MLD Protocol, that is, Query, Report and Done (which is corresponding to Leave of IGMPv2). Like IGMPV2, the Query messages include General Query and Specific Group Query. General Query uses the multicast address FF02::1 of hosts as destination address, the group address is 0; and Specific Group Query use its group address as destination address. The multicast addresses of MLD use 130, 131 and 132 as data types denoting the three kinds of messages mentioned above. Other logic is basically same as IGMPv2.

21.3.2 MLD Configuration Task List

1、Start MLD (Required)

2、Configure MLD auxiliary parameters (Required)

（1）Configure MLD group parameters

1）Configure MLD group filter conditions

（2）Configure MLD query parameters

1）Configure the interval of MLD sending query message

2）Configure the maximum response time of MLD query

3）Configure overtime of MLD query

3、Shut down MLD Protocol

1. Start MLD Protocol

There is no special commands for starting MLD Protocol on EDGECORE series layer 3 switches. MLD Protocol will automatically start up as long as any IPv6 multicast protocol is started on corresponding interface.

Command	Explanation
Global Mode	
Ipv6 pim multicast-routing	To start Global IPv6 Multicast Protocol, the precondition of starting MLD Protocol. The NO operation of corresponding command shuts ipv6 multicast protocol and MLD Protocol. (Required)

Command	**Explanation**
Port Configuration Mode	
ipv6 pim dense-mode | ipv6 pim sparse-mode	Start MLD Protocol. The NO operation of corresponding command shuts MLD Protocol. (Required)

2. Configure MLD auxiliary parameters

（1）Configure MLD group parameters

1）Configure MLD group filter conditions

Command	**Explanation**
Port Configuration Mode	
ipv6 mld access-group ***<acl_name>*** **no ipv6 mld access-group**	Configure the filter conditions of interface for MLD group; the NO operation of this command cancels filter conditions.

（2）Configure MLD Query parameters

1）Configure interval time for MLD to send query messages

2）Configure the maximum response time of MLD query

3）Configure the overtime of MLD query

Command	Explanation
Port Configuration Mode	
ipv6 mld query-interval <*time_val*> **no ipv6 mld query-interval**	Configure the interval of MLD query messages sent periodically; the NO operation of this command restores the default value.
ipv6 mld query-max-response-time <*time_val*> **no ipv6 mld query-max-response-time**	Configure the maximum response time of the interface for MLD query; the NO operation of this command restores the default value.
ipv6 mld query-timeout <*time_val*> **no ipv6 mld query-timeout**	Configure the overtime of the interface for MLD query; the NO operation of this command restores the default value.

3. Shut down MLD Protocol

Command	Explanation
Port Configuration Mode	
no ipv6 pim dense-mode | no ipv6 pim sparse-mode | no ipv6 pim multicast-routing (Global Mode)	Shut down MLD Protocol

21.3.3 Commands for MLD

21.3.3.1 ipv6 mld access-group

Command:ipv6 mld access-group {<*acl_name*>}

no ipv6 mld access-group

Function: Configure the access control of the interface to MLD groups ;the "**no ipv6 mld access-group**" command stops the access control

Parameter: <*acl-name*> is the name of IPv6 access-list

Default: no filter condition

Command Mode: Interface Configuration Mode

Usage Guide: Configure the interface to filter MLD groups, allow or deny some group's join.

Example: Configure the interface vlan2 to accept group FF1E::1:0/112 and deny others

Switch (Config)# ipv6 access-list aclv6 permit FF1E::1:0/112

Switch (Config)# ipv6 access-list aclv6 deny any

Switch (Config)#interface vlan 1

Switch(Config-If-Vlan1)#ipv6 mld access-group aclv6

21.3.3.2 ipv6 mld immediate-leave

Command: ipv6 mld immediate-leave group-list {*<acl-name>*}

no ipv6 mld immediate-leave

Function: Configure MLD to work in the immediate leave mode, that's when the host sends a membership qualification report that equals to leave a group, the router doesn't send query and consider there is no this group's member in the subnet. The **"no ipv6 mld immediate-leave**" command cancels the immediate leave mode

Parameter: *<acl-name>* is the name of IPv6 access-list

Default: Do not configure immediate-leave group

Command Mode: Interface Configuration Mode

Usage Guide: This command is used only when there is only one host in the subnet

Example: Configure access-list"aclv6"as immediate leave mode

Switch(Config-if-Vlan1)#ipv6 mld immediate-leave group-list aclv6

21.3.3.3 ipv6 mld last-member-query-interval

Command: ipv6 mld last-member-query-interval *<interval>*

no ipv6 mld last-member-query-interval

Function: Configure the interface's sending interval of querying specific group. The **"no ipv6 mld last-member-query-interval**" command cancels the manually configured value and restores the default value.

Parameter: *<interval>* is the interval of querying specific group, it ranges from 1000 to 25000ms. It's the integer times of 1000ms. If it's not the integer times of 1000ms, the system will convert it to the integer times of 1000ms

Default: 1000ms.

Command Mode: Interface Configuration Mode

Example: Configure the interface vlan1's MLD last-member-query-count as 2000

Router(Config)#int vlan 1

Router(Config-if-vlan1)#ipv6 mld last-member-query-interval 2000

21.3.3.4 ipv6 mld query-interval

Command: ipv6 mld query-interval *<time_val>*

no ipv6 mld query-interval

Function: Configure the interval of the periodically sent MLD host-query messages; the "**no ipv6 mld query-interval**" command restores the default value.

Parameter: *<time_val>* is the interval of the periodically sent MLD host-query messages; it ranges from 0 to 65535s

Default: Interval of periodically transmitted MLD query message is 125s.

Command Mode: Interface Configuration Mode

Usage Guide: When a interface enables a kind of multicast protocol, it will send MLD host-query messages periodically. This command is used to configure the query period

Example: Configure the interval of the periodically sent MLD host-query messages to 10s

Switch (Config)#interface vlan 1

Switch(Config-If-Vlan1)#ipv6 mld query-interval 10

21.3.3.5 ipv6 mld query-max-response-time

Command: ipv6 mld query-max-response-time <*time_val*>

no ipv6 mld query- max-response-time

Function: Configure the maximum of the response time of MLD queries; the "**no ipv6 mld query- max-response-time**: command restores the default value

Parameter: <*time_val*> is the maximum of the response time of MLD queries, it ranges from 1 to 25s.

Default: 8s.

Command Mode: Interface Configuration Mode

Usage Guide: When the switch receives a query message, the host will set a timer to each multicast group. The timer's value is between 0 to the maximum response time. When any one of the timers decreases to 0, the host will group member announce messages. Configuring the maximum response time reasonablely,the host can swiftly response to the query messages and the router can also get the group members' existing states quickly.

Example: Configure the maximum response time of MLD queries to 20s

Switch (Config)#interface vlan 1

Switch(Config-If-Vlan1)#ipv6 mld query- max-response-time 20

21.3.3.6 ipv6 mld query-timeout

Command: ipv6 mld query-timeout <*time_val*>

no ipv6 mld query-timeout

Function: Configure the interface's timeout of MLD queries; the "**no ipv6 mld query-timeout**" command restores the default value

Parameter: <*time_val*> is the timeout of MLD queries, it ranges from 60 to 300s

Default: Default: 255s

Command Mode: Interface Configuration Mode

Usage Guide: In the share network, when there are more switches that run MLD,one switch will be selected as the querying host and others set a timer to inspect the querying host's state. If no querying packet is received when the timeout is over, a switch will be

reselected as the querying host .

Example: Configure the interface's timeout of MLD queries to 100s

Switch (Config)#interface vlan 1

Switch(Config-If-Vlan1)#ipv6 mld query-timeout 100

21.3.3.7 ipv6 mld access-group

Command: ipv6 mld access-group {<*acl_name*>}

no ipv6 mld access-group

Function: Configure the filter conditions of the interface on the MLD group; the "**no ipv6 mld access-group**" command cancels the filter conditions.

Parameter: <*acl-name*> is the name of the IPv6 access list

Default: No filter condition by default

Command Mode: Interface Mode

Usage Guide: This command can configure the filter on the interface to the groups, permitting or denying certain groups.

Example: Configure the interface vlan1 to permit group FF1E::1:0/112, while denying all others.

Switch (Config)# ipv6 access-list aclv6 permit FF1E::1:0/112

Switch (Config)# ipv6 access-list aclv6 deny any

Switch (Config)#interface vlan 1

Switch(Config-If-Vlan1)#ipv6 mld access-group aclv6

21.3.3.8 ipv6 mld join-group

Command: ipv6 mld join-group <*address*>

no ipv6 mld join-group <address>

Function: Configure the interface to join in certain multicast group; the "**no ipv6 mld join-group <address>**" command cancels joining certain multicast group.

Parameter: <*address*> is a valid IPv6 multicast address

Default: No multicast group joined by factory default

Command Mode: Interface Mode

Usage Guide: The address range of the IPv6 multicast is FFxy::/8, however the (FF02::/16) is permanent addresses which can not be joined in.

Example: Join the interface vlan2 in multicast group with multicast address of ff1e::1:3.

Switch(Config)#interface vlan 2

Switch(Config-if-Vlan2)#ipv6 mld join-group ff1e::1:3

21.3.3.9 ipv6 mld join-group mode source

Command: ipv6 mld join-group <*X:X::X:X*> mode <*include*|*exclude*> source

<.X:X::X:X>

no ipv6 mld join-group <X:X::X:X> source <.X:X::X:X>

Function: Configure the sources of certain multicast group which the interface join in. Note: because of the client group has got only INLCUDE and EXCLUDE modes, if the source mode is not in accordance with current mode configured, the group mode will be changed and the original sources of the other modes configured will be cleared permanently; the “no” form of this command cancels joining certain group.

Parameter: *<X:X::X:X>* is a valid IPv6 multicast address

<include|exclude>：joining mode

<.X:X::X:X>：source list, configure several sources is allowed.

Default: No multicast group to be joined by factory default

Command Mode: Interface Mode

Usage Guide: The address range of the IPv6 multicast is FFxy::/8, however the (FF02::/16) is permanent addresses which can not be joined in. As for sources with mode same as the original one, the source will be added, while for those with different modes, the original sources will be cleared.

Example:

Join vlan2 in multicast group with multicast address of ff1e::1:3, with sources 2003::1 and 2003::2 in INCLUDE mode.

Switch(Config)#interface vlan 2

Switch(Config-if-Vlan2)#ipv6 mld join-group ff1e::1:3 mode include source 2003::1 2003::2

21.3.3.10 ipv6 mld limit

Command:ipv6 mld limit <*state-count*>

no ipv6 mld limit

Function: Configure the MLD state count limit of the interface; the “**no ipv6 mld limit**” command restores the manually configured value to default value

Parameter:<*state-count*>:max MLD state the interface maintains, the valid range is 1-5000.

Default: 400 by default

Command Mode: Interface Mode

Usage Guide: When max state-count is configured, the number of the state the interface saves will only upper to the state-count limit; and when the max state-count is reached, the later new member qualification report received will be ignored. If some MLD group state has already been saved before this command configured, the original states will be removed and the MLD general query will be sent to collect group member qualification reports no more than the max state-count.

Example: Set the MLD state-count limit of the interface vlan2 to 4000

Switch(Config)#interface vlan2

Switch(Config-if-Vlan2)#ipv6 mld limit 4000

21.3.3.11 ipv6 mld static-group

Command: ipv6 mld static-group *<group_address> [source <source_address>]*

no ipv6 mld static-group <group_address> [source <source_address>]

Function: Configure certain static group or static source on the interface. The “no” form of this command cancels certain previously configured static group or static source

Parameter:<group_address> is a valid IPv6 multicast address;<source_address> is a valid IPv6 unicast address.

Default: No static group or static source is configured on the interface by factory default.

Command Mode: Interface Mode

Usage Guide: The valid range of the static group multicast address configured by the interface is the dynamic multicast address specified by the IPv6 protocol. Once the interface configures static group or static source for the multicast address, no matter whether there is membership qualification report of this group or source in the subnet, MLD protocol will consider that the group or source exist. Note: the configured static source is the source to be forwarded.

Example: Configure an MLD static-group ff1e::1:3 on interface vlan2

Switch(Config)#interface vlan 2

Switch(Config-if-Vlan2)#ipv6 mld static-group ff1e::1:3

Configure a static source 2001::1 of the group ff1e::1:3 on interface vlan2

Switch(Config)#int vlan2

Switch(Config-if-Vlan2)#ipv6 mld static-group ff1e::1:3 source 2001::1

21.3.3.12 ipv6 mld version

Command: ipv6 mld version *<version_no>*

no ipv6 mld version

Function: Configure the version of the MLD protocol running on the interface; the “**no ipv6 mld version**” command restores the manually configured version to the default one

Parameter: *<version_no>* is the version number of the MLD protocol,with a valid range of 1-2.

Default: 2 by default

Command Mode: Interface Mode

Usage Guide: While there is routers still not upgraded to version 2 of MLD protocol on the subnet connected, the interface should be configured to corresponding version.

Example: Configure the MLD version to 2.

Switch(Config)#ipv6 mld version 2

21.3.4 MLD Typical Application

As shown in the following figure, add the Ethernet interfaces of Switch A and Switch B to corresponding vlan, and start PIM6 on each vlan interface.

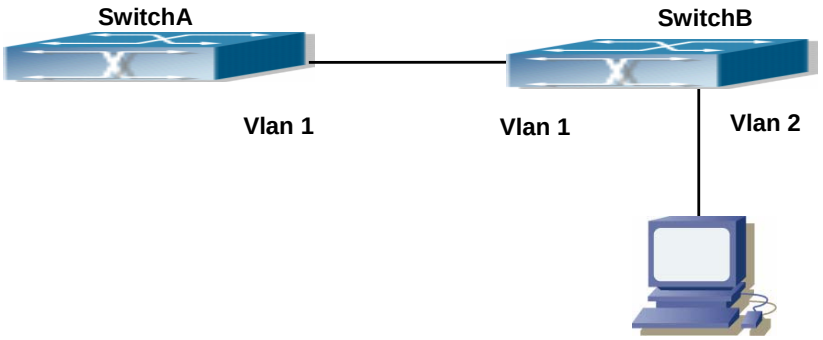


Fig 21-3 Network Topology Diagram

The configuration procedure for SwitchA and SwitchB is as below:

(1) Configure SwitchA:

Switch (Config) #ipv6 pim multicast-routing

Switch (Config) #ipv6 pim rp-address 3FFE::1

Switch (Config) #interface vlan 1

Switch (Config-If-Vlan1) #ipv6 address 3FFE::1/64

Switch (Config-If-Vlan1) #ipv6 pim sparse-mode

(2) Configure SwitchB:

Switch (Config) #ipv6 pim multicast-routing

Switch (Config) #ipv6 pim rp-address 3FFE::1

Switch (Config) #interface vlan1

Switch (Config-If-Vlan1) #ipv6 address 3FFE::2/64

Switch (Config-If-Vlan1) #ipv6 pim sparse-mode

Switch (Config-If-Vlan1) #exit

Switch (Config) #interface vlan2

Switch (Config-If-Vlan2) #ipv6 address 3FFA::1/64

Switch (Config-If-Vlan2) #ipv6 pim sparse-mode

Switch (Config-If-Vlan2) #ipv6 mld query-timeout 150

21.3.5 MLD Troubleshooting

When configuring and using MLD protocol, MLD protocol may fail to work normally due to physical connections, incorrect configuration and so on. So, users shall note the following points:

- ✧ Assure the physical connection is correct.
- ✧ Assure the protocol of interface and link is UP (use show interface command)
- ✧ Assure to start one kind of multicast protocol on the interface
- ✧ Assure the time of the timers of each router on the same network segment is consistent; usually we recommend the default setting.
- ✧ Unicast route shall be used to carry out RPF examination for multicast protocol. So the correctness of unicast route shall be guaranteed above all.

If all attempts fail to solve the problems on MLD, please use debug commands such as debug ipv6 MLD event/packet, and copy DEBUG information in 3 minutes and send to Technology Service Center.

21.3.5.1 Commands for Monitor And Debug

21.3.5.1.1 debug ipv6 mld events

Command: debug ipv6 mld events

no debug ipv6 mld events

Function: Enable the debug switch that displays MLD events. the **"no debug ipv6 mld events**" command disables the debug switch.

Parameter: None

Default: Disabled

Command Mode: Admin Mode

Usage Guide: This switch can be enabled to get MLD events information

Example:

Switch# debug ipv6 mld events

Switch#1970/01/01 07:30:13 IMI: MLD Report recv: src fe80::203:fff:fe12:3457 for ff1e::1:3

1970/01/01 07:30:13 IMI: Processing Report comes from Vlan1, ifindex 2003

1970/01/01 07:30:13 IMI: MLD(Querier) ff1e::1:3 (Vlan1): No Listeners --> Listeners Present

21.3.5.1.2 debug ipv6 mld packet

Command: debug ipv6 mld packet

no debug ipv6 mld packet

Function: Enable the debug switch that displays MLD packets.The **"no debug ipv6 mld events**" command disables the debug switch.

Parameter: None

Default: Disabled

Command Mode: Admin Mode

Usage Guide: This switch can be enabled to get MLD packets information.

Example:

Switch# deb ipv6 mld packet

Switch#1970/01/01 07:33:12 IMI: Recv MLD packet

1970/01/01 07:33:12 IMI: Type: Listener Report (131)

1970/01/01 07:33:12 IMI: Code: 0

1970/01/01 07:33:12 IMI: Checksum: 3b7a

1970/01/01 07:33:12 IMI: Max Resp Delay: 0

1970/01/01 07:33:12 IMI: Reserved: 0

1970/01/01 07:33:12 IMI: Multicast Address: ff1e::1:3

1970/01/01 07:33:12 IMI: MLD Report recv: src fe80::203:fff:fe12:3457 for ff1e::1:3

1970/01/01 07:33:12 IMI: Processing Report comes from Vlan1, ifindex 2003

1970/01/01 07:33:12 IMI: MLD(Querier) ff1e::1:3 (Vlan1): Listeners Present --> Listeners Present

21.3.5.1.3 show ipv6 mld groups

Command: show ipv6 mld groups [{<*ifname* | *group_addr*>}]

Function: Display the MLD group information

Parameter: ***<ifname>*** is the name of the interface . Display the MLD group information. ***<group_addr>*** is the group address. Display the specified group information.

Default: Do not display

Command Mode: Admin Mode

Example:

Switch#sh ipv6 mld group

MLD Connected Group Membership

Group Address	Interface	Uptime	Expires
ff1e::1:3	Vlan1	00:00:16	00:03:14

Switch#

Displayed Information	Explanations
Group Address	Multicast group IP address
Interface	The interface of multicast group
Uptime	The existing time of the multicast group
Expires	The left time to overtime

21.3.5.1.4 show ipv6 mld interface

Command: show ipv6 mld interface [<***ifname***>]

Function: Display the relevant MLD information of an interface

Parameter: ***<ifname>*** is the name of the interface . Display the MLD information of a specific interface.

Default: Do not display

Command Mode: Admin Mode

Example: Display the MLD information of the Ethernet Interface vlan1

```
Switch#show ipv6 mld interface Vlan1
Interface Vlan1(2003)
 Index 2003
 Internet address is fe80::203:fff:fe01:e4a
 MLD querier
 MLD query interval is 100 seconds
 MLD querier timeout is 205 seconds
 MLD max query response time is 10 seconds
 Last member query response interval is 1000 ms
 Group membership interval is 210 seconds
 MLD is enabled on interface
```

21.4 MLD Snooping

21.4.1 MLD Snooping Introduction

MLD, the Multicast Listener Discovery Protocol, is used to realize multicasting in the IPv6. MLD is used by the network equipments such as routers which supports multicast for multicast listener discovery, also used by listeners looking forward to join certain multicast group informing the router to receive data packets from certain multicast address, all of which are done through MLD message exchange. First the router send an MLD Multicast listener Query message through a multicast address which can address all the listeners (namely ff02::1). Once there is a listener who wishes to join the multicast address, it will send a MLD Multicast listener Report back through the multicast address.

MLD Snooping is namely the MLD listening. The switch restricts the multicast traffic from flooding through MLD Snooping, and forward the multicast traffic to ports associated to multicast devices only. The switch listens to the MLD messages between multicast routers and listeners, and maintains the multicast group forwarding list based on the listening result. The switches forwards multicast packets according to the multicast forwarding list

The switch realizes the MLD Snooping function while supporting MLD v2. This way,

the user can acquire IPv6 multicast with the switch.

21.4.2 MLD Snooping Configuration Task

1. Enable the MLD Snooping function
2. Configure the MLD Snooping

1. Enable the **MLD Snooping** function

Command	Explanation
Global Mode	
ipv6 mld snooping **no ipv6 mld snooping**	Enable global MLD Snooping, the "**no ipv6 mld snooping**" command disables the global MLD snooping

2. Configure MLD Snooping

Command	Explanation
Global Mode	
ipv6 mld snooping vlan <*vlan-id*> **no ipv6 mld snooping vlan <*vlan-id*>**	Enable MLD Snooping on specific vlan. The "no" form of this command disables MLD Snooping on specific vlan
ipv6 mld snooping vlan < *vlan-id* > limit {group <*g_limit*> | source <*s_limit*>} **no ipv6 mld snooping vlan < *vlan-id* > limit**	Configure the number of the groups in which the MLD Snooping can join, and the maximum number of sources in each group. The "no" form of this command restores to the default
ipv6 mld snooping vlan <*vlan-id*> l2-general-querier **no ipv6 mld snooping vlan <*vlan-id*> l2-general-querier**	Set the vlan level 2 general querier,which is recommended on each segment. The "no" form of this command cancels the level 2 general querier configuration.
ipv6 mld snooping vlan <*vlan-id*> mrouter-port interface <*interface –name*> **no ipv6 mld snooping vlan <*vlan-id*> mrouter-port interface <*interface –name*>**	Configure the static mrouter port in specific vlan. The "no" form of this command cancels the mrouter port configuration.
ipv6 mld snooping vlan <*vlan-id*> mrpt < *value* > **no ipv6 mld snooping vlan**	Configure the keep-alive time of the mrouter port. The "no" form of this command restores to the default.

<*vlan-id*> mrpt	
ipv6 mld snooping vlan <*vlan-id*> query-interval <*value*> **no ipv6 mld snooping vlan <*vlan-id*> query-interval**	Configure the query interval. The “no” form of this command restores to the default.
ipv6 mld snooping vlan <*vlan-id*> immediate-leave **no ipv6 mld snooping vlan <*vlan-id*> immediate-leave**	Configure immediate leave multicast group function for the MLD Snooping of specify vlan. The “no” form of this command cancels the immediate leave configuration.
ipv6 mld snooping vlan <*vlan-id*> query-mrsp <*value*> **no ipv6 mld snooping vlan <*vlan-id*> query-mrsp**	Configure the query maximum response period. The “no” form of this command restores to the default.
ipv6 mld snooping vlan <vlan-id> query-robustness <*value*> **no ipv6 mld snooping vlan <vlan-id> query-robustness**	Configure the query robustness, the “no” form of this command restores to the default.
ipv6 mld snooping vlan <*vlan-id*> suppression-query-time <*value*> **no ipv6 mld snooping vlan <*vlan-id*> suppression-query-time**	Configure the suppression query time. The “no” form of this command restores to the default

21.4.3 Commands For MLD Snooping Configuration

21.4.3.1 debug mld snooping all/packet/event/timer/mfc

Command: debug mld snooping all/packet/event/timer/mfc

no debug mld snooping all/packet/event/timer/mfc

Function: Enable the debugging of the switch MLD Snooping; the “no” form of this command disables the debugging.

Command Mode: Admin Mode

Default: The MLD Snooping Debugging of the switch is disabled by default

Usage Guide: This command is used for enabling the switch MLD Snooping debugging, which displays the MLD data packet message processed by the switch——packet, event messages——event,timer messages——timer,messages of down streamed hardware entry——mfc,all debug messages——all.

21.4.3.2 ipv6 mld snooping

Command: ipv6 mld snooping

no ipv6 mld snooping

Function: Enable the MLD Snooping function on the switch; the "**no ipv6 mld snooping**" command disables MLD Snooping

Command Mode: Global Mode

Default:MLD Snooping disabled on the switch by default

Usage Guide: Enable global MLD Snooping on the switch, namely allow every vlan to be configured with MLD Snooping; the "no" form of this command will disable MLD Snooping on all the vlans as well as the global MLD snooping

Example: Enable MLD Snooping under global mode.

Switch (Config)#ipv6 mld snooping

21.4.3.3 ipv6 mld snooping vlan

Command: ipv6 mld snooping vlan <*vlan-id*>

no ipv6 mld snooping vlan <*vlan-id*>

Function: Enable MLD Snooping on specified vlan; the "no" form of this command disables MLD Snooping on specified vlan.

Parameter: <*vlan-id*> is the id number of the vlan,with a valid range of <1-4094>.

Command Mode: Global Mode

Default: MLD Snooping disabled on vlan by default

Usage Guide: To configure MLD snooping on certain vlan, the global MLD snooping should be first enabled. Disable MLD snooping on specified vlan with the no ipv6 mld snooping vlan vid" command

Example: Enable MLD snooping on vlan 100 under global mode.

Switch (Config)#ipv6 mld snooping vlan 100

21.4.3.4 ipv6 mld snooping vlan immediate-leave

Command: ipv6 mld snooping vlan <*vlan-id*> immediate-leave

no ipv6 mld snooping vlan <*vlan-id*> immediate-leave

Function: Enable immediate-leave function of the MLD protocol in specified vlan; the "no" form of this command disables the immediate-leave function of the MLD protocol

Parameter: <*vlan-id*> is the id number of specified VLAN,with valid range of <1-4094>.

Command Mode: Global Mode

Default: Disabled by default

Usage Guide: Enabling the immediate-leave function of the MLD protocol will hasten the process the port leaves one multicast group, in which the specified group query of the

group will not be sent and the port will be directly deleted.

Example: Enable the MLD immediate-leave function on vlan 100

Switch (Config)#ipv6 mld snooping vlan 100 immediate-leave

21.4.3.5 ipv6 mld snooping vlan l2-general-querier

Command: ipv6 mld snooping vlan < *vlan-id* > l2-general-querier

no ipv6 mld snooping vlan < *vlan-id* > l2-general-querier

Function: Set the vlan to Level 2 general querier

Parameter: *vlan-id*: is the id number of the VLAN, with a valid range of <1-4094>

Command Mode: Global Mode

Default: vlan is not a MLD Snooping L2 general querier by default.

Usage Guide: It is recommended to configure an L2 general querier on a segment. If before configure with this command, MLD snooping is not enabled on this vlan, this command will no be executed. When disabling the L2 general querier function, MLD snooping will not be disabled along with it. Main function of this command is sending general queries periodically to help the switches within this segment learn mrouter port.

Comment: There are three ways to learn mrouter port in mld snooping:

1. The port which receives MLD query messages
2. The port which receives multicast protocol packets and support PIM
3. The port statically configured.

Example: Set vlan 100 to L2 general querier.

Switch (Config)# ipv6 mld snooping vlan 100 l2-general-querier

21.4.3.6 ipv6 mld snooping vlan limit

Command: ipv6 mld snooping vlan < *vlan-id* > limit {group <*g_limit*> | source <*s_limit*>}

no ipv6 mld snooping vlan < *vlan-id* > limit

Function: Configure number of groups the MLD snooping can join and the maximum number of sources in each group.

Parameter: *vlan-id*: vlan id, the valid range is <1-4094>

***g_limit*:** <1-65535>,max number of groups joined

***s_limit*:** <1-65535>,max number of source entries in each group, consisting of include source and exclude source

Command Mode: Global Mode

Default: Maximum 50 groups by default, with each group capable with 40 source entries.

Usage Guide: When number of joined group reaches the limit, new group requesting for joining in will be rejected for preventing hostile attacks. To use this command, MLD snooping must be enabled on vlan. The “no” form of this command restores the default

other than set to “no limit”. For the safety considerations, this command will not be configured to “no limit”. It is recommended to use default value and if layer 3 MLD is in operation, please make this configuration in accordance with the MLD configuration as possible.

Example: Switch(config)#ipv6 mld snooping vlan 2 limit group 300

21.4.3.7 ipv6 mld snooping vlan mrouter-port interface

Command: ipv6 mld snooping vlan <*vlan-id*> mrouter-port interface (<*ethernet*>|<*port-channel*>)<*ifname*>

no ipv6 mld snooping vlan <*vlan-id*> mrouter-port interface (<*ethernet*>|<*port-channel*>)<*ifname*>

Function: Set the static mrouter port of the vlan; the “no” form of this command cancels the configuration.

Parameter: *vlan-id*: vlan id, the valid range is<1-4094>

ethernet：name of Ethernet port

ifname：Name of interface

***port-channel*: port aggregate**

Command Mode: Global Mode

Default: When a port is made static and dynamic mrouter port at the same time, it’s the static mrouter properties is preferred. Deleting the static mrouter port can only be done with the “no” form of this command.

Example: Switch(config)#ipv6 mld snooping vlan 2 mrouter-port interface ethernet1/13

21.4.3.8 ipv6 mld snooping vlan mrpt

Command: ipv6 mld snooping vlan <*vlan-id*> mart <*value*>

no ipv6 mld snooping vlan <*vlan-id*> mart

Function: Configure the keep-alive time of the mrouter port.

Parameter: *vlan-id*: vlan id, the valid range is <1-4094>

value：mrouter port keep-alive time with a valid range of <1-65535> secs.

Command Mode: Global Mode

Default: 255s

Usage Guide: This configuration is applicable on dynamic mrouter port, but not on static mrouter port. To use this command, MLD snooping must be enabled on the vlan.

Example: Switch(config)#ipv6 mld snooping vlan 2 mrpt 100

21.4.3.9 ipv6 mld snooping vlan query-interval

Command: ipv6 mld snooping vlan <*vlan-id*> query-interval <*value*>

no ipv6 mld snooping vlan <*vlan-id*> query-interval

Function: Configure the query interval

Parameter: ***vlan-id***: vlan id, the valid range is <1-4094>

value：query interval, valid range: <1-65535>secs.

Command Mode: Global Mode

Default: 125s

Usage Guide: It is recommended to use default value and if layer 3 MLD is in operation, please make this configuration in accordance with the MLD configuration as possible.

Example: Switch(config)#ipv6 mld snooping vlan 2 query-interval 130

21.4.3.10 ipv6 mld snooping vlan query-mrsp

Command: ipv6 mld snooping vlan <*vlan-id*> query-mrsp <*value*>

no ipv6 mld snooping vlan <*vlan-id*> query-mrsp

Function: Configure the maximum query response period. The “no” form of this command restores the default value.

Parameter: ***vlan-id***: vlan id, the valid range is<1-4094>

value：query interval, the valid range is <1-25> secs .

Command Mode: Global Mode

Default: 10s

Usage Guide: It is recommended to use default value and if layer 3 MLD is in operation, please make this configuration in accordance with the MLD configuration as possible.

Example: Switch(config)#ipv6 mld snooping vlan 2 query-mrsp 18

21.4.3.11 ipv6 mld snooping vlan query-robustness

Command: ipv6 mld snooping vlan <vlan-id> query-robustness <*value*>

no ipv6 mld snooping vlan <vlan-id> query-robustness

Function: Configure the query robustness; the “no” form of this command restores to the default value

Parameter: ***vlan-id***: vlan id, the valid range is <1-4094>

value：query interval, the valid range is <2-10>secs.

Command Mode: Global Mode

Default: 2

Usage Guide: It is recommended to use default value and if layer 3 MLD is in operation, please make this configuration in accordance with the MLD configuration as possible.

Example: Switch(config)#ipv6 mld snooping vlan 2 query- robustness 3

21.4.3.12 ipv6 mld snooping vlan suppression-query-time

Command: ipv6 mld snooping vlan <*vlan-id*> suppression-query-time <*value*>

no ipv6 mld snooping vlan <*vlan-id*> suppression-query-time

Function: Configure the suppression query time; the “no” form of this command restores the default value.

Parameter: ***vlan-id***: vlan id, valid range: <1-4094>

value：query interval, valid range: <1-65535>secs.

Command Mode: Global Mode

Default: 255s

Usage Guide: This command can only be configured on L2 general querier. The Suppression-query-time represents the period the suppression state maintains when general querier receives queries from layer 3 MLD within the segment. To use this command, the query-intervals in different switches within the same segment must be in accordance. It is recommended to use the default value.

Example: Switch(config)#ipv6 mld snooping vlan 2 suppression-query-time 270

21.4.3.13 show ipv6 mld snooping

Command: show ipv6 mld snooping [vlan <*vlan-id*>]

Parameter: <*vlan-id*> is the number of vlan specified to display the MLD Snooping messages

Command Mode: Admin Mode

Usage Guide: If no vlan number is specified, it will show whether the global MLD snooping is enabled and layer 3 multicast protocol is running, as well as on which vlan the mld snooping is enabled and configured l2-general-querier. If a vlan number is specified, the detailed MLD Snooping messages of this vlan will be displayed.

