Edge-corE

Powered by Accton

ES4704(10)BD Basic
Management Guide

www.edge-core.com

Content

Chapter 1 Switch Management

1.1 Management Options

After purchasing the switch, the user needs to configure the switch for network management. ES4700 series 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:

Connect with serial port
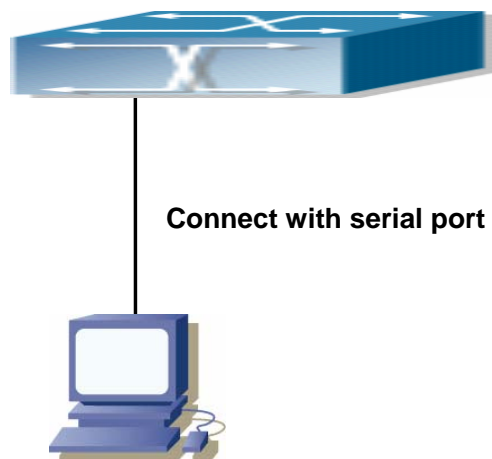
Fig 1-1 Out-of-band Management Configuration Environment

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.
ES4700 series	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.
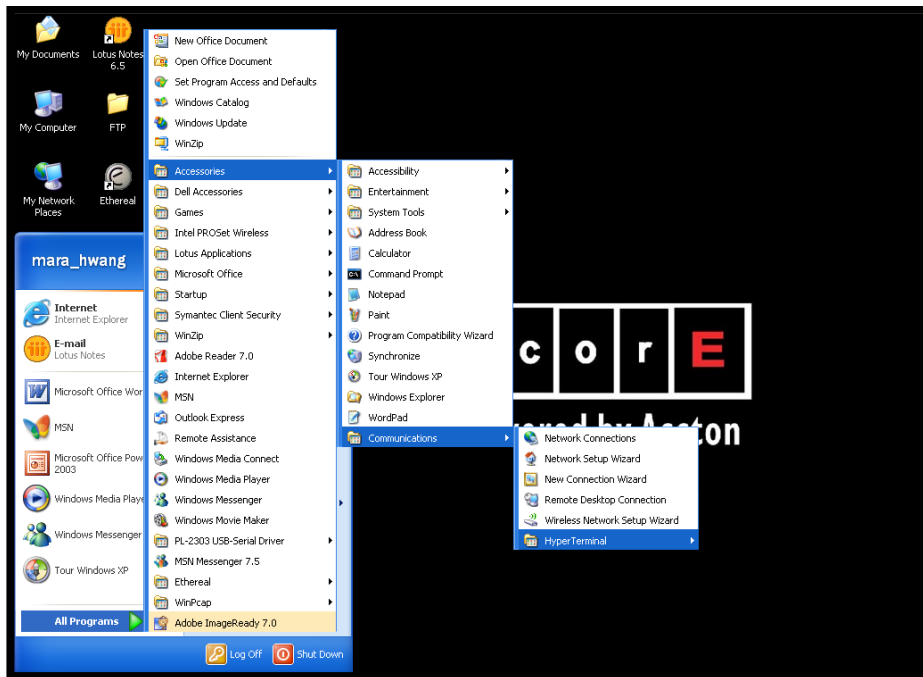
Fig 1-2 Opening HyperTerminal

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

Fig 1-3 Opening HyperTerminal

3) In the "Connecting with" drop-list, select the RS-232 serial port used by the PC, e.g. COM1, and click "OK".
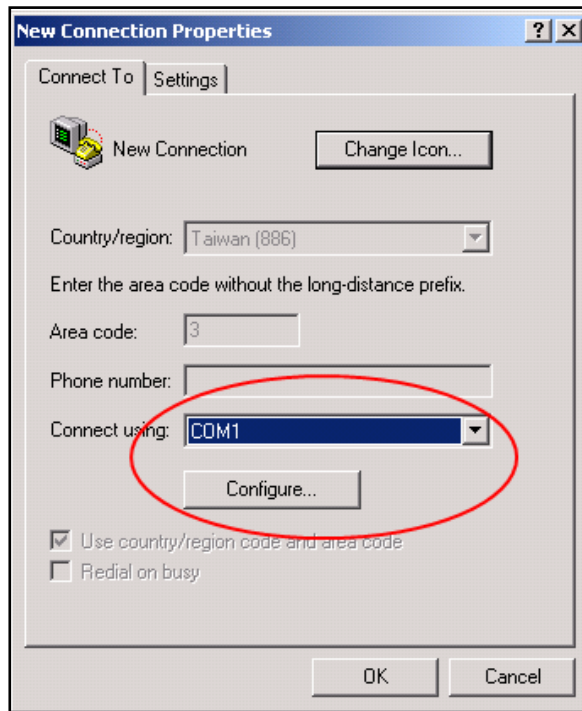
Fig 1-4 Opening HyperTerminal

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 "Revert to default" and click "OK".
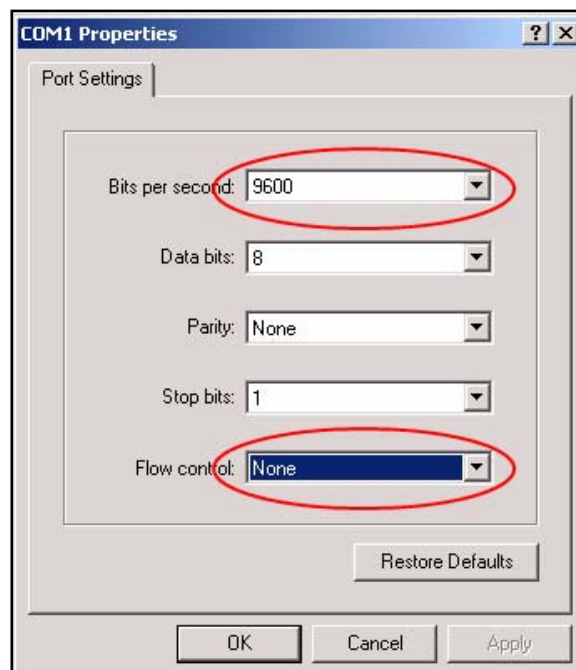
Fig 1-5 Opening HyperTerminal

Step 3 Entering switch CLI interface:

Power on the switch. The following appears in the HyperTerminal windows, that is the CLI configuration mode for ES4700 series.

Testing RAM...

0x077C0000 RAM OK

```
Loading MiniBootROM...
Attaching to file system ...

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

Attaching to file system ...
 ……

--- Performing Power-On Self Tests (POST) ---
DRAM Test....................PASS!
PCI Device 1 Test............PASS!
FLASH Test...................PASS!
FAN Test.....................PASS!
Done All Pass.
------------------ DONE --------------------
Current time is SUN JAN 01 00:00:00 2006
 ……
 Switch>
```

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.

ES4700 seriesis 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.
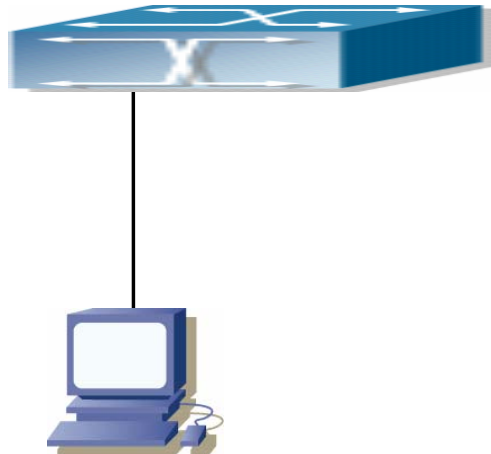
Fig 1-6 Manage the switch by Telnet

Step 1: Configure the IP addresses for the switch and start the Telnet Server function on 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>enable

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

To enable the Telnet Server function, users should type the CLI command telnet-server enable in the global mode as below:

Switch>enable

Switch#config

Switch(config)# telnet-server enable

Step 2: Run Telnet Client program.

    Run Telnet client program included in Windows with the specified Telnet target.
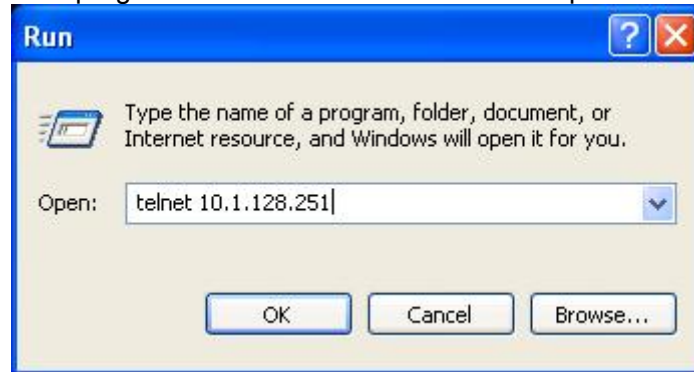
Fig 1-7 Run telnet client program included in Windows

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 *<username>* privilege *<privilege>* [password (0|7) *<password>*]

    To open the local authentication style with the following command: authentication line vty login local. Privilege option must exist and just is 15. Assume an authorized user in the switch has a username of "test", and password of "test", the configuration procedure should like the following:

Switch>enable

Switch#config

Switch(config)#username test privilege 15 password 0 test

Switch(config)#authentication line vty login local

    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 in that in the Console interface.
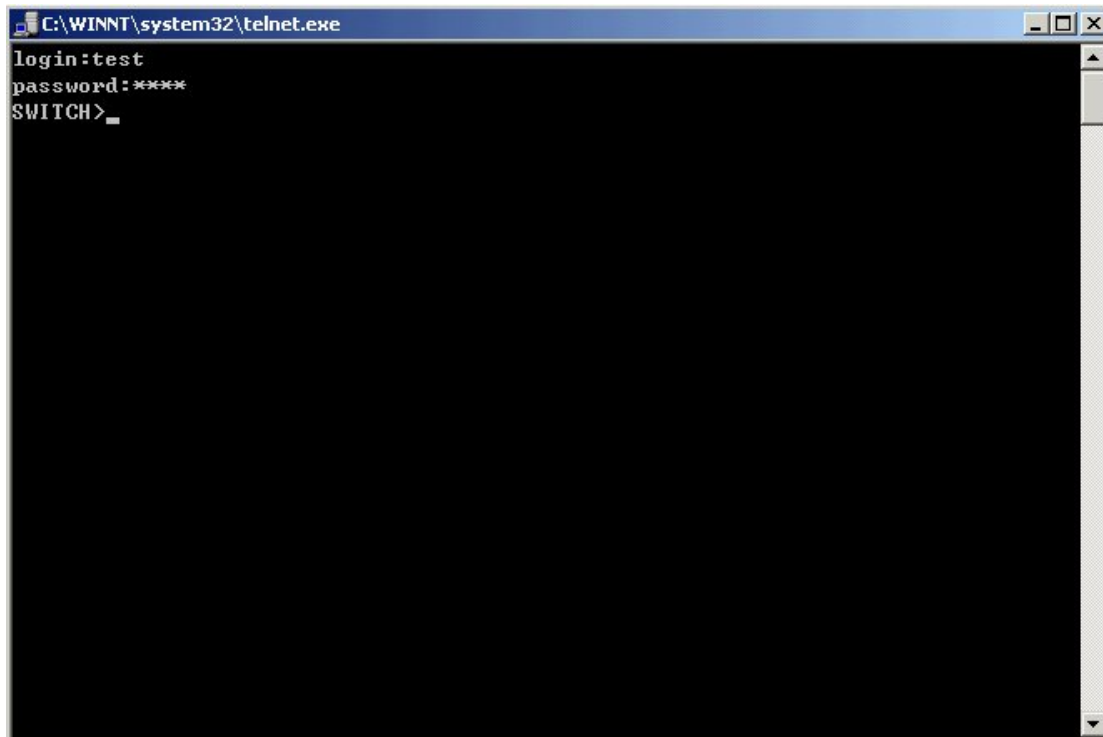
Fig 1-8 Telnet Configuration Interface

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".
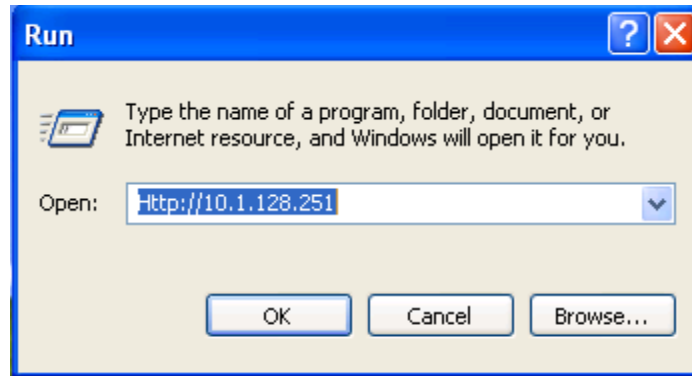
Fig 1-9 Run HTTP Protocol

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>* privilege *<privilege>* [password (0|7) *<password>*].
To open the local authentication style with the following command: **authentication line vty login local.** *Privilege* option must exist and just is 15. Assume an authorized user in the switch has a username of "admin", and password of "admin", the configuration procedure should like the following:

Switch>en
Switch#config
Switch(config)#username admin privilege 15 password 0 admin
Switch(config)#authentication line web login local

The Web login interface is as below:
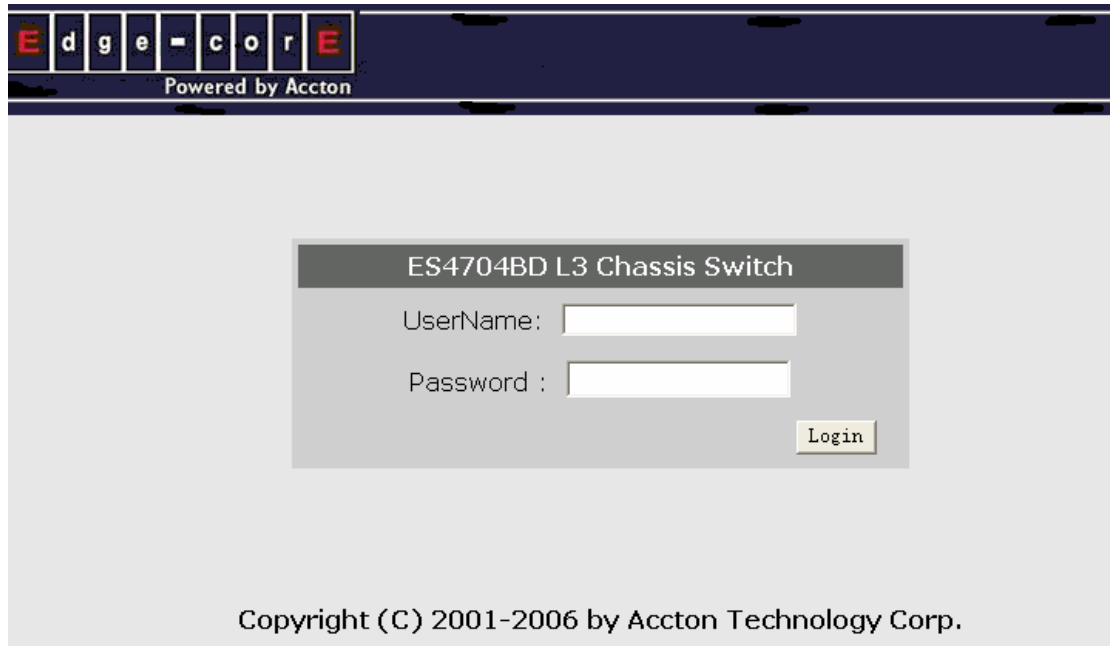
Fig 1-10　Web Login Interface

Input the right username and password, and then the main Web configuration interface is shown as below.
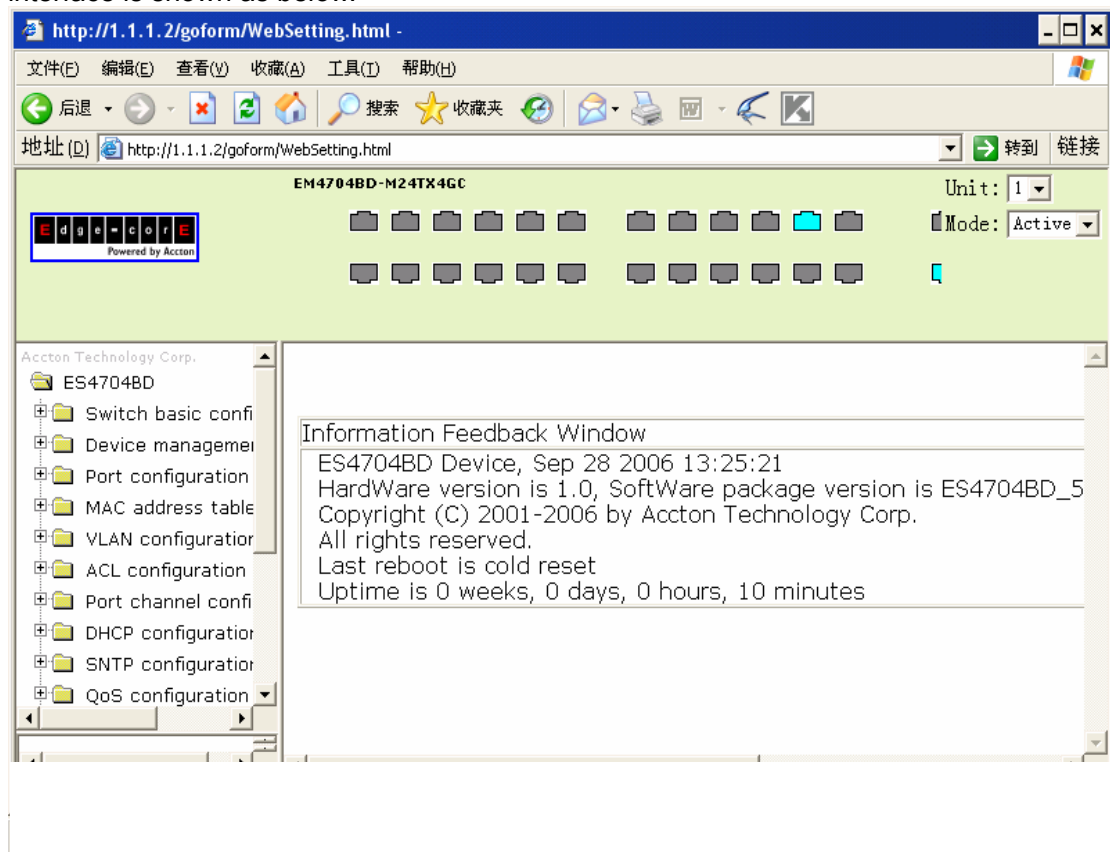
Fig 1-11　Main Web Configuration Interface

1.2 Management Interface

1.2.1 CLI Interface

CLI interface is familiar to most users. As aforementioned, 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
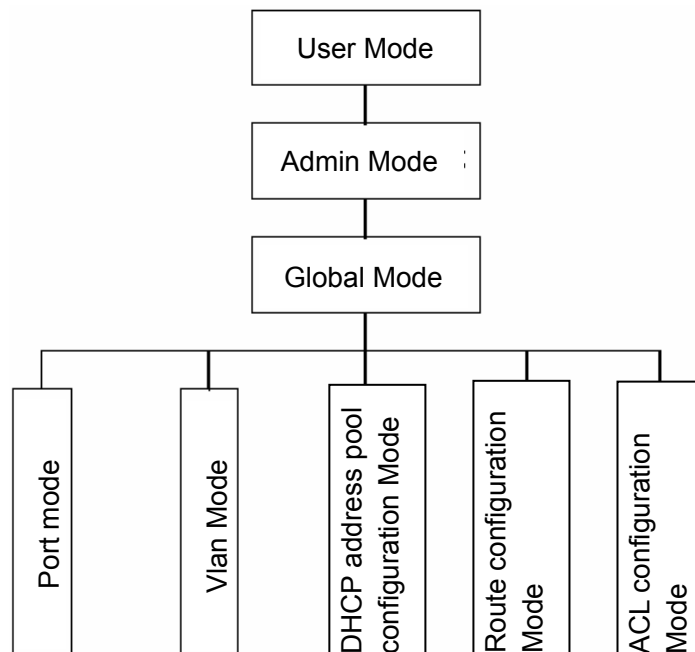
Fig 1-12 Shell Configuration Modes

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 enter 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. ES4700 series 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 Port 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 Port mode for configuration of all the interfaces.