Example:

Summary of the switch MLD snooping

Switch(config)#show ipv6 mld snooping

Global mld snooping status: Enabled

L3 multicasting: running

Mld snooping is turned on for vlan 1(querier)

Mld snooping is turned on for vlan 2

Displayed Information	Explanation
Global mld snooping status	Whether or not the global mld snooping is enabled on the switch
L3 multicasting	Whether or not the layer 3 multicast protocol is running on the switch.
Mld snooping is turned on for vlan 1(querier)	On which vlan of the switch is enabled mld snooping, if the vlan are l2-general-querier.

2. Display the detailed MLD Snooping information of vlan1

Switch#show ipv6 mld snooping vlan 1

Mld snooping information for vlan 1

Mld snooping L2 general querier :Yes(COULD_QUERY)
Mld snooping query-interval :125(s)
Mld snooping max response time :10(s)
Mld snooping robustness :2
Mld snooping mrouter port keep-alive time :255(s)
Mld snooping query-suppression time :255(s)

MLD Snooping Connect Group Membership

Note:*-All Source, (S)- Include Source, [S]-Exclude Source

Groups	Sources	Ports	Exptime	System Level
238.1.1.1	(192.168.0.1)	Ethernet1/8	00:04:14	V2
	(192.168.0.2)	Ethernet1/8	00:04:14	V2

Mld snooping vlan 1 mrouter port

Note:"!"-static mrouter port

!Ethernet1/2

Displayed information	Explanation
Mld snooping L2 general querier	whether or not l2-general-querier is enabled on vlan, the querier display status is set to could-query or suppressed
Mld snooping query-interval	Query interval time of the vlan
Mld snooping max response time	Max response time of this vlan
Mld snooping robustness	Robustness configured on the vlan
Mld snooping mrouter port keep-alive time	Keep-alive time of the dynamic mrouter on this vlan
Mld snooping query-suppression time	timeout of the vlan as l2-general-querier at suppressed status.
MLD Snooping Connect Group Membership	Group membership of the vlan, namely the correspondence between the port and （S,G）.
Mld snooping vlan 1 mrouter port	Mrouter port of the vlan, including both static and dynamic.

21.4.3.14 show mac-address-table multicast

Command: show mac-address-table multicast [vlan <*vlan-id*>]

Function: Display the information of multicast MAC address table

Parameter: <*vlan-id*> ,the VLAN ID included in the entries to be displayed.

Command Mode: Admin Mode

Default: Mapping between the multicast MAC address and port is not displayed by system default.

Usage Guide: This command shows the information on multicast address table of current switch.

Example: Show the multicast mapping in vlan 100

Switch#show mac-address-table multicast vlan 100

Vlan	Mac Address	Type	Ports
100	01-00-5e-01-01-01	MULTI	Ethernet1/2

21.4.4 MLD Snooping Examples

Scenario 1: MLD Snooping Function

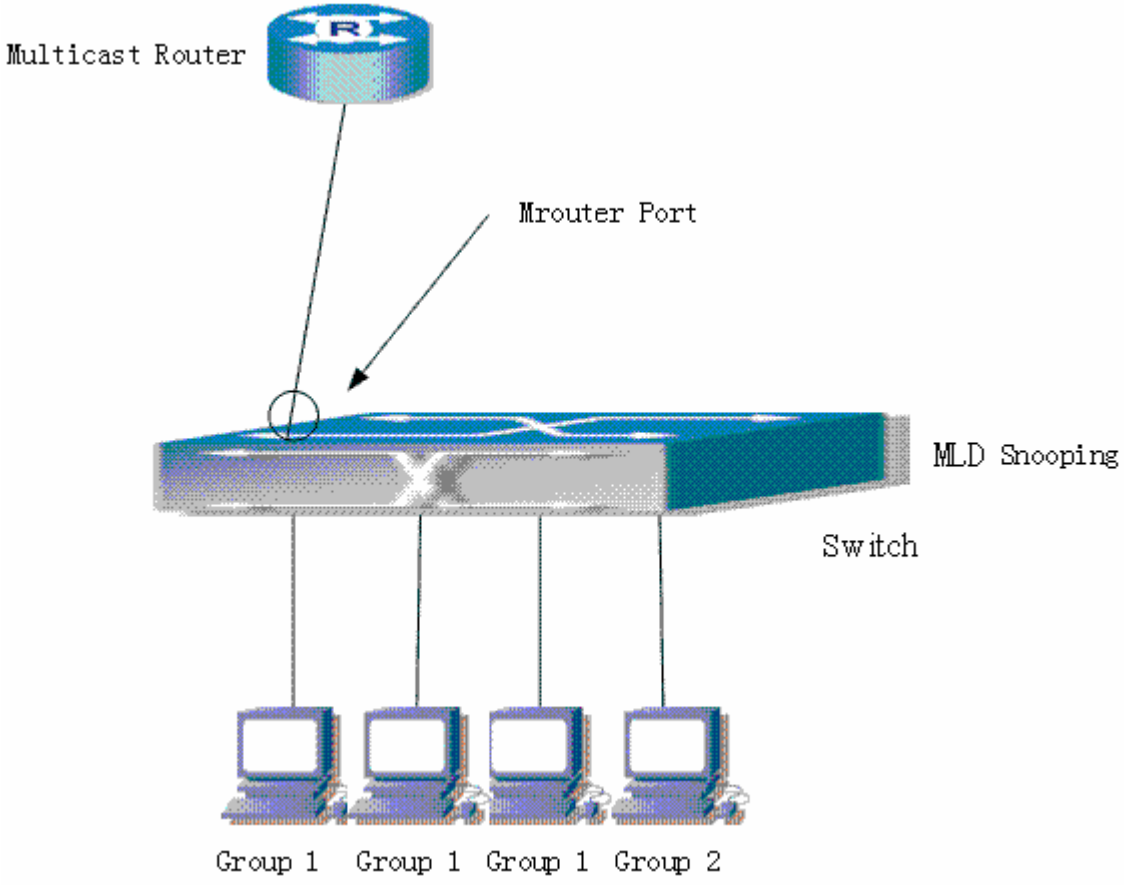


Fig 21-4 Open the switch MLD Snooping Function figure

As shown above, the vlan 100 configured on the switch consists of ports 1, 2, 6, 10, 12. Four hosts are respectively connected to 2, 6, 10, 12 while the multicast router on port 1. Suppose we need mld snooping on vlan 100, however by default, the global mld snooping as well as the mld snooping on each vlan are, therefore first we have to enable the global mld snooping at the same time enable the mld snooping on vlan 100, furthermore we need to set the port 1 of vlan 100 as a mrouter port.

Configuration procedure is as follows.

Switch#config

Switch (config)#ipv6 mld snooping

Switch (config)#ipv6 mld snooping vlan 100

Switch (config)#ipv6 mld snooping vlan 100 mrouter-port interface ethernet 1/1

Multicast configuration

Assume there are two multicast servers: the Multicast Server 1 and the Multicast Server 2, amongst program 1 and 2 are supplied on the Multicast Server 1 while program 3 on the Multicast server 2, using group addresses respectively the Group 1, Group 2 and Group 3. Concurrently multicast application is operating on the four hosts. Two hosts connected to port 2 and 5 are playing program 1 while the host connected to port 10 playing program 2, and the one to port 12 playing program 3.

MLD Snooping interception results:

The multicast table on vlan 100 shows: port1, 2 and 6 are in （Multicasting Server 1, Group1）, port1, 10 are in (Multicasting Server 1,Group2), and port1, 12 are in (Multicasting Server 2, Group3）

All the four hosts successfully receive programs they are interested in. port2, 6 receives no traffic from program2 and 3; port10 receives no traffic from program 1 and 3, and port12 receives no traffic from program1 and 2.

MLD L2-general-querier

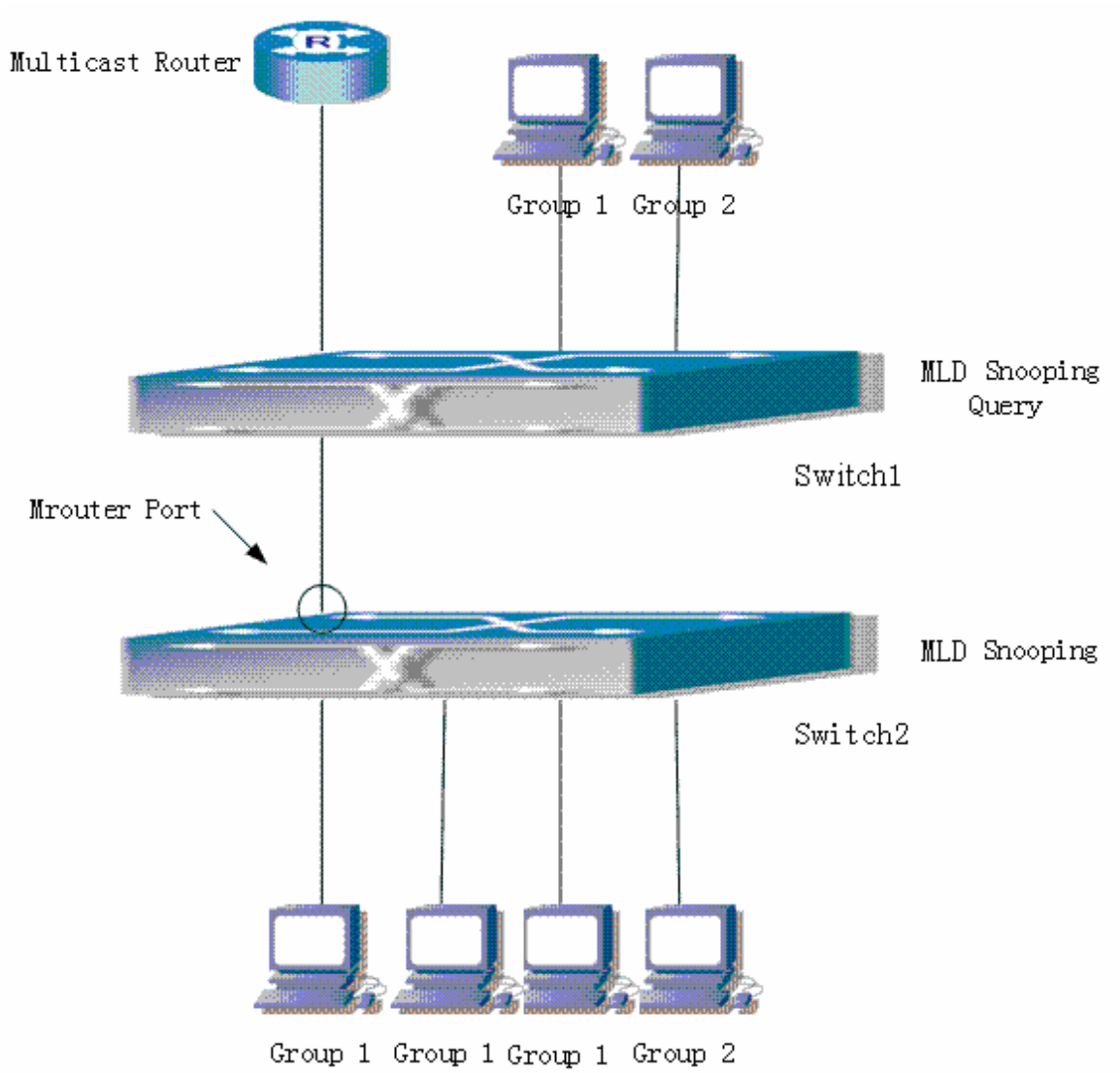


Fig 21-5 Switches as MLD Querier Function figure

Configuration of switch B is the same as the switches in case 1, and here the switch 1 replaces the Multicast Router in case 1. Assume the vlan 60 configured on it contains port 1, 2, 10, 12, amongst port 1 is connected to multicast server, port 2 to switch2. To send Query periodically, global mld snooping has to be enabled while executing the mld snooping vlan 60 l2-general-querier, setting the vlan 60 to a Level 2 General Querier.

Configuration procedure is as follows:

SwitchA#config

SwitchA(config)#ipv6 mld snooping

SwitchA(config)#ipv6 mld snooping vlan 60 l2-general-querier

SwitchB#config

SwitchB(config)#ipv6 mld snooping

SwitchB(config)#ipv6 mld snooping vlan 100

SwitchB(config)#ipv6 mld snooping vlan 100 mrouter interface ethernet 1/1

Multicast configuration

Same as scenario 1

MLD Snooping interception results:

Same as scenario 1

21.4.5 MLD Snooping Troubleshooting

In configuring and using MLD Snooping, the MLD Snooping server may fail to run properly due to physical connection failure, wrong configuration, etc. The user should ensure the following:

(1) Ensure the physical connection is correct

(2) Ensure the MLD Snooping is enabled under global mode (using ipv6 mld snooping)

(3) Ensure the MLD Snooping is configured on the vlan under global mode (using ipv6 mld snooping vlan <vlan-id>）

(4) Ensure there is a vlan configured as a L2 general querier, or there is a static mrouter configured in a segment,

(5) Use command to check if the MLD snooping information is correct.

(6) If the MLD Snooping problem remain unsolved, please use debug mld snooping and other debugging command and copy the DEBUG message within 3 minutes, send the recorded message to the technical server center of our company.

Chapter 22 ACL Configuration

22.1 Introduction to ACL

ACL (Access Control List) is an IP packet filtering mechanism employed in switches, providing network traffic control by granting or denying access through the switches, effectively safeguarding the security of networks. The user can lay down a set of rules according to some information specific to packets, each rule describes the action for a packet with certain information matched: “permit” or “deny”. The user can apply such rules to the incoming or outgoing direction of switch ports, so that data streams in the specific direction of specified ports must comply with the ACL rules assigned.

22.1.1 Access-list

Access-list is a sequential collection of conditions that corresponds to a specific rule. Each rule consist of filter information and the action when the rule is matched. Information included in a rule is the effective combination of conditions such as source IP, destination IP, IP protocol number and TCP port. Access-lists can be categorized by the following criteria:

- Filter information based criterion: IP access-list (layer 3 or higher information), MAC access-list (layer 2 information), and MAC-IP access-list (layer 2 or layer 3 or higher). The current implementation supports IP access-list only, the other two functions will be provided later.
- Configuration complexity based criterion: standard and extended, the extended mode allows more specific filtering of information.
- Nomenclature based criterion: numbered and named.

Description of an ACL should cover the above three aspects.

22.1.2 Access-group

When a set of access-lists are created, they can be applied to traffic of any direction on all ports. Access-group is the description to the binding of an access-list to the specified direction on a specific port. When an access-group is created, all packets from in the specified direction through the port will be compared to the access-list rule to decide whether to permit or deny access.

The current firmware only supports ingress ACL configuration.

22.1.3 Access-list Action and Global Default Action

There are two access-list actions and default actions: “permit” or “deny”

The following rules apply:

- An access-list can consist of several rules. Filtering of packets compares packet conditions to the rules, from the first rule to the first matched rule; the rest of the rules will not be processed.
- Global default action applies only to IP packets in the incoming direction on the ports. For non- incoming IP packets and all outgoing packets, the default forward action is “permit”.
- Global default action applies only when packet flirter is enabled on a port and no ACL is bound to that port, or no binding ACL matches.
- When an access-list is bound to the outgoing direction of a port, the action in the rule can only be “deny”.

22.2 ACL Configuration

22.2.1 ACL Configuration Task Sequence

1. Configuring access-list
   - （1） Configuring a numbered standard IP access-list
   - （2） Configuring a numbered extended IP access-list
   - （3） Configuring a standard IP access-list based on nomenclature
     a) Create a standard IP access-list based on nomenclature
     b) Specify multiple “permit” or “deny” rule entries.
     c) Exit ACL Configuration Mode
   - （4） Configuring an extended IP access-list based on nomenclature.
     a) Create an extensive IP access-list based on nomenclature
     b) Specify multiple “permit” or “deny” rule entries.
     c) Exit ACL Configuration Mode
2. Configuring the packet filtering function
   (1) Enable global packet filtering function
   (2) Configure default action.
3. Configuring time range function

(1) Create the name of the time range

(2) Configure periodic time range

(3) Configure absolute time range

4. Bind access-list to a specific direction of the specified port.
5. Clear the filter information of the specified port

1. Configuring access-list

(1) Configuring a numbered standard IP access-list

Command	**Explanation**
Global Mode	
access-list <*num*> {deny | permit} {{<*sIpAddr*> <*sMask*>} | any | {host <*sIpAddr*>}} **no access-list <*num*>**	Creates a numbered standard IP access-list, if the access-list already exists, then a rule will add to the current access-list; the "**no access-list <*num*>**" command deletes a numbered standard IP access-list.

(2) Configuring a numbered extensive IP access-list

Command	**Explanation**
Global Mode	
access-list <*num*> {deny | permit} icmp {{<*sIpAddr*> <*sMask*>} | any | {host <*sIpAddr*>}} {{<*dIpAddr*> <*dMask*>} | any-destination | {host-destination <*dIpAddr*>}} [<*icmp-type*> [<*icmp-code*>]] [precedence <*prec*>] [tos <*tos*>]	Creates a numbered ICMP extended IP access rule; if the numbered extended access-list of specified number does not exist, then an access-list will be created using this number.
access-list <*num*> {deny | permit} igmp {{<*sIpAddr*> <*sMask*>} | any | {host <*sIpAddr*>}} {{<*dIpAddr*> <*dMask*>} | any-destination | {host-destination <*dIpAddr*>}} [<*igmp-type*>] [precedence <*prec*>] [tos <*tos*>]	Creates a numbered IGMP extended IP access rule; if the numbered extended access-list of specified number does not exist, then an access-list will be created using this number.

access-list <*num*> {deny | permit} tcp {{<*slpAddr*> <*sMask*>} | any | {host <*slpAddr*>}} [s-port <*sPort*>] {{<*dlpAddr*> <*dMask*>} | any-destination | {host-destination <*dlpAddr*>}} [d-port <*dPort*>] [ack | fin | psh | rst | syn | urg] [precedence <*prec*>] [tos <*tos*>]	Creates a numbered TCP extended IP access rule; if the numbered extended access-list of specified number does not exist, then an access-list will be created using this number.
access-list <*num*> {deny | permit} udp {{<*slpAddr*> <*sMask*>} | any | {host <*slpAddr*>}} [s-port <*sPort*>] {{<*dlpAddr*> <*dMask*>} | any-destination | {host-destination <*dlpAddr*>}} [d-port <*dPort*>] [precedence <*prec*>] [tos <*tos*>]	Creates a numbered UDP extended IP access rule; if the numbered extended access-list of specified number does not exist, then an access-list will be created using this number.
access-list <*num*> {deny | permit} {eigrp | gre | igrp | ipinip | ip | <*int*>} {{<*slpAddr*> <*sMask*>} | any | {host <*slpAddr*>}} {{<*dlpAddr*> <*dMask*>} | any-destination | {host-destination <*dlpAddr*>}} [precedence <*prec*>] [tos <*tos*>]	Creates a numbered IP extended IP access rule for other specific IP protocol or all IP protocols; if the numbered extended access-list of specified number does not exist, then an access-list will be created using this number.
no access-list <*num*>	Deletes a numbered extensive IP access-list

3) Configuring a standard IP access-list basing on nomenclature

a. Create a name-based standard IP access-list

Command	**Explanation**
Global Mode	
access-list ip {standard | extended} <name> **no access-list ip {standard | extended} <name>**	Creates a standard IP access-list based on nomenclature; the "**no access-list ip {standard | extended} <name>** " command delete the name-based standard IP access-list

b. Specify multiple "permit" or "deny" rules

Command	**Explanation**

Standard IP ACL Mode	
[no] {deny | permit} {{<*sIpAddr*> <*sMask* >} | any | {host <*sIpAddr*>}}	Creates a standard name-based IP access rule; the "**no**" form command deletes the name-based standard IP access rule

c. Exit name-based standard IP ACL configuration mode

Command	**Explanation**
Standard IP ACL Mode	
Exit	Exits name-based standard IP ACL configuration mode

4) Configuring an name-based extended IP access-list

a. Create an extended IP access-list basing on nomenclature

Command	**Explanation**
Global Mode	
access-list ip {standard | extended} <name> **no access-list ip {standard | extended} <name>**	Creates an extended IP access-list basing on nomenclature; the "**no access-list ip {standard | extended} <name>** " command deletes the name-based extended IP access-list

b. Specify multiple "permit" or "deny" rules

Command	**Explanation**
Extended IP ACL Mode	
[no] {deny | permit} icmp {{<*sIpAddr*> <*sMask*>} | any | {host <*sIpAddr*>}} {{<*dIpAddr*> <*dMask*>} | any-destination | {host-destination <*dIpAddr*>}} [<*icmp-type*> [<*icmp-code*>]] [precedence <*prec*>] [tos <*tos*>]	Creates an extended name-based ICMP IP access rule; the "**no**" form command deletes this name-based extended IP access rule
[no] {deny | permit} igmp {{<*sIpAddr*> <*sMask*>} | any | {host <*sIpAddr*>}} {{<*dIpAddr*> <*dMask*>} | any-destination | {host-destination <*dIpAddr*>}} [<*igmp-type*>] [precedence <*prec*>] [tos <*tos*>]	Creates an extended name-based IGMP IP access rule; the "**no**" form command deletes this name-based extended IP access rule

[no] {deny | permit} tcp {{<*sIpAddr*> <*sMask*>} | any| {host <*sIpAddr*>}} [s-port <*sPort*>] {{<*dIpAddr*> <*dMask*>} | any-destination | {host-destination <*dIpAddr*>}} [d-port <*dPort*>] [ack | fin | psh | rst | syn | urg] [precedence <*prec*>] [tos <*tos*>]	Creates an extended name-based TCP IP access rule; the "**no**" form command deletes this name-based extended IP access rule
[no] {deny | permit} udp {{<*sIpAddr*> <*sMask*>} | any | {host <*sIpAddr*>}} [s-port <*sPort*>] {{<*dIpAddr*> <*dMask*>} | any-destination | {host-destination <*dIpAddr*>}} [d-port <*dPort*>] [precedence <*prec*>] [tos <*tos*>]	Creates an extended name-based UDP IP access rule; the "**no**" form command deletes this name-based extended IP access rule
[no] {deny | permit} {eigrp | gre | igrp | ipinip | ip | <*int*>} {{<*sIpAddr*> <*sMask*>} | any | {host <*sIpAddr*>}} {{<*dIpAddr*> <*dMask*>} | any-destination | {host-destination <*dIpAddr*>}} [precedence <*prec*>] [tos <*tos*>]	Creates an extended name-based IP access rule for other IP protocols; the "**no**" form command deletes this name-based extended IP access rule

c. Exit extended IP ACL configuration mode

Command	**Explanation**
Extended IP ACL Mode	
Exit	Exits extended name-based IP ACL configuration mode

2. Configuring packet filtering function

(1) Enable global packet filtering function

Command	**Explanation**
Global Mode	
Firewall enable	Enables global packet filtering function
Firewall disable	disables global packet filtering function

(2) Configure default action.

Command	**Explanation**
Global Mode	

firewall default {permit |deny [ipv4|ipv6|arp|all]}	Sets default action to "permit" or "deny"

3.Configuring time range function

（1）Create the name of the time range

Command	**Explanation**
Global Mode	
time-range <*time_range_name*>	Create a time range named *time_range_name*
no time-range <*time_range_name*>	Stop the time range function named ***time_range_name***

（2）Configure periodic time range

Command	**Explanation**
Time range Mode	
absolute-periodic{Monday|Tuesday|Wednesday|Thursday|Friday|Saturday|Sunday}<*start_time*>to {Monday|Tuesday|Wednesday|Thursday|Friday|Saturday|Sunday} <*end_time*>	Configure the time range for the request of the week,and every week will run by the time range
periodic{{Monday+Tuesday+Wednesday+Thursday+Friday+Saturday+Sunday}| daily| weekdays | weekend} <*start_time*> to <*end_time*>	
[no]absolute-periodic{Monday|Tuesday|Wednesday|Thursday|Friday|Saturday|Sunday}<*start_time*>to{Monday|Tuesday|Wednesday|Thursday|Friday|Saturday| Sunday} <*end_time*>	stop the function of the time range in the week
[no]periodic{{Monday+Tuesday+Wednesday+Thursday+Friday+Saturday+Sunday}|daily|weekdays| weekend} <*start_time*> to <*end_time*>	

（3）Configure absolute time range

Command	**Explanation**
Global Mode	
Absolute start<*start_time*><*start_data*>[end<*end_time*> <*end_data*>]	Configure absolute time range

[no]absolute start<*start_time*><*start_data*>[end<*end_time*><*end_data*>]	stop the function of the time range

4. Bind access-list to a specific direction of the specified port.

Command	**Explanation**
Physical Interface Mode, VLAN interface Mode	
{ip} access-group <*name*> {in} **no {ip} access-group <*name*> {in}**	Applies an access-list to the specified direction on the port; the "**no {ip} access-group <*name*> {in}**" command deletes the access-list bound to the port.

5. Clear the filter information of the specified port

Command	**Explanation**
Admin Mode	
clear access-group statistic [ethernet<*interface-name*>]	Clear the filter information of the specified port

22.2.2 Commands for ACL

22.2.2.1 absolute-periodic/periodic

Command:

[no] absolute-periodic{Monday|Tuesday|Wednesday|Thursday|Friday|Saturday|Sunday}<start_time>to{Monday|Tuesday|Wednesday|Thursday|Friday|Saturday|Sunday} <end_time>

[no]periodic{{Monday+Tuesday+Wednesday+Thursday+Friday+Saturday+Sunday}|daily| weekdays | weekend} <start_time> to <end_time>

Functions: Define the time-range of different commands within one week, and every week to circulate subject to this time.

Parameters:

Friday （Friday)

Monday （Monday)

Saturday （Saturday)

Sunday （Sunday)

Thursday （Thursday）

Tuesday （Tuesday)

Wednesday （Wednesday)

daily （Every day of the week）

weekdays （Monday thru Friday）

weekend （Saturday thru Sunday）

start_time start time ,HH:MM:SS (hour: minute: second)

end_time end time,HH:MM:SS (hour: minute: second)

Remark: time-range polling is one minute per time, so the time error shall be <= one minute.

Command Mode: time-range mode

Default: No time-range configuration

Usage Guide: Periodic time and date. The definition of period is specific time period of Monday to Saturday and Sunday every week.

day1 hh:mm:ss To day2 hh:mm:ss or {[day1+day2+day3+day4+day5+day6+day7]|weekend|weekdays|daily} hh:mm:ss To hh:mm:ss

Examples: Make configurations effective within the period from9:15:30 to 12:30:00 during Tuesday to Saturday.

Switch(Config)#time-range doc_timer

Switch(Config-Time-Range)# absolute-periodic Tuesday 9:15:30 to Saturday 12:30:00

Make configurations effective within the period from 14:30:00 to 16:45:00 on Monday, Wednesday, Friday and Sunday.

Switch (Config-Time-Range) # periodic Monday Wednesday Friday Sunday 14:30:00 to 16:45:00

22.2.2.2 absolute start

Command:[no]absolute start <*start_time*> <*start_data*> [end <*end_time*> <*end_data*>]

Functions: Define an absolute time-range, this time-range operates subject to the clock of this equipment.

Parameters:*start_time* : start time, HH:MM:SS (hour: minute: second)

end_time **:** end time, HH:MM:SS (hour: minute: second)

start_data **:**start data, the format is, YYYY.MM.DD（year.month.day）

end_data **:** end data, the format is, YYYY.MM.DD（year.month.day）

Remark: time-range is one minute per time, so the time error shall be <= one minute.

Command Mode: Time-range mode

Default: No time-range configuration

Usage Guide: Absolute time and date, assign specific year, month, day, hour, minute of the start, shall not configure multiple absolute time and date, when in repeated configuration, the latter configuration covers the absolute time and date of the former configuration.

Examples: Make configurations effective from 6:00:00 to 13:30:00 from Oct. 1, 2004 to Jan. 26, 2005.

Switch(config)#Time-range doc_timer

Switch (Config-Time-Range) # absolute start 6:00:00 2004.10.1 end 13:30:00 2005.1.26

22.2.2.3 access-list(ip extended)

Command: access-list <*num*> {deny | permit} icmp {{<*sIpAddr*> <*sMask*>} | any-source | {host-source <*sIpAddr*>}} {{<*dIpAddr*> <*dMask*>} | any-destination | {host-destination <*dIpAddr*>}} [<*icmp-type*> [<*icmp-code*>]] [precedence <*prec*>] [tos <*tos*>][time-range<*time-range-name*>]

access-list <*num*> {deny | permit} igmp {{<*sIpAddr*> <*sMask*>} | any-source | {host-source <*sIpAddr*>}} {{<*dIpAddr*> <*dMask*>} | any-destination | {host-destination <*dIpAddr*>}} [<*igmp-type*>] [precedence <*prec*>] [tos <*tos*>][time-range<*time-range-name*>]

access-list <*num*> {deny | permit} tcp {{<*sIpAddr*> <*sMask*>} | any-source | {host-source <*sIpAddr*>}} [s-port {<*sPort*> | range <*sPortMin*> <*sPortMax*>}] {{<*dIpAddr*> <*dMask*>} | any-destination | {host-destination <*dIpAddr*>}} [d-port {<*dPort*> | range <*dPortMin*> <*dPortMax*>}] [ack+ fin+ psh+ rst+ urg+ syn] [precedence <*prec*>] [tos <*tos*>][time-range<*time-range-name*>]

access-list <*num*> {deny | permit} udp {{<*sIpAddr*> <*sMask*>} | any-source | {host-source <*sIpAddr*>}} [s-port {<*sPort*> | range <*sPortMin*> <*sPortMax*>] {{<*dIpAddr*> <*dMask*>} | any-destination | {host-destination <*dIpAddr*>}} [d-port {<*dPort*> | range <*dPortMin*> <*dPortMax*>}] [precedence <*prec*>] [tos <*tos*>][time-range<*time-range-name*>]

access-list <*num*> {deny | permit} {eigrp | gre | igrp | ipinip | ip | <*protocol*>} {{<*sIpAddr*> <*sMask*>} | any-source | {host-source <*sIpAddr*>}} {{<*dIpAddr*> <*dMask*>} | any-destination | {host-destination <*dIpAddr*>}} [precedence <*prec*>] [tos <*tos*>][time-range<*time-range-name*>]

no access-list <*num*>

Functions: Create a numeric extended IP access rule to match specific IP protocol or all IP protocol; if access-list of this coded numeric extended does not exist, thus to create such a access-list.

Parameters: <*num*> is the No. of access-list, 100-199; **<*protocol*> is the No. of**

upper-layer protocol of ip, 0-255; <*slpAddr*> is the source IP address, the format is dotted decimal notation; **<*sMask* >** is the reverse mask of source IP, the format is dotted decimal notation; **<*dIpAddr*>** is the destination IP address, the format is dotted decimal notation; **<*dMask*>** is the reverse mask of destination IP, the format is dotted decimal notation, attentive position o, ignored position1;**<*igmp-type*>**,the type of igmp, 0-15; **<*icmp-type*>**, the type of icmp, 0-255;**<icmp-code>,** protocol No. of icmp, 0-255;**<prec>**, IP priority, 0-7; **<*tos*>**, to value, 0-15; **<*sPort*>**, source port No., 0-65535; **<*sPortMin*>**, the down boundary of source port;； **<*sPortMax*>**, the up boundary of source port; **<*dPortMin*>**, the down boundary of destination port;**<*dPortMax*>**, the up boundary of destination port; **<*dPort*>**, destination port No., 0-65535; **<*time-range-name*>**, the name of time-range.

Command Mode: Global mode

Default: No access-lists configured.

Usage Guide: When the user assign specific **<*num*>** for the first time, ACL of the serial number is created, then the lists are added into this ACL.

<*igmp-type*> represent the type of IGMP packet, and usual values please refer to the following description:

17(0x11): IGMP QUERY packet

18(0x12): IGMP V1 REPORT packet

22(0x16): IGMP V2 REPORT packet

23(0x17): IGMP V2 LEAVE packet

34(0x22): IGMP V3 REPORT packet

19(0x13): DVMR packet

20(0x14): PIM V1 packet

Particular notice: the packet types included here are not the types excluding IP OPTION. Normally, IGMP packet contains OPTION fields, and such configuration is of no use for this type of packet. If you want to configure the packets containing OPTION, please directly use the manner where OFFSET is configured.

Examples: Create the numeric extended access-list whose serial No. is 110. deny icmp packet to pass, and permit udp packet with destination address 192. 168. 0. 1 and destination port 32 to pass.

Switch(Config)#access-list 110 deny icmp any any-destination

Switch(Config)#access-list 110 permit udp any host-destination 192.168.0.1 d-port 32

22.2.2.4 access-list(ip standard)

Command: access-list <*num*> {deny | permit} {{<*slpAddr*> <*sMask* >} | any | {host <*slpAddr*>}}

no access-list <*num*>

Functions: Create a numeric standard IP access-list. If this access-list exists, then add a rule list; the "**no access-list <*num*>**" operation of this command is to delete a numeric standard IP access-list.