1.2.2.4 Port mode

Use the *interface* command under Global Mode can enter the port mode specified. ES4700 series 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 Interface	Type **interface vlan <Vlan-id>** command under Global Mode.	**Switch(Config-if-Vlanx)#**	Configure switch IPs, etc	Use the *exit* 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	**Switch(Config-Router-Rip)#**	Configure RIP protocol parameters.	Use the "*exit*" command to

	under Global Mode.			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

ES4700 series provides various configuration commands. Although all the commands are different, they all abide by the syntax for ES4700 series configuration commands. The general command format of ES4700 series 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

ES4700 series 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 ES4700 series 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

ES4700 series 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 rom" 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

ES4700 series 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.
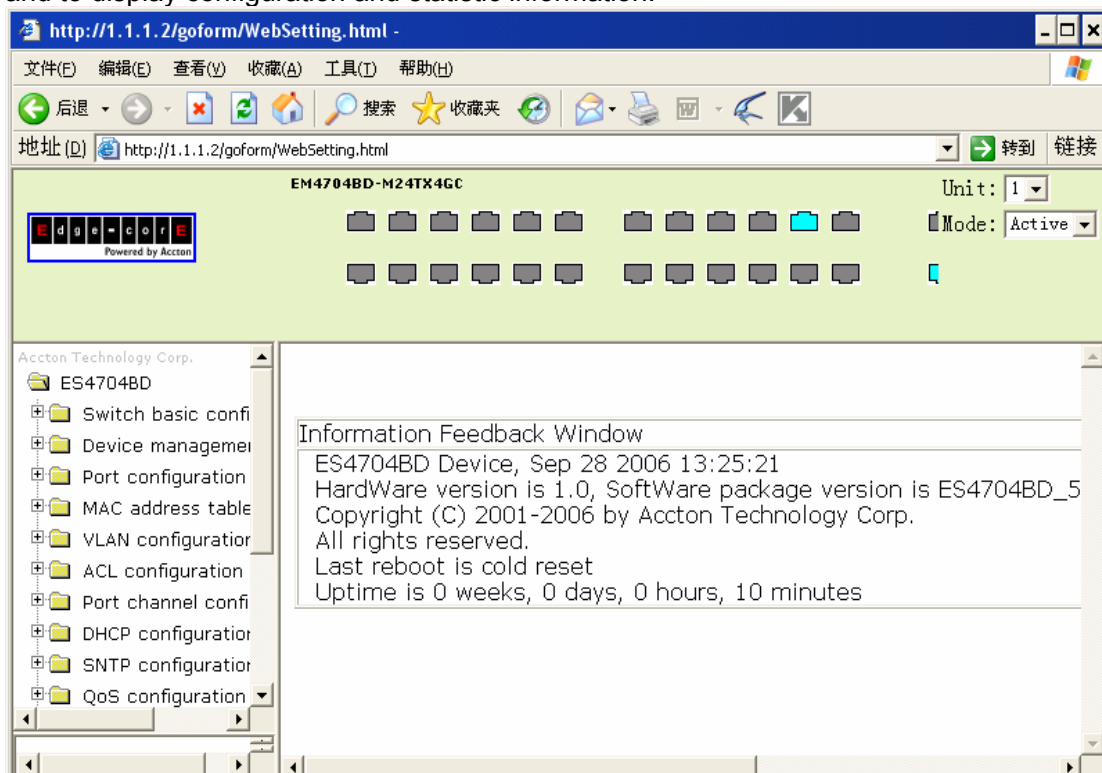
Fig 1-13 Module Front Panel

Chapter 2 Basic Switch Configuration

2.1 Commands for Basic Switch Configuration

Basic switch configuration includes commands for entering and exiting the admin mode, commands for entering and exiting port 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 1	Display version information of the switch
set default	Restore to the factory default
write	Save current configuration parameters to Flash Memory
reload	Hot reset the switch

2.1.1 Command For Basic Configuration

2.1.1.1 authentication line

Command：authentication line {console | vty | web| ftp} login {local | radius | tacacs|}

no authentication line {console | vty | web| ftp } login

Function: Configure VTY (login with Telnet and ssh), Web and Console, so as to select the priority of the authentication mode for the login user. The no form command restores the default authentication mode.

Default: No configuration is enabled for the console login method by default. Local authentication is enabled for the VTY and Web login method by default.

Command Mode: Global Mode.

Usage Guide: The authentication method for Console, VTY and Web login can be configured respectively. And authentication method can be any one or combination of Local, RADIUS or TACCACS. When login method is configuration in combination, the preference goes from left to right. If the users have passed the authentication method, authentication method of lower preferences will be ignored. To be mentioned, if the user receives correspond protocol's answer whether refuse or incept, it will not attempt the next authentication method (Exception: if the local authentication method failed, it will attempt the next authentication method); it will attempt the next authentication method if it receives nothing. And AAA function RADIUS server should be configured before the RADIUS configuration method can be used. And TACACS server should be configured before the TACACS configuration method can be used.

The **authentication line console login** command is exclusive with the "**login**" command. The **authentication line console login** command configures the switch to use the Console login method. And the **login** command makes the Console login to use the passwords configured by the **password** command for authentication.

If local authentication is configured while no local users are configured, users will be able to login the switch via the Console method.

Example:

To configure the telnet and ssh login method to use RADIUS authentication method.

Switch(config)#authentication line vty login radius

Relative Command：aaa enable，radius-server authentication host，tacacs-server authentication host，tacacs-server key

2.1.1.2 authentication securityip

Command：authentication securityip *<ip-addr>*

          no authentication securityip *<ip-addr>*

Function: To configure the trusted IP address for telnet and HTTP login method. The no form of this command will remove the trusted IP address configuration.

Parameters: **<ip-addr>** is the trusted IP address of the client in dotted decimal format which can login the switch.

Default: No trusted IP address is configured by default.

Command Mode: Global Mode.

Usage Guide: IP address of the client which can login the switch is not restricted before the trusted IP address is configured. After the trusted IP address is configured, only clients with trusted IP addresses are able to login the switch. Up to 32 trusted IP addresses can be configured in the switch.

Example: To configure 192.168.1.21 as the trusted IP address.

Switch(config)#authentication securityip 192.168.1.21

2.1.1.3 authentication securityipv6

Command：authentication securityipv6 *<ipv6-addr>*

                no authentication securityipv6 *<ipv6-addr>*

Function: To configure the trusted IPv6 address for the switch. The no form of this command will remove the specified configuration.

Parameters: <ipv6-addr> is the trusted IPv6 address which can login the switch.

Default: No trusted IPv6 addresses are configured by default.

Command Mode: Global Mode.

Usage Guide: IPv6 address of the client which can login the switch is not restricted before the trusted IPv6 address is configured. After the trusted IPv6 address is configured, only clients with trusted IPv6 addresses are able to login the switch. Up to 32 trusted IPv6 addresses can be configured in the switch.

Example: Configure the secure IPv6 address is 2001:da8:123:1::1.

Switch(config)#authentication securityipv6 2001:da8:123:1::1

2.1.1.4 boot img

Command：boot img *<img-file-url>*｛**primary | backup**｝

Function：Configure the first and second img files used in the next boot of the main control boardcard.

Parameters：Primary means to configure the first IMG file, backup means to configure the second IMG file, <img-file-url> is the full path of the booting IMG file, the format of which is as follows:

    1. The file path comprises of three parts: device prefix used as the root directory (flash:/), sub-directory, and the file name. No space is allowed in each part or between two parts.

    2. The suffix of all file names should be .img.

    3. The length of the full file path should be no longer than 128 characters, while the file name no longer than 80 characters.

    4. If the format begins with ”[slot-<slot-ID>#]flash:”，the <slot-ID> in which is the logic slot number of the main control boardcard. Otherwise, the configuration is applied to

the currently active main control boardcard.

Command Mode：Admin Mode.

Default：The factory original configuration only specifies the first booting IMG file, the nos.img file in the FLASH, without the second one.

Usage Guide：This command can only be applied to the active main control boardcard, Users have to configure the first and second img files used in the next booting of the standby main control card by specifying the slot number, and can only use .img files stored in the standby main control boardcard.

Example：Set flash:/nos.img as the second booting IMG file used in the next booting of the standby main control boardcard whose slot number is m2.

Switch#boot img slot-m2#flash:/nos.img backup

2.1.1.5 boot startup-config

Command：**boot startup-config { NULL | *<file-url>* }**

Function：Configure the CGF file used in the next booting of the main control boardcard.

Parameters：The NULL keyword means to use the factory original configuration as the next booting configuration. Setting the he CGF file used in the next booting as NULL equals to implementing "set default" and "write". *<file-url>* is the full path of CGF file used in the next booting.

1. The file path comprises of three parts: device prefix used as the root directory (flash:/), sub-directory, and the file name. No space is allowed in each part or between two parts.

2. The suffix of all file names should be .cfg.

3. The length of the full file path should be no longer than 128 characters, while the file name no longer than 80 characters.

4. If the format begins with "[slot-<slot-ID>#]flash:"，the <slot-ID> in which is the logic slot number of the main control boardcard. Otherwise, the configuration is applied to the currently active main control boardcard.

Command Mode：Admin Mode.

Default：None.

Usage Guide：This command can only be applied to the active main control boardcard, Users have to configure the CFG file used in the next booting of the standby main control card by specifying the slot number, and can only use .cfg files stored in the standby main control boardcard.

Example：Set flash:/ startup.cfg as the CFG file used in the next booting of the main control boardcard whose slot number is m1.

Switch#boot startup-config slot-m1#flash:/ startup.cfg

2.1.1.6 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 1970~2038, *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 august 1 2002

2.1.1.7 config

Command: config [terminal]

Function: Enter Global Mode from Admin Mode.

Parameter: [terminal] indicates terminal configuration.

Command mode: Admin Mode

Example:

Switch#config

2.1.1.8 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

2.1.1.9 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 ----

2.1.1.10 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#

2.1.1.11 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

2.1.1.12 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

2.1.1.13 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#

2.1.1.14 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

CLI provides advanced help feature.   When you need help,

anytime at the command line please press '?'.

If nothing matches, the help list will be empty and you must backup

until entering a '?' shows the available options.

Two styles of help are provided:

1. Full help is available when you are ready to enter a

command argument (e.g. 'show ?') and describes each possible
argument.

2. Partial help is provided when an abbreviated argument is entered
and you want to know what arguments match the input
(e.g. 'show ve?'.)

2.1.1.15 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 ES4700 series.

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

Example: Set the prompt to "Test".

Switch(config)#hostname Test

2.1.1.16 ip host

Command: ip host <hostname> <ip_addr>

         no ip host {*<hostname>*|all}

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; **all** is all of the host name.

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

2.1.1.17 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

2.1.1.18 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.

Example: Enable Web Server function and enable Web configurations.

Switch(config)#ip http server

2.1.1.19 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

2.1.1.20 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: ES4700 series 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.

2.1.1.21 password

Command:password [8]<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

2.1.1.22 ping

Command: ping [[src *<source-address>*] { *<destination-addr>* | host *<hostname>* }]

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

Parameter: *<source-address>* is the source IP host address for assign ping send out, in dot decimal format.

        <destination-addr> is the target host IP address for ping, in dot decimal format.

        <hostname> is the target host name for ping.

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:

(1) Default parameter for ping.

Switch#ping 10.1.128.160

Type ^c to abort.

Sending 5 56-byte ICMP Echos 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.

(2) Set the source address for "ping", while keeping the other parameters their default values.

Switch#ping src 10.1.128.161 10.1.128.160

Type ^c to abort.

Sending 5 56-byte ICMP Echos to 10.1.128.160, using source address 10.1.128.161, timeout is 2 seconds.

!!!!!

Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/0 ms

The example above shows that, the switch use 10.1.128.161 as the source address of the ICMP request messages from "ping", and the IP address of destination device of "ping" is 10.1.128.160. All 5 ICMP request messages each receive a corresponding ICMP reply message, which make the "ping" act is 100% successful. The switch uses "." to represent a failed "ping" act, of which the destination is an unreachable link; and uses "!" to represent a successful "ping" act, of which the destination link is reachable.

(3)

Switch#ping

VRF name:

Target IP address: 10.1.128.160

Use source address option[n]: y

Source IP address: 10.1.128.161

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
Use source address option[n]	whether use source address install option
Source IP address	source IP address for assign ping used
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

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

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 link-local 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 Echos 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 Echos 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 Echos 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 link-local 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

2.1.1.24 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.

2.1.1.25 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

2.1.1.26 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

2.1.1.27 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

2.1.1.28 setup

Command: setup

Function: Enter the Setup Mode of the switch.

Command mode: Admin Mode

Usage Guide: ES4700 series provides a Setup Mode, in which the user can configure IP addresses, etc.

2.1.1.29 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

2.1.1.30 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

2.1.1.31 traceroute

Command: traceroute [source *<ipv4-addr>*]{*<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: *<ipv4-addr>* is the assigned source host IPv4 address in dot decimal format. *<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 30, timeout in 2000 ms.

Command mode: Admin Mode

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

2.1.1.32 traceroute6

Command: traceroute6 [source *<addr>*] {*<ipv6-addr>* | host *<hostname>* }[hops *<hops>*] [timeout *<timeout>*]

Function: This command is for testing the gateways passed by the data packets from the source device to the destination device, so to check the accessibility of the network and further locating the network failure.

Parameter: *<addr>* is the assigned source host IPv6 address in colonned hex notation. *<ipv6-addr>* is the IPv6 address of the destination host,shown in colonned hex notation;*<hostname>* is the name of the remote host; *<hops>* is the max number of the gateways the traceroute6 passed through,ranging between 1-255; *<timeout>* is the timeout period of the data packets,shown in millisecond and ranging between 100~10000.

Default: Default number of the gateways pass by the data packets is 30, and timeout period is defaulted at 2000 ms.

Command Mode: Admin Mode

Usage Guide: Traceroute6 is normally used to locate destination network inaccessible failures.

Example: Switch# traceroute6 2004:1:2:3::4

2.1.1.33 username

Command ：username *<username>* [privilege *<privilege>*] [password {0|7} *<password>*]

    no username *<username>*

Function: To configure local login usernames and passwords along with its privilege level.

Parameters: <username> is the name of the user. **<privilege>** is the maximum privilege level of the commands that the user is able to execute, its value is limited between 1 and 15, and 1 by default. **<password>** is the password for the user. If 7 is appended after the password, the password will be displayed as encrypted text, if 0 is appended, then the password itself will be displayed.

Command Mode: Global Mode.

Usage Guide: There are two available choices for the preferences of the registered commands in the switch. They are 1 and 15. Preference of 1 is for the commands of the normal user configuration mode. Preference of 15 is for the commands registered in modes other than the normal user configuration modes. 16 local users at most can be configured through this command, and the maximum length of the password should be no less than 32.

To be mentioned: Before issuing the command authentication line console login local, it should be made sure that at one user has be configured as preference level of 15, in order to login the switch and make configuration changes in privileged mode and global mode. If there are no configured local users with preference level of 15, while only local authentication is configured for the console login method, the switch can be login without any authentication. When using the web interface to login the switch, only users with preference level of 15 can login the switch, users with preference level other than 15 will be denied.

Example: To configure a administrator account named admin, with the preference level as 15. And configure two normal accounts with its preference level as 1. Then enable local authentication method.

Above all the configurations, only the admin user is able to login the switch in privileged mode through telnet and console login method. user1 and user2 can only login the switch in normal user mode through the telnet and console login method. For HTTP login method, only the admin user can pass the authentication configuration, user1 and user2 will be denied.

Switch(config)#username admin privilege 15 password 0 admin

Switch(config)#username user1 privilege 1 password 7 user1

Switch(config)#username user2 password 0 user2

Switch(config)#authentication line console login local

2.1.1.34 username password

Command:username *<username>* **password** *<0|7>* *<password>*

      no uername *<username>*

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

Parameter: <*username*> is the username. It can't exceed 16 characters; <*0|7*> 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; <*password*> is password. It can't exceed 8 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

2.1.1.35 username nopassword

Command: username <*username*> nopassword

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

Parameter: <*username*> 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

Switch(config)#

2.1.1.36 web language

Command: web language {chinese|english}

Function: Set the language for displaying the HTTP Server information.

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

Command mode: Admin Mode

Default: The default setting is English display.

Usage Guide: The user can select the language according to their preference.

2.1.1.37 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 down or power failure. This is the equivalent to the **copy running-config startup-config** command.

2.2 Commands for Maintenance and Debug

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. ES4700 series 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. ES4700 series can be either the Telnet Server or the Telnet client.

When ES4700 series 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 ES4700 series, as described earlier in the In-band management section. As a Telnet server, ES4700 series allows up to 5 telnet client TCP connections.

And as Telnet client, use **telnet** command under Admin Mode allow the user to login to the other remote hosts. ES4700 series 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. Configurate 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.
username *<username>* **[privilege** *<privilege>*] **[password** {0|7} *<password>*] **no username** *<username>*	Configure user name and password of the telnet. The no form command delete the authorized telnet user. The command privilege of the Telnet user must set to 15.
authenticaion securityip *<ip-addr>* **no authentication securityip** *<ip-addr>* **authenticaion securityipv6** *<ipv6-addr>* **no authentication securityipv6** *<ipv6-addr>*	Configure the secure IP address to login to the switch through Telnet: the "**no**" form command deletes the authorized Telnet secure address.
authentication line {console | vty | web} login {local|radius|tacacs} **no authentication line {console | vty | web} login**	Configure the remote Login authorized style.
Admin Mode	
terminal monitor **no terminal monitor**	Display debug information for Telnet client login to the switch; the **"no terminal monitor"** command disables the debug information.

2. Telnet to a remote host from the switch

Command	Explanation
Admin Mode	
**telnet {<ip-addr>| <ipv6-addr>	host <hostname>} [<port>]**	Login to a remote host with the Telnet client included in the switch.

2.2.3.3 Command 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 max-connection

Command：telnet-server max-connection {<max-connection-number>|default}

Function：Configure the max connection number supported by the Telnet service of the switch.

Parameters：<max-connection-number>: the max connection number supported by the Telnet service, ranging from 5 to 16. The default option will restore the default configuration.

Default：The system default value of the max connection number is 5.

Command Mode：Global Mode

Usage Guide：None.

Example：Set the max connection number supported by the Telnet service as 10.

Switch(config)#telnet-server max-connection 10

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	
terminal monitor **no terminal monitor**	Display SSH debug information on the SSH client side; the "**no terminal monitor**" command stops displaying SSH debug information on the SSH client side.

2.2.4.3 Command 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 max-connection

Command: ssh-server max-connection {<max-connection-number>|default}

Function: Configure the max connection number supported by the SSH service of the switch.

Parameters： <max-connection-number>: the max connection number supported by the SSH service, ranging from 5 to 16. The default option will restore the default configuration.

Default： The system default value of the max connection number is 5.

Command Mode： Global Mode

Usage Guide： None.

Example： Set the max connection number supported by the SSH service as 10.

Switch(config)#ssh-server max-connection 10

2.2.4.3.5 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

2.2.4.3.6 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 32 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.