Parameters: <*num*> is the No. of access-list, 100-199; **<*sIpAddr*>** is the source IP address, the format is dotted decimal notation; **<*sMask* >** is the reverse mask of source IP, the format is dotted decimal notation;

Command Mode: Global mode

Default: No access-lists configured.

Usage Guide: When the user assign specific **<*num*>** for the first time, ACL of the serial number is created, then the lists are added into this ACL.

Examples: Create a numeric standard IP access-list whose serial No. is 20, and permit date packets with source address of 10.1.1.0/24 to pass, and deny other packets with source address of 10.1.1.0/16.

Switch(Config)#access-list 20 permit 10.1.1.0 0.0.0.255

Switch(Config)#access-list 20 deny 10.1.1.0 0.0.255.255

22.2.2.5 clear access-group statistic

Command: clear access-group statistic [ethernet<*interface-name*>]

Functions: Empty packet statistics information of assigned interfaces

Parameters:<*interface-name*>: Interface name

Command Mode: Admin mode

Default: None

Examples: Empty packet statistics information of interface E1/1

Switch#clear access-group statistic

22.2.2.6 firewall

Command: firewall { enable | disable}

Functions: Enable or disable firewall

Parameters: enable means to enable of firewall; **disable** means to disable firewall.

Default: It is no use if default is firewall

Command Mode: Global mode

Usage Guide: Whether enabling or disabling firewall, access rules can be configured. But only when the firewall is enabled, the rules can be used in specific orientations of specific ports. When disabling the firewall, all ACL tied to ports will be deleted.

Examples: Enable firewall

Switch(Config)#firewall enable

22.2.2.7 firewall default

Command: firewall default {permit | deny [ipv4|ipv6|arp|all]}

Functions: Configure default actions of firewall

Parameters: permit means to permit data packets to pass; **deny** means to deny ipv4|ipv6|arp|all data packets to pass

Command Mode: Global mode

Default: Default action is permit.

Usage Guide: This command only influences IP packets from the port entrance, and all packets can pass the switch in other situations.

Examples: Configure firewall default action as permitting packets to pass.

Switch(Config)#firewall default permit

22.2.2.8 access-list ip

Command: access-list ip {standard | extended} <name>

no access-list ip {standard | extended} <name>

Functions: Create a name standard or extended IP access-list; **no access-list ip {standard | extended}<*name*>** action of this command deletes this name standard or extended IP access-list (including all list items);

Parameters: standard means standard IP access-list ; **extended** means extended IP access-list; **<*name*>** name the access-list, the length of character string is 1-16, no pure number sequences permitted.

Command Mode: Global mode

Default: No access-list configured

Usage Guide: After assigning this commands for the first time, only am empty name access-list is created, and no items in the list.

Examples: Create a name extended IP access-list whose name is tcpFlow.

Switch(Config)# access-list ip extended tcpFlow

22.2.2.9 {ip} access-group

Command :{ip } access-group <*name*> {in}[traffic-statistic]

no {ip} access-group <*name*> {in}

Function: Apply a access-list on some direction of port, and determine if ACL rule is added statistic counter or not by options; the “no {ip} access-group <*name*> {in} “command deletes access-list binding on the port.

Parameter: <*name*> is the name for access list, the character string length is from 1 to 16

Command Mode: Physical Interface Mode,Interface Mode

Default: The entry of port is not bound ACL.

Usage Guide: One port can bind an entry rule.

The **standard, extended and nomenclature** of access-list can be bound to **physical port** of layer 3 switch, not binding ACL to layer interface or influx interface.

There are four kinds of package head field based on concerned: MAC ACL, IP CAL, MAC-IP ACL, and IPv6 ACL; to some extent, ACL filter behavior (permit, deny) has a conflict when a data package matches multi types of eight ACLs. The strict priorities are specified for each ACL based on outcome veracity. It can determine final behavior of package filter through priority when the filter behavior has a conflict.

When binding ACL to port, there are some limits as below:

1. Each port can bind a MAC-IP ACL, a IP ACL, a MAC ACL and a IPv6 ACL;
2. When binding 6 ACLs and data package matching the multi ACLs simultaneity, the priority from high to low are shown as below,
   Ingress IPv6 AC;
   Ingress MAC-IP ACL;
   Ingress MAC ACL;
   Ingress IP ACL;

Example: Binding aaa access-list to entry direction of port
Switch(Config-Ethernet1/1)#ip access-group aaa in

22.2.2.10 permit | deny(ip extended)

Command: [no] {deny | permit} icmp {{<*slpAddr*> <*sMask*>} | any-source | {host-source <*slpAddr*>}} {{<*dlpAddr*> <*dMask*>} | any-destination | {host-destination <*dlpAddr*>}} [<*icmp-type*> [<*icmp-code*>]] [precedence <*prec*>] [tos <*tos*>][time-range<*time-range-name*>]

[no] {deny | permit} igmp {{<*slpAddr*> <*sMask*>} | any-source | {host-source <*slpAddr*>}} {{<*dlpAddr*> <*dMask*>} | any-destination | {host-destination <*dlpAddr*>}} [<*igmp-type*>] [precedence <*prec*>] [tos <*tos*>][time-range<*time-range-name*>]

[no] {deny | permit} tcp {{<*slpAddr*> <*sMask*>} | any-source | {host-source <*slpAddr*>}} [s-port {<*sPort*> | range <*sPortMin*> <*sPortMax*>}] {{<*dlpAddr*> <*dMask*>} | any-destination | {host-destination <*dlpAddr*>}} [d-port {<*dPort*> | range <*dPortMin*> <*dPortMax*>}] [ack+fin+psh+rst+urg+syn] [precedence <*prec*>] [tos <*tos*>][time-range<*time-range-name*>]

[no] {deny | permit} udp {{<*slpAddr*> <*sMask*>} | any-source | {host-source <*slpAddr*>}} [s-port {<*sPort*> | range <*sPortMin*> <*sPortMax*>}] {{<*dlpAddr*> <*dMask*>} | any-destination | {host-destination <*dlpAddr*>}} [d-port {<*dPort*> | range <*dPortMin*> <*dPortMax*>}] [precedence <*prec*>] [tos <*tos*>][time-range<*time-range-name*>]

[no] {deny | permit} {eigrp | gre | igrp | ipinip | ip | <*int*>} {{<*slpAddr*>

<*sMask*>} | any-source | {host-source <*sIpAddr*>}} {{<*dIpAddr*> <*dMask*>} | any-destination | {host-destination <*dIpAddr*>}} [precedence <*prec*>] [tos <*tos*>][time-range<*time-range-name*>]

Functions: Create a name extended IP access rule to match specific IP protocol or all IP protocol;

Parameters: <*sIpAddr*> is the source IP address, the format is dotted decimal notation; **<*sMask* >** is the reverse mask of source IP, the format is dotted decimal notation; **<*dIpAddr*>** is the destination IP address, the format is dotted decimal notation; **<*dMask*>** is the reverse mask of destination IP, the format is dotted decimal notation, attentive position o, ignored position 1; **<*igmp-type*>**, the type of igmp, 0-15; **<*icmp-type*>**, the type of icmp, 0-255 ; **<icmp-code>,** protocol No. of icmp, 0-255; **<prec>**, IP priority, 0-7; **<*tos*>**, to value, 0-15; **<*sPort*>**, source port No., 0-65535; **<*sPortMin*>**, the down boundary of source port; **<*sPortMax*>**, the up boundary of source port; **<*dPort*>**, destination port No. 0-65535; **<*dPortMin*>**, the down boundary of destination port;**<*dPortMax*>**, the up boundary of destination port; **<*time-range-name*>**, time range name.

Command Mode: Name extended IP access-list configuration mode

Default: No access-list configured

Examples: Create the extended access-list, deny icmp packet to pass, and permit udp packet with destination address 192. 168. 0. 1 and destination port 32 to pass.

Switch(Config)# access-list ip extended udpFlow

Switch(Config-Ext-Nacl-udpFlow)# deny igmp any any-destination

Switch(Config-Ext-Nacl-udpFlow)# permit udp any host-destination 192.168.0.1 d-port 32

22.2.2.11 permit | deny(ip standard)

Command:{deny | permit} {{<*sIpAddr*> <*sMask*>} | any | {host <*sIpAddr*>}}

no {deny | permit} {{<*sIpAddr*> <*sMask*>} | any | {host<*sIpAddr*>}}

Functions: Create a name standard IP access rule, and '**no {deny | permit} {{<*sIpAddr*> <*sMask*>} | any | {host <*sIpAddr*>}}**' action of this command deletes this name standard IP access rule.

Parameters: <*sIpAddr*> is the source IP address, the format is dotted decimal notation; **<*sMask* >** is the reverse mask of source IP, the format is dotted decimal notation;

Command Mode: Name standard IP access-list configuration mode

Default: No access-list configured

Usage Guide:

Example: Permit packets with source address 10.1.1.0/24 to pass, and deny other packets with source address 10.1.1.0/16.

Switch(Config)# access-list ip standard ipFlow

Switch(Config-Std-Nacl-ipFlow)# permit 10.1.1.0 0.0.0.255
Switch(Config-Std-Nacl-ipFlow)# deny 10.1.1.0 0.0.255.255

22.2.2.12 time-range

Command:[no] time-range <*time_range_name*>
Functions: Create the name of time-range as time range name, enter the time-range mode at the same time.
Parameters:*time_range_name*,time range name must start with letter, and the length cannot exceed 16-character long.
Command Mode: Global mode
Default: No time-range configuration
Examples: Reate a time-range named dc timer.
Switch(config)#Time-range dc_ti

22.3 ACL Example

Scenario:

The user has the following configuration requirement: port 1/10 of the switch connects to 10.0.0.0/24 segment, ftp is not desired for the user.
Configuration description:

a) Create a proper ACL
b) Configuring packet filtering function
c) Bind the ACL to the port

The configuration steps are listed below:

Switch(Config)#access-list 110 deny tcp 10.0.0.0 0.0.0.255 any-destination d-port 21

Switch(Config)#firewall enable
Switch(Config)#firewall default permit
Switch(Config)#interface ethernet 1/10

Switch(Config-Ethernet1/10)#ip access-group 110 in
Switch(Config-Ethernet1/10)#exit
Switch(Config)#exit
Configuration result.:

Switch#show firewall

Firewall Status: Enable.
Firewall Default Rule: Permit.

Switch#show access-lists
access-list 110(used 1 time(s))
access-list 110 deny tcp 10.0.0.0 0.0.0.255 any-destination d-port 21
Switch#show access-group interface ethernet 1/10

interface name:Ethernet1/10
the ingress acl use in firewall is 110.

22.4 ACL Troubleshooting

- ☞ Checking for entries in the ACL is done in a top-down order and ends whenever an entry is matched.
- ☞ Default rule will be used only if no ACL is bound to the specific direction of the port, or no ACL entry is matched.
- ☞ Applies to IP packets incoming on all ports, and has no effect on other types of packets.
- ☞ One port can bound to only one incoming ACL.
- ☞ The number of ACLs that can be successfully bound depends on the content of the ACL bound and the hardware resource limit. Users will be prompted if an ACL cannot be bound due to hardware resource limitation.
- ☞ If an access-list contains same filtering information but conflicting action rules, binding to the port will fail with an error message. For instance, configuring “permit tcp any-source any-destination” and “deny tcp any-source any-destination” at the same time is not permitted.
- ☞ Viruses such as “worm.blaster” can be blocked by configuring ACL to block specific ICMP packets or specific TCP or UDP port packet.

22.4.1 Commands for Monitor And Debug

22.4.1.1 show access-lists

Command: show access-lists [<*num*>|<*acl-name*>]
Functions: Reveal ACL of configuration
Parameters: <*acl-name*>, specific ACL name character string; ***<num>,*** specific ACL No.
Default: None
Command Mode: Admin mode

Usage Guide: When not assigning names of ACL, all ACL will be revealed, used x time （s）indicates the times of ACL to be used.

Examples:

Switch#show access-lists

access-list 10(used 0 time(s))

access-list 10 deny any-source

access-list 100(used 1 time(s))

access-list 100 deny ip any-source any-destination

access-list 100 deny tcp any-source any-destination

access-list 1100(used 0 time(s))

access-list 1100 permit any-source-mac any-destination-mac tagged-eth2 14 2 0800

access-list 3100(used 0 time(s))

access-list 3100 deny any-source-mac any-destination-mac udp any-source s-port 100 any-destination d-port 40000

Displayed information	Explanation
access-list 10(used 1 time(s))	Number ACL10, 0 time to be used
access-list 10 deny any-source	Deny any IP packets to pass
access-list 100(used 1 time(s))	Number ACL10, 1 time to be used
access-list 100 deny ip any-source any-destination	Deny IP packet of any source IP address and destination address to pass
access-list 100 deny tcp any-source any-destination	Deny TCP packet of any source IP address and destination address to pass
access-list 1100 permit any-source-mac any-destination-mac tagged-eth2 14 2 0800	Permit tagged-eth2 with any source MAC addresses and any destination MAC addresses and the packets whose 15th and 16th byte is respectively 0x08 , 0x0 to pass
access-list 3100 permit any-source-mac any-destination-mac udp any-source s-port 100 any-destination d-port 40000	Deny the passage of UDP packets with any source MAC address and destination MAC address, any source IP address and destination IP address, and source port 100 and destination interface 40000

22.4.1.2 show access-group

Command: show access-group [interface [Ethernet] <*name*>]

Functions: Reveal tying situation of ACL on port

Parameters:<*name*>,Interface name

Default: None

Command Mode: Admin mode

Usage Guide: When not assigning interface names, all ACL tied to port will be revealed

Examples:

Switch#show access-group

interface name: Ethernet

the ingress acl use in firewall is 111,packet(s) number is 10.

the egress acl use in firewall is 100,packet(s) number is 10.

interface name: Ethernet

the ingress acl use in firewall is 10,packet(s) number is 10.

Displayed information	Explanation
interface name: Ethernet	Tying situation on port Ethernet1/2
the ingress acl use in firewall is 111.	No. 111 numeric expansion ACL tied to entrance of port Ethernet1/2
the egress acl use in firewall is 100.	No. 100 numeric expansion ACL tied to entrance of port Ethernet1/2
interface name: Ethernet	Tying situation on port Ethernet1/2
the ingress acl use in firewall is 10.	No. 10 standard expansion ACL tied to entrance of port Ethernet1/2
packet(s) number is 10	Number of packets matching this ACL rule

22.4.1.3 show firewall

Command: show firewall

Functions: Reveal configuration information of packet filtering functions

Parameters: None

Default: None

Command Mode: Admin mode

Usage Guide:

Examples:

Switch#show firewall

fire wall is enable

the default action of fire wall is permit

Displayed information	Explanation
fire wall is enable	Packet filtering function enabled
the default action of firewall is permit	Default packet filtering function is permit

22.4.1.4 show time-range

Command: show time-range<*word*>
Functions: Reveal configuration information of time range functions
Parameters: ***word*** assign name of time-range needed to be revealed
Default: None
Command Mode: Admin mode
Usage Guide: When not assigning time-range names, all time-range will be revealed.
Examples:
Switch#show time-range
time-range timer1 (inactive)
absolute-periodic Saturday 0:0:0 to Sunday 23:59:59
time-range timer2 (active)
absolute-periodic Monday 0:0:0 to Friday 23:59:59

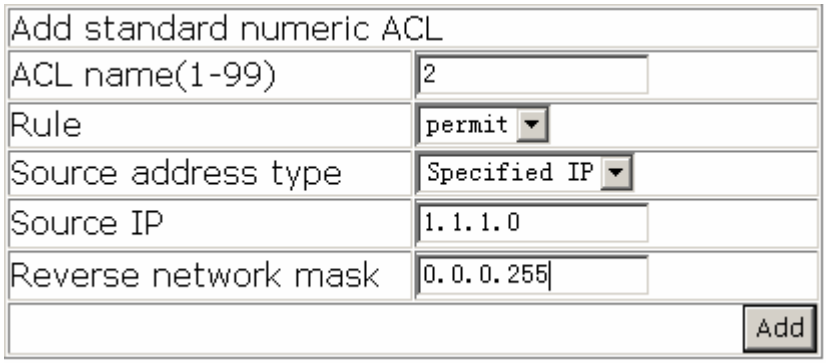
22.5 Web Management

By clicking the ACL configuration icon, it will open up the ACL sub-sections which include the following parts:

- Numeric ACL Configuration -Standard and Extended types
- ACL Name Configuration -Standard and Extended types
- Filter Configuration -- enable global configuration and the default action to bind ACL to the ports

22.5.1 Numeric standard ACL configuration

Click “Numeric ACL Configuration”, and then “Add Standard Numeric ACL” section to enter the configuration page. The explanations of each section are:
ACL number -1- 99
Rule -permit or deny
Source address type -Specified IP address or any randomly allocated IP address
Source IP address
Reverse network mask
Specify the number in the ACL number section and the relative values in the other 4 sections, then click “Add”, the users can then add the new Numeric Standard IP ACL.

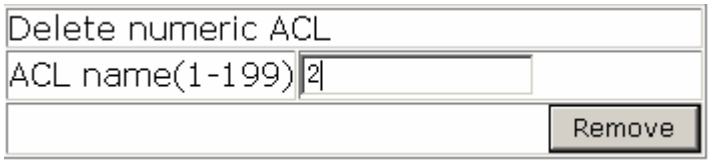


22.5.2 Delete numeric IP ACL

Click “Numeric ACL Configuration”, and then “Delete Numeric ACL” section to enter the configuration page, The explanations of each section are:

ACL number (1-199)

To delete the Numeric ACL, just simply specify the number of ACL and then click the “Remove”.



22.5.3 Configure the numeric extended ACL

There are several extended numeric extended ACLs available:

- Add ICMP numeric extended ACL
- Add IGMP numeric extended ACL
- Add TCP numeric extended ACL
- Add UDP numeric extended ACL
- Add numeric extended ACL for other protocols

By clicking the icons, it will enter the related configuration page

There are several sub-sections in this category:

- ACL number (100-199)
- Rule - permit or deny
- Source address type - Specified IP address or any randomly allocated IP address
- Source IP address
- Reverse network mask
- Target address type - Specified IP address or any randomly allocated IP address
- Destination IP address
- Reverse network mask

- IP precedence
- TOS

Regarding “ICMP numeric extended ACL”, there are two sub-categories:

- ICMP type
- ICMP code

Regarding “IGMP numeric extended ACL”, there is one sub-category:

- IGMP type

Regarding “TCP numeric extended ACL”, there are three sub-categories:

- Source port
- Destination port
- TCP sign

Regarding “UDP numeric extended ACL”, there are two sub-categories:

- Source port
- Target port

Regarding “numeric extended ACL for other protocols”, there is one sub-category: Matched protocol.

- Matched protocol - includes IP, EIGRP, OSPF, IPINIP and Input Protocol manually. If user

selects to input manually, they can just simply key-in the protocol number in the right hand

side of icon.

Example: a user wants to configure the “ Add TCP numeric extended ACL” with the ACL number of 110, deny the source IP address of 10.0.0.0/24 section, and make the target port is 21. Please refer the following configurations and then click the icon of “Add”.

Add TCP numeric extended ACL	
ACL name(100-199)	110
Rule	deny
Source address type	Specified IP
Source IP	10.0.0.0
Reverse network mask	0.0.0.255
Source port (0~65535)	
Target address type	Any IP
Destination IP address	
Reverse network mask	
Destination port(0~65535)	21
TCP sign(optional)	no
Ip precedence	
TOS	
TimeRange name(1-16 character)	
Operation type	Add

22.5.4 Configure and delete the standard ACL name

Click “ACL name configuration” to open up the sub-sections, next click “ACL name configuration” to enter the configuration page. The way to configure the “ACL name configuration” is the same with “Numeric ACL Configuration”. The only difference users should change the ACL number to the ACL name. This should be entered in ACL name not ACL number. CLI command: 1.2.2.6

There are seven sub-sections of this:

- ACL name
- ACL type - standard and extended
- Rule - permit and deny
- Source address type - Specified IP address or any randomly allocated IP address Source IP address
- Reverse network mask
- Operation type -Add or Remove

To add a numeric ACL, specify the ACL name and related value, select the “add” in the Operation type and then click “Apply”.

Add standard ACL name	
ACL name(1-16 character)	ac1
Rule	permit
Source address type	Specified IP
Source IP	1.1.1.0
Reverse network mask	0.0.0.255

22.5.5 Configure extended ACL name configuration

Click “ACL name configuration”, the configuration sections will then be shown. There are 6 types of extended ACL name configurations:

- IP extended ACL name configuration
- ICMP extended ACL name configuration
- IGMP extended ACL name configuration
- TCP extended ACL name configuration
- UDP extended ACL name configuration
- Other protocols extended ACL name configuration

Click the related the configuration web page, the configuration is the same with it is with numeric extended ACL. The only difference is the ACL number needs to be changed to ACL name, and entered into the ACL name rather than number. CLI command: 1.2.2.5.

22.5.6 Firewall configuration

Click “Filter Configuration”, and then “Firewall Configuration” to enter the configuration page. The detailed explanation is as follows:

- Packet filtering -”open” to enable or “close” to disable.
- Firewall default action -”accept” means to allow the packet to pass through and “refuse” to deny the packet.

To enable or disable, users need to click “Apply” to confirm the command.

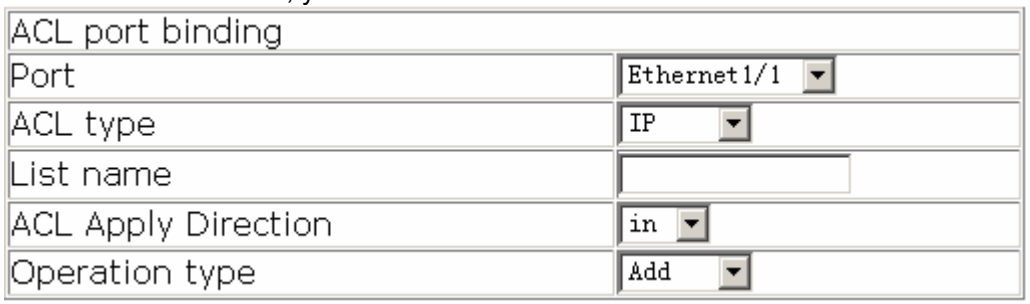
Switch firewall configuration	
Packet filtering	open
Firewall default action	accept

22.5.7 ACL port binding

Click “Filter configuration”, and then select “ACL port binding” to enter the configuration page.
There are five items in this section.

- Port -the target port to bind to ACL
- ACL name -the target ACL name to bind
- Ingress/Egress -the target direction to bind
- Operation type -”Add” or “Remove”

To enable this function, you need to select the action in each item and then click “Apply”.



Chapter 23 802.1x Configuration

23.1 Introduction to 802.1x

The 802.1x protocol originates from 802.11 protocol, the wireless LAN protocol of IEEE, which is designed to provide a solution to doing authentication when users access a wireless LAN. The LAN defined in IEEE 802 LAN protocol does not provide access authentication, which means as long as the users can access a LAN controlling device(such as a LAN Switch), they will be able to get all the devices or resources in the LAN. There was no looming danger in the environment of LAN in those primary enterprise networks.

However, along with the boom of applications like mobile office and service operating networks, the service providers should control and configure the access from user. The prevailing application of WLAN and LAN access in telecommunication networks, in particular, make it necessary to control ports in order to implement the user-level access control. And as a result, IEEE LAN/WAN committee defined a standard, which is 802.1x, to do Port-Based Network Access Control. This standard has been widely used in wireless LAN and ethernet.

"Port-Based Network Access Control" means to authenticate and control the user devices on the level of ports of LAN access devices. Only when the user devices connected to the ports pass the authentication, can they access the resources in the LAN, otherwise, the resources in the LAN won't be available.

23.1.1 The Authentication Structure of 802.1x

The system using 802.1x has a typical Client/Server structure, which contains three entities(as illustrated in the next figure): Supplicant system, Authenticator system, and Authentication server system.

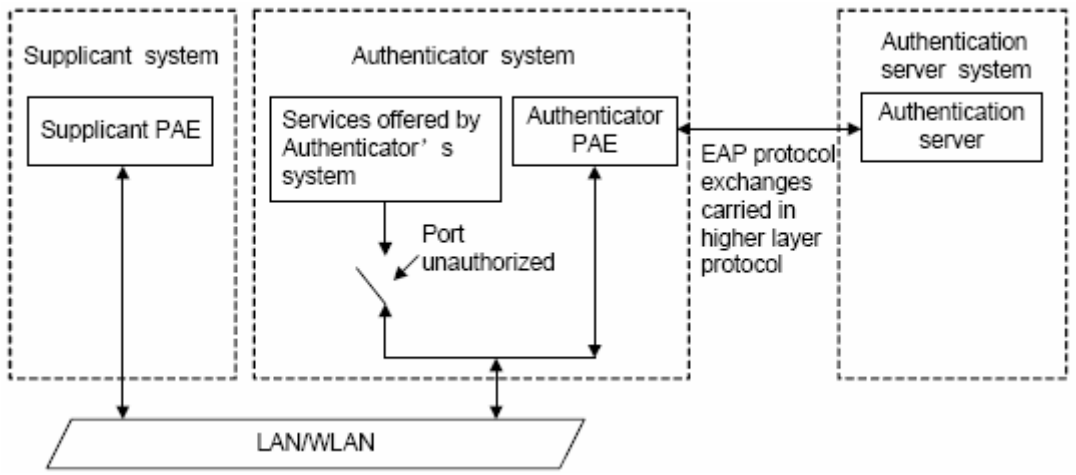


Fig 23-1 The Authentication Structure of 802.1x

- The supplicant system is an entity on one end of the lan segment, should be authenticated by the access controlling unit on the other end of the link. A Supplicant system usually is a user terminal device. Users starts 802.1x authentication by starting supplicant system software. A supplicant system should support EAPOL(Extensible Authentication Protocol over LAN).
- The authenticator system is another entity on one end of the lan segment to authenticate the supplicant systems connected. An authenticator system usually is a network device supporting 802,1x protocol, providing ports to access the lan for supplicant systems. The ports provided can either be physical or logical.
- The authentication server system is an entity to provide authentication service for authenticator systems. The authentication server system is used to authenticate and authorize users, as well as do fee-counting, and usually is a RADIUS (Remote Authentication Dial-In User Service) server, which can store the relative user information, including username, password and other parameters such as the VLAN and ports which the user belongs to.

The three entities above concerns the following basic concepts: PAE of the port, the controlled ports and the controlled direction.

1. PAE

PAE (Port Access Entity) is the entity to implement the operation of algorithms and protocols.

- The PAE of the supplicant system is supposed to respond the authentication request from the authenticator systems and submit user's authentication information to the authenticator system. It can also send authentication request and off-line request to authenticator.
- The PAE of the authenticator system authenticates the supplicant systems

needing to access the LAN via the authentication server system, and deal with the authenticated/unauthenticated state of the controlled port according to the result of the authentication. The authenticated state means the user is allowed to access the network resources, the unauthenticated state means only the EAPOL messages are allowed to be received and sent while the user is forbidden to access network resources.

2. controlled/uncontrolled ports

The authenticator system provides ports to access the LAN for the supplicant systems. These ports can be divided into two kinds of logical ports: controlled ports and uncontrolled ports.-

- ☞ The uncontrolled port is always in bi-directionally connected status, and mainly used to transmit EAPOL protocol frames, to guarantee that the supplicant systems can always send or receive authentication messages.
- ☞ The controlled port is in connected status authenticated to transmit service messages. When unauthenticated, no message from supplicant systems is allowed to be received.
- ☞ The controlled and uncontrolled ports are two parts of one port, which means each frame reaching this port is visible on both the controlled and uncontrolled ports.

3. Controlled direction

In unauthenticated status, controlled ports can be set as unidirectionally controlled or bi-directionally controlled.

- ☞ When the port is bi-directionally controlled, the sending and receiving of all frames is forbidden.
- ☞ When the port is unidirectionally controlled, no frames can be received from the supplicant systems while sending frames to the supplicant systems is allowed.

Notes: At present, this kind of switch only supports unidirectional control.

23.1.2 The Work Mechanism of 802.1x

IEEE 802.1x authentication system uses EAP (Extensible Authentication Protocol) to implement exchange of authentication information between the supplicant system, authenticator system and authentication server system.

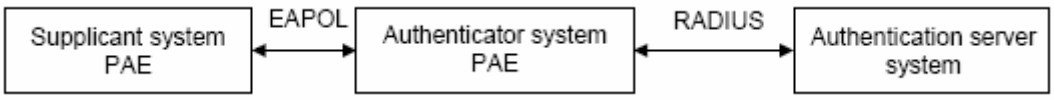


Fig 23-2 the Work Mechanism of 802.1x

- EAP messages adopt EAPOL encapsulation format between the PAE of the supplicant system and the PAE of the authenticator system in the environment of LAN.
- Between the PAE of the authenticator system and the RADIUS server, there are two methods to exchange information: one method is that EAP messages adopt EAPOR (EAP over RADIUS) encapsulation format in RADIUS protocol; the other is that EAP messages terminate with the PAE of the authenticator system, and adopt the messages containing RAP (Password Authentication Protocol) or CHAP (Challenge Handshake Authentication Protocol) attributes to do the authentication interaction with the RADIUS server.
- When the user pass the authentication, the authentication server system will send the relative information of the user to authenticator system, the PAE of the authenticator system will decide the authenticated/unauthenticated status of the controlled port according to the authentication result of the RADIUS server.

23.1.3 The Encapsulation of EAPOL Messages

1. The Format of EAPOL Data Packets

EAPOL is a kind of message encapsulation format defined in 802.1x protocol, and is mainly used to transmit EAP messages between the supplicant system and the authenticator system in order to allow the transmission of EAP messages through the LAN. In IEEE 802/Ethernet LAN environment, the format of EAPOL packet is illustrated in the next figure. The beginning of the EAPOL packet is the Type/Length domain in MAC frames.

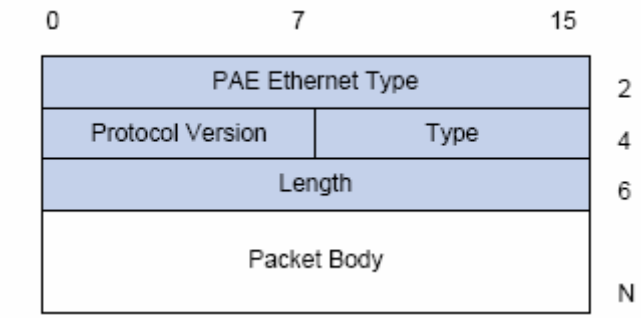


Fig 23-3 the Format of EAPOL Data Packet

PAE Ethernet Type: Represents the type of the protocol whose value is 0x888E.

Protocol Version: Represents the version of the protocol supported by the sender of EAPOL data packets.

Type: represents the type of the EAPOL data packets, including:

- EAP-Packet (whose value is 0x00): the authentication information frame, used to carry EAP messages. This kind of frame can pass through the authenticator system to transmit EAP messages between the supplicant system and the authentication server system.
- EAPOL-Start (whose value is 0x01): the frame to start authentication.
- EAPOL-Logoff (whose value is 0x02): the frame requesting to quit.
- EAPOL-Key (whose value is 0x03): the key information frame.
- EAPOL-Encapsulated-ASF-Alert (whose value is 0x04): used to support the Alerting messages of ASF (Alert Standard Forum). This kind of frame is used to encapsulate the relative information of network management such as all kinds of alerting information, terminated by terminal devices.

Length: represents the length of the data, that is, the length of the “Packet Body”, in byte. There will be no following data domain when its value is 0.

Packet Body: represents the content of the data, which will be in different formats according to different types.

2. The Format of EAP Data Packets

When the value of Type domain in EAPOL packet is EAP-Packet, the Packet Body is in EAP format (illustrated in the next figure).

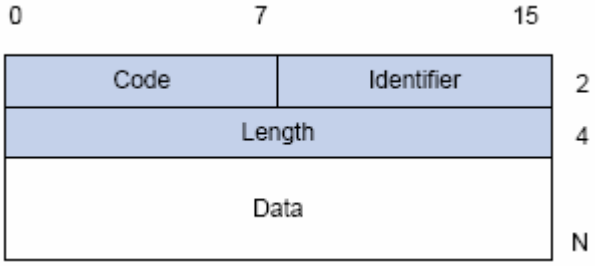


Fig 23-4 the Format of EAP Data Packets

Code: specifies the type of the EAP packet. There are four of them in total: Request（1）,Response（2）,Success（3）,Failure（4）.

- There is no Data domain in the packets of which the type is Success or Failure, and the value of the Length domains in such packets is 4.
- The format of Data domains in the packets of which the type is Request and Response is illustrated in the next figure. Type is the authentication type of EAP, the content of Type data depends on the type. For example, when the value of the type is 1, it means Identity, and is used to query the identity of the other side.