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 or 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)#ssh-server enable
Switch(config)#interface vlan 1
Switch(Config-if-Vlan1)#ip address 100.100.100.200 255.255.255.0
Switch(Config-if-Vlan1)#exit
Switch(config)#ssh-user test password 0 test
```

In IPv6 networks, the terminal should run IPv6-supporing SSH client software, such as putty6. Users should make no modification to configurations on the switch except allocating an IPv6 address for the local host.

2.2.5 Traceroute

Traceroute 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 Traceroute 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 **interface** **switchport** **[ethernet** *<IFNAME>***]**	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

	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 tech-support	
show version 1	Display the version of the switch

2.2.7.1 Command 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

{bgp|dvmrp|igmp|ipv6|isis|ldp|mld|nsm|ospf|other|pim|rip|spanning-tree|vrrp}

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 ospf

OSPF debugging status:

OSPF all IFSM debugging is on

OSPF packet Hello detail debugging is on

OSPF packet Database Description detail debugging is on

OSPF packet Link State Request detail debugging is on

OSPF packet Link State Update detail debugging is on

OSPF packet Link State Acknowledgment detail debugging is on

OSPF all LSA debugging is on

OSPF all NSM debugging is on

OSPF all events debugging is on

OSPF all route calculation 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 19 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

ssh-server timeout 180s

ssh-server authentication-retries 3

ssh-server max-connection number 6

ssh-server login user number 2

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 <IFNAME>]

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

Parameter: <IFNAME> is the port number.

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 : No limit
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>

Function: Display the switch version.

Parameter: Where the range of unit is 1.

Default: None.

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 version 1

ES4700 series Device, Apr 14 2005 11: 19: 29

HardWare version is 2.0, SoftWare version packet is ES4700 series_1.1.0.0, BootRom version is ES4700 series_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 ES4700 series supports have their corresponding debug commands. The users can use the information from debug command 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 systlog (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 2-1 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 interface, topology change, aggregate port state change of the interface are notifications 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 [slot *<slot-ID>* | 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 [slot <*slot-ID*> | 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:<*slot-ID*>is the logical slot number,such as 1,2,3,M1,M2,**This option is only available on high-end stand switch, and not supported in box switch**;<*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.

Example 1: Display the critical log information in the log buffer zone channel and related to the main control chip M1 with index ID between 940 and 946.

Switch#show logging buffered slot M1 level critical range 940 946

/********* Log information on Active Master ***************/

Current messages in NVRAM:946

slot 1: 12, slot 2: 3, slot 3: 17, slot 4: 0,

slot M1: 878, slot M2: 0, slot 5: 0, slot 6: 4,

slot 7: 32, slot 8: 0,

Current messages in SDRAM:24

943 Dec 22 09:11:33 2006 <critical> DEFAULT[app_root]:Clock between master and slave has been synchronized!

942 Dec 22 09:10:57 2006 <critical> DEFAULT[app_root]:Slot M1 is booting, software version:ES4700_5.0.20.3....

941 Dec 20 14:17:49 2006 <critical> MODULE_CHASSIS_LOAD[thotswap]:Slot 7 pushed done

940 Dec 20 14:17:49 2006 <critical> MODULE_CHASSIS_LOAD[thotswap]:Slot 7 is ready to conf

Example 2: Display all the critical information in the log buffer zone channel and related to main control chip M1.

Switch #show logging buffered slot M1 level warning

/********* Log information on Active Master **************/

Current messages in NVRAM:946

slot 1: 12, slot 2: 3, slot 3: 17, slot 4: 0,

slot M1: 878, slot M2: 0, slot 5: 0, slot 6: 4,

slot 7: 32, slot 8: 0,

Current messages in SDRAM:24

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 local1 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 vlan 1
Switch(Config-if-Vlan1)# ip address 100.100.100.1 255.255.255.0
Switch(Config-if-Vlan1)#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 vlan 1
Switch(Config-if-Vlan1)#ipv6 address 3ffe:506::1/64
Switch(Config-if-Vlan1)#exit
Switch(config)#logging 3ffe:506::4 facility local7 level critical

2.3 Reload switch after specified time

2.3.1 Introduce to reload switch after specifid time

Reload switch after specifid time is to reboot the switch without shutdown its power after a specified period of time, usually when updating the switch version. The switch can be rebooted after a period of time instead of immediately after its version being updated successfully.

2.3.2 Reload switch after specifid time Task List

1. Reload switch after specified time

Command	Explanation
Admin mode	
reload after *<HH:MM:SS>*	Reload the switch after a specified period of time.
reload cancel	Cancel the specified time period to reload the switch.

2.3.3 Commands For reload switch after specifid time

2.3.3.1 reload after

Command：**reload after** *<HH:MM:SS>*

Function：Reload the switch after a specified period of time.

Parameters：*<HH:MM:SS>* the specified time period, HH（hours）ranges from 0 to 23, MM（minutes）and SS（seconds）range from 0 to 59.

Command Mode：Admin mode.

Usage Guide：With this command, users can reboot the switch without shutdown its power after a specified period of time, usually when updating the switch version. The switch can be rebooted after a period of time instead of immediately after its version being updated successfully. This command will not be reserved, which means that it only has one-time effect.

Example：Set the switch to automatically reload in 10 hours and 1second.

Switch#reload after 10:00:01

Process with reboot after? [Y/N] y

Related Commands：reload，reload cancel，show reload

2.3.3.2 reload cancel

Command：reload cancel

Function: Cancel the specified time period to reload the switch.

Parameters： None

Command Mode： Admin mode.

Usage Guide： With this command, users can cancel the specified time period to reload the switch, that is, to cancel the configuration of command "reload after". This command will not be reserved.

Example: Prevent the switch to automatically reboot after the specified time.

Switch#reload cancel

 Reload cancel successful.

Related Commands ：reload，reload after，show reload

2.3.3.3 show reload

Command： show reload

Function： Display the user's configuration of command "reload after".

Parameters： None.

Command Mode： Admin mode.

Usage Guide： With this command, users can view the configuration of command " reload after" and check how long a time is left before rebooting the switch.

Example： view the configuration of command " reload after". In the following case, the user set the switch to be rebooted in 10 hours and 1 second, and there are still 9 hours 59 minutes and 48 seconds left before rebooting it.

Switch#show reload

 The original reload after configuration is 10:00:01.

 System will be rebooted after 09:59:48 from now.

Related Commands：reload，reload after，reload cancel

2.4 Debugging and diagnosis for packets received and sent by CPU

2.4.1 Introduction to debugging and diagnosis for packets received and sent by CPU

The following commands are used to debug and diagnose the packets received and sent by CPU, and are supposed to be used with the help of the technical support.

2.4.2 Debugging and diagnosis for packets received and sent by CPU Task List

Command	Explanation
Global Mode	
cpu-rx-ratelimit total <packets> **no cpu-rx-ratelimit total**	Set the total rate of the CPU receiving packets, the "**no cpu-rx-ratelimit total**" command set the total rate of the CPU receiving packets to default.
cpu-rx-ratelimit queue-length <queue-id> <qlen-value> **no cpu-rx-ratelimit queue-length [<queue-id>]**	Set the length of the specified queue, the "**no cpu-rx-ratelimit queue-length <queue-id>**" command set the length to default.
cpu-rx-ratelimit protocol <protocol- type> <packets> **no cpu-rx-ratelimit protocol [<protocol-type>]**	Set the max rate of the CPU receiving packets of the protocol type, the "**no cpu-rx-ratelimit protocol <protocol- type>**" command set the max rate to default.
clear cpu-rx-stat protocol [<protocol-type>]	Clear the statistics of the CPU received packets of the protocol type.
cpu-rx-ratelimit channel <channel- id> <packets> **no cpu-rx-ratelimit channel [<channel- id>]**	Set the max rate of the switching module CPU receiving packets from control channel, the "**no cpu-rx-ratelimit channel <channel- id>**" command set the max rate to default.

2.4.3 Commands for debugging and diagnosis for packets received and sent by CPU

2.4.3.1 cpu-rx-ratelimit total

Command: cpu-rx-ratelimit total <*packets*>

           no cpu-rx-ratelimit total

Function: Set the total rate of the CPU receiving packets, the "**no cpu-rx-ratelimit total**" command set the total rate of the CPU receiving packets to default.

Parameter:<*packets*> is the max number of CPU receiving packets per second.

Command Mode: Global Mode

Default:1200pps.

Usage Guide: The total rate set by the command have an effect on CPU receiving packets, so it is supposed to be used with the help of the technical support..

Example: Set the total rate of the CPU receive packets to 1500pps.

Switch(config)#cpu-rx-ratelimit total 1500

2.4.3.2 cpu-rx-ratelimit queue-length

Command: cpu-rx-ratelimit queue-length <*queue-id*> <*qlen-value*>

           no cpu-rx-ratelimit queue-length <*queue-id*>

Function: Set the length of the specified queue, the "**no cpu-rx-ratelimit queue-length <*queue-id*>**" command set the length to default.

Parameter: <*queue-id*> is the index of specified queue, the range of the queue-id is <0-7>. **<*qlen-value*>** is the queue's length, the range of length is <0-500>pkts,0 indicates closing the queue.

Command Mode: Global Mode

Default: Default length is 100pkts.

Usage Guide: The queue length set by this command have an effect on CPU receiving packets, so it is supposed to be used with the help of the technical support.

Example: Set the length of queue 2 to 150pkts.

Switch(config)#cpu-rx-ratelimit queue-length 2 150

2.4.3.3 cpu-rx-ratelimit protocol

Command: cpu-rx-ratelimit protocol <*protocol-type*> <*packets*>

           no cpu-rx-ratelimit protocol <*protocol-type*>

Function: Set the max rate of the CPU receiving packets of the protocol type, the "**no cpu-rx-ratelimit protocol <*protocol-type*>**" command set the max rate to default.

Parameter: <*protocol-type*> is the type of the protocol, including dot1x，stp，snmp，arp，telnet，http，dhcp，igmp，ssh，bgp，bgp4plus，rip，ripng，ospf，ospfv3，pim，pimv6，unknown-mcast，unknow-mcast6，mld. **<*packets*>** is the max rate of CPU receiving packets of the protocol type, its range is <1-2000> pps.

Command Mode: Global Mode

Default: A different default rate is set for the different type of protocol.

Usage Guide: The rate limit set by this command have an effect on CPU receiving packets, so it is supposed to be used with the help of the technical support.

Example: Set the rate of the CPU receiving the arp packets to 500pps

Switch(config)#cpu-rx-ratelimit protocol arp 500

2.4.3.4 clear cpu-rx-stat protocol

Command: clear cpu-rx-stat protocol [*<protocol-type>*]

Function: Clear the statistics of the CPU received packets of the protocol type.

Parameter: *<protocol- type>* is the type of the protocol of the packet, including dot1x,stp,snmp,arp,telnet,http,dhcp,igmp,ssh,bgp,bgp4plus,rip,ripng,ospf,ospfv3,pim,pimv6, unknown-mcast,unknow-mcast6 and mld.

Command Mode: Global Mode

Usage Guide: This command clear the statistics of the CPU received packets of the protocol type, it is supposed to be used with the help of the technical support.

Example: Clear the statistics of the CPU receives arp packets.

Switch(config)#clear cpu-rx-stat protocol arp

2.4.3.5 cpu-rx-ratelimit channel

Command: cpu-rx-ratelimit channel *<channel- id> <packets>*

no cpu-rx-ratelimit channel *<channel- id>*

Function: Set the max rate of the switching module CPU receiving packets from control channel, the "**no cpu-rx-ratelimit channel *<channel- id>***" command set the max rate to default.

Parameter: *<channel-id>* is the index of channel, the range of the channel-id is <0-15>.

<packets> is the max rate of CPU receiving packets from the control channel, the range of the packets is <0-2000>pps,0 indicates no rate limit of receiving packets from the control channel.

Command Mode: Global Mode

Default: A different default value for different channel.

Usage Guide: The rate limit set by this command have an effect on CPU receiving packets, so it is supposed to be used with the help of the technical support.

Example: Set the rate of the CPU receive packets from channel 1 to 500pps.

Switch(config)#cpu-rx-ratelimit channel 1 500

2.4.3.6 show cpu-rx protocol

Command: show cpu-rx protocol [*<protocol-type>*]

Function: Show the statistics of the CPU received packets of the protocol type.

Parameter: *<protocol- type>* is the type of the protocol of the packet.

Command Mode: Admin Mode

Default: None.

Usage Guide: This command is used to debug, it is supposed to be used with the help of the technical support.

Example： show the statistics of the CPU receiving arp packets

Switch#show cpu-rx protocol arp

Type	Rate-limit	TotPkts	CurState
arp	500	3	allowed

2.4.3.7 debug driver

Command: debug driver {receive|send} [interface {<*interface-name*> |all}] [protocol {<*protocol-type*> |discard |all}][detail]

        no debug driver {receive |send}

Function: Turn on the on-off of showing the information of the CPU receiving or sending packets, the "**no debug driver {receive |send}**" command turn off the on-off.

Parameter: receive|send show the information of receiving or sending packets;

interface {<*interface-list*>|all}:interface-list is the Ethernet port number**, all** indicate all the Ethernet ports.

protocol {<*protocol-type*>|discard |all}： protocol-type is the type of the protocol of the packet，including snmp、telnet、http、dhcp、igmp、hsrp、arp、bgp、rip、ospf、pim、ssh、vrrp、ripng、ospfv3、pimv6、icmpv6、bgp4plus、unknown-mcast、unknown-mcast6、ttl0-2cpu、isis、dot1x、gvrp、stp、lacp、cluster、mld、vrrpv3、ra、uldp、lldp、eapou;**all** means all of the protocol types,**discard** means all the discarded packets.

Detail show detail information.

Command Mode: Admin Mode

Usage Guide: This command is used to debug, it is supposed to be used with the help of the technical support.

Example： Turn on the on-off for showing the receiving packets.

Switch#debug driver receive

2.5 Configurate Switch IP Addresses

All Ethernet ports of ES4700 series 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. ES4700 series 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, ES4700 series 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.

2.5.1 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.

2.5.2 Commands For Configuring Switch IP

2.5.2.1 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: Port 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

2.5.2.2 ip address bootp-client

Command: ip address bootp-client

   no ip address 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: Port 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 BootP, 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

2.5.2.3 ip address dhcp-client

Command: ip address dhcp-client

              no ip address dhcp-client

Function: Enables 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 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: Port 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

2.6 SNMP Configuration

2.6.1 Introduce 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.

2.6.2 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:
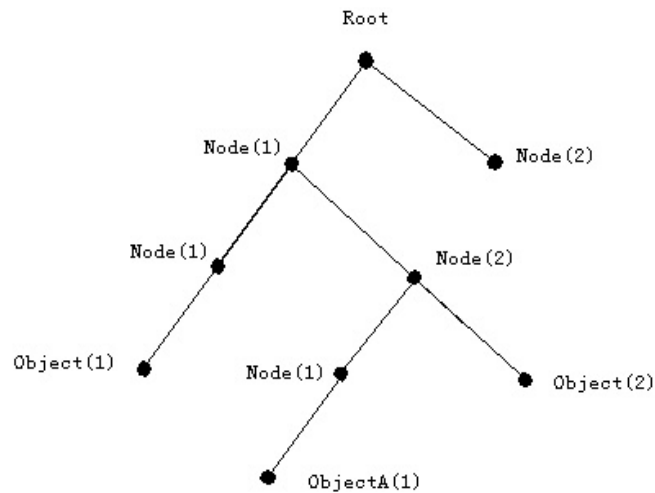
Fig 2-1 ASN.1 Tree Instance

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.

2.6.3 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).

2.6.4 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 security-ip 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**	Configure the local engine **ID** on the switch. This command is used for **SNMP v3**

5. Configure user

Command	Explanation
snmp-server user *<WORD>* *<WORD>* [{encrypted|noentrypted} auth {md5|sha} *<WORD>*] **no snmp-server user *<WORD>***	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	Enable the switch to send Trap message.

no snmp-server enable traps	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.

2.6.5 Command For SNMP

2.6.5.1 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

2.6.5.2 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 supplied	Number of permission for community 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.

2.6.5.3 show snmp status

Command: show snmp status

Function: Display SNMP configuration information.

Command mode: Admin Mode

Example:

Switch#show snmp status

System Name : Vendor

System Contact : 800-xxx-xxxx

System Location : Earth

Trap disable

RMON enable

Community Information:

Security IP is Enabled

V1/V2c Trap Host Information:

V3 Trap Host 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

2.6.5.4 snmp-server community

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

           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 rw private

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

Switch(config)#snmp-server community ro public

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

Switch(config)#snmp-server community ro private

Example 4: Delete community string "private".

Switch(config)#no snmp-server community private

2.6.5.5 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

2.6.5.6 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

2.6.5.7 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

2.6.5.8 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

2.6.5.9 debug snmp kernel

Command: debug snmp kernel

              no debug snmp kernel

Function: Enable the SNMP kernel debugging; the "**no debug snmp kernel**" 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 kernel

2.6.5.10 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

2.6.5.11 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

2.6.5.12 show snmp mib

Command: show snmp mib

Function: Display all MIB supported by the switch

Command Mode: Admin Mode

2.6.5.13 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

2.6.5.14 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

2.6.5.15 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

2.6.5.16 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 isreadview, and the writing is disabled.

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

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

2.6.5.17 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

2.6.5.18 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

2.6.5.19 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 8-32 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 hellohello.

Switch (config)#snmp-server user tester UserGroup encrypted auth md5 hellohello

deletes an User

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

2.6.5.20 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

2.6.6 Typical SNMP Configuration Examples
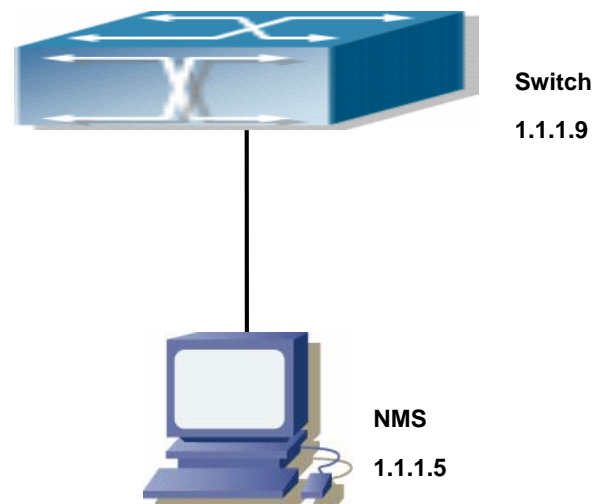
Fig 2-2 Typical SNMP Configuration

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 rw private

Switch(config)#snmp-server community ro public

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 hellohello

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

2.6.7 SNMP Troubleshooting Help

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 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.

2.7 Switch Upgrade

ES4700 series provides two ways for switch upgrade: BootROM upgrade and the TFTP/FTP upgrade under Shell.

2.7.1 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.

2.7.2 BootROM Upgrade

There are two methods for BootROM upgrade: TFTP and FTP, which can be selected at BootROM command settings.
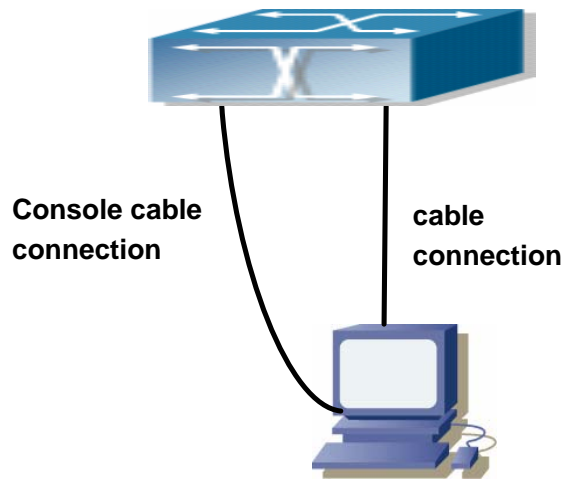
Fig 2-3 Typical topology for switch upgrade in BootROM mode

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 img 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:

ES4700 series 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 ----

2.   CONFIG RUN command

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

[Boot]: config run

Boot File: [nos.img] nos.img

Config File: [boot.conf]

2.7.3 FTP/TFTP Upgrade

2.7.3.1 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 create its own data listening port and

inform 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.

ES4700 series can operate as either FTP/TFTP client or server. When ES4700 series 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, ES4700 series can also upload current configuration files or system files to the remote FTP/TFTP servers(can be hosts or other switches). When ES4700 series 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 ES4700 series.

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 IMG upgrade file. In ES4700 series, the system image file is allowed to save in FLASH only. ES4700 series mandates the name of system image file to be uploaded via FTP in Global Mode to be nos.img, other IMG 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 IMG file). In ES4700 series, the boot file is allowed to save in ROM only. ES4700 series mandates the name of the boot file to be boot.rom.

Configuration file: including start up configuration file and active configuration file. The distinction between start up configuration file and active 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. ES4700 series start up configuration file stores in FLASH only, corresponding to the so called configuration save. To prevent illicit file upload and easier configuration, ES4700

series mandates the name of start up configuration file to be startup-config.

Running configuration file: refers to the active configuration sequence use in the switch. In ES4700 series, the active configuration file stores in the RAM. In the current version, the active 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 active configuration sequence becomes the start up configuration file, which is called configuration save. To prevent illicit file upload and easier configuration, ES4700 series mandates the name of active configuration file to be running-config.

Factory configuration file: The configuration file shipped with ES4700 series 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.

2.7.3.2 FTP/TFTP Configuration

The configurations of ES4700 series as FTP and TFTP clients are almost the same, so the configuration procedures for FTP and TFTP are described together in this manual.

2.7.3.2.1 FTP/TFTP Configuration Task List

1. FTP/TFTP client configuration
   （1） Upload/download the configuration file or system file.
   （2） 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>* **[slot***<slot-id>***]** *<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-timeout *\<seconds \>*	Set maximum retransmission time within timeout interval.

（3）Modify TFTP server connection retransmission time

Command	Explanation
Global Mode	
tftp-server retransmission-number *\<number \>*	Set the retransmission time for TFTP server.

2.7.3.2.2 Command For Switch Upgrade

2.7.3.2.2.1 copy（FTP）

Command: copy *<source-url>* **[slot** *<slot-id>*] *<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; *<slot-id>* is the assign card's slot number to which the 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>* }/*<file name>*,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
boot.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）Obtain system file boot.rom for the No.4 slot line card from the FTP server 2004:1:2:3::6

Switch#copy ftp://Switch:superuser@2004:1:2:3::6/boot.rom slot 4 boot.rom

（4）Save the running configuration files

Switch#copy running-config startup-config

2.7.3.2.2.2 copy（TFTP）

Command: copy *<source-url>* **[slot** *<slot-id>*] *<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 copied; *<slot-id>* is the assign card's slot number to which the 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 differentlocations 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 TFTP address, its form should be: tftp://{*<ipaddress>*|*<ipv6address>*|*<hostname>* }/*<filename>*,amongst *<ipaddress>*|*<ipv6address>* is the IPv4 or IPv6 address of the TFTP server/client,*<hostname>* is the name of the host mapping with the IPv6 address,it does not support the filedownload 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
boot.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）Obtain system file boot.rom for the No.4 slot line card from the TFTP server 2004:1:2:3::6

Switch#copy tftp://Switch:superuser@2004:1:2:3::6/boot.rom slot 4 boot.rom

（4）Save the running configuration files

Switch#copy running-config startup-config

2.7.3.2.2.3 Switch#copy running-config startup-config 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.

2.7.3.2.2.4 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

2.7.3.2.2.5 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

2.7.3.2.2.6 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.

2.7.3.2.2.7 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.

2.7.3.2.2.8 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

2.7.3.2.2.9 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

2.7.3.2.2.10 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

2.7.4 FTP/TFTP Configuration Examples

It is the same configuration switch for IPv4 addresses and IPv6 addresses. The example only for the IPv4 addresses configuration.

Switch

10.1.1.2
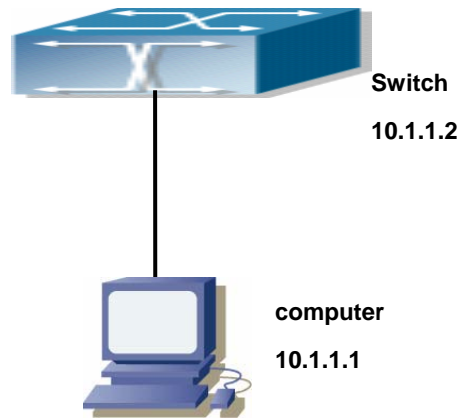
computer

10.1.1.1

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)#interface 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)#interface 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)#interface 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 Admin password 0 switch

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)#interface 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 upgrades the assign card's "boot.rom" file through FTP/TFTP mode.

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 "boot.rom" file in the computer for the No.4 slot's line card of 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 "boot.rom" file to the appropriate FTP server directory on the computer.

The configuration procedures of the switch is 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)#no shut

Switch(Config-if-Vlan1)#exit

Switch(config)#exit

Switch#copy ftp://Switch:switch@10.1.1.1/boot.rom slot 4 boot.rom

With the above commands, the switch will have the "boot.rom" file in the computer downloaded to the No.4 slot line card's FLASH.

■ **TFTP Configuration**

Computer side configuration:

Start TFTP server software on the computer and place the "boot.rom" file to the appropriate TFTP server directory on the computer.

The configuration procedures of the switch is 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)#no shut

Switch(Config-if-Vlan1)#exit

Switch(config)#exit

Switch#copy tftp://10.1.1.1/boot.rom slot 4 boot.rom

With the above commands, the switch will have the "boot.rom" file in the computer downloaded to the No.4 slot line card's FLASH.

Scenario 5: 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)#interface 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)#interface 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: ES4700 series 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".

ES4700 series:

Switch(config)#interface 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.

2.7.5 FTP/TFTP Troubleshooting Help

2.7.5.1 FTP Troubleshooting Help

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.

2.7.5.2 TFTP Troubleshooting Help

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

2.8 Jumbo Configuration

2.8.1 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.

2.8.2 Jumbo Configuration Task Sequence

1.Configure enable Jumbo function

Command	Explanation
jumbo enable [<mtu-value>] **no jumbo enable**	Enable/disable sending/receiving function of the Jumbo frames

2.8.3 Jumbo Command

Command：jumbo enable [<mtu-value>]

　　　　　　no jumbo enable

Function：Configure the MTU size of JUMBO frame, enable the Jumbo receiving/sending function. The "**no jumbo enable**" command restores to the normal frame range of 64 —1518.

Parameter： mtu-value: the MTU value of jumbo frame that can be received, in byte, ranging from <1500-9000>. The corresponding frame size is <1518/1522-9018/9022>. Without setting is parameter, the allowed max frame size is 9018/9022.

Default： Jumbo function not enabled by default.

Command Mode： Global Mode

Usage Guide: Set switch of both ends jumbo necessarily, or jumbo frame will be dropped at the switch has not be set.

Example: Enable the jumbo function of the switch.

Switch(config)#jumbo enable

2.9 sFlow Configuration

2.9.1 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.

2.9.2 sFlow Configuration Task

1. Configure sFlow Collector address

Command	Explanation
Global mode and port 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
Port 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
Port 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
Port 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
Port 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

2.9.3 Commands For sFlow

2.9.3.1 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 Port 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 port mode, this IP address and port configured at port 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

2.9.3.2 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

2.9.3.3 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

2.9.3.4 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: Port 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

2.9.3.5 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: Port 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

2.9.3.6 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: Port 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 e3/2 to 20 seconds.

Switch(Config-If-Ethernet3/2)#sflow counter-interval 20

2.9.3.7 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 egress group sampling, the valid range is 1000~16383500

Command Mode: Port 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 e3/2 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

2.9.3.8 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.

2.9.4 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)# interface ethernet3/1

Switch (Config-If-Ethernet3/1)#sflow rate input 10000

Switch (Config-If-Ethernet3/1)#sflow rate output 10000

Switch (Config-If-Ethernet3/1)#sflow counter-interval 20

Switch (Config-If-Ethernet3/1)#exit

Switch (config)#interface ethernet3/2

Switch (Config-If-Ethernet3/2)#sflow rate input 20000

Switch (Config-If-Ethernet3/2)#sflow rate output 20000

Switch (Config-If-Ethernet3/2)#sflow counter-interval 40

2.9.5 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 port 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.

2.10 TACACS+ Configuration

2.10.1 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+.

2.10.2 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	Explanntion
Global Mode	
tacacs-server authentication host *<IPaddress>* [[port {*<portNum>*}] [timeout *<seconds>*] [key <string>] [primary]] **no tacacs-server authentication host *<IPaddress>***	Configure the IP address, listening port number, the value of timeout timer and the key string of the TACACS+ server; the "no" form of this command deletes the TACACS+ authentication server.

3) Configure the TACACS+ authentication timeout time

Command	Explanation
Global Mode	

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

2.10.3 Commands for TACACS+

2.10.3.1 tacacs-server authentication host

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

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

Function: Configure the IP address, listening port number, the value of timeout timer and the key string of the TACACS+ server; the "no" form of this command deletes TACACS+ authentication server.

Parameter: *<ip-address>* is the IPof 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; *<seconds>* is the value of TACACS+ authentication timeout timer, shown in seconds and the valid range is 1~60; **<string>** is the key string, containing maximum 16 characters; **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, port number, timeout timer value and the key string 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. The parameters key and timeout is used to configure the self-key and self-timeout, if the switch is not configure the timeout*<seconds>* and key<string>, it will use the global value and key by command tacacs-server timeout*<seconds>* and tacacs-server key <string>. 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, and use the global configured key.

Switch(config)#tacacs-server authentication host 192.168.1.2

2.10.3.2 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

2.10.3.3 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

2.10.3.4 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

2.10.4 Typical TACACS+ Scenarios
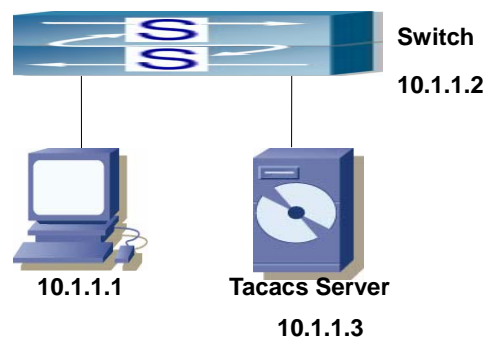
Fig 2-6 TACACS Configuration

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 vty tacacs local

2.10.5 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.

2.11 RADIUS Configuration

2.11.1 RADIUS Introduction

2.11.1.1 AAA and RADIUS Introduction

AAA is short for Authentication，Authorization and Accounting, it provide a consistency framework for the network management safely. According to the three functions of Authentication, Authorization, Accounting, the framework can meet the access control for the security network: which one can visit the network device, which access-level the user can have and the accounting for the network resource.

RADIUS (Remote Authentication Dial In User Service), is a kind of distributed and client/server protocol for information exchange. The RADIUS client is usually used on network appliance to implement AAA in cooperation with 802.1x protocol. The RADIUS server maintains the database for AAA, and communicate with the RADIUS client through RADIUS protocol. The RADIUS protocol is the most common used protocol in the AAA framework.

2.11.1.2 Message structure for RADIUS

The RADIUS protocol uses UDP to deliver protocol packets. The packet format is shown as below.
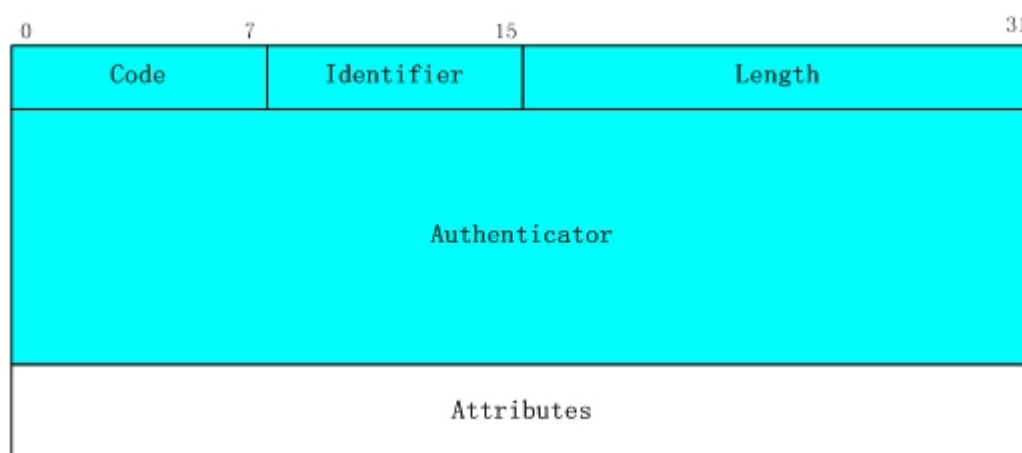
Fig 2-7 Message structure for RADIUS

Codefield(1octets): is the type of the RADIUS packet. Available value for the Code field is show as below:

1 Access-Request
2 Access-Accept
3 Access-Reject
4 Accounting-Request
5 Accounting-Response
11 Access-Challenge

Identifier field (1 octet) : Identifier for the request and answer packets.

Length field (2 octets) : The length of the overall RADIUS packet, including Code, Identifier, Length, Authenticator and Attributes

Authenticator field (16 octets): used for validation of the packets received from the RADIUS server. Or it can be used to carry encrypted passwords. This field falls into two kinds: the Request Authenticator and the Response Authenticator.

Attribute field: used to carry detailed information about AAA. An Attribute value is formed by Type, Length, and Value fields.

☞ Type field (1 octet), the type of the attribute value, which is shown as below:

Property	Type of property	Property	Type of property
1	User-Name	23	Framed-IPX-Network
2	User-Password	24	State
3	CHAP-Password	25	Class
4	NAS-IP-Address	26	Vendor-Specific
5	NAS-Port	27	Session-Timeout
6	Service-Type	28	Idle-Timeout
7	Framed-Protocol	29	Termination-Action
8	Framed-IP-Address	30	Called-Station-Id
9	Framed-IP-Netmask	31	Calling-Station-Id
10	Framed-Routing	32	NAS-Identifier
11	Filter-Id	33	Proxy-State
12	Framed-MTU	34	Login-LAT-Service
13	Framed-Compression	35	Login-LAT-Node
14	Login-IP-Host	36	Login-LAT-Group
15	Login-Service	37	Framed-AppleTalk-Link
16	Login-TCP-Port	38	Framed-AppleTalk-Network

17	(unassigned)	39	Framed-AppleTalk-Zone
18	Reply-Message	40-59	(reserved for accounting)
19	Callback-Number	60	CHAP-Challenge
20	Callback-Id	61	NAS-Port-Type
21	(unassigned)	62	Port-Limit
22	Framed-Route	63	Login-LAT-Port

☞ Length field (1 octet), the length in octets of the attribute including Type, Length and Value fields.

☞ Value field, value of the attribute whose content and format is determined by the type and length of the attribute.

2.11.2 RADIUS Configuration

1. Enable the authentication and accounting function.
2. Configure the RADIUS authentication key.
3. Configure the RADIUS server.
4. Configure the parameter of the RADIUS service.
5. Configure the IP address of the RADIUS NAS.

1. Enable the authentication and accounting function.

Command	Explanation
Global Mode	
aaa enable **no aaa enable**	To enable the AAA authentication function. The no form of this command will disable the AAA authentication function.
aaa-accounting enable **no aaa-accounting enable**	To enable AAA accounting. The no form of this command will disable AAA accounting.
aaa-accounting update {enable | disable}	Enable or disable the update accounting function.

2. Configure the RADIUS authentication key.

Command	Explanation
Global Mode	

Command	Explanation
radius-server key *<string>* no radius-server key	To configure the encryption key for the RADIUS server. The no form of this command will remove the configured key.

3. Configure the RADIUS server.

Command	Explanation
Global Mode	
radius-server authentication host {*<IPaddress>*|*<IPv6address>*} [[port {*<portNum>*}] [key *<string>*] [primary] [access-mode {dot1x|telnet}] no radius-server authentication host *<IPaddress>*	Specifies the IP address and listening port number, cipher key, whether be primary server or not and access mode for the RADIUS server; the no command deletes the RADIUS authentication server.
radius-server accounting host {*<IPaddress>*|*<IPv6address>*} [[port {*<portNum>*}] [primary]] no radius-server accounting host *<IPaddress>*	To configure the IP/IPv6 adddress and the port number for the accounting RADIUS server. The no form of this command will remove the RADIUS server configuration.

4. Configure the parameter of the RADIUS service.

Command	Explanation
Global Mode	
radius-server dead-time *<minutes>* no radius-server dead-time	To configure the interval that the RADIUS becomes available after it is down. The no form of this command will restore the default configuration.
radius-server retransmit *<retries>* no radius-server retransmit	To configure retry times for the RADIUS packets. The no form of this command restore the default configuration.
radius-server timeout *<seconds>* no radius-server timeout	To configure the timeout value for the RADIUS server. The no form of this command will restore the default configuration.

radius-server accounting-interim-update timeout *<seconds>* **no radius-server accounting-interim-update timeout**	To configure the update interval for accounting. The no form of this command will restore the default configuration.

5. Configure the IP address of the RADIUS NAS

Command	Explanation
Global Mode	
radius nas-ipv4 *<ip-address>* **no radius nas-ipv4**	To configure the source IP address for the RADIUS packets for the switch.
radius nas-ipv6 *<ipv6-address>* **no radius nas-ipv6**	To configure the source IPv6 address for the RADIUS packets for the switch.

2.11.3 Commands for RADIUS

2.11.3.1 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: Enable AAA function for the switch.

Switch(config)#aaa enable

2.11.3.2 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 "log-off" message will not be sent to the RADIUS authentication server.

Example: Enable AAA accounting for the switch.

Switch(config)#aaa-accounting enable

2.11.3.3 aaa-accounting update enable

Command: aaa-accounting update {enable|disable}

Function: Enable or disable the update accounting function.

Command Mode: Global Mode.

Default: Enabled.

Usage Guide: After the update accounting function is enabled, the switch will sending accounting message to each online user on time.

Example: Disable the update accounting function for switch.

Switch(config)#aaa-accounting update disable

2.11.3.4 debug aaa packet

Command ：debug aaa packet {send|receive|all} interface{ethernet <interface-number> | <interface-name>}

no debug aaa packet {send|receive|all} interface{ethernet <interface-number> | <interface-name>}

Function： Enable the debug information of aaa about receiving and sending packets; the no operation of this command will disable such debug information.

Parameters：send： Enable the debug information of aaa about sending packets.

receive： Enable the debug information of aaa about receiving packets.

all： Enable the debug information of aaa about both sending and receiving packets.

<interface-number>: the number of interface.

<interface-name>: the name of interface.

Command Mode： Admin Mode

Usage Guide： By enabling the debug information of aaa about sending and receiving packets, users can check the messages received and sent by Radius protocol, which might help diagnose the cause of faults if there is any.

Example：Enable the debug information of aaa about sending and receiving packets on interface1/1.

Switch#debug aaa packet all interface ethernet 1/1

2.11.3.5 debug aaa detail attribute

Command：**debug aaa detail attribute interface** **{ethernet** *<interface-number>|* *<interface-name>}*

no debug aaa detail attribute interface **{ethernet** *<interface-number>|* *<interface-name>}*

Function：Enable the debug information of aaa about Radius attribute details; the no operation of this command will disable that debug information.

Parameters：*<interface-number>***:** the number of the interface.

*<interface-name>***:** the name of the interface.

Command Mode：Admin Mode.

Usage Guide：By enabling the debug information of aaa about Radius attribute details, users can check Radius attribute details of Radius messages, which might help diagnose the cause of faults if there is any.

Example：Enable the debug information of aaa about Radius attribute details on interface 1/1.

Switch#debug detail attribute interface ethernet 1/1

2.11.3.6 debug aaa detail connection

Command：**debug aaa detail connection**

no debug aaa detail connection

Function：Enable the debug information of aaa about connection details; the no operation of this command will disable that debug information.

Parameters：None.

Command Mode：Admin Mode.

Usage Guide：By enabling the debug information of aaa about connection details, users can check connection details of aaa, which might help diagnose the cause of faults if there is any.

Example：Enable the debug information of aaa about connection details

Switch#debug aaa detail connection

2.11.3.7 debug aaa detail event

Command：**debug aaa detail event**

no debug detail event

Function：Enable the debug information of aaa about events; the no operation of this

command will disable that debug information.

Parameters：None.

Command Mode：Admin Mode.

Usage Guide：By enabling the debug information of aaa about events, users can check the information of all kinds of event generated in the operation process of Radius protocol, which might help diagnose the cause of faults if there is any.

Example：Enable the debug information of aaa about events.

Switch#debug aaa detail event

2.11.3.8 debug aaa error

Command：**debug aaa error**

　　　　　　no debug error

Function：Enable the debug information of aaa about errors; the no operation of this command will disable that debug information.

Parameters：None.

Command Mode：Admin Mode.

Usage Guide：By enabling the debug information of aaa about errors, users can check the information of all kinds of errors that occurs in the operation process of Radius protocol, which might help diagnose the cause of faults if there is any.

Example：Enable the debug information of aaa about errors.

Switch#debug aaa error

2.11.3.9 radius nas-ipv4

Command:radius nas-ipv4 *<ip-address>*

　　　　　no radius nas-ipv4

Function: Configure the source IP address for RADIUS packet sent by the switch. The "**no radius nas-ipv4**" command delete the configuration.

Parameter: *<ip-address>* is the source IP address of the RADIUS packet, in dotted decimal notation, it mast be a valid unicast IP address.

Default: No specific source IP address for RADIUS packet is configured, the IP address of the interface from which the RADIUS packets are sent is used as source IP address of RADIUS packet.

Command mode: Globle Mode.

Usage guide: The source IP address must belongs to one of the IP interface of the switch, otherwise an failure message of binding IP address will be returned when the switch send RADIUS packet. We suggest using the IP address of loopback interface as source IP address, it avoids that the packets from RADIUS server are dropped when the interface link-down.

Example: Configure the source ip address of RADIUS packet as 192.168.2.254.

Switch#radius nas-ipv4 192.168.2.254

2.11.3.10 radius nas-ipv6

Command: radius nas-ipv6 *<ipv6-address>*

    no radius nas-ipv6

Function: Configure the source IPv6 address for RADIUS packet sent by the switch. The "**no radius nas-ipv4**" command delete the configuration.

Parameter: *<ipv6-address>* is the source IPv6 address of the RADIUS packet, it mast be a valid unicast IPv6 address.

Default: No specific source IPv6 address for RADIUS packet is configured, the IPv6 address of the interface from which the RADIUS packets are sent is used as source IPv6 address of RADIUS packet.

Command mode: Globle Mode.

Usage guide: The source IPv6 address must belongs to one of the IPv6 interface of the switch, otherwise an failure message of binding IPv6 address will be returned when the switch send RADIUS packet. We suggest using the IPv6 address of loopback interface as source IPv6 address, it avoids that the packets from RADIUS server are dropped when the interface link-down.

Example: Configure the source ipv6 address of RADIUS packet as 2001:da8:456::1.

Switch#radius nas-ipv6 2001:da8:456::1

2.11.3.11 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

2.11.3.12 radius-server authentication host

Command: radius-server authentication host {<ipv4-address >|<ipv6-address>} [port <port-number>] [key <string>] [primary] [access-mode {dot1x|telnet}]

           no radius-server authentication host { ipv4-address >|<ipv6-address>}

Function: Specifies the IP address and listening port number, cipher key, whether be primary server or not and access mode for the RADIUS server; the no 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;

           <string> is cipher key string;

           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 last.

           [access-mode {dot1x|telnet}] designates the current RADIUS server only use 802.1x authentication or telnet authentication, all services can use current RADIUS server by default.

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, cipher key string and access mode 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. When the first server has responded (whether the authentication is successed or failed), switch does not send the authentication request to the next. If **primary** is specified, then the specified RADIUS server will be the primary server. It will use the cipher key which be configured by **radius-server key <string>** global command if the current RADIUS server not configure key<string>. Besides, it can designate the current RADIUS server only use 802.1x authentication or telnet authentication via access-mode option. It is not configure access-mode option and all services can use current RADIUS server by default.

Example: Setting the RADIUS authentication server address as 200.1.1.1.

Switch(config)#radius-server authentication host 200.1.1.1

2.11.3.13 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

2.11.3.14 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

2.11.3.15 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

2.11.3.16 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

2.11.3.17 radius-server accounting-interim-update timeout

Command：**radius-server accounting-interim-update timeout** *<seconds>*

no radius-server accounting-interim-update timeout

Function：Set the interval of sending fee-counting update messages; the no operation of this command will reset to the default configuration.

Parameters：*<seconds>* is the interval of sending fee-counting update messages, in seconds, ranging from 60 to 3600.

Command Mode：Global mode.

Default：The default interval of sending fee-counting update messages is 300 seconds.

User Guide：This command set the interval at which NAS sends fee-counting update messages. In order to realize the real time fee-counting of users, from the moment the user becomes online, NAS will send a fee-counting update message of this user to the RADIUS server at the configured interval.

The interval of sending fee-counting update messages is relative to the maximum number of users supported by NAS. The smaller the interval, the less the maximum number of the users supported by NAS; the bigger the interval, the more the maximum number of the users supported by NAS. The following is the recommended ratio of interval of sending fee-counting update messages to the maximum number of the users supported by NAS:

The recommended ratio of the interval of sending fee-counting update messages to the maximum number of the users supported by NAS

The maximum number of users	The interval of sending fee-counting update messages(in seconds)
1~299	300（default value）
300~599	600
600~1199	1200
1200~1799	1800
≥1800	3600

Example：The maximum number of users supported by NAS is 700, the interval of sending fee-counting update messages 1200 seconds.

Switch(config)#radius-server accounting-interim-update timeout 1200

2.11.3.18 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 ---------------

2.11.3.19 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 ---------------

2.11.3.20 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	Displays the authentication server number and corresponding IP address, UDP port number, Primary server or not, down or not, and socket number.

.Socket No	
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.

2.11.3.21 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

2.11.4 RADIUS Typical Example

2.11.4.1 IPv4 Radius Example
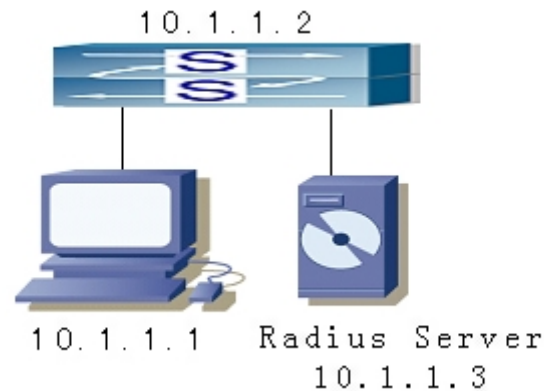
Fig 2-8 The Topology of IEEE802.1x configuration

A computer connects to a switch, of which the IP address is 10.1.1.2 and connected with a RADIUS authentication server without Ethernet1/2; IP address of the server is 10.1.1.3 and the authentication port is defaulted at 1812, accounting port is defaulted at 1813.

Configure steps as 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

2.11.4.2 IPv6 RadiusExample
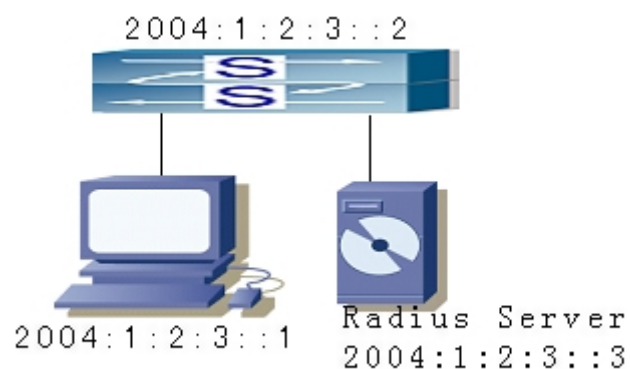
Fig 2-9 The Topolopy of IPv6 Radius configuration

A computer connects to a switch, of which the IP address is 2004:1:2:3::2 and connected with a RADIUS authentication server; IP address of the server is 2004:1:2:3::3 and the authentication port is defaulted at 1812, accounting port is defaulted at 1813.

Configure steps as below:Switch(config)#interface vlan 1
Switch(Config-if-vlan1)#ipv6 address 2004:1:2:3::2/64
Switch(Config-if-vlan1)#exit
Switch(config)#radius-server authentication host 2004:1:2:3::3
Switch(config)#radius-server accounting host 2004:1:2:3::3
Switch(config)#radius-server key test
Switch(config)#aaa enable
Switch(config)#aaa-accounting enable

2.11.5 RADIUS Troubleshooting

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

☞ First make sure good condition of the RADIUS server physical connection;

☞ Second all interface and link protocols are in the UP state (use "show interface" command);

☞ Then ensure the RADIUS key configured on the switch is in accordance with the one configured on RADIUS server;

☞ Finally ensure to connect to the correct RADIUS server.

2.12 Web Management

2.12.1 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.

2.12.1.1 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 clock configuration	
HH:MM:SS	2 3 : 0 : 0
YYYY.MM.DD	2 0 0 2 . 8 . 1

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

Example: configure the Hostname as "London" and IP address as 200.121.1.1 and then click on the "Apply" button. This configuration will be applied to the switch.

Basic host configuration	
Host name	London
IP address	200.121.1.1

Users should click "Switch basic configuration" and "Configure exec timeout" to configure the timeout of quitting Admin mode.

2.12.1.2 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.

Configure exec timeout	
Timeout	6

2.12.2 SNMP configuration

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

2.12.2.1 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.

Snmp manager Configure		
Community string (0-255 character)	Access priority	State
public	Read only	Valid
private	Read and write	Valid
	Read only	Invalid
	Read only	Invalid

2.12.2.2 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.

TRAP manager configuration		
Trap receiver	Community string	State
41.1.1.100	trap	Valid
		Invalid
		Invalid
		Invalid
		Invalid
		Invalid
		Invalid
		Invalid

2.12.2.3 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.

Configure ip address of snmp manager	
Security ip address	State
41.1.1.100	Valid
	Invalid
	Invalid
	Invalid
	Invalid
	Invalid

2.12.2.4 SNMP statistics

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