When the type is 4, it means MD5-Challenge, like PPP CHAP protocol, contains query messages.

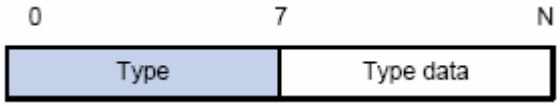


Fig 23-5 the Format of Data Domain in Request and Response Packets

Identifier: to assist matching the Request and Response messages.

Length: the length of the EAP packet, covering the domains of Code, Identifier, Length and Data, in byte.

Data: the content of the EAP packet, depending on the Code type.

23.1.4 The Encapsulation of EAP Attributes

RADIUS adds two attribute to support EAP authentication: EAP-Message and Message-Authenticator. Please refer to the Introduction of RADIUS protocol in “AAA-RADIUS-HWTACACS operation” to check the format of RADIUS messages.

1. EAP-Message

As illustrated in the next figure, this attribute is used to encapsulate EAP packet, the type code is 79, String domain should be no longer than 253 bytes. If the data length in an EAP packet is larger than 253 bytes, the packet can be divided into fragments, which then will be encapsulated in several EAP-Messages attributes in their original order.

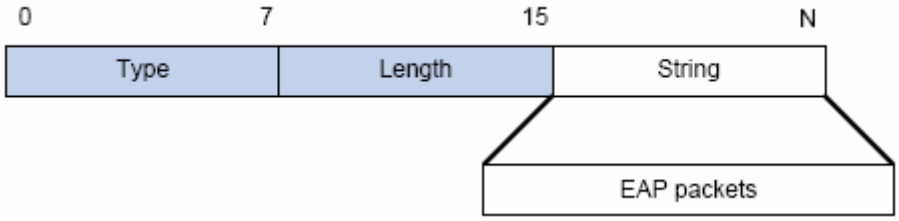


Fig 23-6 the Encapsulation of EAP-Message Attribute

2. Message-Authenticator

As illustrated in the next figure, this attribute is used in the process of using authentication methods like EAP and CHAP to prevent the access request packets from being eavesdropped. Message-Authenticator should be included in the packets containing the EAP-Message attribute, or the packet will be dropped as an invalid one.

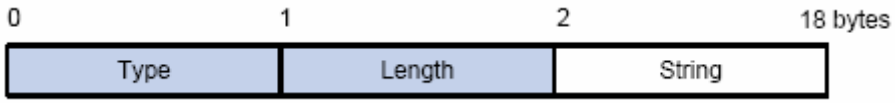


Fig 23-7 Message-Authenticator Attribute

23.1.5 The Authentication Methods of 802.1x

The authentication can either be started by supplicant system initiatively or by devices. When the device detects unauthenticated users to access the network, it will send supplicant system EAP-Request/Identity messages to start authentication. On the other hand, the supplicant system can send EAPOL-Start message to the device via supplicant software.

802.1x system supports EAP relay method and EAP termination method to implement authentication with the remote RADIUS server. The following is the description of the process of these two authentication methods, both started by the supplicant system.

23.1.5.1 EAP Relay Mode

EAP relay is specified in IEEE 802.1x standard to carry EAP in other high-level protocols, such as EAP over RADIUS, making sure that extended authentication protocol messages can reach the authentication server through complicated networks. In general, EAP relay requires the RADIUS server to support EAP attributes: EAP-Message and Message-Authenticator.

EAP is a widely-used authentication frame to transmit the actual authentication protocol rather than a special authentication mechanism. EAP provides some common function and allows the authentication mechanisms expected in the negotiation, which are called EAP Method. The advantage of EAP lies in that EAP mechanism working as a base needs no adjustment when a new authentication protocol appears. The following figure illustrates the protocol stack of EAP authentication method.

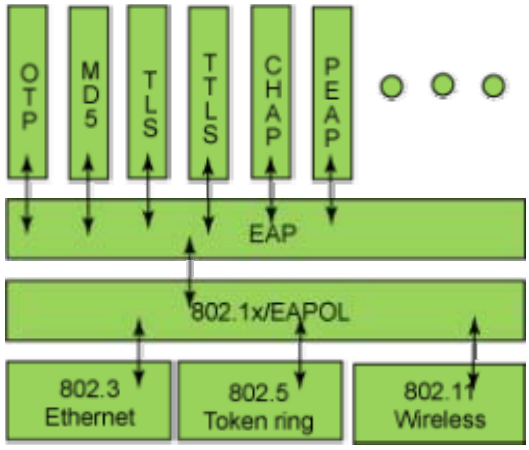


Fig 23-8 the Protocol Stack of EAP Authentication Method

By now, there are more than 50 EAP authentication methods has been developed, the differences among which are those in the authentication mechanism and the

management of keys. The 4 most common EAP authentication methods are listed as follows:

- **EAP-MD5**
- **EAP-TLS**（Transport Layer Security）
- **EAP-TTLS**（Tunneled Transport Layer Security）
- **PEAP**（Protected Extensible Authentication Protocol）
- **EAP-MD5**
- **EAP-TLS**（Transport Layer Security）
- **EAP-TTLS**（Tunneled Transport Layer Security）
- **PEAP**（Protected Extensible Authentication Protocol）

They will be described in detail in the following part.

Attention：

- The switch, as the access controlling unit of Pass-through, will not check the content of a particular EAP method, so can support all the EAP methods above and all the EAP authentication methods that may be extended in the future.
- In EAP relay, if any authentication method in EAP-MD5, EAP-TLS, EAP-TTLS and PEAP is adopted, the authentication methods of the supplicant system and the RADIUS server should be the same.

1. EAP-MD5 Authentication Method

EAP-MD5 is an IETF open standard which providing the least security, since MD5 Hash function is vulnerable to dictionary attacks.

The following figure illustrated the basic operation flow of the EAP-MD5 authentication method.

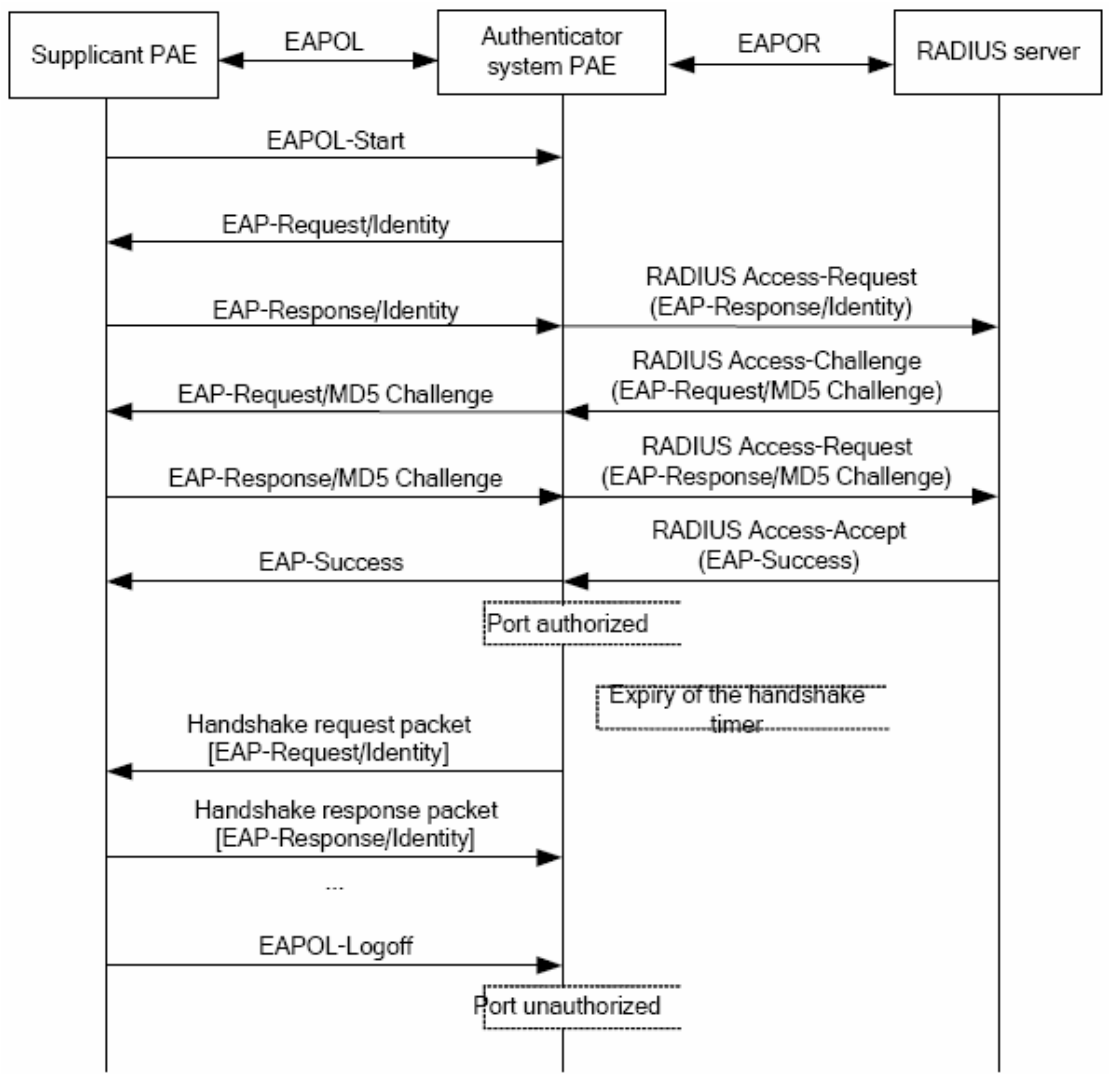


Fig 23-9 the Authentication Flow of 802.1x EAP-MD5

2. EAP-TLS Authentication Method

EAP-TLS is brought up by Microsoft based on EAP and TLS protocols. It uses PKI to protect the id authentication between the supplicant system and the RADIUS server and the dynamically generated session keys, requiring both the supplicant system and the Radius authentication server to possess digital certificate to implement bidirectional authentication. It is the earliest EAP authentication method used in wireless LAN. Since every user should have a digital certificate, this method is rarely used practically considering the difficult maintenance. However it is still one of the safest EAP standards, and enjoys prevailing supports from the vendors of wireless LAN hardware and software.

The following figure illustrates the basic operation flow of the EAP-TLS authentication method.

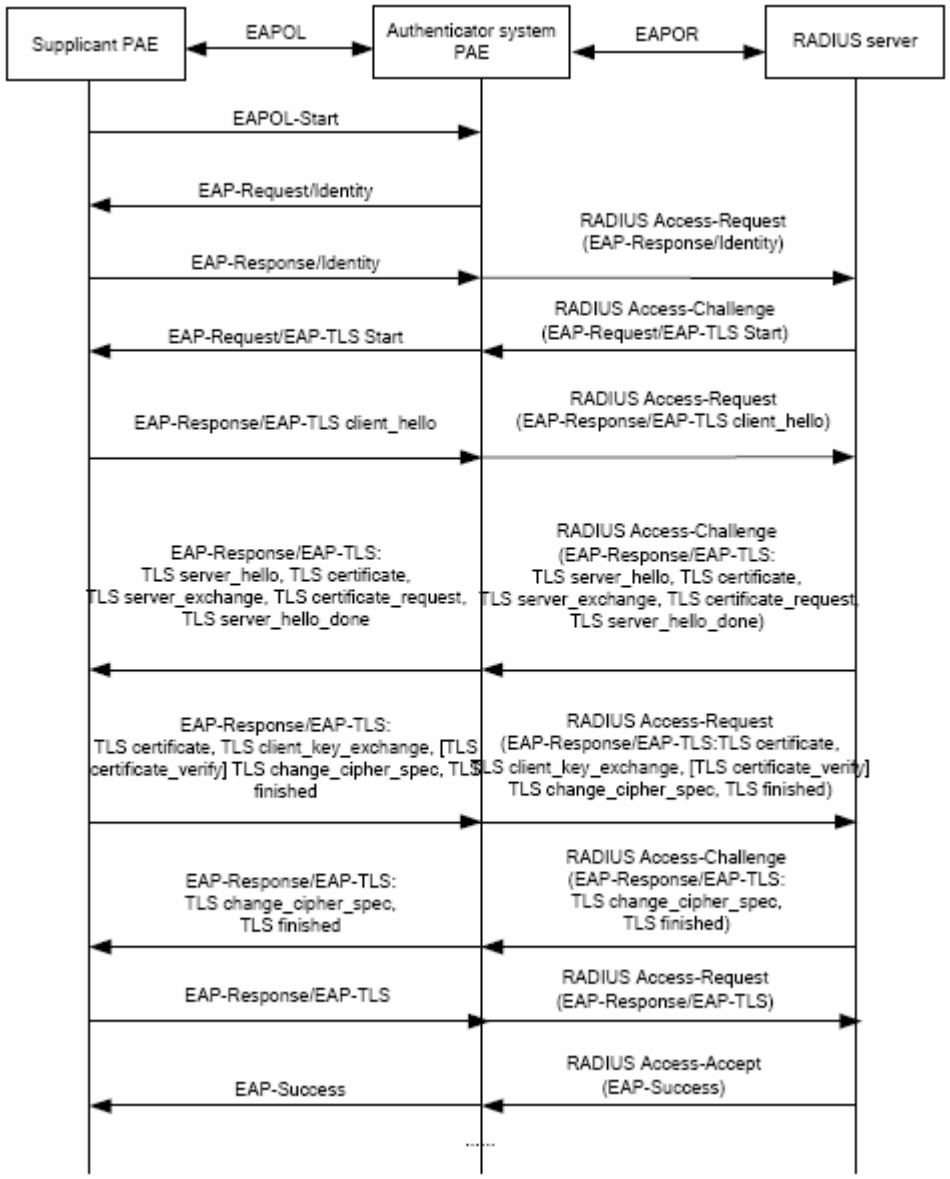


Fig 23-10 the Authentication Flow of 802.1x EAP-TLS

3. EAP-TTLS Authentication Method

EAP-TTLS is a product of the cooperation of Funk Software and Certicom. It can provide an authentication as strong as that provided by EAP-TLS, but without requiring users to have their own digital certificate. The only request is that the Radius server should have a digital certificate. The authentication of users' identity is implemented with passwords transmitted in a safely encrypted tunnel established via the certificate of the authentication server. Any kind of authentication request including EAP, PAP and MS-CHAPV2 can be transmitted within TTLS tunnels.

4. PEAP Authentication Method

EAP-PEAP is brought up by Cisco, Microsoft and RAS Security as a recommended open standard. It has long been utilized in products and provides very good security. Its

design of protocol and security is similar to that of EAP-TTLS, using a server's PKI certificate to establish a safe TLS tunnel in order to protect user authentication.

The following figure illustrates the basic operation flow of PEAP authentication method.

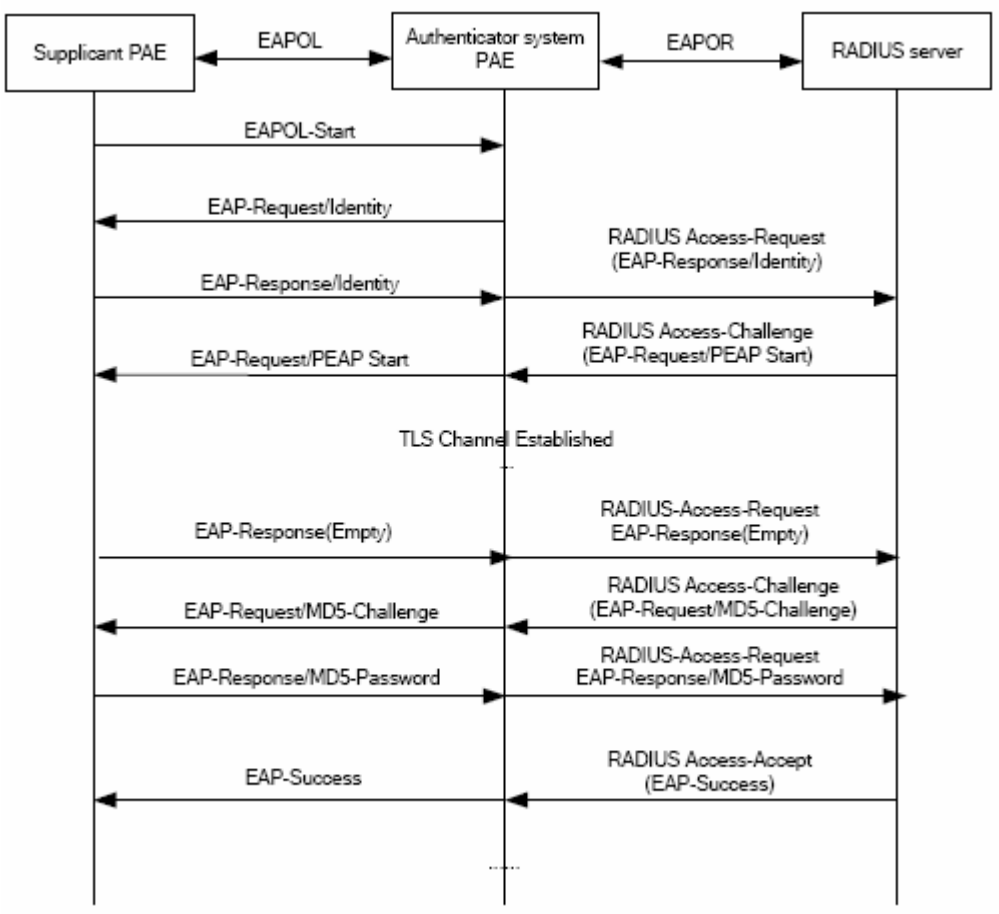


Fig 23-11 the Authentication Flow of 802.1x PEAP

23.1.5.2 EAP Termination Mode

In this mode, EAP messages will be terminated in the access control unit and mapped into RADIUS messages, which is used to implement the authentication, authorization and fee-counting. The basic operation flow is illustrated in the next figure.

In EAP termination mode, the access control unit and the RADIUS server can use PAP or CHAP authentication method. The following figure will demonstrate the basic operation flow using CHAP authentication method.

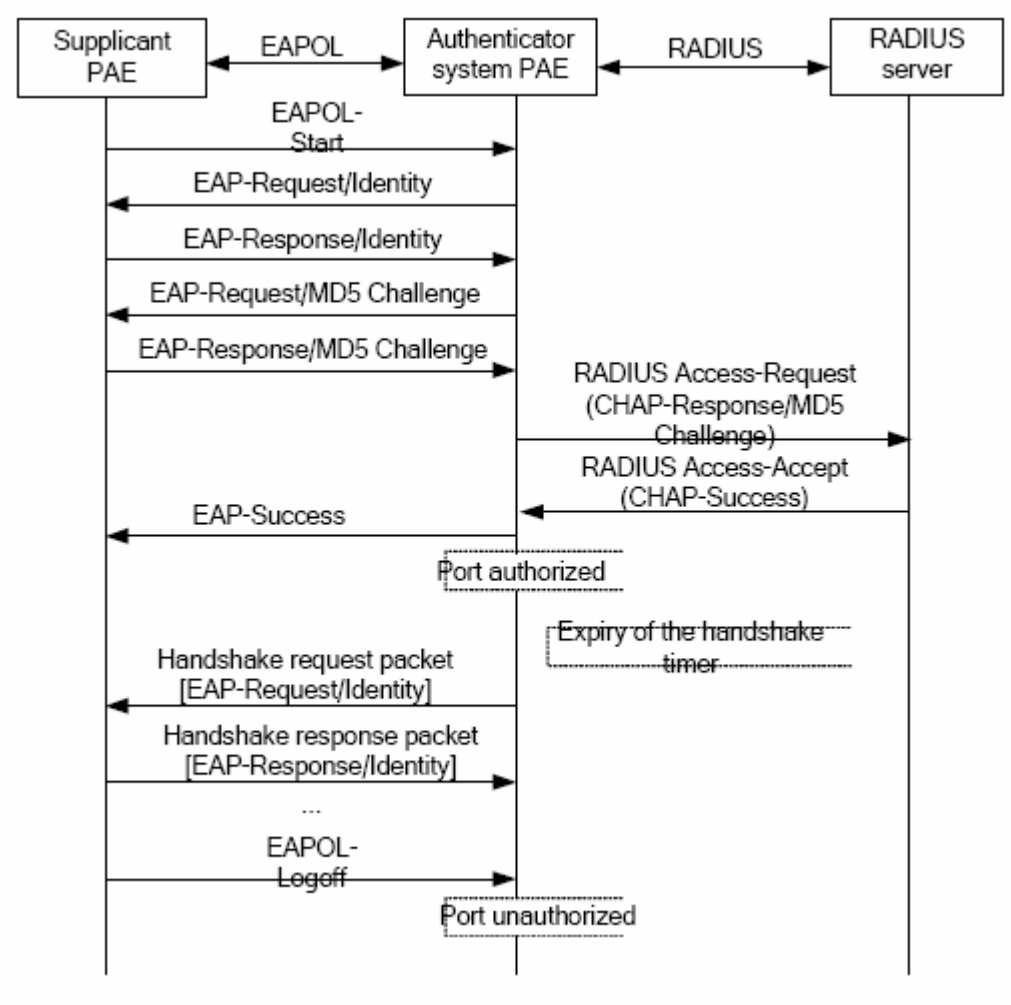


Fig 23-12 the Authentication Flow of 802.1x EAP Termination Mode

23.1.6 The Extension and Optimization of 802.1x

Besides supporting the port- based access authentication method specified by the protocol, devices also extend and optimize it when implementing the EAP relay mode and EAP termination mode of 802.1x.

- ☞ Supports some applications in the case of which one physical port can have more than one users
- ☞ There are three access control methods (the methods to authenticate users): port-based, MAC-based and user-based (IP address+ MAC address+ port).
  - ◆ When the port-based method is used, as long as the first user of this port passes the authentication, all the other users can access the network resources without being authenticated. However, once the first user is offline, the network won't be available to all the other users.
  - ◆ When the MAC-based method is used, all the users accessing a port

should be authenticated separately, only those pass the authentication can access the network, while the others can not. When one user becomes offline, the other users will not be affected.

- When the user-based (IP address+ MAC address+ port) method is used, all users can access limited resources before being authenticated. There are two kinds of control in this method: standard control and advanced control. The user-based standard control will not restrict the access to limited resources, which means all users of this port can access limited resources before being authenticated. The user-based advanced control will restrict the access to limited resources, only some particular users of the port can access limited resources before being authenticated. Once those users pass the authentication, they can access all resources.

Attention: when using private supplicant systems, user-based advanced control is recommended to effectively prevent ARP cheat.

The maximum number of the authenticated users can be 4000, but less than 2000 will be preferred.

23.1.7 The Features of VLAN Allocation

1. Auto VLAN

Auto VLAN feature enables RADIUS server to change the VLAN to which the access port belongs, based on the user information and the user access device information. When an 802.1x user passes authentication on the server, the RADIUS server will send the authorization information to the device, if the RADIUS server has enabled the VLAN-assigning function, then the following attributes should be included in the Access-Accept messages:

- Tunnel-Type = VLAN (13)
- Tunnel-Medium-Type = 802 (6)
- Tunnel-Private-Group-ID = VLANID

The VLANID here means the VID of VLAN, ranging from 1 to 4094. For example, Tunnel-Private-Group-ID = 30 means VLAN 30.

When the switch receives the assigned Auto VLAN information, the current Access port will leave the VLAN set by the user and join Auto VLAN.

Auto VLAN won't change or affect the port's configuration. But the priority of Auto VLAN is higher than that of the user-set VLAN, that is Auto VLAN is the one takes effect when the authentication is finished, while the user-set VLAN do not work until the user become offline.

Notes: At present, Auto VLAN can only be used in the port-based access control mode, and on the ports whose link type is Access.

2. Guest VLAN

Guest VLAN feature is used to allow the unauthenticated user to access some specified resources.

The user authentication port belongs to a default VLAN (Guest VLAN) before passing the 802.1x authentication, with the right to access the resources within this VLAN without authentication. But the resources in other networks are beyond reach. Once authenticated, the port will leave Guest VLAN, and the user can access the resources of other networks.

In Guest VLAN, users can get 802.1x supplicant system software, update supplicant system or update some other applications (such as anti-virus software, the patches of operating system). The access device will add the port into Guest VLAN if there is no supplicant getting authenticated successfully in a certain stretch of time because of lacking exclusive authentication supplicant system or the version of the supplicant system being too low.

Once the 802.1x feature is enabled and the Guest VLAN is configured properly, a port will be added into Guest VLAN, just like Auto VLAN, if there is no response message from the supplicant system after the device sends more authentication-triggering messages than the upper limit (EAP-Request/Identity) from the port.

- ☞ The authentication server assigns an Auto VLAN, and then the port leaves Guest VLAN and joins the assigned Auto VLAN. When the user becomes offline, the port will be allocated to the specified Guest VLAN again.
- ☞ The authentication server assigns an Auto VLAN, and then the port leaves Guest VLAN and joins the specified VLAN. When the user becomes offline, the port will be allocated to the specified Guest VLAN again.

23.2 802.1x Configuration Task List

1. Enable IEEE 802.1x function
2. Access management unit property configuration
   1) Configure port authentication status
   2) Configure access management method for the port: MAC-based or port-based.
   3) Configure expanded 802.1x function
3. User access devices related property configuration (optional)

4. RADIUS server related property configuration

1) Configure RADIUS authentication key.

2) Configure RADIUS Server

3) Configure RADIUS Service parameters.

1. Enable 802.1x function

Command	Explanation
Global Mode	
aaa enable **no aaa enable**	Enables the AAA authentication function in the switch; the "**no aaa enable**" command disables the AAA authentication function.
aaa-accounting enable **no aaa-accounting enable**	Enables the accounting function in the switch; the "**no aaa-accounting enable**" command disables the accounting function
dot1x enable **no dot1x enable**	Enables the 802.1x function in the switch and ports; the "**no dot1x enable**" command disables the 802.1x function.

2. Access management unit property configuration

1) Configure port authentication status

Command	**Explanation**
Port Mode	
dot1x port-control {auto|force-authorized|force-unauthorized } **no dot1x port-control**	Sets the 802.1x authentication mode; the "**no dot1x port-control**" command restores the default setting.

2) Configure port access management method

Command	Explanation
Port Mode	
dot1x port-method { userbased | macbased | portbased} **no dot1x port-method**	Sets the port access management method; the "**no dot1x port-method**" command restores MAC-based access management.
dot1x max-user macbased <*number*> **no dot1x max-user macbased**	Sets the maximum number of access users for the specified port; the "**no dot1x max-user macbased**" command restores the default setting of allowing 1 user.
dot1x max-user userbased <*number*> **no dot1x max-user userbased**	Set the upper limit of the number of users allowed to access the specified port, only used when the access control mode of the port is userbased; the "**no dot1x max-user userbased**" command is used to reset the limit to 10 by default.
dot1x guest-vlan <*vlanID*> **no dot1x guest-vlan**	Set the guest vlan of the specified port; the "**no dot1x guest-vlan**" command is used to delete the guest vlan.

3) Configure expanded 802.1x function

Command	Explanation
Global Mode	
dot1x macfilter enable **no dot1x macfilter enable**	Enables the 802.1x address filter function in the switch; the "**no dot1x macfilter enable**" command disables the 802.1x address filter function.
dot1x accept-mac <*mac-address*> [interface <*interface-name*>] **no dot1x accept-mac <*mac-address*> [interface <*interface-name*>]**	Adds 802.1x address filter table entry, the "**no dot1x accept-mac**" command deletes 802.1x filter address table entries.
dot1x eapor enable **no dot1x eapor enable**	Enables the EAP relay authentication function in the switch; the "**no dot1x eapor enable**" command sets EAP local end authentication.

3. Supplicant related property configuration

Command	Explanation
Global Mode	

dot1x max-req <*count*> **no dot1x max-req**	Sets the number of EAP request/MD5 frame to be sent before the switch re-initials authentication on no supplicant response, the "**no dot1x max-req**" command restores the default setting.
dot1x re-authentication **no dot1x re-authentication**	Enables periodical supplicant authentication; the "**no dot1x re-authentication**" command disables this function.
dot1x timeout quiet-period <*seconds*> **no dot1x timeout quiet-period**	Sets time to keep silent on port authentication failure; the "**no dot1x timeout quiet-period**" command restores the default value.
dot1x timeout re-authperiod <*seconds*> **no dot1x timeout re-authperiod**	Sets the supplicant re-authentication interval; the "**no dot1x timeout re-authperiod**" command restores the default setting.
dot1x timeout tx-period <*seconds*> **no dot1x timeout tx-period**	Sets the interval for the supplicant to re-transmit EAP request/identity frame; the "**no dot1x timeout tx-period**" command restores the default setting.
Admin Mode	
dot1x re-authenticate [interface <*interface-name*>]	Enables IEEE 802.1x re-authentication (no wait timeout requires) for all ports or a specified port.

4. Authentication Server (RADIUS server) related property configuration

1) Configure RADIUS authentication key.

Command	**Explanation**
Global Mode	
radius-server key <*string*> no radius-server key	Specifies the key for RADIUS server; the **"no radius-server key"** command deletes the key for RADIUS server.

2) Configuring RADIUS Server

Command	**Explanation**
Global Mode	

radius-server authentication host {*<IPaddress>*|*<IPv6address>*} [[port {*<portNum>*}] [primary]] **no radius-server authentication host *<IPaddress>***	Specifies the IP address or IPv6 address and listening port number for RADIUS authentication server; the “no radius-server authentication host <IPaddress>“ command deletes the RADIUS server
radius-server accounting host {*<IPaddress>*|*<IPv6address>*} [[port {*<portNum>*}] [primary]] **no radius-server accounting host *<IPaddress>***	Specifies the IP address or IPv6 address and listening port number for RADIUS accounting server; the “no radius-server authentication host <IPaddress>“ command deletes the RADIUS server

3) Configure RADIUS Service parameters.

Command	**Explanation**
Global Mode	
radius-server dead-time *<minutes>* **no radius-server dead-time**	Configures the restore time when RADIUS server is down; the “**no radius-server dead-time**” command restores the default setting.
radius-server retransmit *<retries>* **no radius-server retransmit**	Configures the re-transmission times for RADIUS; the “**no radius-server retransmit**” command restores the default setting
radius-server timeout *<seconds>* **no radius-server timeout**	Configures the timeout timer for RADIUS server; the “**no radius-server timeout**” command restores the default setting.

23.3 Commands for 802.1x

23.3.1 aaa enable

Command: aaa enable

no aaa enable

Function: Enables the AAA authentication function in the switch; the "no AAA enable"

command disables the AAA authentication function.

Command mode: Global Mode

Parameters: N/A.

Default: AAA authentication is not enabled by default.

Usage Guide: The AAA authentication for the switch must be enabled first to enable IEEE 802.1x authentication for the switch.

Example: Enabling AAA function for the switch.

Switch(Config)#aaa enable

23.3.2 aaa-accounting enable

Command:aaa-accounting enable

no aaa-accounting enable

Function: Enables the AAA accounting function in the switch: the "**no aaa-accounting enable**" command disables the AAA accounting function.

Command mode: Global Mode

Default: AAA accounting is not enabled by default.

Usage Guide: When accounting is enabled in the switch, accounting will be performed according to the traffic or online time for port the authenticated user is using. The switch will send an “accounting started” message to the RADIUS accounting server on starting the accounting, and an accounting packet for the online user to the RADIUS accounting server every five seconds, and an “accounting stopped” message is sent to the RADIUS accounting server on accounting end. Note: The switch send the “user offline” message to the RADIUS accounting server only when accounting is enabled, the “user offline” message will not be sent to the RADIUS authentication server.

Example: Enabling AAA accounting for the switch.

Switch(Config)#aaa-accounting enable

23.3.3 dot1x accept-mac

Command: dot1x accept-mac <*mac-address*> [interface <*interface-name*>]

no dot1x accept-mac <*mac-address*> [interface <*interface-name*>]

Function: Adds a MAC address entry to the dot1x address filter table. If a port is specified, the entry added applies to the specified port only. If no port is specified, the entry added applies to all the ports. The “**no dot1x accept-mac <*mac-address*> [interface <*interface-name*>]**” command deletes the entry from dot1x address filter table.

Parameters: <*mac-address*> stands for MAC address; **<*interface-name*>** for interface

name and port number.

Command mode: Global Mode

Default: N/A.

Usage Guide: The dot1x address filter function is implemented according to the MAC address filter table, dot1x address filter table is manually added or deleted by the user. When a port is specified in adding a dot1x address filter table entry, that entry applies to the port only; when no port is specified, the entry applies to all ports in the switch. When dot1x address filter function is enabled, the switch will filter the authentication user by the MAC address. Only the authentication request initialed by the users in the dot1x address filter table will be accepted, the rest will be rejected.

Example: Adding MAC address 00-01-34-34-2e-0a to the filter table of Ethernet 1/5.