```
Information Feedback Window
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
```

2.12.2.5 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.

RMON and TRAP configuration	
Snmp Agent state	Open
RMON state	Open
Trap state	Open

2.12.3 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

2.12.3.1 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.

TFTP client service	
Server IP address	10.1.1.1
Local file name(1-100 character)	nos.img
Server file name(1-100 character)	nos.img
Operation type	○Upload ◉Download
Transmission type	○ascii ◉binary

2.12.3.2 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."

TFTP server service	
Server state	Open ▾
TFTP Timeout(5-3600 second)	2 0
TFTP Retransmit times(1-20)	5

2.12.3.3 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".

FTP client service	
Server IP address	10.1.1.1
User (1-100)	switch
Password(1-100)	switch
Local file name(1-100)	nos.img
Server file name(1-100)	nos.img
Transmission type	○ascii ⦿binary
	Upload Download

2.12.3.4 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."

FTP server service	
FTP server State	Open ⌄
FTP Timeout(5-3600 second)	6 0 0

2.12.4 Maintenance and debug command

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 version-to display the number/version of the switch.

2.12.4.1 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."

PING	
IP address	192.168.1.180
Host name	

2.12.4.2 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."

Show port information(VLAN mode, VLAN ID, Trunk information)	
Port	1/1 ▾

2.12.4.3 Others

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

Example:

to display the clock:

```
Information Feedback Window
Current time is FRI APR 20 18:14:13 2007
```

to display FLASH files:

```
Information Feedback Window
boot.rom                        392,472 1900-01-01 00:00:00 --SH
boot.conf                            85 1900-01-01 00:00:00 --SH
nos.img                  10,079,280 2007-04-20 16:25:50 ----
startup-config                1,695 2007-04-20 16:19:48 ----

Total 10473532 byte(s) in 4 file(s), free 23080900 byte(s).
```

2.12.5 Basic introduction to switch

Users should click "Switch basic configuration" and "Switch basic information" to enter into the configuration page and make configuration nodes

Words and phrases are explained in the following:

● Device type-type of device

● Software version-the number/version of software

● Hardware version-the number/version of hardware

● Prompt-prompts of command-line interface

```
Information Feedback Window
  ES4710BD Device, Feb 12 2007 18:41:36
  HardWare version is 1.0, SoftWare package version is ES4710BD_5.2.1.0,
  Copyright (C) 2001-2006 by Accton Technology Corp.
  All rights reserved.
  Last reboot is cold reset
  Uptime is 0 weeks, 0 days, 1 hours, 46 minutes
```

2.12.6 Switch Maintenance

On the left directory of the root page, users should click "Switch maintenance" to configure maintenance nodes through web interface.

2.12.6.1 Exit current web configuration

Users should quit the web-login by clicking "Switch maintenance" and "Exit current web configuration."

```
Exit current web configuration
```

2.12.6.2 Save current running-config

Users should save the current running-config by clicking "Switch maintenance", "Save current running-config" and "Apply".

```
Save current running-config
```

2.12.6.3 Reboot

Users should reboot the switch by clicking "Switch maintenance."

```
Reboot
```

```
Save current configuration before reboot?
⊙ Yes ○ No
```

2.12.6.4 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."

```
Reboot with the default configuration
```

2.12.7 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.

2.12.8 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.