Switch(Config)#dot1x accept-mac 00-01-34-34-2e-0a interface ethernet 1/5

23.3.4 dot1x eapor enable

Command: dot1x eapor enable

no dot1x eapor enable

Function: Enables the EAP relay authentication function in the switch; the "**no dot1x eapor enable**" command sets EAP local end authentication.

Command mode: Global Mode

Default: EAP relay authentication is used by default.

Usage Guide: The switch and RADIUS may be connected via Ethernet or PPP. If an Ethernet connection exists between the switch and RADIUS server, the switch needs to authenticate the user by EAP relay (EAPoR authentication); if the switch connects to the RADIUS server by PPP, the switch will use EAP local end authentication (CHAP authentication). The switch should use different authentication methods according to the connection between the switch and the authentication server.

Example: Setting EAP local end authentication for the switch.

Switch(Config)#no dot1x eapor enable

23.3.5 dot1x enable

Command: dot1x enable

no dot1x enable

Function: Enables the 802.1x function in the switch and ports: the "**no dot1x enable**" command disables the 802.1x function.

Command mode: Global Mode and Interface Mode.

Default: 802.1x function is not enabled in global mode by default; if 802.1x is enabled

under Global Mode, 802.1x will not be enabled for the ports by default.

Usage Guide: The 802.1x authentication for the switch must be enabled first to enable 802.1x authentication for the respective ports. If Spanning Tree or MAC binding is enabled on the port, or the port is a Trunk port or member of port aggregation group, 802.1x function cannot be enabled for that port unless such conditions are removed.

Example: Enabling the 802.1x function of the switch and enable 802.1x for port 1/12.

Switch(Config)#dot1x enable

Switch(Config)#interface ethernet 1/12

Switch(Config-Ethernet1/12)#dot1x enable

23.3.6 dot1x guest-vlan

Command：dot1x guest-vlan <*vlanid*>

no dot1x guest-vlan

Function：Set the guest-vlan of the specified port; the "**no dot1x guest-vlan**" command is used to delete the guest-vlan.

Parameters：*<vlanid>* the specified Vlan id, ranging from 1 to 4095。

Command Mode：Interface Mode.

Default Settings：There is no 802.1x guest-vlan function on the port.

User Guide：The access device will add the port into Guest VLAN if there is no supplicant getting authenticated successfully in a certain stretch of time because of lacking exclusive authentication supplicant system or the version of the supplicant system being too low.

In Guest VLAN, users can get 802.1x supplicant system software, update supplicant system or update some other applications(such as anti-virus software, the patches of operating system). When a user of a port within Guest VLAN starts an authentication, the port will remain in Guest VLAN in the case of a failed authentication. If the authentication finishes successfully, there are two possible results:

- ☞ The authentication server assigns an Auto VLAN, causing the port to leave Guest VLAN to join the assigned Auto VLAN. After the user gets offline, the port will be allocated back into the specified Guest Vlan.
- ☞ The authentication server assigns an Auto VLAN, then the port leaves Guest VLAn and joins the specified VLAN. When the user becomes offline, the port will be allocated to the specified GuestVlan again.

Attention:

- ☞ There can be different Guest VLAN set on different ports, while only one Guest VLAN is allowed on one port.
- ☞ Only when the access control mode is portbased, the Guest VLAN can take

effect. If the access control mode of the port is macbased or userbased, the Guest VLAN can be successfully set without taking effect.

Examples： Set Guest-Vlan of port Ethernet1/3 as Vlan 10.

Switch(Config-Ethernet1/3)#dot1xguest-vlan 10

23.3.7 dot1x macfilter enable

Command: dot1x macfilter enable

no dot1x macfilter enable

Function: Enables the dot1x address filter function in the switch; the "**no dot1x macfilter enable**" command disables the dot1x address filter function.

Command mode: Global Mode

Default: dot1x address filter is disabled by default.

Usage Guide: When dot1x address filter function is enabled, the switch will filter the authentication user by the MAC address. Only the authentication request initialed by the users in the dot1x address filter table will be accepted.

Example: Enabling dot1x address filter function for the switch.

Switch(Config)#dot1x macfilter enable

23.3.8 dot1x max-req

Command: dot1x max-req <*count*>

no dot1x max-req

Function: Sets the number of EAP request/MD5 frame to be sent before the switch re-initials authentication on no supplicant response; the "**no dot1x max-req**" command restores the default setting.

Parameters: < *count*> is the times to re-transfer EAP request/ MD5 frames, the valid range is 1 to 10.

Command mode: Global Mode

Default: The default maximum for retransmission is 2.

Usage Guide: The default value is recommended in setting the EAP request/ MD5 retransmission times.

Example: Changing the maximum retransmission times for EAP request/ MD5 frames to 5 times.

Switch(Config)#dot1x max-req 5

23.3.9 dot1x max-user

Command: dot1x max-user macbased<*number*>

no dot1x max-user macbased

Function: Sets the maximum users allowed to connect to the port; the "**no dot1x max-user**" command restores the default setting.

Parameters: < *number*> is the maximum users allowed, the valid range is 1 to 254.

Command mode: Port configuration Mode.

Default: The default maximum user allowed is 1.

Usage Guide: This command is available for ports using MAC-based access management, if MAC address authenticated exceeds the number of allowed user, additional users will not be able to access the network.

Example: Setting port 1/3 to allow 5 users.

Switch(Config-Ethernet1/3)#dot1x max-user macbased 5

23.3.10 dot1x max-user userbased

Command：dot1x max-user userbased <*number*>

no dot1x max-user userbased

Function：Set the upper limit of the number of users allowed to access the specified port when using user-based access control mode; the "no dot1x max-user userbased" command is used to reset the default value .

Parameters：***<number>*** the maximum number of users allowed to access the network, ranging from 1 to 1~128.

Command Mode：Interface Mode.

Default Settings：The maximum number of users allowed to access each port is 128 by default.

User Guide：This command can only take effect when the port adopts user-based access control mode. If the number of authenticated users exceeds the upper limit of the number of users allowed to access the network, those extra users can not access the network.

Examples：Set the maximum number of users allowed to access the network on port Ethernet1/3 as 5.

Switch(Config-Ethernet1/3)#dot1x max-user userbased 5

23.3.11 dot1x port-control

Command: dot1x port-control {auto|force-authorized|force-unauthorized }

no dot1x port-control

Function: Sets the 802.1x authentication status; the "**no dot1x port-control**" command restores the default setting.

Parameters: auto enable 802.1x authentication, the port authorization status is determined by the authentication information between the switch and the supplicant; **force-authorized** sets port to authorized status, unauthenticated data is allowed to pass through the port; **force-unauthorized** will set the port to non-authorized mode, the switch will not provide authentication for the supplicant and prohibit data from passing through the port.

Command mode: Port configuration Mode

Default: When 802.1x is enabled for the port, **auto** is set by default.

Usage Guide: If the port needs to provide 802.1x authentication for the user, the port authentication mode should be set to **auto**.

Example: Setting port1/1 to require 802.1x authentication mode.

Switch(Config)#interface ethernet 1/1

Switch(Config-Ethernet1/1)#dot1x port-control auto

23.3.12 dot1x port-method

Command: dot1x port-method { userbased | macbased | portbased}

no dot1x port-method

Function: Sets the access management method for the specified port; the "**no dot1x port-method**" command restores the default access management method.

Parameters: userbased sets user-based access management; **macbased** sets the MAC-based access management method; **portbased** sets port-based access management.

Command mode: Port configuration Mode

Default: None.

Usage Guide: MAC-based access management is better than port-based access management in both security and management, port-based access management is suggested only for special usages.

Example: Setting port-based access management for port 1/4.

Switch(Config-Ethernet1/4)#dot1x port-method portbased

23.3.13 dot1x re-authenticate

Command: dot1x re-authenticate [interface <*interface-name*>]

Function: Enables real-time 802.1x re-authentication (no wait timeout requires) for all ports or a specified port.

Parameters: <*interface-nam*> stands for port number, omitting the parameter for all ports.

Command mode: Global Mode

Usage Guide: This command is an Admin Mode command. It makes the switch to re-authenticate the client at once without waiting for re-authentication timer timeout. This command is no longer valid after authentication.

Example: Enabling real-time re-authentication on port 1/8.

Switch(Config)#dot1x re-authenticate interface ethernet 1/8

23.3.14 dot1x re-authentication

Command: dot1x re-authentication

no dot1x re-authentication

Function: Enables periodical supplicant authentication; the "**no dot1x re-authentication**" command disables this function.

Command mode: Global Mode

Default: Periodical re-authentication is disabled by default.

Usage Guide: When periodical re-authentication for supplicant is enabled, the switch will re-authenticate the supplicant at regular interval. This function is not recommended for common use.

Example: Enabling the periodical re-authentication for authenticated users.

Switch(Config)#dot1x re-authentication

23.3.15 dot1x timeout quiet-period

Command: dot1x timeout quiet-period <*seconds*>

no dot1x timeout quiet-period

Function: Sets time to keep silent on supplicant authentication failure; the "**no dot1x timeout quiet-period**" command restores the default value.

Parameters: <*seconds*> is the silent time for the port in seconds, the valid range is 1 to 65535.

Command mode: Global Mode

Default: The default value is 10 seconds.

Usage Guide: Default value is recommended.

Example: Setting the silent time to 120 seconds.

Switch(Config)#dot1x timeout quiet-period 120

23.3.16 dot1x timeout re-authperiod

Command:dot1x timeout re-authperiod <*seconds*>

no dot1x timeout re-authperiod

Function: Sets the supplicant re-authentication interval; the "**no dot1x timeout re-authperiod**" command restores the default setting.

Parameters: <*seconds*> is the interval for re-authentication, in seconds, the valid range is 1 to 65535.

Command mode: Global Mode

Default: The default value is 3600 seconds.

Usage Guide:dot1x re-authentication must be enabled first before supplicant re-authentication interval can be modified. If authentication is not enabled for the switch, the supplicant re-authentication interval set will not take effect.

Example: Setting the re-authentication time to 1200 seconds.

Switch(Config)#dot1x timeout re-authperiod 1200

23.3.17 dot1x timeout tx-period

Command: dot1x timeout tx-period <*seconds*>

no dot1x timeout tx-period

Function: Sets the interval for the supplicant to re-transmit EAP request/identity frame; the "**no dot1x timeout tx-period**" command restores the default setting.

Parameters: <*seconds*> is the interval for re-transmission of EAP request frames, in seconds; the valid range is 1 to 65535.

Command mode: Global Mode

Default: The default value is 30 seconds.

Usage Guide: Default value is recommended.

Example: Setting the EAP request frame re-transmission interval to 1200 seconds.

Switch(Config)#dot1x timeout tx-period 1200

23.3.18 radius-server accounting host

Command:radius-server accounting host {<*ipv4-address*>|<*ipv6-address*>} [port <port-number>] [primary]

no radius-server accounting host {<*ipv4-address*>|<*ipv6-address*>}

Function: Specifies the IPv4/IPv6 address and listening port number for RADIUS accounting server; the "**no radius-server authentication host <*IPaddress*>**" command deletes the RADIUS accounting server

Parameters: 〈*ipv4-address*〉|〈*ipv6-address*〉 stands for the server IPv4/IPv6 address; **<*port-number*>** for server listening port number from 0 to 65535; **primary** for primary server. Multiple RADIUS sever can be configured and would be available. RADIUS

server will be searched by the configured order if **primary** is not configured, otherwise, the specified RADIUS server will be used first.

Command mode: Global Mode

Default: No RADIUS accounting server is configured by default.

Usage Guide: This command is used to specify the IPv4/IPv6 address and port number of the specified RADIUS server for switch accounting, multiple command instances can be configured. The ***<port-number>*** parameter is used to specify accounting port number, which must be the same as the specified accounting port in the RADIUS server; the default port number is 1813. If this port number is set to 0, accounting port number will be generated at random and can result in invalid configuration. This command can be used repeatedly to configure multiple RADIUS servers communicating with the switch, the switch will send accounting packets to all the configured accounting servers, and all the accounting servers can be backup servers for each other. If **primary** is specified, then the specified RADIUS server will be the primary server.

Example: Sets the RADIUS accounting server of IP address to 100.100.100.60 as the primary server, with the accounting port number as 3000.

Switch(Config)#radius-server accounting host 100.100.100.60 port 3000 primary

23.3.19 radius-server authentication host

Command: radius-server authentication host {*<ipv4-address >|<ipv6-address>*} [port <port-number>] [primary]

no radius-server authentication host { *ipv4-address >|<ipv6-address>*}

Function: Specifies the IP address and listening port number for the RADIUS server; the "**no radius-server authentication host *<IPaddress>***" command deletes the RADIUS authentication server

Parameters: *<ipv4-address >|<ipv6-address>* stands for the server IPv4/IPv6 address; ***<port-number>*** for listening port number, from 0 to 65535, where 0 stands for non-authentication server usage; **primary** for primary server.

Command mode: Global Mode

Default: No RADIUS authentication server is configured by default.

Usage Guide: This command is used to specify the IPv4/IPv6 address and port number of the specified RADIUS server for switch authentication, multiple command instances can be configured. The port parameter is used to specify authentication port number, which must be the same as the specified authentication port in the RADIUS server, the default port number is 1812. If this port number is set to 0, the specified server is regard as non-authenticating. This command can be used repeatedly to configure multiple RADIUS servers communicating with the switch, the configured order is used as the

priority for the switch authentication server. If **primary** is specified, then the specified RADIUS server will be the primary server.

Example: Setting the RADIUS authentication server address as 200.1.1.1.

Switch(Config)#radius-server authentication host 200.1.1.1

23.3.20 radius-server dead-time

Command: radius-server dead-time <*minutes*>

no radius-server dead-time

Function: Configures the restore time when RADIUS server is down; the "**no radius-server dead-time**" command restores the default setting.

Parameters: < *minute* > is the down -restore time for RADIUS server in minutes, the valid range is 1 to 255.

Command mode: Global Mode

Default: The default value is 5 minutes.

Usage Guide: This command specifies the time to wait for the RADIUS server to recover from inaccessible to accessible. When the switch acknowledges a server to be inaccessible, it marks that server as having invalid status, after the interval specified by this command; the system resets the status for that server to valid.

Example: Setting the down-restore time for RADIUS server to 3 minutes.

Switch(Config)#radius-server dead-time 3

23.3.21 radius-server key

Command: radius-server key <*string*>

no radius-server key

Function: Specifies the key for the RADIUS server (authentication and accounting); the "no radius-server key" command deletes the key for RADIUS server.

Parameters: <*string*> is a key string for RADIUS server, up to 16 characters are allowed.

Command mode: Global Mode

Usage Guide: The key is used in the encrypted communication between the switch and the specified RADIUS server. The key set must be the same as the RADIUS server set, otherwise, proper RADIUS authentication and accounting will not perform properly.

Example: Setting the RADIUS authentication key to be "test".

Switch(Config)# radius-server key test

23.3.22 radius-server retransmit

Command: radius-server retransmit <*retries*>

no radius-server retransmit

Function: Configures the re-transmission times for RADIUS authentication packets; the "**no radius-server retransmit**" command restores the default setting

Parameters: <*retries*> is a retransmission times for RADIUS server, the valid range is 0 to 100.

Command mode: Global Mode

Default: The default value is 3 times.

Usage Guide: This command specifies the retransmission time for a packet without a RADIUS server response after the switch sends the packet to the RADIUS server. If authentication information is missing from the authentication server, AAA authentication request will need to be re-transmitted to the authentication server. If AAA request retransmission count reaches the retransmission time threshold without the server responding, the server will be considered to as not working, the switch sets the server as invalid.

Example: Setting the RADIUS authentication packet retransmission time to five times.

Switch(Config)# radius-server retransmit 5

23.3.23 radius-server timeout

Command: radius-server timeout <*seconds*>

no radius-server timeout

Function: Configures the timeout timer for RADIUS server; the "**no radius-server timeout**" command restores the default setting.

Parameters: <*seconds*> is the timer value (second) for RADIUS server timeout, the valid range is 1 to 1000.

Command mode: Global Mode

Default: The default value is 3 seconds.

Usage Guide: This command specifies the interval for the switch to wait RADIUS server response. The switch waits for corresponding response packets after sending RADIUS Server request packets. If RADIUS server response is not received in the specified waiting time, the switch resends the request packet or sets the server as invalid according to the current conditions.

Example: Setting the RADIUS authentication timeout timer value to 30 seconds.

Switch(Config)# radius-server timeout 30

23.4 802.1x Application Example

23.4.1 Examples of Guest Vlan Applications

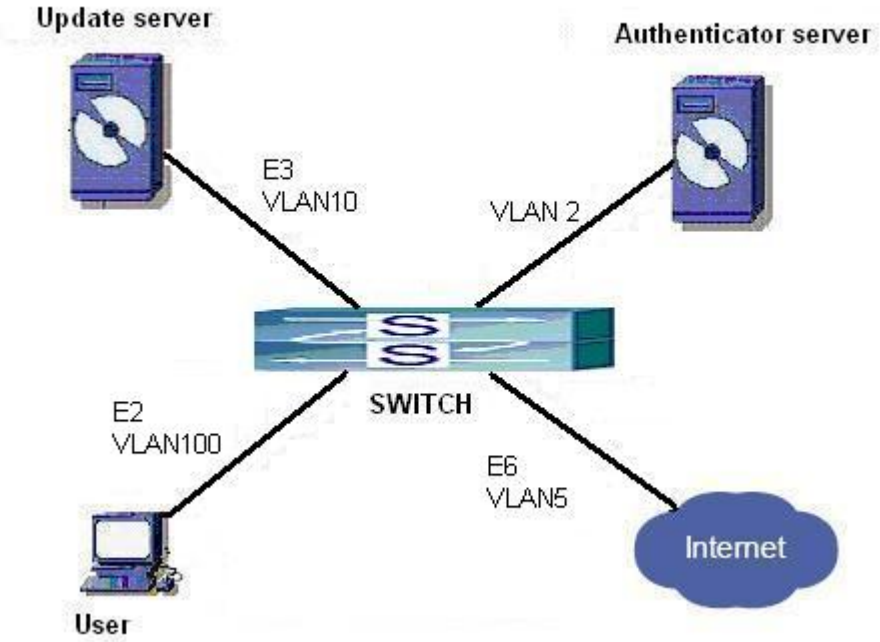


Fig 23-13 The Network Topology of Guest VLAN

Notes: in the figures in this session, E2 means Ethernet 1/2, E3 means Ethernet 1/3 and E6 means Ethernet 1/6.

As showed in the next figure, a switch accesses the network using 802.1x authentication, with a RADIUS server as its authentication server. Ethernet1/2, the port through which the user accesses the switch belongs to VLAN100; the authentication server is in VLAN2; Update Server, being in VLAN10, is for the user to download and update supplicant system software; Ethernet1/6, the port used by the switch to access the Internet is in VLAN5.

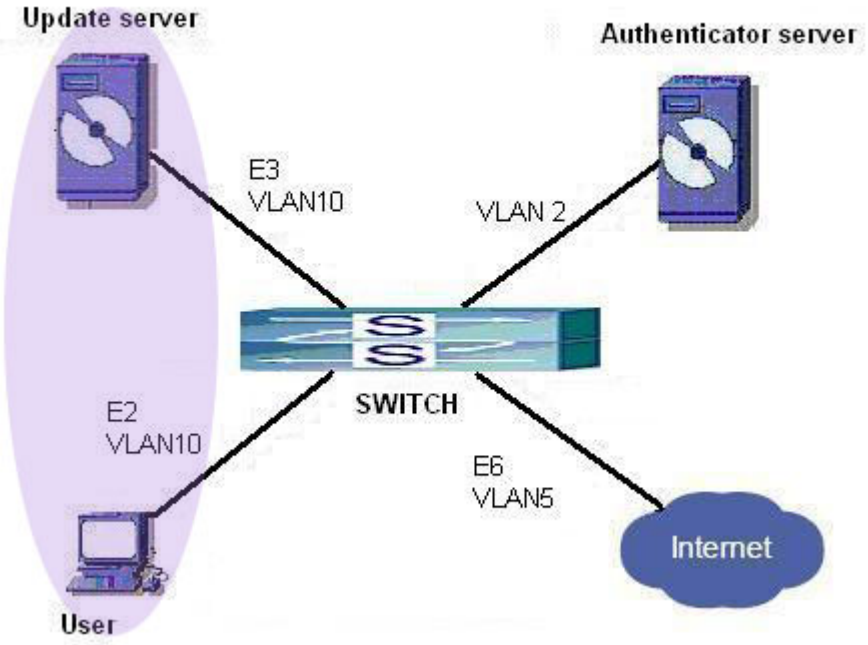


Fig 23-14 User Joining Guest VLAN

As illustrated in the up figure, on the switch port Ethernet1/2, the 802.1x feature is enabled, and the VLAN10 is set as the port's Guest VLAN. Before the user gets authenticated or when the user fails to do so, port Ethernet1/2 is added into VLAN10, allowing the user to access the Update Server.

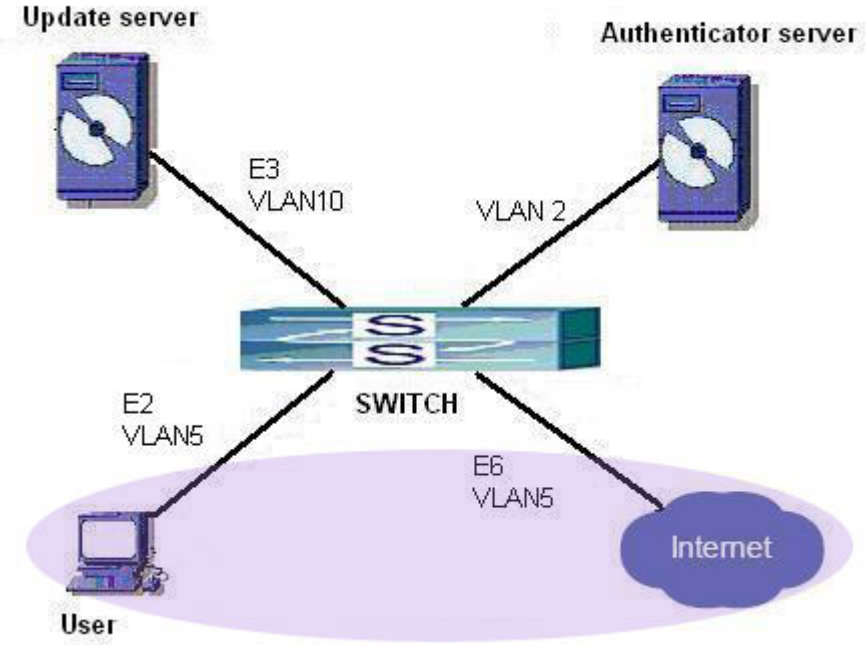


Fig 23-15 User Being Online, VLAN Being Offline

As illustrated in the up figure, when the users become online after a successful

authentication, the authentication server will assign VLAN5, which makes the user and Ethernet1/6 both in VLAN5, allowing the user to access the Internet.

The following are configuration steps:

Configure RADIUS server.

Switch(Config)#radius-server authentication host 10.1.1.3

Switch(Config)#radius-server accounting host 10.1.1.3

Switch(Config)#radius-server key test

Switch(Config)#aaa enable

Switch(Config)#aaa-accounting enable

Create VLAN100.

Switch(Config)#vlan 100

Enable the global 802.1x function

Switch(Config)#dot1x enable

Enable the 802.1x function on port Ethernet1/2

Switch(Config)#interface ethernet 1/2

Switch(Config-Ethernet1/2)#dot1x enable

Set the link type of the port as **access** mode.

Switch(Config-Ethernet1/2)#switch-port mode access

Set the access control mode on the port as **portbased.**

Switch(Config-Ethernet1/2)#dot1x port-method portbased

Set the access control mode on the port as **auto.**

Switch(Config-Ethernet1/2)#dot1x port-control auto

Set the port's Guest VLAN as 100.

Switch(Config-Ethernet1/2)#dot1x guest-vlan 100

Switch(Config-Ethernet1/2)#exit

Using the command of **show running-config** or **show interface ethernet 1/2**, users can check the configuration of Guest VLAN. When there is no online user, no failed user authentication or no user gets offline successfully, and more authentication-triggering messages (EAP-Request/Identity) are sent than the upper limit defined, users can check whether the Guest VLAN configured on the port takes effect

with the command **show vlan id 100**.

23.4.2 Examples of IPv4 Radius Applications

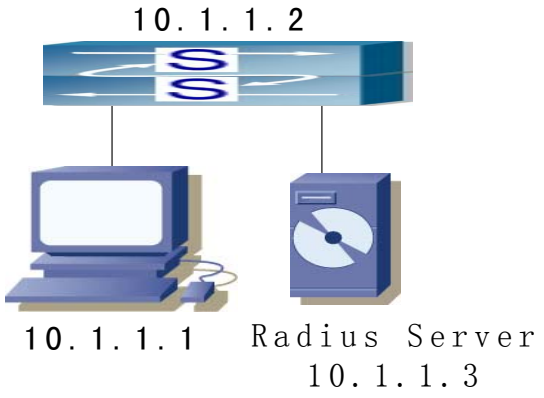


Fig 23-16 IEEE 802.1x Configuration Example Topology

The PC is connecting to port 1/2 of the switch; IEEE 802.1x authentication is enabled on port 1/2; the access mode is the default MAC-based authentication. The switch IP address is 10.1.1.2. Any port other than port 1/2 is used to connect to RADIUS authentication server, which has an IP address of 10.1.1.3, and use the default port 1812 for authentication and port 1813 for accounting. IEEE 802.1x authentication client software is installed on the PC and is used in IEEE 802.1x authentication.

The configuration procedures are listed below:

Switch(Config)#interface vlan 1
Switch(Config-if-vlan1)#ip address 10.1.1.2 255.255.255.0
Switch(Config-if-vlan1)#exit
Switch(Config)#radius-server authentication host 10.1.1.3
Switch(Config)#radius-server accounting host 10.1.1.3
Switch(Config)#radius-server key test
Switch(Config)#aaa enable
Switch(Config)#aaa-accounting enable
Switch(Config)#dot1x enable
Switch(Config)#interface ethernet 1/2
Switch(Config-Ethernet1/2)#dot1x enable
Switch(Config-Ethernet1/2)#dot1x port-control auto
Switch(Config-Ethernet1/2)#exit

23.5 802.1x Troubleshooting

It is possible that 802.1x be configured on ports and 802.1x authentication be settled to auto, but switch can't be to authenticated state after the user runs 802.1x supplicant software. Here are some possible causes and solutions:

- ☞ If 802.1x cannot be enabled for a port, make sure the port is not executing Spanning tree, or MAC binding, or configured as a Trunk port or for port aggregation. To enable the 802.1x authentication, the above functions must be disabled.
- ☞ If the switch is configured properly but still cannot pass through authentication, connectivity between the switch and RADIUS server, the switch and 802.1x client should be verified, and the port and VLAN configuration for the switch should be checked, too.
- ☞ Check the event log in the RADIUS server for possible causes. In the event log, not only unsuccessful logins are recorded, but prompts for the causes of unsuccessful login. If the event log indicates wrong authenticator password, radius-server key parameter shall be modified; if the event log indicates no such authenticator, the authenticator needs to be added to the RADIUS server; if the event log indicates no such login user, the user login ID and password may be wrong and should be verified and input again.
- ☞ Too frequent access to RADIUS data such as run "show aaa" commands may cause the user to be unable to pass through the authentication due to RADIUS data share violation. And the same reason may force users to go offline on re-authentication in the use. As a result, it is recommended to minimize operation to RADIUS data when users are authenticating or re-authenticating.

23.5.1 Commands for Monitor and debug

23.5.1.1 debug aaa

Command:debug aaa

no debug aaa

Function: Enables AAA debugging information; the " **no debug aaa"** command disables the AAA debugging information**.**

Command mode: Admin Mode

Parameters: N/A.

Usage Guide:Enabling AAA debugging information allows the check of RADIUS negotiation process and is helpful in troubleshooting.

Example: Enabling AAA debugging information.

Switch#debug aaa

23.5.1.2 debug dot1x

Command: debug dot1x

no debug dot1x

Function: Enables dot1x debugging information; the " **no debug dot1x"** command disables the dot1x debugging information**.**

Command mode: Admin Mode

Parameters: N/A.

Usage Guide: Enabling dot1x debug information allows the check of dot1x protocol negotiation process and is helpful in troubleshooting.

Example: Enabling dot1x debugging information.

Switch#debug dot1x

23.5.1.3 show aaa authenticated-user

Command: show aaa authenticated-user

Function: Displays the authenticated users online.

Command mode: Admin Mode

Usage Guide: Usually the administrator is concerned only with the online user information, the other information displayed is used for troubleshooting by technical support.

Example:

Switch#show aaa authenticated-user

---------- authenticated users ----------

UserName Retry RadID Port EapID ChapID OnTime UserIP MAC

---------- total: 0 ----------

23.5.1.4 show aaa authenticating-user

Command: show aaa authenticating-user

Function: Display the authenticating users.

Command mode: Admin Mode

Usage Guide: Usually the administrator concerns only information about the authenticating user , the other information displays is used for troubleshooting by the technical support.

Example:

Switch#show aaa authenticating-user

---------- authenticating users ----------

User-name Retry-time Radius-ID Port Eap-ID Chap-ID Mem-Addr State

---

---------- total: 0 ----------

23.5.1.5 show aaa config

Command: show aaa config

Function: Displays the configured commands for the switch as a RADIUS client.

Command mode: Admin Mode

Usage Guide: Displays whether AAA authentication, accounting are enabled and information for key, authentication and accounting server specified.

Example:

Switch#show aaa config（For Boolean value, 1 stands for TRUE and 0 for FALSE）

---------- AAA config data ----------

Is Aaa Enabled = 1

Is Account Enabled= 1

MD5 Server Key = aa

authentication server sum = 2

authentication server[0].Host IP = 30.1.1.30

.Udp Port = 1812

.Is Primary = 1

.Is Server Dead = 0

.Socket No = 0

authentication server[1].Host IP = 192.168.1.218

.Udp Port = 1812

.Is Primary = 0

.Is Server Dead = 0

.Socket No = 0

accounting server sum = 2

accounting server[0].Host IP = 30.1.1.30

.Udp Port = 1813

.Is Primary = 1

.Is Server Dead = 0

.Socket No = 0

accounting server[1].Host IP = 192.168.1.218

.Udp Port = 1813

.Is Primary = 0

.Is Server Dead = 0

.Socket No = 0

Time Out = 3

Retransmit = 3

Dead Time = 5

Account Time Interval = 0

Displayed information	Description
Is AAA Enabled	Indicates whether AAA authentication is enabled or not. 1 for enable and 0 for disable.
Is Account Enabled	Indicates whether AAA accounting is enabled or not. 1 for enable and 0 for disable.
MD5 Server Key	Displays the key for RADIUS server.
authentication server sum	The number of authentication servers.
authentication server[X].Host IP .Udp Port .Is Primary .Is Server Dead .Socket No	Displays the authentication server number and corresponding IP address, UDP port number, Primary server or not, down or not, and socket number.
accounting server sum	The number of accounting servers.
accounting server[X].Host IP .Udp Port .Is Primary .Is Server Dead .Socket No	Displays the accounting server number and corresponding IP address, UDP port number, Primary server or not, down or not, and socket number.
Time Out	Displays the timeout value for RADIUS server.
Retransmit	Displays the retransmission times for RADIUS server authentication packets.
Dead Time	Displays the down-restoration time for RADIUS server.
Account Time Interval	Displays accounting time interval.

23.5.1.6 show dot1x

Command: show dot1x [interface <*interface-list*>]

Function: Displays dot1x parameter related information, if parameter information is added, corresponding dot1x status for corresponding port is displayed.

Parameters: ***<interface-list>*** is the port list. If no parameter is specified, information for all ports is displayed.

Command mode: Admin Mode

Usage Guide: The dot1x related parameter and dot1x information can be displayed with "show dot1x" command.

Example:

1. Display information about dot1x global parameter for the switch.

```
Switch#show dot1x
Global 802.1x Parameters
   reauth-enabled          no
   reauth-period           3600
   quiet-period            10
   tx-period               30
   max-req                  2
   authenticator mode      passive

Mac Filter Disable
MacAccessList :
dot1x-EAPoR Enable

802.1x is enabled on ethernet 1
Authentication Method:Port based
   Status                  Authorized
   Port-control            Auto
   Supplicant              00-03-0F-FE-2E-D3

Authenticator State Machine
   State                   Authenticated
Backend State Machine
   State                   Idle
Reauthentication State Machine
   State                   Stop
```

Displayed information	Explanation
Global 802.1x Parameters	Global 802.1x parameter information
reauth-enabled	Whether re-authentication is enabled or not

reauth-period	Re-authentication interval
quiet-period	Silent interval
tx-period	EAP retransmission interval
max-req	EAP packet retransmission interval
authenticator mode	Switch authentication mode
Mac Filter	Enables dot1x address filter or not
MacAccessList	Dot1x address filter table
Dot1x-EAPoR	Authentication method used by the switch (EAP relay, EAP local end)
802.1x is enabled on ethernet 1	Indicates whether dot1x is enabled for the port
Authentication Method:	Port authentication method (MAC-based, port-based)
Status	Port authentication status
Port-control	Port authorization status
Supplicant	Authenticator MAC address
Authenticator State Machine	Authenticator state machine status
Backend State Machine	Backend state machine status
Reauthentication State Machine	Re-authentication state machine status

23.5.1.7 show radius count

Command: show radius {authencated-user|authencating-user} count

Function: Displays the statistics for users of RADIUS authentication.