```
Telnet server state
Telnet server state    Open ▼
```

2.12.9 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".

Telnet server Security IP	
Security IP address	100.1.1.1
Operation	Add Security IP address

Telnet server Security IP list
end of security IP

2.12.10 RADIUS client configuration

Click "Authentication configuration", "RADIUS client configuration", to open Radius client configuration management list Users may the configure switch Radius client.

2.12.10.1 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

2.12.10.2 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's 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

2.12.10.3 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.

RADIUS accounting server configuration	
Accounting server IP	10.0.0.1
Accounting server port(optional)	
Primary accounting server	Primary accounting server
Operation type	Add accounting server

RADIUS accounting server configuration list		
server IP	port num	Primary server

Chapter 3 Device Management

3.1 Device Management Brief

The device management function of ES4700 series provides information about line card status, line card operation debugging, power supply and fan status. This function enables the maintenance and management of the physical devices and restart of the switch and line cards, and hot swapping of the cards. ES4700 series supports dual-master mode. If 2 master management cards are present in the system, the master control board in the smaller slot number becomes the Active Master and the other board becomes the Standby Master.

3.2 Device Management Configuration

3.2.1 Switch Basic Configuration

Command: reset slot <*slotno*>
Function: Resets specified card.
Parameters: < *slotno*> is the slot number, or the card located in that slot, the valid range is 1 to 4, M1, M2, and 5 to 8.
Command mode: Admin Mode
Usage Guide: This command can reset all line cards and Standby Master board, but not the Active Master board.

3.3 Device Management Troubleshooting Help

3.3.1 Monitor and Debug Command

3.3.1.1 show slot

Command: show slot [<*slotno*>]
Function: to display basic information of every module

Parameter: <slotno> is the number of the slot (The range value: 1 to 4, M1, M2, and 5 to 8)

Default: if slotno does not specify any, then the default displays all of the module information.

Command mode: Admin Mode

Example:

Switch# show slot 1

--------slot : 1--------

Inserted: YES

slot type is: EM4704BD-M12GX-SFP

work mode: active master

work state: RUNNING

software version is: RW-1.3.2

hardware version is: 1.1

bootrom version is: 1.3.1

serialNo is: N043900039

manufactureDate is: 2004/09/10

temperature is: 33.4375

3.3.1.2 show fan

Command: show fan

Function:to display whether the fan exists or not

Parameter: None

Default: not display

Command mode: Admin Mode

Instructions: "fan board Inserted：" means whether the fan exists or not. One fan tray contains four fans.

Example:

Switch# show fan

----------fan information----------

fan board Inserted: OK

3.3.1.3 show power

Command: show power

Function: to display whether the power exists or not

Parameter: None

Default: not display

Command mode: Admin Mode

Usage guide: "OK" means the power exits. "NO" means the power does not exist.

Example:

Switch# show power

----------power information----------
power1 Inserted: OK
power2 Inserted: NO

3.3.1.4 debug devsm

Command: debug devsm { *send | receive | state* **}**

       no debug devsm {*send | receive | state* **}**

Function: Displays the device management packet traffic and cards status conditions.

The "**no debug devsm {***send | receive | state* **}**" command disables DEBUG display.

Parameters:send displays outgoing device management packets.

       receive displays incoming device management packets.

      state displays card status change information

Default: Debugging information is disabled by default.

Command mode: Admin Mode

3.4 Card Hot-Swap Operation

ES4700 series supports hot swapping of cards. Hot swapping of non-master management cards/cards will not affect the normal operation of other line cards.

3.4.1 Card Hot-Insertion

The cards are automatically powered once inserted into the slots. A blinking RUN indicator in 1Hz indicates the card is working normally. User entry recognition by the switch will be stopped during the hot insertion of cards and resumed once the cards enter normal operation mode.

3.4.2 Card Hot-Remove
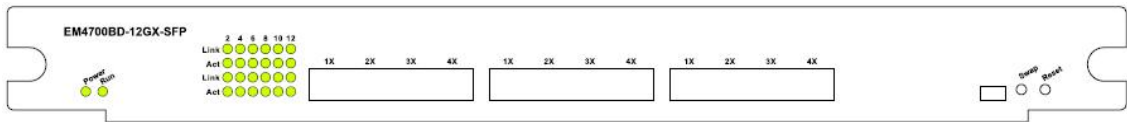
If the cards need to be replaced during normal operation, the following guidelines should be followed:

◆ Hot-remove the the card to be repleaced. the master control board will display a message of "pull out",and the card status becomes destroyed.

◆ Insert the new card. the master control board will display a message of "push in".After the card run normally,the master control board will display the link state of the card's port.

Note: Active Master control board can not be removed online.

3.5 Configuration Restoration Rules

When the switch starts up, the system will reload the information saved in the "StartUp-Config" configuration file from the FLASH. If the card in slot N mismatches the card type saved in "StartUp-Config", then the configuration for that card will not be reloaded.

When the system is operating normally and a user removes a card, the system keeps all the information configured for that card but won't write to FLASH, the information will be lost upon system restart.

When the system is operating normally and the user hot-inserts a card into a slot with a different card inserted previously, the system will not reload configuration; if the slot has a same type of card as the one inserted previously, then the system will try to reload the saved card's configuration; if the saved card's configuration is empty, the slot configuration information recorded in "StartUp-Config" configuration file will be loaded.

3.6 Active-Standby Alternation

The switch supports Active-Standby alternation, i.e., when master management cards are present and working normally, the user can switch the master control board role between Active Master and Standby Master. The "show slot" command can be used to determine the Active Master, non-Active master is the Standby Master. When performing Active-Standby alternation, the user should press the SWAP button of Active Master and remove the board, or just remove the Active Master directly, the Standby Master will then become Active Master. After Active-Standby alternation, the configuration of the switch will revert to the configuration saved in "startup-config".

3.7 Command for device management

3.7.1 debug devsm

Command:debug devsm { *send | receive | state* **}**

   no debug devsm {*send | receive | state* }

Function: Displays the device management packet traffic and cards status conditions. The "**no debug devsm** {*send | receive | state* }" command disables DEBUG display.

Parameters: send displays outgoing device management packets.

   receive displays incoming device management packets.

   state displays card status change information

Default: Debugging information is disabled by default.

Command mode: Admin Mode

3.7.2 force runcfg-sync

Command: force runcfg-sync

Function Enforce the synchronizing running-config from active master to standby master

Command Mode: Admin mode

Usage Guide: When the running-config varies from the startup-configure, this command synchronizes running-configure from active master to standby master, so that the new running-config will be used as restoration when performing the switchover.

3.7.3 force switchover

Command: force switchover

Function: Enforce the active master switched to standby master

Command Mode: Admin Mode

Usage Guide: When standby master exits, if this command is executed on active master will trigger the switchover, and the former standby master will become the new active master.

3.7.4 reset slot

Command: reset slot *<slotno>*

Function: Resets specified card.

Parameters: < *slotno*> is the slot number, or the card located in that slot, the valid range is 1 to 4, M1, M2, and 5 to 8.

Command mode: Admin Mode

Usage Guide: This command can reset all line cards and Standby Master board, but not the Active Master board.

3.7.5 runcfg-sync

Command: runcfg-sync [<*interval*>]

Function: Configure the running-config synchronous interval.

Parameter: <*interval*> is the synchronous time interval which is shown in minutes and ranges from 5 to 1440 or 0, in which 0 refers to the auto synchronization function is disabled, no parameter followed refers to enabled running-config synchronizing function. When the configuration file changes, default synchronization interval is 5 minutes.

Command Mode: Global mode

Default: Auto synchronization function enabled by default, default synchronization interval is 5 minutes.

Usage Guide: This command is for configuring the interval between which the active master synchronizes the running-config to standby master regularly. Undersized interval configuration will result in unnecessary load to the switch. The auto synchronization function is recommended to be disabled if the configuration is stable or will be saved with write command after changes take place.

Example: Set the running-config synchronization interval to 1440 minutes

Switch(config)#runcfg-sync 1440

3.7.6 show fan

Command: show fan

Function: Shows whether the fan tray is in place and its running status.

Parameters: N/A.

Default: No display by default.

Command mode: Admin Mode

Usage Guide: "fan board Inserted:YES" for fan in place; "fan board Inserted:NO" for fan not in place."fan status:FAULt" for an error status,"fan status:NORMAL" indicate that fan is running normally.

Example:

Switch # show fan

----------fan board information----------

fan1 board Inserted: NO

fan2 board Inserted: YES

fan3 board Inserted: YES

fan2 status: FAULT

fan3 status: NORMAL

3.7.7 show power

Command: show power

Function: Shows if the power supply is in place.

Parameters: N/A.

Default: No display by default.

Command mode: Admin Mode

Usage Guide: "YES" for power supply in place; "NO" for power supply not in place.

Example:

Switch # show power

----------power information----------

power1 Inserted: NO

power2 Inserted: NO

power3 Inserted: YES

3.7.8 show slot

Command: show slot [<*slotno*>]

Function: Show basic informations of each chips

Parameter: <*slotno*> is the number of the slot the chip resides, ranging between 1~4 for 4 slots device or 1~8 for 8 slots device

Default: All chip information will be listed by default if now *slotno* is specified

Command Mode: Admin mode

Example:
Switch# show slot 1

--------------------Slot : 1--------------------

Inserted: YES

Module type: EM4704BD-M12GX-SFP

Work mode: ACTIVE MASTER

Work state: RUNNING

Software package version: 5.0.7.0

Local software version: 4.0.7.0

Hardware version: 1.1

Bootrom version: 1.5.11

Serial number: 2514521475

Manufacture date: 2005/10/02

Temperature: 46.6250

Chapter 4 Port Configuration

4.1 Introduction to Port

ES4700 series comes with line cards and master management cards. Line cards provide various network ports. The master management cards provide console interface and network management port. The Console interface and network management port are used for out-of-band management of the switch. This chapter focuses on network ports and the network management port.

Network ports are provided by the line cards. The port index is marked on the panels of all the line cards for the ES4700 series.To distinguish between ports in different line cards, the port nomination (in the sense of software) provided by the ES4700 series system is "ethernet X/Y", where X stands for the slot number for the card and Y stands for the number marked in the card panel. For instance, a EM4700BD-12GX-SFP line card is inserted to slot 1, then port 3 of this card corresponds to "ethernet 1/3". If the user needs to configure some network ports, the "**interface ethernet <interface-list>**" command can be used 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 of the card in slot 1 and ports 8, 9, 10 on the card in slot 3, the command would look like: **interface ethernet 1/2-5;3/8-10.** 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.

The Network management port is located above the Console interface on the master management cards, marked as "Ethernet", the software configuration name for this port is "**Ethernet0**". The user can use the command "**interface Ethernet 0**" to access the network port configuration mode. The user can use programs such as Telnet, Web management and FTP to manage the switch through a Ethernet cable connected to the network management port. The network management port can neither perform data forwarding like the network interfaces, nor use Layer 2 protocols (like RSTP) and Layer 3 routing protocols, nor identify the cable type automatically (such as crossover cables that are required to directly connect to a PC). The network management port supports connection speeds of 10/100 Mbps, it can have an IP address configured in addition to properties such as speed and duplex mode. If the switch has 2 master control cards and

both are operating normally, only the Ethernet port in the Active Master can be used as the network management port. When Active-Standby occurs, the network management port will change accordingly.

4.2 Port Configuration

4.2.1 Network Port Configuration

4.2.1.1 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
   （10） Set the interval at which counting the flow through a line card port of a rack mount switch

1. Enter the Ethernet port configuration mode

Command	Explanation
Port mode	
interface ethernet *<interface-list>*	Enters the network port configuration mode.

2. Configure the properties for the Ethernet ports

Command	Explanation
Port 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 (This command is not supported on the ES4700 series line card ports of 1000MB and above)
**speed-duplex {auto	force10-half	force10-full	force100-half	force100-full	force100-fx [module-type {auto-detected |no-phy-integrated	phy-integrated}] |{ {force1g-half	force1g-full} [nonegotiate [master	slave]] } }** **no speed-duplex**	Sets port speed and duplex mode of 100/1000Base-TX or 100Base-FX 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.
remote-statistics interval <seconds>	Set the interval at which counting the flow through a line card port of a rack mount switch.

4.2.1.2 Command for Network Port Configuration

4.2.1.2.1 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 ports; **copper-preferred-auto** for copper cable port first; **sfp-forced** for fiber cable forces to use fiber cable port; **sfp-preferred-auto** for fiber cable port first.

Command mode: Port 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 consist 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 or copper cable port: Hardware is Gigabit-combo, active is fiber (copper).

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

4.2.1.2.2 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

4.2.1.2.3 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: Port Mode.

Default: No port name by default.

Usage Guide: This command is for helping the user 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

4.2.1.2.4 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: Port 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. ES4704BD'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: Enable the flow control function in ports 1/1-8.

Switch(config)#interface ethernet 1/1-8

Switch(Config-Port-Range)#flow control

4.2.1.2.5 interface ethernet

Command: interface ethernet *<interface-list>*

Function: Enters Ethernet Port 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 Port mode to Global Mode.

Example: Entering the Ethernet Port mode for ports 1/1, 2/4-5, 3/8.

Switch(config)#interface ethernet 1/1;2/4-5;3/8

4.2.1.2.6 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: Port 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: Enable loopback test in Ethernet ports 1/1 -8

Switch(config)#interface ethernet 1/1-8

Switch(Config-Port-Range)#loopback

4.2.1.2.7 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 ES4704BD line card 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: Port 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 3/5 -8 to straight-through cable only.

Switch(config)#interface ethernet 3/5-8

Switch(Config-Port-Range)#mdi normal

4.2.1.2.8 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 or 100Base-FX interface. For combo port, this command applies to the 1000Base-TX port only but has no effect on the 1000Base-TX port. To change the negotiation mode, speed and duplex mode of 1000Base-FX port, use **speed-duplex** command instead.

Example: Port 1 of SwitchA is connected to port 1 of SwitchB, the following will disable the negotiation for both ports.

SwitchA(config)#interface ethernet1/1

SwitchA(Config-If-Ethernet1/1)#no negotiation

SwitchB(config)#interface ethernet1/1

SwitchB(Config-If-Ethernet1/1)#no negotiation

4.2.1.2.9 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: Port 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 of the chip on slot 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

4.2.1.2.10 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>** is the limit of packet number, ranging from 1 to 1488905. For non-10GB ports, the unit of <packets> is PPS, that is, the value of <packets> is the number of packets allowed to pass per second; for 10GB ports, the unit is KPPS, that is, the value of <packets> multiplies 1000 makes the number of packets allowed, so the value should be less than 14880.

Command mode: Port 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 above mentioned 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) of slot 2 to allow 3 broadcast packets per second.

Switch(config)#interface ethernet 2/8-10
Switch(Config-Port-Range)#rate-suppression broadcast 3

4.2.1.2.11 rate-violation

Command：rate-violation <packets> [recovery <time>]

no rate-violation

Function: Enable the limit on packet reception rate function, and set the packet reception rate in one second, the no command delete the function of limit on packet reception rate. The rate-violation means the packet reception rate, that is, the number of received packets per second, regardless of their type.

Parameters: <packets> the max number of packets allowed to pass through the port.

recovery: means after a period of time the port can recover "Shutdown" to "UP" again. **<time>** is the timeout of recovery. For example, if the shutdown of a port happens after the packet reception rate exceeding the limit, the port will be "up" again when the user-defined timeout period expires. The default timeout is 300s, while 0 means the recovery will never happen.

Command Mode: Port Mode

Default: There is no limit on packet reception rate by default.

Usage Guide： This command is mainly used to detect the abnormal port flow. For example, when there are a large number of broadcast messages caused by a loop, which affect the processing of other tasks of the switch, the port will be shut down to guarantee the normal operation of the switch.

Example: If users set the rate-violation of port 8-10 (GB ports) of the switch as 10000pps and the port recovery time as 1200 seconds, when the packet reception rate exceeds 10000, the port will but shut down, and then, after 1200 seconds, the port will be UP again.

Switch(config)#interface ethernet 1/8-10

Switch(Config-Port-Range)#rate-violation 10000 recovery 1200

4.2.1.2.12 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; 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

4.2.1.2.13 shutdown

Command:shutdown

              no shutdown

Function: Shuts down the specified Ethernet port; the "**no shutdown**" command opens the port.

Command mode: Port 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

4.2.1.2.14 speed-duplex

Command: speed-duplex {auto | force10-half | force10-full | force100-half | force100-full | force100-fx [module-type {auto-detected |no-phy-integrated | phy-integrated}] |{ {force1g-half | force1g-full} [nonegotiate [master | slave]] } }

no speed-duplex

Function: Sets the speed and duplex mode for 1000Base-TX, 100Base-TX or 100Base-FX 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; **force100-fx** for forced 100Mbps at full-duplex mode; **module-type** is the type of 100Base-FX module; **auto-detected:** automatic to detect; **no-phy-integrated:** there is no phy-integratd 100Base-TX module; **phy-integrated:** phy-integratd 100Base-TX module; **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: Port configuration Mode

Default: Auto-negotiation for speed and duplex mode is set by default.

Usage Guide: This command sets the speed and duplex mode for ports.

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 SwitchA is connected to port 1 of SwitchB, the following will set both ports in forced 100Mbps at half-duplex mode.

SwitchA(config)#interface ethernet1/1

SwitchA(Config-If-Ethernet1/1)#speed-duplex force100-half

SwitchB(config)#interface ethernet1/1

SwitchB(Config-If-Ethernet1/1)#speed-duplex force100-half

4.2.1.2.15 remote-statistics interval

Command：remote-statistics interval *<seconds>*

Function： Set the interval at which counting the flow through a line card port of a rack mount switch.

Parameters： *<seconds>* the interval at which counting the flow through a line card port, in seconds, ranging from 5 to 300. The value should be a multiple of 5.

Command Mode: Global mode.

Default: The default interval at which counting the flow through a line card port is 60 seconds.

User Guide: On a rack mount switch, every line card will automatically notify the main control card of the flow information of its ports at a regular interval. The main control card records the flow information of every port on all line cards. When the network management software sends a request to the main control card, the latter will send the low information of every port on all line cards saved locally back to the software. Thus, network management software will not affect other tasks while normally monitoring flows.

Please pay attention to that: the shorter the interval at which line cards notify the main control cards of flow is, the more accurate the flow-counting, but the more system resources will be taken, vice versa. So, in practical operation, this interval should be chosen properly according to reality. Or, some glitches might appear due to the period of time taken by the network management software to read the flow information, and the situation that the interval at which the network management software monitors the flows of the switches and the interval at which the line cards notify the main control card of their flows do not match.

In practical operation, in order to get an accurate flow statistic information while avoiding major effects on operation of the switches from the network management software, it is recommended that the interval at which the network management software monitors the flows of the switches is 10 times of the interval at which the line cards notify the main control card of their flows. Since the default value of the interval at which the line cards notify the main control card of their flows is 60 seconds, it is recommended that the interval at which the network management software monitors the flows of the switches is 600 seconds, i.e. 10 minutes.

Example： Given that the interval at which the network management software monitors the flows of the switches is 900 seconds, so set the interval at which the line cards notify the main control card of their flows on the switch as 90 seconds.

Switch(config)#remote-statistics interval 90

4.2.2 VLAN Interface Configuration

4.2.2.1 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 Port 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

4.2.2.2 Command For Vlan Interface

4.2.2.2.1 interface vlan

Command: interface vlan <*vlan-id*>

          no interface vlan <*vlan-id*>

Function: Enters Port 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 Port mode for VLAN1.

Switch(config)#interface vlan 1

4.2.2.2.2 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: Port 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, ES4700 series 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

4.2.2.2.3 shutdown

Command: shutdown

        no shutdown

Function: Shuts down the specified VLAN Interface; the "**no shutdown**" command opens the VLAN interface.

Command mode: Port 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: Enable VLAN1 interface of the switch.

Switch(Config-if-Vlan1)#no shutdown

4.2.3 Network Management Port Configuration

4.2.3.1 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） 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
ip address <ip-address> <mask> **no ip address [<ip-address> <mask>]**	Configures or cancels the IP address for network management port.

4.2.3.2 Command for Network Management Port Configuration

4.2.3.2.1 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-If-Ethernet0)#duplex full

4.2.3.2.2 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 Port mode to Global Mode.

Example: Entering network management port mode.

Switch(config)#interface ethernet 0

Switch(Config-If-Ethernet0)#

4.2.3.2.3 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-If-Ethernet0)#ip address 192.168.1.10 255.255.255.0

4.2.3.2.4 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: Enable the network management interface.

Switch(config)#interface ethernet 0

Switch(Config-If-Ethernet0)#no shutdown

4.2.3.2.5 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-If-Ethernet0)#speed force100

4.3 Port Mirroring Configuration

4.3.1 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.

This switch supports 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.

4.3.2 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.

4.3.3 Command For Mirroring Configuration

4.3.3.1 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

4.3.3.2 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

4.3.4 Device Mirroring Troubleshooting Help

If a problems occurs 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.

4.4 Port Configuration Example
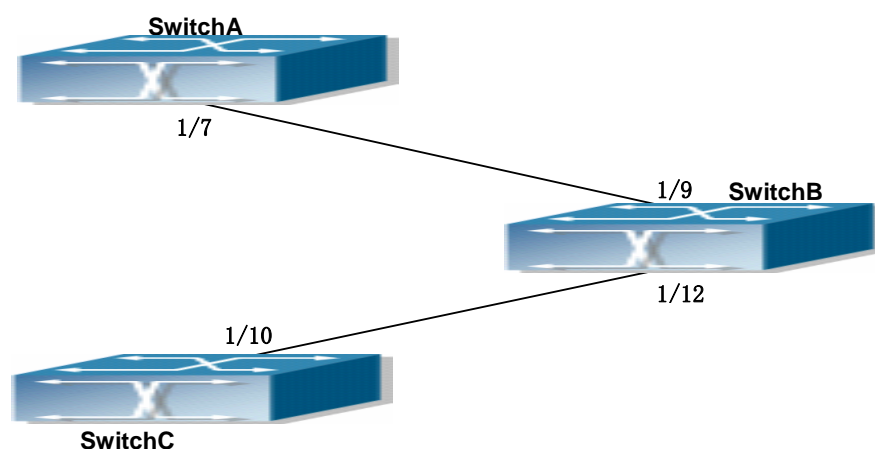
Fig 4-1 Port Configuration Example

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

4.5 Port Troubleshooting Help

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.

4.6 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.

4.6.1 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.

4.6.2 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 configuration			
Port	mdi	Admin status	speed/duplex status
Ethernet1/1	auto	no shutdown	Auto

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
```

4.6.3 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 2/1, 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.

```
Bandwidth control
Port              Bandwidth control level        Control type
                       (1-10000Mb)
Ethernet1/1  ▾    100                            Ingress         ▾
```

4.6.4 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.

4.6.5 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.

L3 interface configuration					
VLAN Port	Port IP address	Port network mask	Port status	Operation type	
Vlan10	192.168.1.180	255.255.255.0	no shutdown	Add address	

4.6.6 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.

L3 interface IP mode	
VLAN Port	Vlan10
IP mode	Specify IP address

4.6.7 Port mirroring configuration

Click "Port configuration", "Port mirroring configuration" to enter port mirroring configuration management table to do port mirroring configurations.

4.6.8 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.

Source port mirroring configuration		
source interface list	Mirror direction	destination interface
1 / 1 — 4	rx	Ethernet1/5

4.6.9 Port debug and maintenance

Click Port configuration, Port debug and maintenance and open the Port debug and maintenance management list to get port information.

4.6.10 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 5 Port Loopback Detection Function Configuration

5.1 Introduction to Port Loopback Detection Function

With the development of switches, more and more users begin to access the network through Ethernet switches. In enterprise network, users access the network through layer-2 switches, which means urgent demands for both internet and the internal layer 2 Interworking. When layer 2 Interworking is required, the messages will be forwarded through MAC addressing the accuracy of which is the key to a correct Interworking between users. In layer 2 switching, the messages are forwarded through MAC addressing. Layer 2 devices learn MAC addresses via learning source MAC address, that is, when the port receives a message from an unknown source MAC address, it will add this MAC to the receive port, so that the following messages with a destination of this MAC can be forwarded directly, which also means learn the MAC address once and for all to forward messages.

When a new source MAC is already learnt by the layer 2 device, only with a different source port, the original source port will be modified to the new one, which means to correspond the original MAC address with the new port. As a result, if there is any loopback existing in the link, all MAC addresses within the whole layer 2 network will be corresponded with the port where the loopback appears (usually the MAC address will be frequently shifted from one port to another), causing the layer 2 network collapsed. That is why it is a necessity to check port loopbacks in the network. When a loopback is detected, the detecting device should send alarms to the network management system, ensuring the network manager is able to discover, locate and solve the problem in the network and protect users from a long-lasting disconnected network.

Since detecting loopbacks can make dynamic judgment of the existence of loopbacks in the link and tell whether it has gone, the devices supporting port control (such as port isolation and port MAC address learning control) can maintain that automatically, which will not only reduce the burden of network managers but also response time, minimizing the effect caused loopbacks to the network.

5.2 Port Loopback Detection Function Configuration

5.2.1 Port Loopback Detection Function Configuration Task List

1. Configure the time interval of loopback detection
2. Enable the function of port loopback detection
3. Configure the control method of port loopback detection
4. Display and debug the relevant information of port loopback detection
5. Configure loopback-detection control mode (automatic recovery enabled or not)

1. Configure the time interval of loopback detection

Command	Explanation
Global Mode	
loopback-detection interval-time <loopback> <no-loopback> **no loopback-detection interval-time**	Configure the time interval of loopback detection

2. Enable the function of port loopback detection

Command	Explanation
Port Mode	
loopback-detection specified-vlan <vlan-list> **no loopback-detection specified-vlan <vlan-list>**	Enable and disable the function of port loopback detection

3. Configure the control method of port loopback detection

Command	Explanation
Port Mode	
loopback-detection control {shutdown |block| learning } **no loopback-detection control**	Enable and disable the function of port loopback detection control

4. Display and debug the relevant information of port loopback detection

Command	Explanation

Admin Mode	
debug loopback-detection **no debug loopback-detection**	Enable the debug information of the function module of port loopback detection. The no operation of this command will disable the debug information.
show loopback-detection [interface ***<interface-list>]***	Display the state and result of the loopback detection of all ports, if no parameter is provided; otherwise, display the state and result of the corresponding ports.

5. Configure loopback-detection control mode (automatic recovery enabled or not)

Command	Explanation
Global Configuration Mode	
loopback-detection control-recovery **timeout <integer>**	Configure the loopback-detection control mode (automatic recovery enabled or not) or recovery time.

5.2.2 Command for Port Loopback Detection Function

5.2.2.1 loopback-detection control

Command: loopback-detection control {shutdown |block| learning }
　　　　　no loopback-detection control

Function: Enable the function of loopback detection control on a port, the no operation of this command will disable the function.

Parameters: shutdown set the control method as shutdown, which means to close down the port if a port loopback is found.

　　　　　Block set the control method as block, which means to block a port by allowing bpdu and loopback detection messages only if a port loopback is found.

　　　　　Learning disable the control method of learning MAC addresses on the port, not forwarding traffic and delete the MAC address of the port.

Default: Disable the function of loopback diction control.

Command Mode: Port Mode.

Usage Guide: If there is any loopback, the port will not recovery the state of be controlled after enabling control operation on the port. If the overtime is configured, the

ports will recovery normal state when the overtime is time-out. If the control method is block, the corresponding relationship between instance and vlan id should be set manually by users, it should be noticed when be used.

Example：Enable the function of loopback detection control under port1/2 mode.

Switch(config)#interface ethernet 1/2

Switch(Config-If-Ethernet1/2)#loopback-detection control shutdown

Switch(Config-If-Ethernet1/2)#no loopback-detection control

5.2.2.2 loopback-detection specified-vlan

Command：**loopback-detection specified-vlan *<vlan-list>***

             no loopback-detection specified-vlan [*<vlan-list>*]

Function：Enable the function of loopback detection on the port and specify the VLAN to be checked; the no operation of this command will disable the function of detecting loopbacks through this port or the specified VLAN.

Parameters：*<vlan-list>* the list of VLANs allowed passing through the port. Given the situation of a trunk port, the specified vlans can be checked. So this command is used to set the vlan list to be checked.

Default：Disable the function of detecting the loopbacks through the port.

Command Mode：Port Mode.

Usage Guide：If a port can be a TRUNK port of multiple Vlans, the detection of loopbacks can be implemented on the basis of port+Vlan, which means the objects of the detection can be the specified Vlans on a port. If the port is an ACCESS port, only one Vlan on the port is allowed to be checked despite the fact that multiple Vlans can be configured. This function is not supported under Port-channel.

Example：Enable the function of loopback detection under port 1/2 mode.

Switch(config)#interface ethernet 1/2

Switch(Config-If-Ethernet1/2)#switchport mode trunk

Switch(Config-If-Ethernet1/2)#switchport trunk allowed vlan all

Switch(Config-If-Ethernet1/2)#loopback-detection specified-vlan 1;3;5-20

Switch(Config-If-Ethernet1/2)#no loopback-detection specified-vlan 1;3;5-20

5.2.2.3 loopback-detection interval-time

Command：**loopback-detection interval-time *<loopback> <no-loopback>***

            no loopback-detection interval-time

Function：Set/close the loopback detection interval.

Parameters：*<loopback >* the detection interval if any loopback is found, ranging from 5 to 300, in seconds.

             <no-loopback > the detection interval if no loopback is found, ranging from

1 to 30, in seconds.

Default：The default value is 5s with loopbacks existing, and 3s otherwise.

Command Mode：Global Mode.

Usage Guide：When there is no loopback detection, the detection interval can be relatively shorter, for too short a time would be a disaster for the whole network if there is any loopback. So, a relatively longer interval is recommended when loopbacks exist.

Example：Set the loopback diction interval as 35,15.

Switch(config)#loopback-detection interval-time 35 15

5.2.2.4 loopback-detection control-recovery timeout

Command: loopback-detection control-recovery timeout <0-3600>

Function: This command is used to recovery to uncontrolled state after a special time when a loopback being detected by the port entry be controlled state.

Parameters: <0-3600> second is recovery time for be controlled state, 0 is not recovery state.

Default: The recovery is not automatic by default.

Command Mode: Global Configuration Mode.

Usage Guide: When a port detects a loopback and works in control mode, the ports always work in control mode and not recover. The port will not sent packet to detection in shutdown mode, however, the port will sent loopback-detection packet to detection whether have loopback in block or learning mode. If the recovery time is configured, the ports will recovery normal state when the overtime is time-out. The recovery time is a useful time for shutdown control mode, because the port can keep on detection loopback in the other modes, so suggest not to use this command.

Examples: Enable automatic recovery of the loopback-detection control mode after 30s.

Switch(config)#loopback-detection control-recovery timeout 30

5.2.2.5 show loopback-detection

Command：**show loopback-detection [interface *<interface-list>*]**

Function：Display the state of loopback detection on all ports if no parameter is provided, or the state and result of the specified ports according to the parameters.

Parameters：*<interface-list>* the list of ports to be displayed, for example: ethernet 1/1.

Command Mode：Admin and Config Mode.

Usage Guide：Display the state and result of loopback detection on ports with this command.

Example：Display the state of loopback detection on port 4.

Switch(config)#show loopback-detection interface ethernet 1/4

loopback detection config and state information in the switch!

PortName	Loopback Detection	Control Mode	Is Controlled
Ethernet1/4	Enable	Shutdown	No

5.2.2.6 debug loopback-detection

Command：debug loopback-detection

Function：After enabling the loopback detection debug on a port, BEBUG information will be generated when sending, receiving messages and changing states.

Parameters：None.

Command Mode：Admin Mode.

Default：Disabled by default..

Usage Guide：Display the message sending, receiving and state changes with this command.

Example：

Switch#debug loopback-detection

%Jan 01 03:29:18 2006 Send loopback detection probe packet:dev Ethernet1/10, vlan id 1

%Jan 01 03:29:18 2006 Send loopback detection probe packet:dev Ethernet1/10, vlan id 2

5.3 Port Loopback Detection Function Example
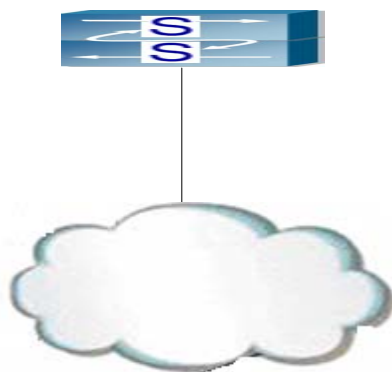
Fig 5-1　A Typical Example of Port Loopback Detection

As shown in the above configuration, the switch will detect the existence of loopbacks in the network topology. After enabling the function of loopback detection on the port connecting the switch with the outside network, the switch will notify the

connected network about the existence of a loopback, and control the port on the switch to guarantee the normal operation of the whole network.

The configuration task sequence of SWITCH:

Switch(config)#loopback-detection interval-time 35 15

Switch(config)#interface ethernet 1/1

Switch(Config-If-Ethernet1/1)#loopback-detection special-vlan 1-3

Switch(Config-If-Ethernet1/1)#loopback-detection control block

If adopting the control method of "block", "mstp" should be globally enabled. And the correspondence between the spanning tree instance and the vlan should be configured.

Switch (Config-If-Ethernet1/1)#spanning-tree

Switch (config)#spanning-tree mst con

Switch (config)#spanning-tree mst configuration

Switch (Config-Mstp-Region)#instance 1 v

Switch (Config-Mstp-Region)#instance 1 vlan 1

Switch (Config-Mstp-Region)#instance 2 vlan 2

Switch (Config-Mstp-Region)#

5.4 Troubleshooting Help on Port Loopback Detection

The function of port loopback detection is disabled by default and should only be enabled if required.

With normal configuration, after enabling the function of port loopback detection, the "debug loopback detection" command can be used to check the detailed information of loopback detection and the validity of the detection result, if there is an obvious loopback in the connected network.

Chapter 6 ULDP Function Configuration

6.1 ULDP Function Introduction

Unidirectional link is a common error state of link in networks, especially in fiber links. Unidirectional link means that only one port of the link can receive messages from the other port, while the latter one can not receive messages from the former one. Since the physical layer of the link is connected and works normal, via the checking mechanism of the physical layer, communication problems between the devices can not be found. As shown in Graph, the problem in fiber connection can not be found through mechanisms in physical layer like automatic negotiation.
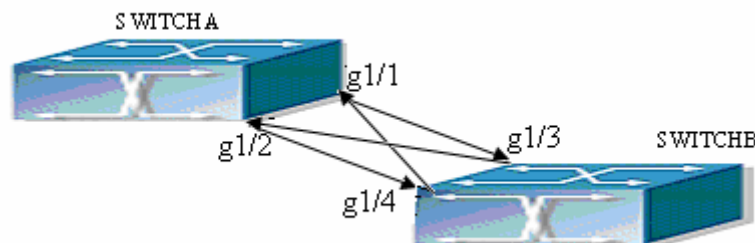
Fig 6-1 Fiber Cross Connection
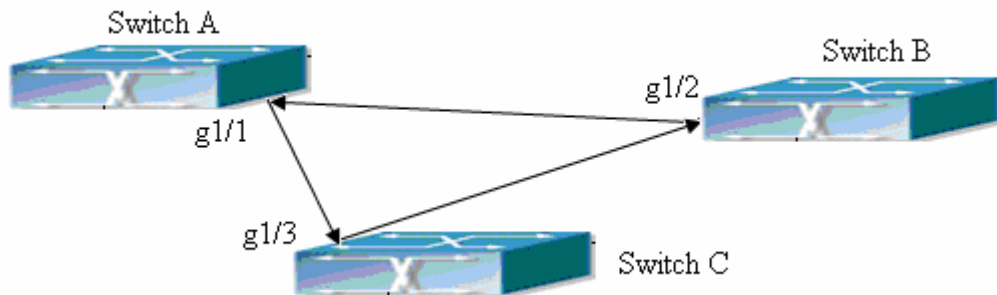
Fig 6-2 One End of Each Fiber Not Connected

This kind of problem often appears in the following situations: GBIC (Giga Bitrate Interface Converter) or interfaces have problems, software problems; hardware becomes unavailable or operates abnormally. Unidirectional link will cause a series of problems, such as spinning tree topological loop, broadcast black hole.

ULDP (Unidirectional Link Detection Protocol) can help avoid disasters that could happen in the situations mentioned above. In a switch connected via fibers or copper Ethernet line (like ultra five-kind twisted pair), ULDP can monitor the link state of physical links. Whenever a unidirectional link is discovered, it will send warnings to users and can disable the port automatically or manually according to users' configuration.

The ULDP of switches recognizes remote devices and check the correctness of link connections via interacting ULDP messages. When ULDP is enabled on a port, protocol state machine will be started, which means different types of messages will be sent at different states of the state machine to check the connection state of the link by exchanging information with remote devices. ULDP can dynamically study the interval at which the remote device sends notification messages and adjust the local TTL (time to live) according to that interval. The time intervals of notification messages and reset in ULDP can be configured by users, so that ULDP can respond faster to connection errors in different network environments.

The premise of ULDP working normally is that link works in duplex mode, which means ULDP is enabled on both ends of the link, using the same method of authentication and password.

6.2 ULDP Configuration Task Sequence

1. Globally enable ULDP function
2. Enable ULDP function on a port
3. Configure aggressive mode globally
4. Configure aggressive mode on a port
5. Configure the method to shut down unidirectional links
6. Configure the interval of Hello messages
7. Configure the interval of Recovery
8. Reset the port shut down by ULDP
9. Display and debug the relative information of ULDP

1. Globally enable ULDP function

Command	Explanation
Global configuration mode	
uldp enable **uldp disable**	Globally enable or disable ULDP function

2. Enable ULDP function on a port

Command	Explanation
Port configuration mode	
uldp enable **uldp disable**	Enable or disable ULDP function on a port

3. Configure aggressive mode globally

Command	Explanation
Global configuration mode	
uldp aggressive-mode **no uldp aggressive-mode**	Set the global working mode

4. Configure aggressive mode on a port

Command	Explanation
Port configuration mode	
uldp aggressive-mode **no uldp aggressive-mode**	Set the working mode of the port

5. Configure the method to shut down unidirectional links

Command	Explanation
Global configuration mode	
uldp manual-shutdown **no uldp manual-shutdown**	Configure the method to shut down unidirectional links

6. Configure the interval of Hello messages

Command	Explanation
Global configuration mode	
uldp hello-interval *<integer>* **no uldp hello-interval**	Configure the interval of Hello messages, ranging from 5 seconds to 100 seconds. The value is 10 seconds by default.

7. Configure the interval of Recovery

Command	Explanation
Global configuration mode	
uldp recovery-time *<integer>* **no uldp recovery-time** *<integer>*	Configure the interval of Recovery, ranging from 30 seconds to 86400 seconds. The value is 0 second by default.

8. Reset the port shut down by ULDP

Command	Explanation
Global mode or port mode	

	Reset all ports in global configuration mode.
uldp reset	Rest the specified port in port configuration mode.

9. Display and debug the relative information of ULDP

Command	Explanation
Admin mode	
show uldp [interface ethernet IFNAME]	Display ULDP information. No parameter means to display global ULDP information. The parameter specifying a port will display global information and the neighbor information of the port.
debug uldp fsm interface ethernet <IFname> **no debug uldp fsm interface ethernet <IFname>**	Enable or disable the debug switch of the state machine transition on the specified port.
debug uldp error **no debug uldp error**	Enable or disable the debug switch of error information.
debug uldp event **no debug uldp event**	Enable or disable the debug switch of event information.
debug uldp packet {receive|send} **no debug uldp packet {receive|send}**	Enable or disable the type of messages can be received and sent on all ports
debug uldp {hello|probe|echo| unidir|all}[receive|send] interface ethernet <IFname> **no debug uldp {hello|probe|echo| unidir|all}[receive|send] interface ethernet <IFname>**	Enable or disable the content detail of a particular type of messages on the specified port.

6.3 ULDP Configuration

6.3.1 uldp enable

Command: uldp enable

Function: ULDP will be enabled after issuing this command. In port configuration mode,

this command will enable ULDP for the port.

Parameters: None.

Command Mode: Global mode and port mode.

Default: By default ULDP is not configured.

Usage Guide: ULDP can be configured for the ports only if ULDP is enabled globally. If ULDP is enabled globally, it will be effect for all the existing fiber ports. For copper ports and fiber ports which are available after ULDP is enabled, this command should be issued in the port configuration mode to make ULDP be effect.

Example: To enable ULDP in global configuration mode:

Switch(config)#uldp enable

6.3.2 uldp disable

Command: uldp disable

Function: To disable ULDP configuration through this command.

Parameters: None.

Command Mode: Global mode and port mode.

Default: By default ULDP is not enabled.

Usage Guide: When ULDP is disabled globally, then ULDP in all the ports will be disabled.

Example: To disable the ULDP configuration in global configuration mode.

Switch(config)#uldp disable

6.3.3 uldp hello-interval

Command: uldp hello-interval *<integer>*

             no uldp hello-interval

Function: To configure the interval for ULDP to send hello messages. The no form of this command will restore the default interval for the hello messages.

Parameters: The interval for the Hello messages, with its value limited between 5 and 100 seconds.

Command Mode: Global mode.

Default: 10 seconds by default.

Usage Guide: Interval for hello messages can be configured only if ULDP is enabled globally.

Example: To configure the interval of hello messages to be 12 seconds.

Switch(config)#uldp hello-interval 12

6.3.4 uldp aggressive-mode

Command: uldp aggressive-mode

        no uldp aggressive-mode

Function: To configure ULDP to work in aggressive mode. The no form of this command will restore the normal mode.

Parameters: None.

Command Mode: Global mode and port mode.

Default: Normal mode.

Usage Guide: The ULDP working mode can be configured only if it is enabled globally. When ULDP aggressive mode is enabled globally, all the existing fiber ports will work in aggressive mode. For the copper ports and fiber ports which are available after the configuration is available, aggressive mode should be enabled in interface configuration mode.

Example: To enable ULDP aggressive mode globally.

Switch(config)#uldp aggressive-mode

6.3.5 uldp manual-shutdown

Command: uldp manual-shutdown

        no uldp manual-shutdown

Function: To configure ULDP to work in manual shutdown mode.

Parameters: None.

Command Mode: Global mode.

Default: Auto mode.

Usage Guide: This command can be issued only if ULDP has been enabled globally.

Example: To enable manual shutdown globally.

Switch(config)#uldp manual-shutdown

6.3.6 uldp reset

Command: uldp reset

Function: To reset the port when ULDP is shutdown.

Parameters: None.

Command Mode: Globally mode and port mode.

Default: None.

Usage Guide: This command can only be effect only if the specified interface is disabled by ULDP.

Example: To reset all the port which are disabled by ULDP.

Switch(config)#uldp reset

6.3.7 uldp recovery-time

Command: uldp recovery-time<*integer*>

        no uldp recovery-time

Function: To configure the interval for ULDP recovery. The no form of this command will restore the default configuration.

Parameters: Recovery-time is the time out value for the ULDP recovery timer. Its value is limited between 30 and 86400 seconds.

Command Mode: Global mode.

Default: 0 is set by default which means the recovery is disabled.

Usage Guide: If an interface is shutdown by ULDP, and the recovery timer times out, the interface will be reset automatically. If the recovery timer is set to 0, the interface will not be reset.

Example: To set the recovery timer to be 600 seconds.

Switch(config)#uldp recovery-time *600*

6.3.8 show uldp

Command: show uldp [interface ethernet<*interface-name*>]

Function: To show the global ULDP configuration and status of a interface. If <interface-name> is specified, ULDP configuration and status about the specified interface as well as its neighbors' will be displayed.

Parameters: Interface name.

Command Mode: Admin mode.

Default : None.

Usage Guide: If no parameters are appended, the global ULDP information will be displayed. If the interface name is specified, information about the interface and its neighbors will be displayed along with the global information.

Example: To display the global ULDP information.

Switch(config)#show uldp

6.3.9 debug uldp fsm interface ethernet

Command: debug uldp fsm interface ethernet <*IFname*>

        no debug uldp fsm interface ethernet <*IFname*>

Function: To enable debugging information for ULDP for the specified interface. The no form of this command will disable the debugging information.

Parameters: Interface name.

Command Mode: Admin mode.

Default: Disabled by default.

Usage Guide: This command can be used to display the information about state transitions of the specified interfaces.

Example: To enable debugging information about state transitions of interface ethernet 1/1.

Switch#debug uldp fsm interface ethernet 1/1

6.3.10 debug uldp error

Command: debug uldp error

        no debug uldp error

Function: Enable the error message debug function, the no form command disable the function.

Parameter: None.

Command Mode: Admin Mode.

Default: Disabled.

Usage Guide: Use this command to display the error message.

Example: Display the error message.

Switch#debug uldp error

6.3.11 debug uldp event

Command: debug uldp event

        no debug uldp event

Function: Enable the message debug function to display the event; the no form command disable this function.

Parameter: None.

Command Mode: Admin Mode

Default: Disabled.

Usage Guide: Use this command to display all kinds of event information.

Example: Display event information.

Switch#debug uldp event

6.3.12 debug uldp packet

Command: debug uldp packet [receive|send]

        no debug uldp packet [receive|send]

Function: Enable receive and send packet debug function, after that. Display the type and interface of the packet which receiving and sending on the client.

Parameter: None.

Command Mode: Admin Mode.

Default: Disabled.

Usage Guide: Use this command to display the packet that receiving on each interface.

Switch#debug uldp packet receive

6.3.13 debug uldp interface ethernet

Command: debug uldp {hello|probe|echo|unidir|all}[receive|send] interface ethernet <*IFname*>

        no debug uldp {hello|probe|echo|unidir|all}[receive|send] interface ethernet <*IFname*>

Function: Enable the debug function of display the packet details. After that, display some kings of the packet details of terminal interface.

Parameter: Name of the interface.

Command Mode: Admin Mode.

Default: Disabled.

Usage Guide: Use this command to display the Hello packet details receiving on the interface Ethernet 1/1.

Switch#debug uldp hello receive interface Ethernet 1/1

6.4 ULDP Function Typical Examples
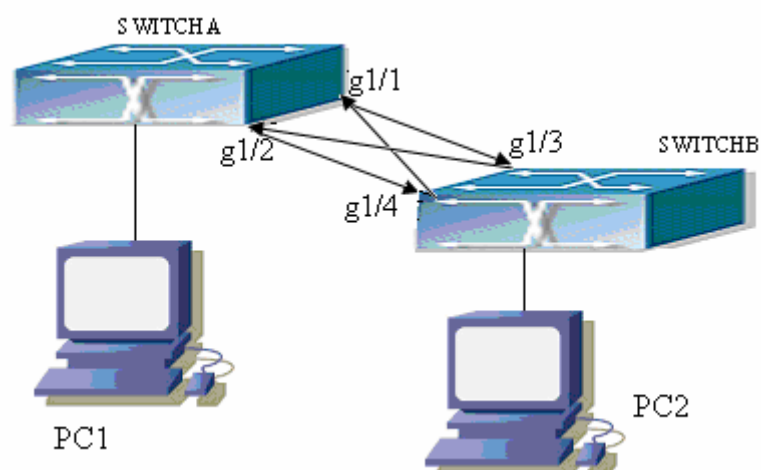
Fig 6-3 Fiber Cross Connection
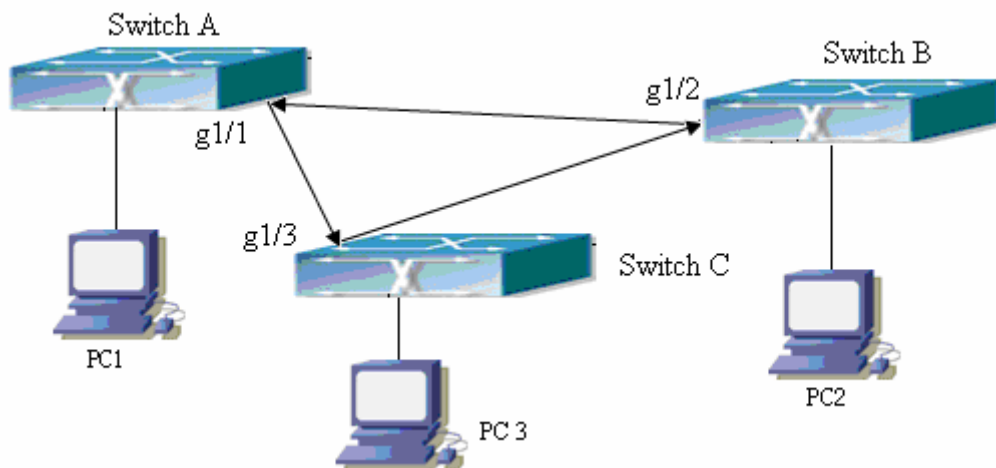
Fig 6-4 One End of Each Fiber Not Connected

In the network topology, port g1/1 and port g1/2 of SWITCH A as well as port g1/3 and port g1/4 of SWITCH B are all fiber ports. And the connection is cross connection. The physical layer is connected and works normally, but the data link layer is abnormal. ULDP can discover and disable this kind of error state of link. The final result is that port g1/1, g1/2 of SWITCH A and port g1/3, g1/4 of SWITCH B are all shut down by ULDP. Only when the connection is correct, can the ports work normally (won't be shut down).