Parameters: **authencated-user** displays the authenticated users online;

authencating-user displays the authenticating users.

Command mode: Admin Mode

Usage Guide: The statistics for RADIUS authentication users can be displayed with the "show radius count" command.

Example:

1. Display the statistics for RADIUS authenticated users.

Switch #show radius authencated-user count

---------- Radius user statistic----------

The authencated online user num is: 1

The total user num is: 1

2. Display the statistics for RADIUS authenticated users and others.

Switch #sho radius authencating-user count

---------- Radius user statistic----------

The authencating user num is: 0

The stopping user num is: 0

The stopped user num is: 0
The total user num is: 1

23.6 Web Management

Click “Authentication configuration”, to open authentication configuration management list. Users may configure switch 802.1x authentication function.

23.6.1 RADIUS client configuration

Click “Authentication configuration”, “RADIUS client configuration”, to open Radius client configuration management list Users may the configure switch Radius client.

23.6.1.1 RADIUS global configuration

Click “Authentication configuration”, “RADIUS client configuration”, “RADIUS global configuration” to configure Radius global configuration information:

- Authentication status -Enables, disables switch AAA authentication function. Disable radius Authentication, disable AAA authentication function; Enable radius Authentication, enable
- AAA authentication function.
- Accounting Status -Enables, disables switch AAA accounting function. Disable Accounting, disable accounting function; Enable Accounting, enable accounting function.
- RADIUS key -Configures RADIUS server authentication key.（includes authentication and accounting）
- System recovery time (1-255 minutes) -Configures the recover time after RADIUS server dead. Equivalent to 2.2.2.18.
- RADIUS Retransmit times (0-100) -Configures the number of RADIUS authentication message retransmit times.
- RADIUS server timeout (1-1000 seconds) -Configures RADIUS server timeout timer.

Example: Choose Authentication status as Enable radius Authentication, select Accounting Status as Enable Accounting, configure RADIUS key as “aaa”, configure System recovery time as 10 seconds, configure RADIUS Retransmit times as 5 times, configure RADIUS server timeout as 30 seconds, and lastly, click Apply button. The configuration will then be applied to the switch.

RADIUS configuration	
Authentication status	Enable radius Authentication
Accounting Status	Enable Accounting
RADIUS key	aaa
System recovery time	10
RADIUSRetransmit times(0-100)	5
RADIUS server timeout(1-1000 second)	30

23.6.1.2 RADIUS authentication configuration

Click “Authentication configuration”, “RADIUS client configuration”, “RADIUS authentication configuration” to configure the RADIUS authentication server IP address and monitor port ID.

- Authentication server IP -Server IP address. Authentication server port (optional) - Is the server monitor port ID, with range: 0~65535, where “0” means it are not working as an authentication server.
- Primary authentication server-Primary Authentication server, is the primary server; Non-Primary Authentication server, is the non-primary server.
- Operation type -Add authentication server, adds an authentication server; Remove authentication server, remove an authentication server.

Example: Configure Authentication server IP as 10.0.0.1, Authentication server port as default port, select Primary Authentication server, choose Operation type as “Add authentication server”, and then click the Apply button, to add this authentication server.

RADIUS authentication server configuration	
Authentication server IP	10.0.0.1
Authentication server port(optional)	
Primary authentication server	Primary authentication server
Operation type	Add authenticating server

RADIUS server configuration list		
Server IP	Port num	Primary server

23.6.1.3 RADIUS accounting configuration

Click “Authentication configuration”, “RADIUS client configuration”, “RADIUS accounting configuration” to configure the RADIUS accounting server’s IP address and monitor port ID.

Accounting server IP - server IP address.

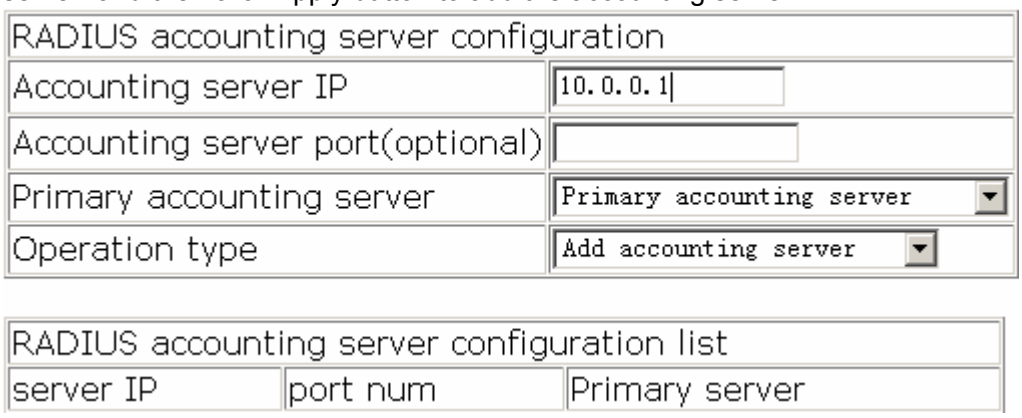
Accounting server port(optional) -is the accounting server port ID, with range: 0~65535,

where “0” means that it’s not work as authentication server.

Primary accounting server -Primary Accounting server, is the primary server; Non-Primary Accounting server, is the non-primary server.

Operation type -Add accounting server, adds an accounting server; Remove accounting server, removes an accounting server

Example: Configure Accounting server IP as 10.0.0.1, Accounting server port as default port, choose Primary accounting server, choose Operation type as “Add accounting server” and then click Apply button to add the accounting server.



23.6.2 802.1X configuration

Click “Authentication configuration”, “802.1X configuration” to open the 802.1x function configuration management list and configure the switch 802.1x function.

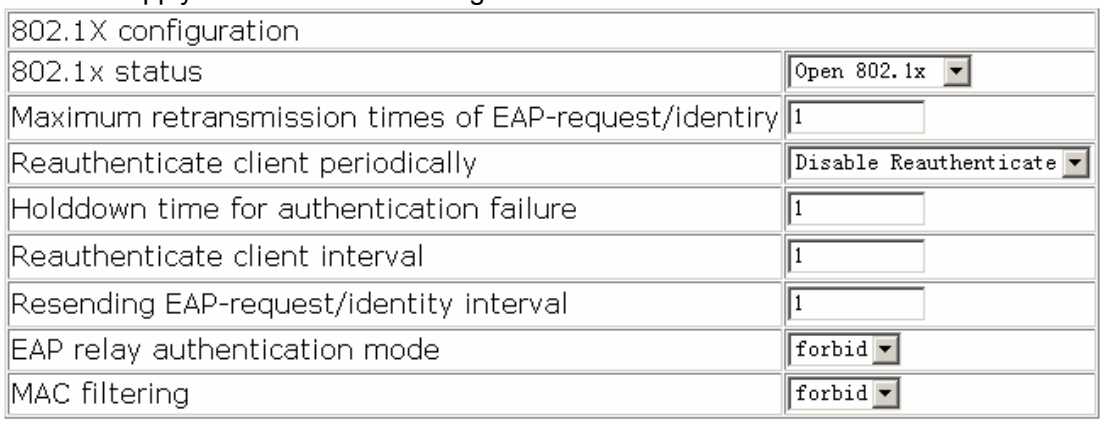
23.6.2.1 802.1X configuration

Click “Authentication configuration”, “802.1X configuration”, “802.1X configuration” to configure the 802.1x global configurations:

- 802.1x status -Enables, disables the switch 802.1x function.
- Maximum retransmission times of EAP-request/identity(1-10 second) - Configures sending EAP-request/MD5 frame the maximum times before switch did not receive suppliant response and restart authentication.
- Re-authenticate client periodically - permit, forbid to make seasonal re-authentication for suppliant.
- Holddown time for authentication failure(1-65535 second) - Configures suppliant quiet-period status time after authentication failure.
- Re-authenticate client interval(1-65535 second) - Configures time interval of switch re-authentication client.
- Resending EAP-request/identity interval(1-65535 second) - Configures time interval of switch retransfer EAP-request/identity frame to suppliant.

- EAP relay authentication mode - Configures switch to adopt EAP relay method to make authentication; use the “no” command to configure switch to adopt EAP local terminating method to make authentication.
- MAC filtering -Enables, disables the switch dot1x address filter function.

Example: Choose 802.1x status as Open 802.1x, Configure Maximum retransmission times of EAP-request/identity as 1, choose Re-authenticate client periodically as Disable Re-authenticate, configure Holddown time for authentication failure as 1, configure Reauthenticate client interval as 1, configure Resending EAP-request/identity interval as 1, choose EAP relay authentication mode as forbid, choose MAC filtering as forbid and then click Apply button to set the configurations.



23.6.2.2 802.1X port authentication configuration

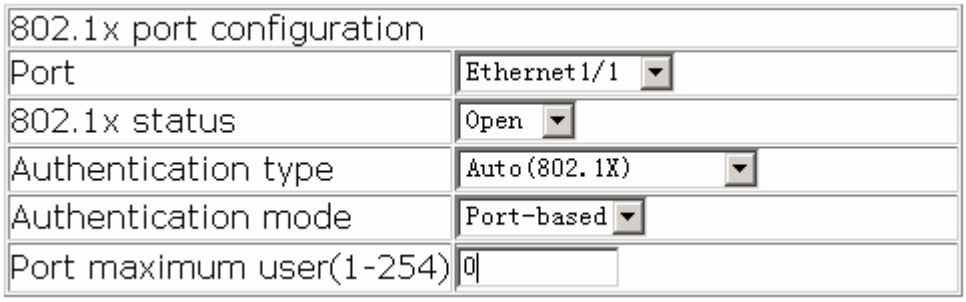
Click “Authentication configuration”, “802.1X configuration”, “802.1X port authentication configuration” to Configure port 802.1x function

- Port -assigns port
- 802.1x status -port 802.1x status, Open, 802.1x function is open; Close, 802.1x function is close.
- Authentication type - Configures port 802.1x authentication status. Auto means enable 802.1x authentication. According to switch and suppliant authentication information, to confirm that the port is in authenticated status or unauthenticated status, force-authorized is configured port as authenticated status, allowing unauthenticated data to pass across the port; for force-unauthorized configure port unauthenticated status, switch not provide suppliant authentication service in this port, not permit any port pass across this port.
- Authentication mode -Configures the access control method for a specific port. Mac-based is access control method which is based on MAC address; port-based

access control method which is based on port.

- Port maximum user(1-254) - Configures the permission maximum user for specific port.

Example: Choose Ethernet port1/1, choose 802.1x status as Open, choose Authentication type as auto, choose Authentication mode as port based, configure Port maximum user as 10 and then click the Set button to apply this configuration to switch.

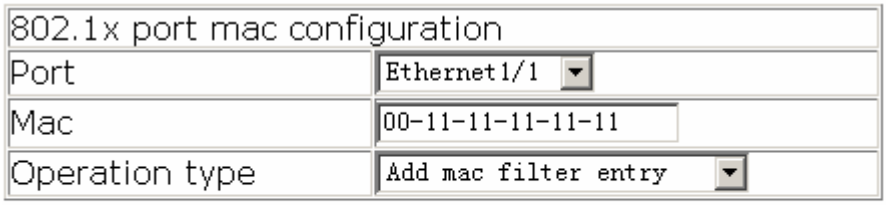


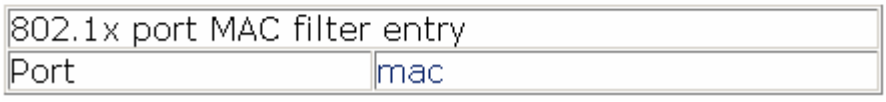
23.6.2.3 802.1X port mac configuration

Click “Authentication configuration”, “802.1X configuration”, “802.1x port mac configuration” to Add a MAC address table to dot1x address filter.

- Port -If specify port, the added list only suitable for specific port, specify All Ports, the added list suitable for all port.
- Mac -adds MAC address
- Operation type -adds, removes filter MAC

Example: Choose Ethernet port 1/1, configure MAC as 00-11-11-11-11-11, choose Operation type as Add mac filter entry, and then click the Apply button to apply this configuration to switch.





23.6.2.4 802.1X port status list

Click “Authentication configuration”, “802.1X configuration”, and “802.1x port status list” to display port 802.1x configuration information, and make re-authentication for the specific port.

- Port -assign port
- 802.1x status -port 802.1x status
- Authentication type -Authentication type

- Authentication status -Authentication status
- Authentication mode -Authentication mode

Example: Choose Ethernet port 1/1, then Click Reauthenticate button, the user in Ethernet port 1/1 will be force to make re-authentication.

802.1x port status list	
Port	Ethernet1/1
802.1x status	Open
Authentication type	force-unauthorized
Authentication status	Authenticated
Authentication mode	Mac-based
	Reauthenticate

Chapter 24 The Number Limitation Function Of Port, MAC in VLAN and IP Configuration

24.1 Introduction to the Number Limitation Function of Port, MAC in VLAN and IP

MAC address list is used to identify the mapping relationship between the destination MAC addresses and the ports of switch. There are two kinds of MAC addresses in the list: static MAC address and dynamic MAC address. The static MAC address is set by users, having the highest priority (will not be overwritten by dynamic MAC address), and will always be effective; dynamic MAC address is learnt by the switch through transmitting data frames, and will only be effective in a specific time range. When the switch receives a data framed waiting to be transmitted, it will study the source MAC address of the data frame, build a mapping relationship with the receiving port, and then look up the MAC address list for the destination MAC address. If any matching list entry is found, the switch will transmit the data frame via the corresponding port, or, the switch will broadcast the data frame over the VLAN it belongs to. If the dynamically learnt MAC address matches no transmitted data in a long time, the switch will delete it from the MAC address list.

Usually the switch supports both the static configuration and dynamic study of MAC address, which means each port can have more than one static set MAC addresses and dynamically learnt MAC addresses, and thus can implement the transmission of data traffic between port and known MAC addresses. When a MAC address becomes out of date, it will be dealt with broadcast. No number limitation is put on MAC address of the ports of our current switches; every port can have several MAC addressed either by configuration or study, until the hardware list entries are exhausted. To avoid too many MAC addresses of a port, we should limit the number of MAC addresses a port can have.

For each INTERFACE VLAN, there is no number limitation of IP; the upper limit of the number of IP is the upper limit of the number of user on an interface, which is, at the same time, the upper limit of ARP and ND list entry. There is no relative configuration command can be used to control the sent number of these list entries. To enhance the

security and the controllability of our products, we need to control the number of MAC address on each port and the number of ARP, ND on each INTERFACE VLAN. The number of static or dynamic MAC address on a port should not exceed the configuration. The number of user on each VLAN should not exceed the configuration, either.

Limiting the number of MAC and ARP list entry can avoid DOS attack to a certain extent. When malicious users frequently do MAC or ARP cheating, it will be easy for them to fill the MAC and ARP list entries of the switch, causing successful DOS attacks.

To summer up, it is very meaningful to develop the number limitation function of port, MAC in VLAN and IP. ES4700BD series switch can control the number of MAC address of ports and the number ARP, ND list entry of ports and VLAN through configuration commands.

Limiting the number of dynamic MAC and IP of ports:

1. Limiting the number of dynamic MAC. If the number of dynamically learnt MAC address by the switch is already larger than or equal with the max number of dynamic MAC address, then shutdown the MAC study function on this port, otherwise, the port can continue its study.

2. Limiting the number of dynamic IP. If the number of dynamically learnt ARP and ND by the switch is already larger than or equal with the max number of dynamic ARP and ND, then shutdown the ARP and ND study function of this port, otherwise, the port can continue its study.

Limiting the number of dynamic MAC and IP of interfaces:

1. Limiting the number of dynamic MAC. If the number of dynamically learnt MAC address by the VLAN of the switch is already larger than or equal with the max number of dynamic MAC address, then shutdown the MAC study function of all the ports in this VLAN, otherwise, all the ports in this VLAN can continue their study (except special ports).

2. Limiting the number of dynamic IP. If the number of dynamically learnt ARP and ND by the switch is already larger than or equal with the max number of dynamic ARP and ND, then the VLAN will not study any new ARP or ND, otherwise, the study can be continued.

24.2 The Number Limitation Function of Port, MAC in VLAN and IP Configuration Task Sequence

1. Enable the number limitation function of MAC、IP on ports
2. Enable the number limitation function of MAC、IP in VLAN
3. Configure the timeout value of querying dynamic MAC.

4．Display and debug the relative information of number limitation of MAC、IP on ports

1． Enable the number limitation function of MAC、IP on ports

Command	Explanation
Port configuration mode	
switchport mac-address dynamic maximum <value> **no switchport mac-address dynamic maximum**	Enable and disable the number limitation function of MAC on the ports
switchport arp dynamic maximum <value> **no switchport arp dynamic maximum**	Enable and disable the number limitation function of ARP on the ports
switchport nd dynamic maximum <value> **no switchport nd dynamicmaximum**	Enable and disable the number limitation function of ND on the ports

2． Enable the number limitation function of MAC、IP in VLAN

Command	Explanation
Interface configuration mode	
Ip mac-address dynamic maximum <value> **no ip mac-address dynamicmaximum**	Enable and disable the number limitation function of MAC in the VLAN
Ip arp dynamic maximum <value> **no ip arp dynamic maximum**	Enable and disable the number limitation function of ARP in the VLAN
Ipv6 nd dynamic maximum <value> **no ipv6 nd dynamic maximum**	Enable and disable the number limitation function of NEIGHBOR in the VLAN

3． Configure the timeout value of querying dynamic MAC.

Command	Explanation
Global configuration mode	
mac-address query timeout <seconds>	Configure the timeout value of querying dynamic MAC.

4． Display and debug the relative information of number limitation of MAC、IP on ports

Command	Explanation
Admin mode	
show mac-address dynamic count {vlan <vlan-id>|interface ethernet <portName>}	Display the number of dynamic MAC in corresponding ports and VLAN
show arp-dynamic count {vlan <vlan-id>|interface ethernet <portName>}	Display the number of dynamic ARP in corresponding ports and VLAN
show nd-dynamic count {vlan <vlan-id>|interface ethernet <portName>}	Display the number of dynamic NEIGHBOUR in corresponding ports and VLAN
debug switchport mac count **no debug switchport mac count**	All kinds of debug information when limiting the number of MAC on ports
debug switchport arp count **no debug switchport arp count**	All kinds of debug information when limiting the number of ARP on ports
debug switchport nd count **no debug switchport nd count**	All kinds of debug information when limiting the number of NEIGHBOUR on ports
debug ip mac count **no debug ip mac count**	All kinds of debug information when limiting the number of MAC in VLAN
debug ip arp count **no debug switchport mac count**	All kinds of debug information when limiting the number of ARP in VLAN
debug ipv6 nd count **no debug switchport mac count**	All kinds of debug information when limiting the number of NEIGHBOUR in VLAN

24.3 Command for The Number Limitation Function of Port, MAC in VLAN and IP

24.3.1 switchport mac-address dynamic maximum

Command：switchport mac-address dynamic maximum <*value*>

no switchport mac-address dynamic maximum

Function：Set the max number of dynamic MAC address allowed by the port, and, at the same time, enable the number limitation function of dynamic MAC address on the port; "no switchport mac-address dynamic maximum" command is used to disable the number limitation function of dynamic MAC address on the port.

Parameters：**<*value*>** upper limit of the number of dynamic MAC address of the port, ranging from 1 to 4096.

Default Settings：The number limitation function of dynamic MAC address on the port is disabled.

Command Mode：Port mode.

Usage Guide：When configuring the max number of dynamic MAC address allowed by the port, if the number of dynamically learnt MAC address on the port is already larger than the max number of dynamic MAC address to be set, the extra dynamic MAC addresses will be deleted. This function is mutually exclusive to functions such as dot1x, MAC binding, if the functions of dot1x, MAC binding or TRUNK are enabled on the port, this function will not be allowed.

Examples：

Enable the number limitation function of dynamic MAC address in port 1/2 mode, the max number to be set is 20

Switch(Config)#interface ethernet 1/2

Switch(Config-Ethernet1/2)# switchport mac-address dynamic maximum 20

Disable the number limitation function of dynamic MAC address in port 1/2 mode.

Switch(Config-Ethernet1/2)#no switchport mac-address dynamic maximum

24.3.2 ip mac-address dynamic maximum

Command：**ip mac-address dynamic maximum <*value*>**

no ip mac-address dynamic maximum

Function：Set the max number of dynamic MAC address allowed in the VLAN, and, at the same time, enable the number limitation function of dynamic MAC address in the VLAN; "no ip mac-address dynamic maximum" command is used to disable the number limitation function of dynamic MAC address in the VLAN.

Parameters：**<*value*>** upper limit of the number of MAC address in the VLAN, ranging from 1 to 4096.

Default Settings：The number limitation function of dynamic MAC address in the VLAN is disabled.

Command Mode：Interface mode.

Usage Guide：When configuring the max number of dynamic MAC allowed in the VLAN, if the number of dynamically learnt MAC address in the VLAN is already larger than the

max number to be set, the extra dynamic MAC addresses will be deleted. After enabling number limitation function of dynamic MAC in the VLAN, the number limitation of MAC is only applied to general access port, the number of MAC on TURNK ports and special ports which has enabled dot1x, MAC binding function will not be limited or counted.

Examples：

Enable the number limitation function of dynamic MAC address in VLAN 1, the max number to be set is 50

Switch(Config)#interface ethernet 1/2

Switch(Config-if-Vlan1)# ip mac-address dynamic maximum 50

Enable the number limitation function of dynamic MAC address in VLAN 1.

Switch(Config-if-Vlan1)#no ip mac-address dynamic maximum

24.3.3 switchport arp dynamic maximum

Command：switchport arp dynamic maximum <*value*>

no switchport arp dynamic maximum

Function：Set the max number of dynamic ARP allowed by the port, and, at the same time, enable the number limitation function of dynamic ARP on the port; “no switchport arp dynamic maximum” command is used to disable the number limitation function of dynamic ARP on the port.

Parameters：<*value*> upper limit of the number of dynamic ARP of the port, ranging from 1 to 4096.

Default Settings：The number limitation function of dynamic ARP on the port is disabled.

Command Mode：Port mode.

Usage Guide：When configuring the max number of dynamic ARP allowed by the port, if the number of dynamically learnt ARP on the port is already larger than the max number to be set, the extra dynamic ARP will be deleted. TRUNK ports do not supports this function.

Examples：

Enable the number limitation function of dynamic ARP in port 1/2 mode, the max number to be set is 20

Switch(Config)#interface ethernet 1/2

Switch(Config-Ethernet1/2)# switchport arp dynamic maximum 20

Disable the number limitation function of dynamic ARP in port 1/2 mode.

Switch(Config-Ethernet1/2)#no switchport arp dynamic maximum

24.3.4 switchport nd dynamic maximum

Command：switchport nd dynamic maximum <*value*>

no switchport nd dynamic maximum

Function：Set the max number of dynamic NEIGHBOR allowed by the port, and, at the same time, enable the number limitation function of dynamic NEIGHBOR on the port; “no switchport nd dynamic maximum” command is used to disable the number limitation function of dynamic NEIGHBOR on the port.

Parameters：**<***value***>** upper limit of the number of dynamic NEIGHBOR of the port, ranging from 1 to 4096.

Default Settings：The number limitation function of dynamic ARP on the port is disabled.

Command Mode：Port mode.

Usage Guide：When configuring the max number of dynamic NEIGHBOR allowed by the port, if the number of dynamically learnt NEIGHBOR on the port is already larger than the max number to be set, the extra dynamic NEIGHBOR will be deleted. TRUNK ports do not supports this function.

Examples：

Enable the number limitation function of dynamic NEIGHBOR in port 1/2 mode, the max number to be

20.

Switch(Config)#interface ethernet 1/2

Switch(Config-Ethernet1/2)# switchport nd dynamic maximum 20

Disable the number limitation function of dynamic NEIGHBOR in port 1/2 mode.

Switch(Config-Ethernet1/2)#no switchport nd dynamic maximum

24.3.5 ip arp dynamic maximum

Command：ip arp dynamic maximum <*value*>

no ip arp dynamic maximum

Function：Set the max number of dynamic ARP allowed in the VLAN, and, at the same time, enable the number limitation function of dynamic ARP in the VLAN; “no ip arp dynamic maximum” command is used to disable the number limitation function of dynamic ARP in the VLAN.

Parameters：**<***value***>** upper limit of the number of dynamic ARP in the VLAN, ranging from 1 to 4096.

Default Settings：the number limitation function of dynamic ARP in the VLAN is disabled.

Command Mode：Interface mode.

Usage Guide：When configuring the max number of dynamic ARP allowed in the VLAN, if the number of dynamically learnt ARP in the VLAN is already larger than the max number to be set, the extra dynamic ARP will be deleted.

Examples：

Enable the number limitation function of dynamic ARP in VLAN 1, the max number to be set is 50

Switch(Config)#interface ethernet 1/2

Switch(Config-if-Vlan1)# ip arp dynamic maximum 50

Disable the number limitation function of dynamic ARP in VLAN 1

Switch(Config-if-Vlan1)#no ip arp dynamic maximum

24.3.6 ipv6 nd dynamic maximum

Command：ipv6 nd dynamic maximum <*value*>

no ipv6 nd dynamic maximum

Function：Set the max number of dynamic NEIGHBOR allowed in the VLAN, and, at the same time, enable the number limitation function of dynamic NEIGHBOR in the VLAN; “no ipv6 nd dynamic maximum” command is used to disable the number limitation function of dynamic NEIGHBOR in the VLAN.

Parameters：<*value*> upper limit of the number of dynamic NEIGHBOR in the VLAN, ranging from 1 to 4096.

Default Settings：the number limitation function of dynamic NEIGHBOR in the VLAN is disabled.

Command Mode：Interface mode.

Usage Guide：When configuring the max number of dynamic NEIGHBOR allowed in the VLAN, if the number of dynamically learnt NEIGHBOR in the VLAN is already larger than the max number to be set, the extra dynamic NEIGHBOR will be deleted.

Examples：

Enable the number limitation function of dynamic NEIGHBOR in VLAN 1, the max number to be set is 50

Switch(Config)#interface ethernet 1/2

Switch(Config-if-Vlan1)# ipv6 nd dynamic maximum 50

Disable the number limitation function of dynamic NEIGHBOR in VLAN 1

Switch(Config-if-Vlan1)#no ipv6 nd dynamic maximum

24.3.7 mac-address query timeout

Command：mac-address query timeout <*seconds*>

Function：Set the timeout value of querying dynamic MAC

Parameter：<*seconds*> is timeout value, in second, ranging from 5 to 300

Default Settings：Default value is 60 seconds

Command Mode：Global mode

Usage Guide：After enabling the number limitation of MAC, users can use this command to configure the timeout value of querying dynamic MAC. If the data traffic is very large, the timeout value can be shorter, otherwise, it can be longer. Users can set it according to actual situation.

Examples：

Set the timeout value of quering dynamic MAC as 30 seconds

Switch(Config)# mac-address query timeout 30

24.3.8 show mac-address dynamic count

Command：**show mac-address dynamic count { (vlan <1-4096>)| interface ethernet *<portName>*}**

Function：Display the number of dynamic MAC of corresponding port and VLAN.

Parameters：***<vlan-id>***display the specified vlan ID. ***<portName>*** is the name of layer-2 port

Command Mode：Admin Mode

Usage Guide：Use this command to display the number of dynamic MAC of corresponding port and VLAN.

Examples：Display the number of dynamic MAC of the port and VLAN which are configured with number limitation function of MAC

Switch(Config)# show mac-address dynamic count interface ethernet 1/3

Port	MaxCount	CurrentCount
Ethernet1/3	5	1

Switch(Config)# show mac-address dynamic count vlan 1

Vlan	MaxCount	CurrentCount
1	55	15

24.3.9 show arp-dynamic count

Command：**show arp-dynamic count { (vlan <1-4096>)| interface ethernet *<portName>*}**

Function：Display the number of dynamic ARP of corresponding port and VLAN.**Parameters**：***<vlan-id>*** is play the specified vlan ID.***<portName>*** is the name of layer-2 port

Command Mode：Admin Mode

Usage Guide：Use this command to display the number of dynamic ARP of corresponding port and VLAN.

Examples：Display the number of dynamic ARP of the port and VLAN which are configured with number limitation function of ARP

```
Switch(Config)# show arp-dynamic count interface ethernet 1/3
 Port                MaxCount                CurrentCount
-------------------------------------------------------------------------------------------------
 Ethernet1/3              5                       1
-------------------------------------------------------------------------------------------------
Switch(Config)# show arp-dynamic count vlan 1
 Vlan                MaxCount                CurrentCount
-------------------------------------------------------------------------------------------------
 1                        55                      15
-------------------------------------------------------------------------------------------------
```

24.3.10 show nd-dynamic count

Command：**show nd-dynamic count { (vlan <1-4096>)| interface ethernet *<portName>*}**

Function：Display the number of dynamic ND of corresponding port and VLAN.

Parameters：***<vlan-id>*** is play the specified vlan ID.***<portName>*** is the name of layer-2 port

Command Mode：Admin Mode

Usage Guide：Use this command to display the number of dynamic ND of corresponding port and VLAN.

Examples：Display the number of dynamic ND of the port and VLAN which are configured with number limitation function of ND

```
Switch(Config)# show nd-dynamic count interface ethernet 1/3
 Port                MaxCount                CurrentCount
-------------------------------------------------------------------------------------------------
 Ethernet1/3              5                       1
-------------------------------------------------------------------------------------------------
```

Switch(Config)# show nd-dynamic count vlan 1

Vlan	MaxCount	CurrentCount
1	55	15

24.3.11 debug switchport mac count

Command：debug switchport mac count

no debug switchport mac count

Function：When the number limitation function debug of mac on the port, if the number of dynamic MAC and the number of MAC on the port is larger than the max number allowed, users will see debug information.” no debug switchport mac count” command is used to disable the number limitation function debug of mac on the port.

Parameters：None

Command Mode：Admin Mode

Default Settings：None

Usage Guide：Display the debug information of the number of dynamic mac on the port

Examples：

Switch#debug switchport mac count

%Jun 14 16:04:40 2007 Current mac count 21 is more than or equal to the maximum limit in port Ethernet3/1

!!%Jun 14 16:04:40 2007 Mac learning will be stopped and some mac will be delete !!

24.3.12 debug switchport arp count

Command：debug switchport arp count

no debug switchport arp count

Function：When the number limitation function debug of arp on the port, if the number of dynamic arp and the number of arp on the port is larger than the max number allowed, users will see debug information.” no debug switchport arp count” command is used to disable the number limitation function debug of arp on the port.

Parameters：None

Command Mode：Admin Mode

Default Settings：None

Usage Guide：Display the debug information of the number of dynamic arp on the port

Examples：

Switch#debug switchport arp count

%Jun 14 16:04:40 2007 Current arp count 21 is more than or equal to the maximum limit in port Ethernet3/1

!!%Jun 14 16:04:40 2007 Arp learning will be stopped and some mac will be delete !!

24.3.13 debug switchport nd count

Command：debug switchport nd count

no debug switchport nd count

Function：When the number limitation function debug of nd on the port, if the number of dynamic nd and the number of nd on the port is larger than the max number allowed, users will see debug information.” no debug switchport nd count” command is used to disable the number limitation function debug of nd on the port.

Parameters：None

Command Mode：Admin Mode

Default Settings：None

Usage Guide：Display the debug information of the number of dynamic nd on the port

Examples：

Switch#debug switchport arp count

%Jun 14 16:04:40 2007 Current neighbor count 21 is more than or equal to the maximum limit in port Ethernet3/1

!!%Jun 14 16:04:40 2007 Neighbor learning will be stopped and some mac will be delete !!

24.3.14 debug ip mac count

Command：debug ip mac count

no debug ip mac count

Function：When the number limitation function debug of mac in the VLAN, if the number of dynamic mac and the number of mac in the VLAN is larger than the max number allowed, users will see debug information.” no debug ip mac count” command is used to disable the number limitation function debug of mac in the VLAN.

Parameters：None

Command Mode：Admin Mode

Default Settings：None

Usage Guide：Display the debug information of the number of dynamic mac in the VLAN.

Examples：

Switch#debug ip mac count

%Jun 14 16:04:40 2007 Current mac count 21 is more than or equal to the maximum limit in vlan 1!!

%Jun 14 16:04:40 2007 Mac learning will be stopped and some mac will be delete !!

24.3.15 debug ip arp count

Command：debug ip arp count

no debug ip arp count

Function：When the number limitation function debug of arp in the VLAN, if the number of dynamic arp and the number of arp in the VLAN is larger than the max number allowed, users will see debug information.” no debug ip arp count” command is used to disable the number limitation function debug of arp in the VLAN.

Parameters：None

Command Mode：Admin Mode

Default Settings：None

Usage Guide：Display the debug information of the number of dynamic arp in the VLAN.

Examples：

Switch#debug ip mac count

%Jun 14 16:04:40 2007 Current arp count 21 is more than or equal to the maximum limit in vlan 1!!

%Jun 14 16:04:40 2007Arp learning will be stopped and some arp will be delete !!

24.3.16 debug ipv6 nd count

Command：debug ipv6 nd count

no debug ipv6 nd count

Function：When the number limitation function debug of neighbor in the VLAN, if the number of dynamic neighbor and the number of neighbor in the VLAN is larger than the max number allowed, users will see debug information.” no debug ip neighbor count” command is used to disable the number limitation function debug of neighbor in the VLAN.

Parameters：None

Command Mode：Admin Mode

Default Settings：None

Usage Guide：Display the debug information of the number of dynamic neighbor in the VLAN.

Examples：

Switch#debug ip mac count

%Jun 14 16:04:40 2007 Current neighbor count 21 is more than or equal to the maximum limit in vlan 1!!

%Jun 14 16:04:40 2007Neighbor learning will be stopped and some neighbor will be delete !!

24.4 The Number Limitation Function of Port, MAC in VLAN and IP Typical Examples

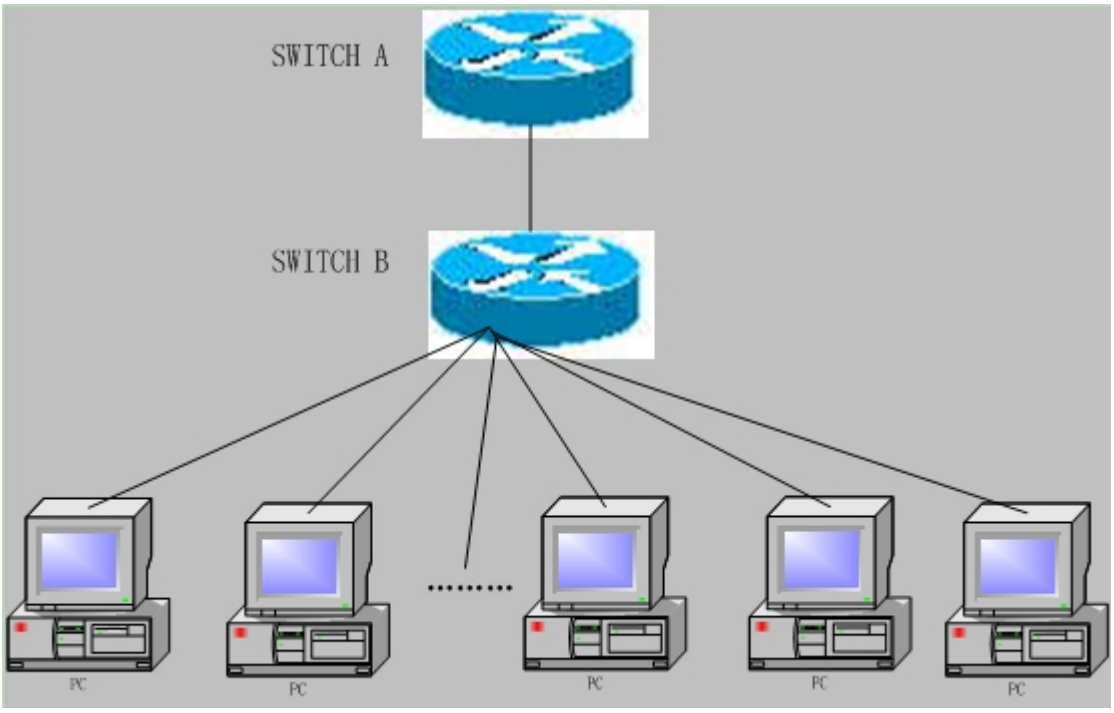


Fig 24-1 The Number Limitation of Port, MAC in VLAN and IP Typical Configuration Example

In the network topology above, SWITCH B connects to many PC users, before enabling the number limitation function of port, MAC in VLAN and IP, if the system hardware has no other limitation, SWTICH A and SWTICH B can get the MAC, ARP, ND list entries of all the PC, so limiting the MAC, ARP list entry can avoid DOS attack to a certain extent. When malicious users frequently do MAC or ARP cheating, it will be easy for them to fill the MAC and ARP list entries of the switch, causing successful DOS attacks. Limiting the MAC, ARP list entry can prevent DOS attack.

On port 3/1 of SWITCH A, set the max number can be learnt of dynamic MAC

address as 20, of dynamic ARP address as 20, NEIGHBOR list entry as 10. In VLAN 1, set the max number of dynamic MAC address as 30, of dynamic ARP address as 30, NEIGHBOR list entry as 20.

SWITCH A configuration task sequence:
Switch(config)#
Switch (config)#int ethernet 3/1
Switch (Config-If-Ethernet3/1)#switchport mac-address dynamic maximum 20
Switch (Config-If-Ethernet3/1)#switchport arp dynamic maximum 20
Switch (Config-If-Ethernet3/1)#switchport nd dynamic maximum 10
Switch (Config-if-Vlan1)#ip mac-address dynamic maximum 30
Switch (Config-if-Vlan1)#ip arp dynamic maximum 30
Switch (Config-if-Vlan1)#ipv6 nd dynamic maximum 20

24.5 The Number Limitation Function Of Port, MAC in VLAN and IP Troubleshooting Help

The number limitation function of port, MAC in VLAN and IP is disabled by default, if users need to limit the number of user accessing the network, they can enable it. If the number limitation function of MAC address can not be configured, please check whether Spanning-tree, dot1x, TRUNK is running on the switch and whether the port is configured as a MAC-binding port. The number limitation function of MAC address is mutually exclusive to these configurations, so if the users need to enable the number limitation function of MAC address on the port, they should check these functions mentioned above on this port are disabled.

If all the configurations are normal, after enabling the number limitation function of port, MAC in VLAN and IP, users can use debug commands to debug every limitation, check the details of number limitations and judge whether the number limitation function is correct. If there is any problem, please sent result to technical service center.

Chapter 25 VRRP Configuration

25.1 Introduction to VRRP

VRRP (Virtual Router Redundancy Protocol) is a fault tolerant protocol designed to enhance connection reliability between routers (or L3 Ethernet switches) and external devices. It is developed by the IETF for local area networks (LAN) with multicast/broadcast capability (Ethernet is a Configuration Example) and has wide applications.

All hosts in one LAN generally have a default route configured to specified default gateway, any packet destined to an address outside the native segment will be sent to the default gateway via this default route. These hosts in the LAN can communicate with the external networks. However, if the communication link connecting the router serving as default game and external networks fails, all hosts using that gateway as the default next hop route will be unable to communicate with the external networks.

VRRP emerged to resolve such problem. VRRP runs on multiple routers in a LAN, simulating a "virtual" router (also referred to as a "Standby cluster") with the multiple routes. There is an active router (the "Master") and one or more backup routers (the "Backup") in the Standby cluster. The workload of the virtual router is actually undertaken by the active router, while the Backup routers serve as backups for the active router.

The virtual router has its own "virtual" IP address (can be identical with the IP address of some router in the Standby cluster), and routers in the Standby cluster also have their own IP address. Since VRRP runs on routes or Ethernet Switches only, the Standby cluster is transparent to the hosts with the segment. To them, there exists only the IP address of the Virtual Router instead of the actual IP addresses of the Master and Backup(s). And the default gateway setting of all the hosts uses the IP address of the Virtual Router. Therefore, hosts within the LAN communicate with the other networks via this Virtual Router. But basically, they are communicating with the other networks via the Master. In the case when the Master of the Standby cluster fails, a backup will take over its task and become the Master to serve all the hosts in the LAN, so that uninterrupted communication between LAN hosts and external networks can be achieved.

To sum it up, in a VRRP Standby cluster, there is always a router/Ethernet serving as the active router (Master), while the rest of the Standby cluster servers act as the backup router(s) (Backup, can be multiple) and monitor the activity of Master all the time. Should the Master fail, a new Master will be elected by all the Backups to take over the

work and continue serving the hosts within the segment. Since the election and take-over duration is brief and smooth, hosts within the segment can use the Virtual Router as normal and uninterrupted communication can be achieved.

25.2 Configuration Task List

1) Create/Remove the Virtual Router (required)
2) Configure VRRP dummy IP and interface (required)
3) Activate/Deactivate Virtual Router (required)
4) Configure VRRP authentication (optional)
5) Configure VRRP sub-parameters (optional)
6) Configure the preemptive mode for VRRP
7) Configure VRRP priority
8) Configure VRRP Timer intervals
9) Configure VRRP interface monitor

1. Create/Remove the Virtual Router

Command	Explanation
Global Mode	
[no] router vrrp <*vrid*>	Creates/Removes the Virtual Router

2. Configure VRRP Dummy IP Address and Interface

Command	Explanation
VRRP protocol configuration mode	
virtual-ip <*ip*> **no virtual-ip**	Configures VRRP Dummy IP address; **the "no virtual-ip"** command removes the virtual IP address.
interface{IFNAME | Vlan <*ID*>} **no interface**	Configures VRRP interface, the "no interface" command removes the interface

3. Activate/Deactivate Virtual Router

Command	Explanation
VRRP protocol configuration mode	
Enable	Activates the Virtual Router
Disable	Deactivates the Virtual Router

4. Configure VRRP Authentication

Command	Explanation
Interface Mode	
ip vrrp authentication string <*string*> **no ip vrrp authentication string**	Configures the simple authentication strings for VRRP packets sending on the interface, the **"no ip vrrp authentication string"** command removes the authentication string.

5. Configure VRRP Sub-parameters

(1) Configure the preemptive mode for VRRP

Command	Explanation
VRRP protocol configuration mode	
preempt-mode {true| false}	Configures the preemptive mode for VRRP

(2) Configure VRRP priority

Command	Explanation
VRRP protocol configuration mode	
Priority < *priority* >	Configures VRRP priority

(3) Configure VRRP Timer intervals

Command	Explanation
VRRP protocol configuration mode	
advertisement-interval <time>	Configures VRRP timer value (in seconds)

(4) Configure VRRP interface monitor

Command	Explanation
VRRP protocol configuration mode	
circuit-failover {IFNAME | Vlan <*ID*>} **no circuit-failover**	Configures VRRP interface monitor, the **"no circuit-failover"** removes monitor to the interface

25.3 Commands for VRRP

25.3.1 advertisement-interval

Commands:advertisement-interval <*adver_interval*>

no advertisement-interval

Function: Sets the vrrp timer values; the **"no advertisement-interval"** command restores the default setting.

Parameters: <***adver_interval***> is the interval for sending VRRP packets in seconds, ranging from 1 to 10.

Default: The default **<*adver_interval*>** is 1second.

Command mode: VRRP protocol configuration mode

Usage Guide:The Master in a VRRP Standby cluster will send VRRP packets to member routers (or L3 Ethernet switch) to announce its properness at a specific interval; this interval is referred to as *adver_interval*. If a Backup does not receive the VRRP packets sent by the Master after a certain period (specified by *master_down_interval*), then it assume the Master is no longer operating properly, therefore turns its status to Master.

The user can use this command to adjust the VRRP packet sending interval of the Master. For members in the same Standby cluster, this property should be set to a same value. To Backup, the value of *master_down_interval* is three times that of adver_interval. Extraordinary large traffic or timer setting differences between routers (or L3 Ethernet switches) may result in *master_down_interval* and invoke instant status changes. Such situations can be avoided through extending *adver_interval* interval and setting longer preemptive delay time.

Example: Configuring vrrp Timer value to 3

Switch(Config-Router-Vrrp)# advertisement-interval 3

25.3.2 circuit-failover

Commands:circuit-failover <*ifname*> <*value_reduced*>

no circuit-failover

Function: Configures the vrrp monitor interface

Parameters: < *ifname* > is the name for the interface to be monitored

<*value_reduced*> stands for the amount of priority decreased, the default value is 1~253

Default: Not configured by default.

Command mode: VRRP protocol configuration mode

Usage Guide: The interface monitor function is a valuable extension to backup function, which not only enable VRRP to provide failover function on router (or L3 Ethernet switch) fail, but also allow decreasing the priority of a router (or L3 Ethernet switch) to ensure smooth implementation of backup function when status of that network interface is **down**.

When this command is used, if the status of an interface monitored turns from **up** to **down**, then the priority of that very router (or L3 Ethernet switch) in its Standby cluster will decrease, lest Backup cannot changes its status due to lower priority than the Master when the Master fails.

Example: Configuring vrrp monitor interface to vlan 2 and decreasing amount of priority to 10.

Switch(Config-Router-Vrrp)# circuit-failover vlan 2 10

25.3.3 debug vrrp

Commands: debug vrrp [**all | event | packet** [**recv| send**]]

no debug vrrp [**all | event | packet** [**recv| send**]]

Function: Displays information for VRRP standby cluster status and packet transmission; the **"no debug vrrp"** command disables the debug information.

Default: Debugging information is disabled by default.

Command mode: Admin Mode

Example:

Switch#debug vrrp

VRRP SEND[Hello]: Advertisement sent for vrid=[10], virtual-ip=[10.1.10.1]

VRRP SEND[Hello]: Advertisement sent for vrid=[10], virtual-ip=[10.1.10.1]

VRRP SEND[Hello]: Advertisement sent for vrid=[10], virtual-ip=[10.1.10.1]

VRRP SEND[Hello]: Advertisement sent for vrid=[10], virtual-ip=[10.1.10.1]

25.3.4 disable

Commands: disable

Function: Deactivates VRRP

Parameters: N/A.

Default: Not configured by default.

Command mode: VRRP protocol configuration mode

Usage Guide: Deactivates a Virtual Router. VRRP configuration can only be modified when VRRP is deactivated.

Example: Deactivating a Virtual Router numbered as 10

Switch(config)# router vrrp 10

Switch (Config-Router-Vrrp)# disable

25.3.5 enable

Commands: enable

Function: Activates VRRP

Parameters: N/A.

Default: Not configured by default.

Command mode: VRRP protocol configuration mode

Usage Guide: Activates the appropriate Virtual Router. Only a router (or L3 Ethernet switch) interface started by this enable command is part of Standby cluster. VRRP virtual IP and interface must be configured first before starting Virtual Router.

Example: Activating the Virtual Router of number 10

Switch(config)# router vrrp 10

Switch(Config-Router-Vrrp)# enable

25.3.6 interface

Commands: interface{IFNAME | Vlan <*ID*>}

no interface

Function: Configures the VRRP interface

Parameters: interface{IFNAME | Vlan <*ID*>} stands for the interface name.

Default: Not configured by default.

Command mode: VRRP protocol configuration mode

Usage Guide: This command adds a layer 3 interface to an existing Standby cluster. The "**no interface**" command removes the L3 interface from the specified Standby cluster.

Example: Configuring the interface as "interface vlan 1"

Switch(Config-Router-Vrrp)# interface vlan 1

25.3.7 preempt-mode

Commands: preempt-mode{true| false}

Function: Configures the preemptive mode for VRRP

Parameters: N/A.

Command mode: VRRP protocol configuration mode

Default: Preemptive mode is set by default

Usage Guide: If a router (or L3 Ethernet switch) requiring high priority needs to preemptively become the active router (or L3 Ethernet switch), the preemptive mode should be enabled.

Example: Setting non-preemptive VRRP mode

Switch(Config-Router-Vrrp)# preempt-mode false

25.3.8 priority

Commands: priority <*value*>

no priority

Function: Configures VRRP priority; the **"no priority"** restores the default value 100. Priority is always 254 for IP Owner.

Parameters: < *value*> is the priority value, ranging from 1 to 254.

Default: The priority of all **backup** routers (or L3 Ethernet switch) in a Standby cluster is 100; the Master router (or L3 Ethernet switch) in all Standby cluster is always 254.

Command mode: VRRP protocol configuration mode

Usage Guide: Priority determines the ranking of a router (or L3 Ethernet switch) in a Standby cluster, the higher priority the more likely to become the Master. When a router (or L3 Ethernet switch) is configured as Master dummy IP address, its priority is always 254 and does not allow modification. When 2 or more routers (or L3 Ethernet switch) with the same priority value present in a Standby cluster, the router (or L3 Ethernet switch) with the greatest VLAN interface IP address becomes the Master.

Example: Setting VRRP priority to 150.

Switch(Config-Router-Vrrp)# priority 150

25.3.9 router vrrp

Commands: router vrrp <*vrid*>

no router vrrp <*vrid*>

Function: Creates/Removes the Virtual Router

Parameters: < *vrid* > is the Virtual Router number ranging from 1 to 255.

Default: Not configured by default.

Command mode: Global Mode

Usage Guide: This command is used to create/remove Virtual Router, which is identified by a unique Virtual Router number. Virtual Router configurations are only available when a Virtual Router is created.

Example: Configuring a Virtual Router with number 10

Switch(config)# router vrrp 10

25.3.10 show vrrp

Commands: show vrrp [**<*vrid*>**]

Function: Displays status and configuration information for the VRRP standby cluster.

Command mode: All Modes

Example:

```
Switch# show vrrp
  VrId <1>
  State is Initialize
  Virtual IP is 10.1.20.10 (Not IP owner)
  Interface is Vlan2
  Priority is 100
  Advertisement interval is 1 sec
  Preempt mode is TRUE
VrId <10>
  State is Initialize
  Virtual IP is 10.1.10.1 (IP owner)
  Interface is Vlan1
  Configured priority is 255, Current priority is 255
  Advertisement interval is 1 sec
  Preempt mode is TRUE
  Circuit failover interface Vlan1, Priority Delta 10, Status UP
```

Displayed information	Explanation
State	Status
Virtual IP	Dummy IP address
Interface	Interface Name
Priority	Priority
Advertisement interval	Timer interval
Preempt	Preemptive mode
Circuit failover interface	Interface Monitor information

25.3.11 virtual-ip

Commands: virtual-ip <*A.B.C.D*>

no virtual-ip

Function: Configures the VRRP dummy IP address

Parameters: <***A.B.C.D***> is the IP address in decimal format.

Default: Not configured by default.

Command mode: VRRP protocol configuration mode

Usage Guide: This command adds a dummy IP address to an existing Standby cluster. The "no virtual-ip" command removes the dummy IP address from the specified Standby cluster. Each Standby cluster can have only one dummy IP.

Example: Setting the backup dummy IP address to 10.1.1.1.

Switch(Config-Router-Vrrp)# virtual-ip 10.1.1.1

25.4 Typical VRRP Scenario

As shown in the figure below, SwitchA and SwitchB are Layer 3 Ethernet Switches in the same group and provide redundancy for each other.

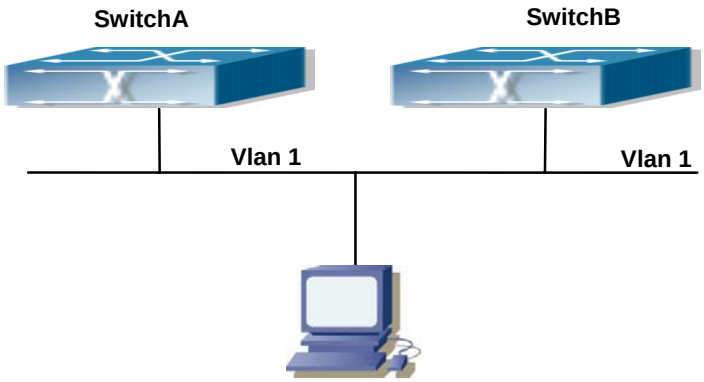


Fig 25-1 VRRP Network Topology

Configuration of SwitchA:

SwitchA(config)#interface vlan 1

SwitchA (Config-If-Vlan1)# ip address 10.1.1.1 255.255.255.0

SwitchA (Config-If-Vlan1)#exit

SwitchA (config)#router vrrp 1

SwitchA(Config-Router-Vrrp)# virtual-ip 10.1.1.5

SwitchA(Config-Router-Vrrp)# interface vlan 1

SwitchA(Config-Router-Vrrp)# enable

Configuration of SwitchB:

SwitchB(config)#interface vlan 1

SwitchB (Config-if-Vlan1)# ip address 10.1.1.7 255.255.255.0

SwitchB (Config-if-Vlan1)#exit

SwitchB(config)#router vrrp 1

SwitchB (Config-Router-Vrrp)# virtual-ip 10.1.1.5

SwitchB(Config-Router-Vrrp)# interface vlan 1

SwitchB(Config-Router-Vrrp)# enable

25.5 VRRP Troubleshooting

In configuring and using VRRP protocol, the VRRP protocol may fail to run properly due to reasons such as physical connection failure or wrong configurations. The user should ensure the following:

- ✧ Good condition of the physical connection.
- ✧ All interface and link protocols are in the UP state (use “show interface” command).
- ✧ Ensure VRRP is enabled on the interface.
- ✧ Verify the authentication mode of different routers (or L3 Ethernet switches) in the same standby cluster are the same.
- ✧ Verify the timer time of different routers (or L3 Ethernet switches) in the same standby cluster are the same.
- ✧ Verify the dummy IP address is in the same network segment of the interface’s actual IP address.
- ✧ If VRRP problems persist after the above-mentioned procedures, please run debugging commands like “debug vrrp”, and copy the DEBUG information in 3 minutes and send the information to Edge-Core technical service center.

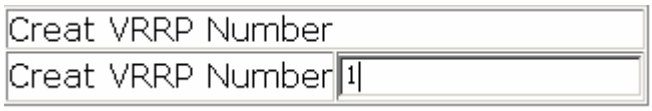
25.6 Web Management

Click “VRRP control” to enter VRRP control configuration mode to manage VRRP features for the switch.

25.6.1 Create VRRP Number

Click “VRRP control” to enter "Create VRRP Number".

Example: Enter 1 for virtual router number and click Apply to create a virtual router with VRRP number 1. Click Remove to remove Virtual Router 1.

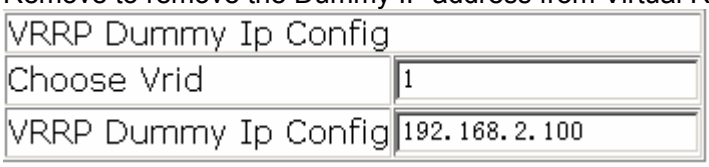


25.6.2 Configure VRRP Dummy IP

Click “VRRP control” to configure VRRP and enter "VRRP Dummy IP Config".

Example: Enter the created Virtual Router number 1, VRRP Dummy IP address 192.168.2.100. Click Apply to add the Dummy IP address to Virtual Router number. Click

Remove to remove the Dummy IP address from Virtual Router number 1.



25.6.3 Configure VRRP Port

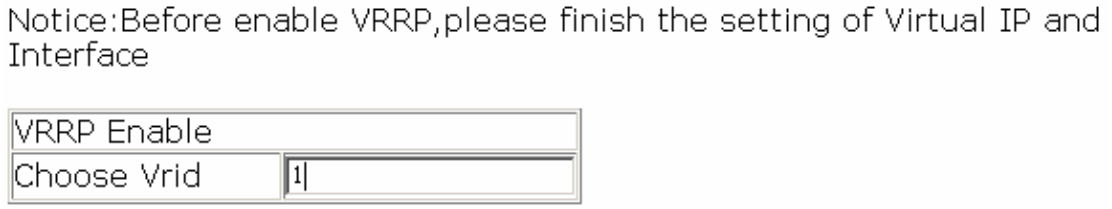
Click “VRRP control” to configure VRRP and enter "VRRP Port".

Example: Enter created Virtual Router number "1" and VLAN port IP "23". Click Apply to add port 23 to Virtual Router number 1. Click Remove to remove port 23 from Virtual Router number 1.

25.6.4 Activate Virtual Router

Click “VRRP control” to configure VRRP and enter "Enable Virtual Router".

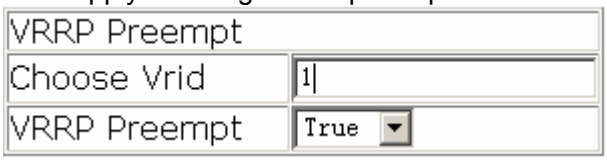
Example: Enter the created Virtual Router number "1". Click Enable to activate Virtual Router number 1. Click Disable to deactivate Virtual Router number 1.



25.6.5 Configure Preemptive Mode For VRRP

Click “VRRP control” to configure VRRP and enter "VRRP Preempt".

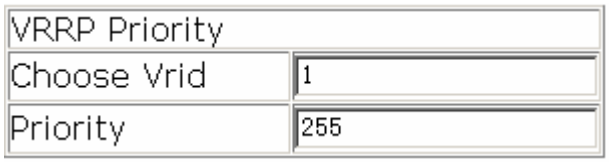
Example: Enter "1" for Virtual Router number and choose TRUE for "VRRP Preempt". Click Apply to configure the preemptive mode for virtual router number 1 to "True".



25.6.6 Configure VRRP priority

Click “VRRP control” to configure VRRP and enter "VRRP Priority".

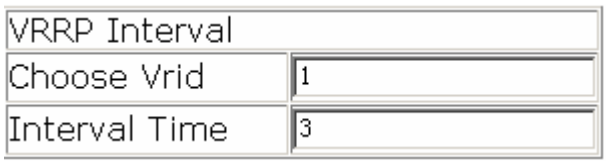
Example: Enter the created Virtual Router number "1" and priority. Click Enable to set the priority of virtual router number 1 to "255". Click Disable to disable the priority of Virtual Router number 1.



25.6.7 Configure VRRP Timer interval

Click “VRRP control” to configure VRRP and enter "VRRP Interval".

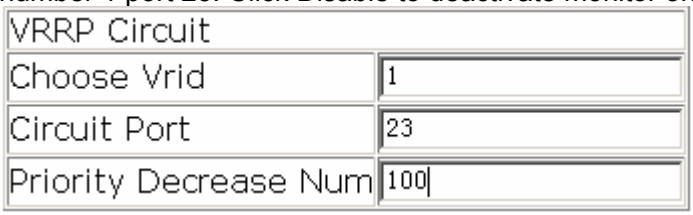
Example: Enter created Virtual Router number "1" and interval "3". Click Enable to set the interval of virtual router number 1 to "3". Click Disable to disable the interval of Virtual Router number 1.



25.6.8 Configure VRRP Interface Monitor

Click “VRRP control” to configure VRRP and enter "VRRP Circuit".

Example: Enter "1" for the created Virtual Router number, 23 for monitor port name and 100 for priority decreasing amount. Click Enable to activate monitor on Virtual Router number 1 port 23. Click Disable to deactivate monitor on Virtual Router number 1 port 23.



25.6.9 Configure Authentication Mode For VRRP

Click “VRRP control” to enter "VRRP AuthenMode" and configure VRRP authentication mode.

Example: Choose created "Vlan1" for Port and "yes" for AuthenMode. Click Apply to finish Port Vlan1 authentication mode configuration.

VRRP AuthenMode	
Port	Vlan1
AuthenMode	yes

Chapter 26 MRPP Configuration

26.1 MRPP introduction

MRPP (Multi-layer Ring Protection Protocol), is a link layer protocol applied on Ethernet loop protection. It can avoid broadcast storm caused by data loop on Ethernet ring, and restore communication among every node on ring network when the Ethernet ring has a break link.MRPP is the expansion of EAPS(Ethernet link automatic protection protocol).

MRPP protocol is similar to STP protocol on function, MRPP has below characters, compare to STP protocol:

<1> MRPP specifically uses to Ethernet ring topology

<2> fast convergence, less than 1 s. ideally it can reach 100- 50 ms.

26.1.1 Conception Introduction

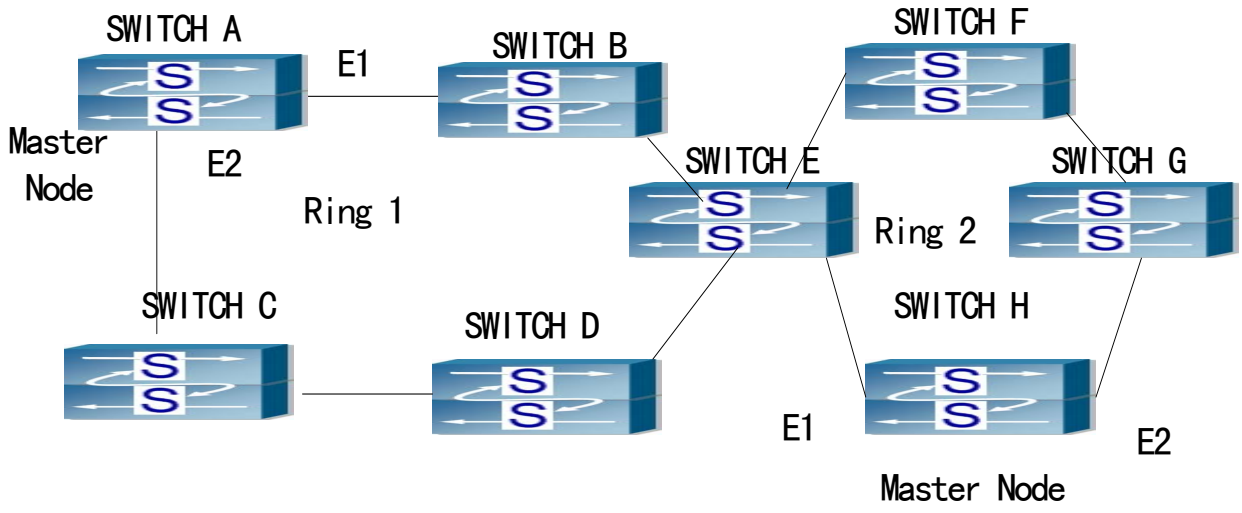


Fig 26-1MRPP Sketch Map

1.Control VLAN

Control VLAN is a virtual VLAN, only used to identify MRPP protocol packet transferred in the link. To avoid confusion with other configured VLAN, avoids configuring control VLAN ID to be the same with other configured VLAN ID. The different MRPP ring should configure the different control VLAN ID.

2.Ethernet Ring (MRPP Ring)

Ring linked Ethernet network topology.

Each ring has two states.

Health state: The whole ring net work physical link is connected.

Break state: one or a few physical link break in ring network

3.nodes

Each switch is named after a node on Ethernet. The node has some types:

Primary node: each ring has a primary node, it is main node to detect and defend.

Transfer node: except for primary node, other nodes are transfer nodes on each ring.

The node role is determined by user configuration. As shown 1.1, Switch A is primary node of Ring 1, Switch B. Switch C; Switch D and Switch E are transfer nodes of Ring 1.

4.Primary port and secondary port

The primary node and transfer node have two ports connecting to Ethernet separately, one is primary port, and another is secondary port. The role of port is determined by user configuration.

Primary port and secondary port of primary node

The primary port of primary node is used to send ring health examine packet (hello), the secondary port is used to receive Hello packet sending from primary node. When the Ethernet is in health state, the secondary port of primary node blocks other data in logical and only MRPP packet can pass. When the Ethernet is in break state, the secondary port of primary node releases block state, and forwards data packets.

there are no difference on function between Primary port and secondary port of transfer node.

The role of port is determined by user configuration. As shown 1.1, Switch A E1/1 is primary port, E1/2 is secondary port.

5. Timer

The two timers are used when the primary node sends and receives MRPP protocol packet: Hello timer and Fail Timer.

Hello timer: define timer of time interval of health examine packet sending by primary node primary port.

Fail timer: define timer of overtime interval of health examine packet receiving by primary node primary port. The value of Fail timer must be more than or equal to the 3 times of value of Hello timer.

26.1.2 MRPP Protocol Packet Types

Packet Type	Explanation
Hello packet (Health examine packet) Hello	The primary port of primary node evokes to detect ring, if the secondary port of primary node can receive Hello packet in configured overtime, so the ring is normal.
LINK-DOWN (link Down event packet)	After transfer node detects Down event on port, immediately sends LINK-DOWN packet to primary node, and inform primary node ring to fail.
LINK-DOWN-FLUSH_FDB packet	After primary node detects ring failure or receives LINK-DOWN packet, open blocked secondary port, and then uses two ports to send the packet, to inform each transfer node to refresh own MAC address.
LINK-UP-FLUSH_FDB packet	After primary detects ring failure to restore normal, and uses packet from primary port, and informs each transfer node to refresh own MAC address.

26.1.3 MRPP Protocol Operation System

1. Link Down Alarm system

When transfer node finds themselves belonging to MRPP ring port Down, it sends link Down packet to primary node immediately. The primary node receives link down packet and immediately releases block state of secondary port, and sends LINK-DOWN-FLUSH-FDB packet to inform all of transfer nodes, refreshing own MAC address forward list.

2. Poll System

The primary port of primary node sends Hello packet to its neighbors timely according to configured Hello-timer.

If the ring is health, the secondary port of primary node receives health detect packet, and the primary node keeps secondary port.

If the ring is break, the secondary port of primary node can't receive health detect packet when timer is over time. The primary releases the secondary port block state, and sends LINK-DOWN-FLUSH_FDB packet to inform all of transfer nodes, to refresh own MAC address forward list.

3. Ring Restore

After the primary node occur ring fail, if the secondary port receives Hello packet

sending from primary node, the ring has been restored, at the same time the primary node block its secondary port, and sends its neighbor LINK-UP-Flush-FDB packet.

After MRPP ring port refresh UP on transfer node, the primary node maybe find ring restore after a while. For the normal data VLAN, the network maybe forms a temporary ring and creates broadcast storm. To avoid temporary ring, transfer node finds it to connect to ring network port to refresh UP, immediately block temporarily (only permit control VLAN packet pass), after only receiving LINK-UP-FLUSH-FDB packet from primary node, and releases the port block state.

26.2 MRPP Configuration Task List

1) Globally enable MRPP
2) Configure MRPP ring
3) Display and debug MRPP relevant information

1) Globally enable MRPP

Command	Explanation
Global Mode	
MRPP enable ***no MRPP enable***	Globally enable and disable

2) Configure MRPP ring

Command	Explanation
Global Mode	
MRPP ring <INT> **no MRPP ring <INT>**	Create MRPP ring. format “no” deletes MRPP ring and its configuration
MRPP ring mode	
Control-vlan <INT> **No Control-vlan**	Configure control VLAN ID, format “no” deletes configured control VLAN ID.
Primary-port Ethernet IFNAME	Specify primary port of MRPP ring
Secondary-port Ethernet IFNAME	Specify secondary port of MRPP ring
Node-mode {master | transit}	Configure node type of MRPP ring (primary node or secondary node)
Hello-timer <INT> **No hello-timer**	Configure Hello packet timer sending from primary node of MRPP ring, format “no” restores default timer value

Fail-timer <INT> **No fail-timer**	Configure Hello packet overtime timer sending from primary node of MRPP ring, format “no” restores default timer value
Enable **No enable**	Enable MRPP ring, format “no” disables enabled MRPP ring

3) Display and debug MRPP relevant information

Command	Explanation
Admin Mode	
debug MRPP **no debug MRPP**	Disable MRPP module debug information, format “no” disable MRPP debug information output
Show MRPP {<INT>|}	Display MRPP ring configuration information
Show MRPP statistics {<INT>|}	Display receiving data package statistic information of MRPP ring
clear MRPP statistics {<INT>|}	Clear receiving data package statistic information of MRPP ring

26.3 Commands For MRPP

26.3.1 clear mrpp statistics

Command :clear mrpp statistics {<INT>|}

Function：Clear statistic information of MRPP data package of MRPP ring receiving and transferring.

Parameter： <INT> is MRPP ring Id, the valid range is from 1 to 4096, if not specified ID, it clears all of MRPP ring statistic information.

Command Mode： Admin Mode

Default：

Usage Guide：

Example： Clear statistic information of MRPP ring 4000 of switch.

Switch#clear mrpp statistics 4000

26.3.2 control-vlan

Command：control-vlan <VID>

no control-vlan

Function： Configure control VLAN ID of MRPP ring; the "no control-vlan" command deletes control VLAN ID.

Parameter：*<VID>* expresses control VLAN ID, the valid range is from 1 to 4094.

Command Mode： MRPP ring mode

Default： None

Usage Guide： The command specifies Virtual VLAN ID of MRPP ring, currently it can be any value in 1-4094.To avoid confusion, it is recommended that the ID is non-configured VLAN ID, and the same to MRPP ring ID. In configuration of MRPP ring of the same MRPP loop switches, the control VLAN ID must be the same, otherwise the whole MRPP loop may can't work normally or form broadcast.

Example： Configure control VLAN of mrpp ring 4000 is 4000.

Switch(Config)# mrpp ring 4000

Switch(mrpp-ring-4000)#control-vlan 4000

26.3.3 debug mrpp

Command :debug mrpp

no debug mrpp

Function： Open MRPP debug information; "no description" command disables MRPP debug information

Command Mode： Admin Mode

Parameter： None

Usage Guide： Enable MRPP debug information, and check message process of MRPP protocol and receive data package process, it is helpful to monitor debug.

Example： Enable debug information of MRPP protocol.

Switch#debug mrpp

26.3.4 enable

Command：enable

no enable

Function： Enable configured MRPP ring, the "no enable" command disables this enabled MRPP ring.

Parameter：

Command Mode： MRPP ring mode

Default： Default disable MRPP ring.

Usage Guide： Executing this command, it must enable MRPP protocol, and enable all of option needed to be configured of the MRPP ring.

Example： Configure MRPP ring 4000 of switch to primary node, and enable the MRPP ring.

Switch(Config)# mrpp enable
Switch(Config)# mrpp ring 4000
Switch(mrpp-ring-4000)#control-vlan 4000
Switch(mrpp-ring-4000)#primary-port ethernet 4/1
Switch(mrpp-ring-4000)#secondary-port ethernet 4/3
Switch(mrpp-ring-4000)#fail-timer 18
Switch(mrpp-ring-4000)#hello-timer 6
Switch(mrpp-ring-4000)#enable

26.3.5 fail-timer

Command：fail-timer <INT>

no fail-timer

Function： Configure if the primary node of MRPP ring receive Timer interval of Hello packet or not, the “no fail-timer” command restores default timer interval.

Parameter： ***<INT>*** valid range is from 1 to 3000s.

Command Mode： MRPP ring mode

Default： Default configure timer interval 3s.

Usage Guide： If primary node of MRPP ring doesn’t receives Hello packet from primary port of primary node on configured fail timer, the whole loop is fail. Transfer node of MRPP doesn’t need this timer and configure. To avoid time delay by transfer node forwards Hello packet, the value of fail timer must be more than or equal to 3 times of Hello timer. On time delay loop, it needs to modify the default and increase the value to avoid primary node doesn’t receive Hello packet on fail timer due to time delay.

Example： Configure fail timer of MRPP ring 4000 to 10s.

Switch(Config)# mrpp ring 4000
Switch(mrpp-ring-4000)#fail-timer 10

26.3.6 hello-timer

Command：hello-timer <INT>

no hello-timer

Function： Configure timer interval of Hello packet from primary node of MRPP ring, the “no hello-timer” command restores timer interval of default.

Parameter： ***<INT>*** valid range is from 1 to 100s.

Command Mode： MRPP ring mode

Default： Default configuration timer interval is 1s.

Usage Guide：The primary node of MRPP ring continuously sends Hello packet on configured Hello timer interval, if secondary port of primary node can receive this packet in configured period; the whole loop is normal, otherwise fail. Transfer node of MRPP ring doesn't need this timer and configure.

Example： Configure hello-timer of MRPP ring 4000 to 3 seconds.

Switch(Config)# mrpp ring 4000

Switch(mrpp-ring-4000)#hello-timer 3

26.3.7 mrpp enable

Command：mrpp enable

no mrpp enable

Function： Enable MRPP protocol module, the "**no mrpp enable**" command disables MRPP protocol.

Parameter：

Command Mode： Global Mode

Default： The system doesn't enable MRPP protocol module

Usage Guide： If it needs to configure MRPP ring, it enables MRPP protocol. Executing "no mrpp enable" command, it ensures to disable the switch enabled MRPP ring.

Example： Globally enable MRPP

Switch(Config)#mrpp enable

26.3.8 mrpp ring

Command：mrpp ring <INT>

no mrpp ring <INT>

Function： Create MRPP ring, and access MRPP ring mode, the "no mrpp ring**<INT>**" command deletes configured MRPP ring.

Parameter： ***<INT>*** is MRPP ring ID, the valid range is from 1 to 4096

Command Mode： Global Mode

Usage Guide： If this MRPP ring doesn't exist it create new MRPP ring when executing the command, and then it enter MRPP ring mode. It needs to ensure disable this MRPP ring when executing the "no mrpp ring" command.

Switch(Config)# mrpp ring 100

26.3.9 node-mode

Command： node-mode {maser|transit}

Function： Configure the type of the node to primary node or secondary node.

Parameter：

Command Mode： MRPP ring mode

Default： Default the node mode is secondary node.

Usage Guide：。

Example： Configure the switch to primary node. MRPP ring 4000

Switch(Config)# mrpp ring 4000

Switch(mrpp-ring-4000)#node-mode master

26.3.10 primary-port

Command：primary-port ethernet IFNAME

Function： Specify MRPP ring primary-port

Parameter： IFNAME is port name, the port must be switch layer 2 physical port.

Command Mode： MRPP ring mode

Default： None

Usage Guide： The command specifies MRPP ring primary port. Primary node uses primary port to send Hello packet, secondary port is used to receive Hello packet from primary node. There are no difference on function between primary port and secondary of secondary node.

Example： Configure the primary of MRPP ring 4000 to Ethernet 4/1.

Switch(Config)# mrpp ring 4000

Switch(mrpp-ring-4000)#primary-port ethernet 4/1

26.3.11 secondary-port

Command：secondary-port ethernet IFNAME

Function： Specify secondary of MRPP ring

Parameter： IFNAME is port name, the port must be switch layer 2 physical port

Command Mode： MRPP ring mode

Default： None

Usage Guide： The command specifies secondary port of MRPP ring. The primary node uses secondary port to receive Hello packet from primary node. There are no difference on function between primary port and secondary of secondary node.

Example： Configure secondary port of MRPP ring to 4/3.

Switch(Config)# mrpp ring 4000
Switch(mrpp-ring-4000)#secondary-port Ethernet 4/3 -

26.3.12 show mrpp

Command： show mrpp {<INT>|}
Function： Display MRPP ring configuration.
Parameter： <INT> is MRPP ring ID, the valid range is from 1 to 4096, if not specified ID, it display all of MRPP ring configuration.
Command Mode： Admin Mode
Default：
Usage Guide：
Example： Display configuration of MRPP ring 4000 of switch
Switch# show mrpp 4000

26.3.13 show mrpp statistics

Command： show mrpp statistics {<INT>|}
Function： Display statistic information of data package of MRPP ring receiving and transferring
Parameter： <INT> is MRPP ring ID, the valid range is from 1 to 4096, if not specified ID, it displays all of MRPP ring statistic information.
Command Mode： Admin Mode
Default：
Usage Guide：
Example： Display statistic information of MRPP ring 4000 of switch.
Switch# show mrpp statistic 4000

26.4 MRPP typical scenario

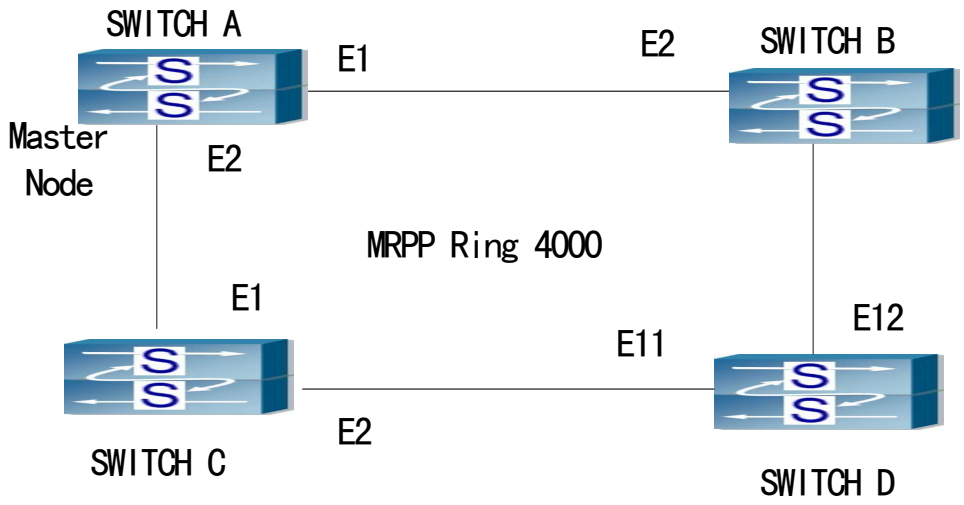


Fig 26-2MRPP typical configuration scenario 1

The above topology often occurs on using MRPP protocol. The multi switch constitutes a single MRPP ring, all of the switches only are configured an MRPP ring, thereby constitutes a single MRPP ring.

In above configuration, SWITCH A configuration is primary node of MRPP ring, and configures E1/1 to primary port, E1/2 to secondary port. Other switches are secondary nodes of MRPP ring, configures primary port and secondary port separately.

To avoid ring, it should temporarily disable one of the ports of primary node, when it enables each MRPP ring in the whole MRPP ring; and after all of the nodes are configured, open the port.

When disable MRPP ring, it needs to insure the MRPP ring doesn't have ring.

SWITCH A configuration Task Sequence:

Switch(Config)#MRPP enable

Switch(Config)#MRPP ring 4000

Switch(MRPP-ring-4000)#control-vlan 4000

Switch(MRPP-ring-4000)#primary-port Ethernet 1/1

Switch(MRPP-ring-4000)#secondary-port Ethernet 1/2

Switch(MRPP-ring-4000)#fail-timer 18

Switch(MRPP-ring-4000)#hello-timer 5

Switch(MRPP-ring-4000)#node-mode master

Switch(MRPP-ring-4000)#enable

Switch(MRPP-ring-4000)#exit

Switch(Config)#

SWITCH B configuration Task Sequence:

Switch(Config)#MRPP enable

```
Switch(Config)#MRPP ring 4000
Switch(MRPP-ring-4000)#control-vlan 4000
Switch(MRPP-ring-4000)#primary-port Ethernet 1/1
Switch(MRPP-ring-4000)#secondary-port Ethernet 1/2
Switch(MRPP-ring-4000)#enable
Switch(MRPP-ring-4000)#exit
Switch(Config)#
```

SWITCH C configuration Task Sequence:

```
Switch(Config)#MRPP enable
Switch(Config)#MRPP ring 4000
Switch(MRPP-ring-4000)#control-vlan 4000
Switch(MRPP-ring-4000)#primary-port Ethernet 1/1
Switch(MRPP-ring-4000)#secondary-port Ethernet 1/2
Switch(MRPP-ring-4000)#enable
Switch(MRPP-ring-4000)#exit
Switch(Config)#
```

SWITCH D configuration Task Sequence:

```
Switch(Config)#MRPP enable
Switch(Config)#MRPP ring 4000
Switch(MRPP-ring-4000)#control-vlan 4000
Switch(MRPP-ring-4000)#primary-port Ethernet 1/11
Switch(MRPP-ring-4000)#secondary-port Ethernet 1/12
Switch(MRPP-ring-4000)#enable
Switch(MRPP-ring-4000)#exit
Switch(Config)#
```

26.5 MRPP troubleshooting

The normal operation of MRPP protocol depends on normal configuration of each switch on MRPP ring, otherwise it is very possible to form ring and broadcast storm:

- Configuring MRPP ring, you'd better disconnected the ring, and wait for each switch configuration, then open the ring.
- When the MRPP ring of enabled switch is disabled on MRPP ring, it ensures the ring of the MRPP ring has been disconnected.
- When there is broadcast storm on MRPP ring, it disconnects the ring firstly, and ensures if each switch MRPP ring configuration on the ring is correct or not; if correct,

restores the ring, and then observes the ring is normal or not.

In normal configuration, it still forms ring broadcast storm or ring block, please open debug function of primary node MRPP, and used show MRPP statistics command to observe states of primary node and transfer node and statistics information is normal or not, and then sends results to our Technology Service Center.

Chapter 27 Cluster Configuration

27.1 Introduction to cluster network management

Cluster network management is an in-band configuration management. Unlike CLI, SNMP and Web Config which implement a direct management of the target switches through a management workstation, cluster network management implements a direct management of the target switches (member switches) through an intermediate switch (commander switch). A commander switch can manage multiple member switches. As soon as a Public IP address is configured in the commander switch, all the member switches which are configured with private IP addresses can be managed remotely. This feature economizes public IP addresses which are short of supply. Cluster network management can dynamically discover cluster feature enabled switches (candidate switches). Network administrators can statically or dynamically add the candidate switches to the cluster which is already established. Accordingly, they can configure and manage the member switches through the commander switch. When the member switches are distributed in various physical locations (such as on the different floors of the same building), cluster network management has obvious advantages. Moreover, cluster network management is an in-band management. The commander switch can communicate with member switches in existing network. There is no need to build a specific network for network management.

Cluster network management has the following features:

- Save IP addresses
- Simplify configuration tasks
- Indifference to network topology and distance limitation
- Auto detecting and auto establishing
- With factory default settings, multiple switches can be managed through cluster network management
- The commander switch can upgrade and configure any member switches in the cluster

27.2 Cluster Network Management Configuration Sequence

1. Enable or disable cluster function
2. Create cluster
    1) Create or delete cluster
    2) Configure private IP address pool for member switches of the cluster
    3) Add or remove a member switch
3. Configure attributes of the cluster in the commander switch
    1) Enable or disable joining the cluster automatically
    2) Set holdtime of heartbeat of the cluster
    3) Set interval of sending heartbeat packets among the switches of the cluster
    4) Clear the list of candidate switches discovered by the commander switch
4. Configure attributes of the cluster in the candidate switch
    1) Set interval of sending cluster register packet
5. Remote cluster network management
    1) Remote configuration management
    2) Reboot member switch
    3) Remotely upgrade member switch

1. Enable or disable cluster

Command	Explanation
Global Mode	
cluster run **no cluster run**	Enable or disable cluster function in the switch

2. Create a cluster

Command	Explanation
Global Mode	
cluster commander <*cluster-name*> ***[vlan<vlan-id>]*** **no cluster commander**	Create or delete a cluster
cluster ip-pool<*commander-ip*> **no cluster ip-pool**	Configure private IP address pool for member switches of the cluster
cluster member {candidate-sn <*cand-sn*> | mac-address <*mac-add*> [<*mem-id*>] }[password <*pass*>] **no cluster member < *mem-id* >**	Add or remove a member switch

3.Configure attributes of the cluster in the commander switch

Command	Explanation
Global Mode	
cluster auto-add enable **no cluster auto-add enable**	Enable or disable adding newly discovered candidate switch to the cluster
cluster holdtime < second> **no cluster holdtime**	Set holdtime of heartbeat of the cluster
cluster heartbeat <*interval*> **no cluster heartbeat**	Set interval of sending heartbeat packets among the switches of the cluster
clear cluster candidate-table	Clear the list of candidate switches discovered by the commander switch

4. Configure attributes of the cluster in the candidate switch

Command	Explanation
Global Mode	
cluster register timer <*timer-value*> **no cluster register timer**	Set interval of sending cluster register packet

5. Remote cluster network management

Command	Explanation
Admin Mode	
rcommand member <mem-id>	In the commander switch, this command is used to configure and manage member switches.
rcommand commander	In the member switch, this command is used to configure the member switch itself.
cluster reset member<mem-id>	In the commander switch, this command is used to reset the member switch.
cluster update member <mem-id> <src-url> <dst-url> [ascii | binary]	In the commander switch, this command is used to remotely upgrade the member switch. It can only upgrade nos.img file.

27.3 Commands for cluster

27.3.1 cluster run

Command:cluster run

no cluster run

Function: Enable cluster function; the "**no cluster run**" command disables cluster function.

Command mode: Global Mode

Default: Cluster function is disabled by default.

Instructions: This command enables cluster function. Cluster function has to be enabled before implementing any other cluster commands. The "**no cluster run**" disables cluster function.

Example: Disable cluster function in the local switch.

Switch (Config)#no cluster run

27.3.2 cluster register timer

Command:cluster register timer<time-value>

no cluster register timer

Function: Sets interval of sending cluster register packet; the "**no cluster register timer**" command restores the default setting.

Parameter: ***<timer-value>*** is interval of sending cluster register packet in seconds, valid range is 30 to 65535.

Command mode: Global Mode

Default: Cluster register timer is 60 seconds by default.

Example: Set the interval of sending cluster register packet to 80 seconds.

Switch(Config)#cluster register timer 80

27.3.3 cluster ip-pool

Command:cluster ip-pool <*commander-ip*>

no cluster ip-pool

Function: Configure private IP address pool for member switches of the cluster.

Parameter: ***<commander-ip>*** is the IP address of the commander switch in dotted decimal format. The value of the last byte in IP address is lower than (255-200).

Command mode: Global Mode

Default: There is no private IP address pool by default.

Instructions: Before creating the cluster, users have to set the private IP address pool in the commander switch. The cluster can't be created if the private IP address pool is not set. When candidate switches join the cluster, the commander switch assigns a private IP address for each member switch. These IP addresses are used to communicate between the commander switch and the member switches. This command can be only used in a non-member switch. As soon as the cluster is created, the users can't modify the IP address pool. The "no cluster ip-pool" command clears the address pool and there is no default setting to be restored.

Example: Set the private IP address pool for the member switches to 192.168.1.64

Switch(config)#cluster ip-pool 192.168.1.64

27.3.4 cluster commander

Command:cluster commander <*cluster-name*> [vlan <*vlan-id*>]

no cluster commander

Function: Enables a commander switch, create a cluster, or modify a cluster's name; the "**no cluster commander**" command deletes the cluster.

Parameter: ***<cluster-name>*** is the cluster's name; ***<vlan-id>*** is the VLAN of the Layer 3 device which the cluster belongs to. If it is omitted, the cluster belongs to VLAN1.

Command mode: Global Mode

Default: There is no cluster by default.

Instructions: This command sets the switch as a commander switch and creates a cluster. Before executing this command, users must configure a private IP address pool. If users executes this command again, the cluster's name will be changed and this information is distributed to the member switches. If users execute this command in a member switch, an error will be displayed. If users execute this command again with a new vlan id, the new vlan id is invalid.

Notice: On layer3 interface configured as cluster commander , avoid configuring RIP,OSPF routing protocol, otherwise, those routing protocols will not work.

Example: Set the switch as a commander switch. The cluster's name is admin and the vlan-id is vlan

Switch(config)#cluster commander admin vlan 2

27.3.5 cluster member

Command:cluster member {candidate-sn <*cand-sn*> | mac-address <*mac-add*> [<*mem-id*>]} [password <*pass*>]

no cluster member <*mem-id* >

Function: Add a candidate switch to the cluster in the commander switch; the "**no cluster member <*mem-id* >**" command deletes a member switch from the cluster.

Parameter: <*mem-id*> is the member ID, valid range is 1 to 23; **<*cand-sn*>** is the sequence number of the switch in the candidate switch list, valid range is 0 to 127. Users can use ";" or "-" to specify multiple numbers or successive numbers; **<*mac-add*>** is the MAC address of the member switch in the format of XX-XX-XX-XX-XX-XX; **<*pass*>** is the privileged password of the member switch.

Command mode: Global Mode

Instructions: When this command is executed in the commander switch, the switch with **<*mac-add*>** or **<*cand-sn*>** will be added to the cluster which the commander switch belongs to. If this command is executed in a non-commander switch, an error will be displayed.

Example: In the commander switch, add the candidate switch which has the sequence number as 17 and password as mypassword to the cluster.

Switch(config)#cluster member candidate-sn 17 password mypassword

27.3.6 cluster auto-add enable

Command: cluster auto-add enable

no cluster auto-add enable

Function: When this command is executed in the commander switch, the newly discovered candidate switches will be added to the cluster as a member switch automatically; the "**no cluster auto-add enable**" command disables this function.

Command mode: Global Mode

Default: This function is disabled by default. That means that the candidate switches are not automatically added to the cluster.

Instructions: When this command is executed in the commander switch and the commander switch receives the cluster register packets sent by the new switch, the commander switch adds the candidate switch to the cluster. If this command is executed in a non-commander switch, an error will be displayed.

Example: Enable the auto adding function in the commander switch.

Switch(config)#cluster auto-add enable

27.3.7 rcommand member

Command: rcommand member <*mem-id*>

Function: In the commander switch, this command is used to remotely manage the member switches in the cluster.

Parameter: <*mem-id*> is the cluster ID of the member switch, valid rang is 1 to 23.

Command mode: Admin Mode

Instructions: Enter the Admin Mode of the member switch and configure the member switch remotely. Use "**exit**" to quit the configuration interface of the member switch. If this command is executed in a non-commander switch, an error will be displayed.

Example: In the commander switch, enter the configuration interface of the member switch with mem-id 15.

Switch#rcommand member 15

27.3.8 rcommand commander

Command: rcommand commander

Function: In the member switch, use this command to configure the commander switch.

Command mode: Admin Mode

Instructions: This command is used to configure the commander switch remotely. Users have to telnet the commander switch by passing the authentication. The command "**exit**" is used to quit the configuration interface of the commander switch. If this command is executed in the commander switch, an error will be displayed.

Example: In the member switch, enter the configuration interface of the commander switch.

Switch#rcommand commander

27.3.9 cluster reset member

Command: cluster reset member *<mem-id>*

Function: In the commander switch, this command can be used to reset the member switch.

Parameter: *<mem-id>* is the cluster ID of the member switch, valid rang is 1 to 23.

Command mode: Admin Mode

Instructions: In the commander switch, users can use this command to reset a member switch. If this command is executed in a non-commander switch, an error will be displayed.

Example: In the commander switch, reset the member switch 16.

Switch#cluster reset member 16

27.3.10 cluster update member

Command: cluster update member *<mem-id>* *<src-url>* *<dst-url>* [ascii | binary]

Function: In the commander switch, this command is used to remotely upgrade the member switch.

Parameter: *<mem-id>* is the cluster ID of the member switch, valid rang is 1 to 23; ***<src-url>*** is the source path of the file which need to be copied; ***<dst-url>*** is the destination path of the file which need to be copied; **ascii** means that the file is transmitted in ASCII format; **binary** means that the file is transmitted in binary format. When ***<src-url>*** is a FTP address, its format is like: ftp: //<*username*>: <*password*>@<*ipaddress*>/<*filename*>. <*username*> is the FTP user name, <*password*> is the FTP password, <*ipaddress*> is the IP address of the FTP server and <*filename*> is the file name. When ***<src-url>*** is a TFTP address, its format is like: tftp: //<*ipaddress*>/<*filename*>. <*ipaddress*> is the IP address of the TFTP server and <*filename*> is the file name.

The special keywords of filename:

Keyword	**Source address or destination address**
startup-config	Startup configuration file
nos.img	System file
boot.rom	System startup file

Command mode: Admin Mode

Instructions: The commander switch sends the remote upgrade command to the member switch. The member switch is upgraded and reset. If this command is executed

in a non-commander switch, an error will be displayed. It can only upgrade nos.img file.

Example: In the commander switch sends the remote upgrade command to the member switch which has mem-id as 10, src-url as ftp: //admin: admin@192.168.1.1/nos.img and dst-url as nos.img

Switch#cluster update member 10 192.168.1.2 ftp: //admin: admin@192.168.1.1/nos.img nos.img

27.3.11 cluster holdtime

Command:cluster holdtime < *second*>

no cluster holdtime

Function: In the commander switch, set holdtime of heartbeat of the cluster; the "**no cluster holdtime**" command restores the default setting.

Parameter: <*second*> is the holdtime of heartbeat of the cluster, valid range is 20 to 65535. The holdtime of heartbeat means the maximum valid time of heartbeat packets. When the heartbeat packets are received again, the holdtime is reset. If no heartbeat packets are received in the holdtime, the cluster is invalid.

Command mode: Global Mode

Default: The holdtime of heartbeat is 80 seconds by default.

Instructions: In the commander switch, this command is used to set the holdtime of heartbeat. And this information is distributed to all the member switches. If this command is executed in a non-commander switch and the value is less than the current holdtime, the setting is invalid and an error is displayed.

Example: Set holdtime of heartbeat of the cluster to 100 seconds

Switch(config)#cluster holdtime 100

27.3.12 cluster heartbeat

Command:cluster heartbeat <*interval*>

no cluster heartbeat

Function: In the commander switch, set interval of sending heartbeat packets among the switches of the cluster; the "**no cluster heartbeat**" command restores the default setting.

Parameter: <*interval*> is the interval of heartbeat of the cluster, valid range is 1 to 65535.

Command mode: The interval of heartbeat is 8 seconds by default.

Default: Global Mode

Instructions: In the commander switch, this command is used to set the interval of heartbeat. And this information is distributed to all the member switches. If this command

is executed in a non-commander switch and the value is more than the current holdtime, the setting is invalid and an error is displayed.

Example: Set the interval of sending heartbeat packets of the cluster to 10 seconds.

Switch(config)#cluster heartbeat 10

27.3.13 clear cluster candidate-table

Command: clear cluster candidate-table

Function: Clear the list of candidate switches discovered by the commander switch.

Command mode: Admin Mode

Instructions: In the commander switch, this command is used to clear the list of candidate switches discovered by the commander switch. If this command is executed in a non-commander switch, an error will be displayed.

Example: Clear the list of candidate switches discovered by the commander switch

Switch#clear cluster candidate-table

27.4 Examples of Cluster Administration

Scenario

The four switches SwitchA-SwitchD, amongst the SwitchA is the command switch and other switches are member switch. The SwitchB and SwitchD is directly connected with the command switch, SwitchC connects to the command switch through SwitchB

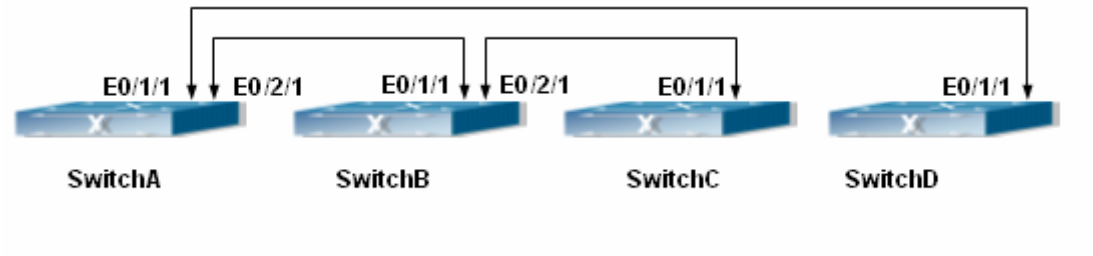


Fig 27-1 Cluster Administration Configuration

Configuration Procedure

1. Configure the command switch

Configuration of SwitchA

Switch(Config)#cluster run

Switch(Config)#cluster ip-pool 1.2.3.4

Switch(Config)#cluster commander 4650

Switch(Config)#cluster auto-add enable

2. Configure the member switch

Configuration of SwitchB-SwitchD

Switch(Config)#cluster run

27.5 Cluster Administration Troubleshooting

27.5.1 Cluster Administration Debugging and Monitoring Command

27.5.1.1 show cluster

Command: show cluster

Function: Display the basic information of the member or command switch

Command Mode: Admin Mode

Example： Execute this command on the switch 1234

Switch#show cluster

Command switch for cluster 1234

Total number of members: 6

Status: 3 Inactive

Time since last status change: 20 hours,30 minutes,15 seconds

Heartbeat interval: 8 seconds

Heartbeat hold-time: 80 seconds

Cluster's snmp rw community string:public

27.5.1.2 show cluster members

Command: show cluster members

Function: Display the statistic information of the joined members on the switch

Command Mode: Admin Mode

Usage Guide: Executing this command on the switch will display the information of the joined member switches such as member ID, MAC address, equipment name and type, status (UP/DOWN)

27.5.1.3 show cluster candidates

Command: show cluster candidates

Function: Display the statistic information of the candidate member switches on the command switch

Command Mode: Admin Mode

Usage Guide: Executing this command on the switch will display the information of the candidate member switches such as member ID, MAC address, IP address, equipment name and type

27.5.1.4 debug cluster packets

Command: debug cluster packets {register |build |heartbeat } {in|out}

no cluster packets {register|build |heartbeat } {in|out}

Function: Enable the debugging message of cluster admin receiving and sending packets; the “no” form of this command disables the enabled debugging messages

Parameter: Register displays a register packet of cluster administration. **Build** displays join a cluster or delete packet from the cluster administration. **Heartbeat** packet for check if cluster admin members are working properly; **in** parameter displays the debugging messages related to the command or member switches receiving packets; **out** parameter displays the debugging messages related to the command or member switches sending packets

Command Mode：Admin Mode

27.5.1.5 debug cluster application

Command：**debug cluster application**

no debug cluster application

Function：Display debugging message on data transmission between the switches when the command or member switch joins a cluster

Command Mode：Admin Mode

27.5.1.6 debug cluster statemach

Command：**debug cluster statemach**

no debug cluster statemach

Function：Enable the debugging message of the changes in member switches and command switch direct protocol state machine when a cluster admin member joining the cluster, the “no” form of this command disables the enabled debugging messages.

Command Mode：Admin Mode

27.5.1.7 Cluster administration troubleshooting

When encountering problems in applying the cluster admin, please check the following possible causes

☞ If the command switch is correctly configured and the auto adding function (cluster

auto-add enable) is enabled. If the ports connected the command switch and member switch belongs to Vlan1 (assumed to be in Vlan1 under current application)

- ☞ Whether the connection between the command switch and the member switch is correct. We can use the debug cluster packets to check if the command and the member switches can receive and process related cluster admin packets correctly