Switch A configuration sequence:
SwitchA(config)#uldp enable
SwitchA(config)#interface ethernet 1/1
SwitchA(Config-If-Ethernet1/1)#uldp enable
SwitchA(Config-If-Ethernet1/1)#exit
SwitchA(config)#interface ethernet 1/2
SwitchA (Config-If-Ethernet1/2)#uldp enable

Switch B configuration sequence:
SwitchB(config)#uldp enable
SwitchB(config)#interface ethernet 1/3
SwitchB(Config-If-Ethernet1/3)#uldp enable
SwitchB(Config-If-Ethernet1/3)#exit
SwitchB(config)#interface ethernet 1/4
SwitchB(Config-If-Ethernet1/4)#uldp enable

As a result, port g1/1, g1/2 of SWITCH A are all shut down by ULDP, and there is notification information on the CRT terminal of PC1.

%Oct 29 11:09:50 2007 A unidirectional link is detected!　Port Ethernet1/1 need to be shut down!

%Oct 29 11:09:50 2007 Unidirectional port Ethernet1/1 shut down!

%Oct 29 11:09:50 2007 A unidirectional link is detected!　Port Ethernet1/2 need to be shut down!

%Oct 29 11:09:50 2007 Unidirectional port Ethernet1/2 shut down!

Port g1/3, and port g1/4 of SWITCH B are all shut down by ULDP, and there is notification information on the CRT terminal of PC1.

%Oct 29 11:09:50 2007 A unidirectional link is detected!　Port Ethernet1/3 need to be shut down!

%Oct 29 11:09:50 2007 Unidirectional port Ethernet1/3 shut down!

%Oct 29 11:09:50 2007 A unidirectional link is detected!　Port Ethernet1/4 need to be shut down!

%Oct 29 11:09:50 2007 Unidirectional port Ethernet1/4 shut down!

6.5 ULDP Troubleshooting Help

Configuration Notice:

☞ In order to ensure that ULDP can discover that the one of fiber ports has not connected or the ports are incorrectly cross connected, the ports have to work in duplex mode and have the same rate.

☞ If the automatic negotiation mechanism of the fiber ports with one port misconnected decides the working mode and rate of the ports, ULDP won't take effect no matter enabled or not. In such situation, the port is considered as "Down".

☞ In order to make sure that neighbors can be correctly created and unidirectional links can be correctly discovered, it is required that both end of the link should enable ULDP, using the same authentication method and password. At present, no password is needed on both ends.

☞ The hello interval of sending hello messages can be changed (it is10 seconds by default and ranges from 5 to 100 seconds) so that ULDP can respond faster to connection errors of links in different network environments. But this interval should be less than 1.3 of the STP convergence time. If the interval is too long, a STP loop will be generated before ULDP discovers and shuts down the unidirectional connection port. If the interval is too short, the network burden on the port will be increased, which means a reduced bandwidth.

☞ ULDP does not handle any LACP event. It treats every link of TRUNK group (like Port-channal, trunk ports) as independent, and handles each of them respectively.

- ☞ ULDP does not compact with similar protocols of other vendors, which means users can not use ULDP on one end and use other similar protocols on the other end.

- ☞ ULDP function is disabled by default. After globally enabling ULDP function, the debug switch can be enabled simultaneously to check the debug information. There are several DEBUG commands provided to print debug information, such as information of events, state machine, errors and messages. Different types of message information can also be printed according to different parameters.

- ☞ The Recovery timer is disabled by default and will only be enabled when the users have configured recovery time (30-86400 seconds).

- ☞ Reset command and reset mechanism can only reset the ports automatically shut down by ULDP. The ports shut down manually by users or by other modules won't be reset by ULDP.

Chapter 7 Configuration of LLDP Function Operation

7.1 Introduction to LLDP Function

Link Layer Discovery Protocol (LLDP) is a new protocol defined in 802.1ab. It enables neighbor devices to send notices of their own state to other devices, and enables all ports of every device to store information about them. If necessary, the ports can also send update information to the neighbor devices directly connected to them, and those neighbor devices will store the information in standard SNMP MIBs. The network management system can check the layer-two connection state from MIB. LLDP won't configure or control network elements or flows, but only report the configuration of layer-two. Another content of 802.1ab is to utilizing the information provided by LLDP to find the conflicts in layer-two. IEEE now uses the existing physical topology, interfaces and Entity MIBs of IETF.

To simplify, LLDP is a neighbor discovery protocol. It defines a standard method for Ethernet devices, such as switches, routers and WLAN access points, to enable them to notify their existence to other nodes in the network and store the discovery information of all neighbor devices. For example, the detail information of the device configuration and discovery can both use this protocol to advertise.

In specific, LLDP defines a general advertisement information set, a transportation advertisement protocol and a method to store the received advertisement information. The device to advertise its own information can put multiple pieces of advertisement information in one LAN data packet to transport. The type of transportation is the type length value (TLV) field. All devices supporting LLDP have to support device ID and port ID advertisement, but it is assumed that, most devices should also support system name, system description and system performance advertisement. System name and system description advertisement can also provide useful information for collecting network flow data. System description advertisement can include data such as the full name of the advertising device, hardware type of system, the version information of software operation system and so on.

802.1AB Link Layer Discovery Protocol will make searching the problems in an enterprise network an easier process and can strengthen the ability of network management tools to discover and maintain accurate network topology structure.

Many kinds of network management software use "Automated Discovery" function to

trace the change and condition of topology, but most of them can reach layer-three and classify the devices into all IP subnets at best. This kind of data are very primitive, only referring to basic events like the adding and removing of relative devices instead of details about where and how these devices operate with the network.

Layer 2 discovery covers information like which devices have which ports, which switches connect to other devices and so on; it can also display the routs between clients, switches, routers, application servers and network servers. Such details will be very meaningful for schedule and investigate the source of network failure.

LLDP will be a very useful management tool, providing accurate information about network mirroring, flow data and searching network problems.

7.2 LLDP Function Configuration Task Sequence

1. Globally enable LLDP function
2. Configure the port-based LLDP function switch
3. Configure the operating state of port LLDP
4. Configure the intervals of LLDP updating messages
5. Configure the aging time multiplier of LLDP messages
6. Configure the sending delay of updating messages
7. Configure the intervals of sending Trap messages
8. Configure to enable the Trap function of the port
9. Configure the optional information-sending attribute of the port
10. Configure the size of space to store Remote Table of the port
11. Configure the type of operation when the Remote Table of the port is full
12. Display and debug the relative information of LLDP

1. Globally enable LLDP function

Command	Explanation
Global mode	
lldp enable **lldp disable**	Globally enable or disable LLDP function.

2. Configure the port-base LLDP function switch

Command	Explanation
Port mode	
lldp enable **lldp disable**	Configure the port-base LLDP function switch.

3. Configure the operating state of port LLDP

Command	Explanation
Port mode	
lldp mode (send|receive|both|disable)	Configure the operating state of port LLDP.

4. Configure the intervals of LLDP updating messages

Command	Explanation
Global mode	
lldp tx-interval *<integer>* **no lldp tx-interval**	Configure the intervals of LLDP updating messages as the specified value or default value.

5. Configure the aging time multiplier of LLDP messages

Command	Explanation
Global mode	
lldp msgTxHold *<value>* **no lldp msgTxHold**	Configure the aging time multiplier as the specified value or default value.

6. Configure the sending delay of updating messages

Command	Explanation
Global mode	
lldp transmit delay *<seconds>* **no lldp transmit delay**	Configure the sending delay of updating messages as the specified value or default value.

7. Configure the intervals of sending Trap messages

Command	Explanation
Global mode	
lldp notification interval *<seconds>* **no lldp notification interval**	Configure the intervals of sending Trap messages as the specified value or default value.

8. Configure to enable the Trap function of the port

Command	Explanation
Port configuration mode	
lldp trap *<enable|disable>*	Enable or disable the Trap function of the port.

9. Configure the optional information-sending attribute of the port

Command	Explanation
Port configuration mode	
lldp transmit optional tlv [portDesc] [sysName] [sysDesc] [sysCap] **no lldp transmit optional tlv**	Configure the optional information-sending attribute of the port as the option value of default values.

10. Configure the size of space to store Remote Table of the port

Command	Explanation
Port configuration mode	
lldp neighbors max-num <*value*> **no lldp neighbors max-num**	Configure the size of space to store Remote Table of the port as the specified value or default value.

11. Configure the type of operation when the Remote Table of the port is full

Command	Explanation
Port configuration mode	
lldp toomanyneighbors {discard|delete}	Configure the type of operation when the Remote Table of the port is full.

12. Display and debug the relative information of LLDP

Command	Explanation
Admin mode and global mode	
show lldp	Display the current LLDP configuration information.
show lldp interface ethernet <*IFNAME*>	Display the LLDP configuration information of the current port.
show lldp traffic	Display the information of all kinds of counters.
show lldp neighbors interface ethernet <*IFNAME*>	Display the information of LLDP neighbors of the current port.
show debugging lldp	Display all ports with LLDP debug enabled.
Admin mode	
debug lldp **no debug lldp**	Enable or disable the DEBUG switch.

debug lldp packets interface ethernet *<IFNAME>* **no debug lldp packets interface ethernet** *<IFNAME>*	Enable or disable the DEBUG packet-receiving and sending function in port or global mode.
Port mode	
clear lldp remote-table	Clear Remote-table of the port.

7.3 LLDP Function Commands

7.3.1 lldp enable

Command：**lldp enable**

    lldp disable

Function：Globally enable LLDP function; the no operation of this command globally disables LLDP function.

Parameters：None.

Default：Disable LLDP functions.

Command Mode：Global mode.

Usage Guide: If LLDP function is globally enabled, it will be enabled on every port.

Example：Enable LLDP function on the switch.

Switch(config)#lldp enable

7.3.2 lldp enable(Port)

Command：**lldp enable**

    lldp disable

Function：Enable the LLDP function module of ports in port configuration mode ; the no operation of this command will disable the LLDP function module of ports.

Parameters：None.

Default：the LLDP function module of ports is enabled by default in port configuration mode.

Command Mode：Port configuration mode

Usage Guide：When LLDP is globally enabled, it will be enabled on every port. The switch on a port is used to disable this function when it is unnecessary on the port.

Example：Disable LLDP function of port on the port ethernet 1/5 of the switch.

Switch(config)#in ethernet 1/5

Switch(Config-If-Ethernet1/5)#lldp disable

7.3.3 lldp mode

Command：lldp mode {send|receive|both|disable}
Function：Configure the operating state of lldp function of the port.
Parameters：send: Configure the LLDP function as only being able to send messages.
receive: Configure the LLDP function as only being able to receive messages.
both: Configure the LLDP function as being able to both send and receive messages.
disable: Configure the LLDP function as not being able to send or receive messages.
Default：The operating state of the port is "both".
Command Mode：Port configuration mode.
Usage Guide：Choose the operating state of the lldp Agent on the port. The configuration can only be done when the lldp function is already enabled.
Example：Configure the state of port ethernet 1/5 of the switch as "receive".
Switch(config)#in ethernet 1/5
Switch(Config-If-Ethernet1/5)#lldp mode receive

7.3.4 lldp tx-interval

Command：lldp tx-interval *<integer>*
          no lldp tx-interval
Function：Set the interval of sending update messages on all the ports with LLDP function enabled, the value of which ranges from 5 to 32768 seconds and is 30 seconds by default.
Parameters：*<integer>* is the interval of sending updating messages, ranging from 5to32768.
Default：30 seconds.
Command Mode：Global mode.
Usage Guide：After configuring the interval of sending messages, LLDP messages can only be received after a period as long as configured. The interval should be less than or equal with half of aging time, for a too long interval will cause the state of being aged and reconstruction happen too often, while a too short interval will increase the flow of the network and decrease the bandwidth of the port. The value of the aging time of messages is the product of the multiplier and the interval of sending messages. The maximum aging time is 65535 seconds.
When tx-interval is the default value and transmit delay is configured via some commands, tx-interval will become four times of the latter, instead of the default 40.

Example：Set the interval of sending messages as 40 seconds.

Switch(config)#lldp tx-interval 40

7.3.5 lldp msgtxhold

Command：**lldp msgTxHold <value>**

no lldp msgTxHold

Function：Set the multiplier value of the aging time carried by update messages sent by the all ports with LLDP function enabled. The value ranges from 2 to 10.

Parameters：*<value>* is the aging time multiplier, ranging from 2 to 10.

Default：the value of the multiplier is 4 by default.

Command Mode：Global mode.

Usage Guide：After configuring the multiplier, the aging time is defined as the product of the multiplier and the interval of sending messages, and its maximum value is 65535 seconds.

Example：Set the value of the aging time multiplier as 6.

Switch(config)#lldp msgtxhold 6

7.3.6 lldp transmit delay

Command: lldp transmit delay *<seconds>*

no lldp transmit delay

Function：Since local information might change frequently because of the variability of the network environment, there could be many update messages sent in a short time. So a delay is required to guarantee an accurate statistics of local information.

When transmit delay is the default value and tx-interval is configured via some commands, transmit delay will become one fourth of the latter, instead of the default 2.

Parameters：*<seconds>* is the time interval, ranging from 1 to 8192 seconds.

Default：The interval is 2 seconds by default.

Command Mode：Global mode.

Usage Guide：When the messages are being sent continuously, a sending delay is set to prevent the Remote information from being updated repeatedly due to sending messages simultaneously.

Example：Set the delay of sending messages as 3 seconds.

Switch(config)#lldp transmit delay 3

7.3.7 lldp notification interval

Command: lldp notification interval <seconds>

    no lldp notification interval

Function：When the time interval ends, the system is set to check whether the Remote Table has been changed. If it has, the system will send Trap to the SNMP management end.

Parameters：**<seconds>**is the time interval, ranging from 5 to 3600 seconds.

Default：The time interval is 5 seconds.

Command Mode：Global mode.

Usage Guide：After configuring the notification time interval, a "trap" message will be sent at the end of this time interval whenever the Remote Table changes,.

Example：Set the time interval of sending Trap messages as 20 seconds.

Switch(config)#lldp notification interval 20

7.3.8 lldp trap

Command：**lldp trap {enable|disable}**

Function：enable : configure to enable the Trap function on the specified port;disable: configure to disable the Trap function on the specified port.

Parameters：None.

Default：The Trap function is disabled on the specified port by default.

Command Mode：Port configuration mode.

Usage Guide: The function of sending Trap messages is enabled on the port.

Example：Enable the Trap function on port ethernet 1/5 of the switch.

Switch(config)#in ethernet 1/5

Switch(Config-If-Ethernet1/5)#lldp trap enable

7.3.9 lldp transmit optional tlv

Command：**lldp transmit optional tlv [portDesc] [sysName] [sysDesc] [sysCap]**

    no lldp transmit optional tlv

Function：Configure the type of optional TLV of the port.

Parameters：**portDesc:** the description of the port. **sysName:** the system name.

sysDesc: the description of the system.**sysCap:** the capability of the system.

Default：The messages carry no optional TLV by default.

Command Mode：Port configuration mode.

Usage Guide: When configuring the optional TLV, each TLV can only appear once in a message. **portDesc** optional TLV represents the name of local port, such as ethernet 4/5；**sysName** optional TLV represents the name of local system, such as Switch1；

sysDesc optional TLV represents the description of local system, such as Switch Device, Nov 15 2007 09:36:37HardWare version is 1.0.0.0SoftWare package version is Switch_5.5.5.1BootRom version is Switch_1.6.13All rights reserved. Last reboot is cold resetUptime is 0 weeks, 0 days, 0 hours, 25 minutes；**sysCap** optional TLV represents the capability of local system, for example: it is 4 in a Edge-Core switch.

Example：Configure that port ethernet 1/5 of the switch carries portDesc and sysCap TLV

Switch(config)#in ethernet 1/5

Switch(Config-If-Ethernet1/5)#lldp transmit optional tlv portdesc syscap

7.3.10 lldp neighbors max-num

Command：**lldp neighbors max-num *<value>***

          no lldp neighbors max-num

Function：Set the maximum number of entries can be stored in Remote MIB.

Parameters：*<value>* is the configured number of entries, ranging from 5 to 500.

Default：The maximum number of entries can be stored in Remote MIB is 100.

Command Mode：Port configuration mode.

Usage Guide: The maximum number of entries can be stored in Remote MIB.

Example：Set the Remote as 200 on port ethernet 1/5 of the switch.

Switch(config)#in ethernet 1/5

Switch(Config-If-Ethernet1/5)#lldp neighbors max-num 200

7.3.11 lldp tooManyNeighbors

Command：**lldp tooManyNeighbors {discard|delete}**

Function：Set which operation will be done when the Remote Table is full.

Parameters：discard：discard the current message; delete：Delete the message with the least TTL in the Remoter Table.

Default: Discard.

Command Mode：Port configuration mode.

Usage Guide: When the Remote MIB is full, Discard means to discard the received message; Delete means to the message with the least TTL in the Remoter Table.

Example：Set port ethernet 1/5 of the switch as delete

Switch(config)#in ethernet 1/5

Switch(Config-If-Ethernet1/5)#lldp tooManyNeighbors delete

7.3.12 show lldp

Command：show lldp

Function： Display the configuration information of global LLDP, such as the list of all the ports with LLDP enabled, the interval of sending update messages, the configuration of aging time, the interval needed by the sending module to wait for re-initialization, the interval of sending TRAP, the limitation of the number of the entries in the Remote Table.

Parameters： None.

Default： Do not display the configuration information of global LLDP.

Command Mode： Admin mode and Global mode.

Usage Guide： Users can check all the configuration information of global LLDP by using "show lldp".

Example： Check the configuration information of global LLDP after it is enabled on the switch.

Switch(config)#show lldp

-----LLDP GLOBAL INFORMATIONS-----

LLDP enabled port : Ethernet 1/1

LLDP interval :30

LLDP txTTL :120

LLDP txShutdownWhile :2

LLDP NotificationInterval :5

LLDP txDelay :20

-------------END------------------

7.3.13 show lldp traffic

Command：show lldp traffic

Function： Display the statistics of LLDP data packets.

Parameters： None.

Default： Do not display the statistics of LLDP data packets.

Command Mode： Admin mode and Global mode.

Usage Guide： Users can check the statistics of LLDP data packets by using "show lldp traffic".

Example： Check the statistics of LLDP data packets after LLDP is enabled on the switch.

Switch(config)#show lldp traffic

PortName	Ageouts	FramesDiscarded	FramesInErrors	FramesIn	FramesOut	TLVsDiscarded	TLVsUnrecognized
Ethernet1/1	0	0	0	0	7	0	0

7.3.14 show lldp interface ethernet

Command：show lldp interface ethernet *<IFNAME>*

Function：Display the configuration information of LLDP on the port, such as: the working state of LLDP Agent.

Parameters： None.

Default： Do not display the configuration information of LLDP on the port.

Command Mode： Admin mode and Global mode.

Usage Guide： Users can check the configuration information of LLDP on the port by using "show lldp interface ethernet XXX".

Example： Check the configuration information of LLDP on the port after LLDP is enabled on the switch.

Switch(config)#show lldp interface ethernet 1/1

Port name :   ethernet 1/1

LLDP Agent Adminstatus : Both

LLDP Optional TLV : portDecs sysName sysDesc sysCap

LLDP Trap Status : disable

LLDP maxRemote :100

LLDP Overflow handle : discard

LLDP interface remote status : Full

7.3.15 show lldp neighbors interface ethernet

Command：show lldp neighbors interface ethernet *<IFNAME>*

Function： Display the LLDP neighbor information of the port.

Parameters： None.

Default： Do not display the LLDP neighbor information of the port.

Command Mode： Admin mode and Global mode.

Usage Guide： Users can check the LLDP neighbor information of the port by using "show lldp neighbors interface ethernet XXX".

Example： Check the LLDP neighbor information of the port after LLDP is enabled on the port.

Switch(config)#show lldp neighbors interface ethernet 1/1

7.3.16 show debugging lldp

Command: show debugging lldp

Function： Display all ports with lldp debug enabled.

Parameters: None.

Default: None.

Command Mode: Admin and Config Mode.

Usage Guide：With show debugging lldp, all ports with lldp debug enabled will be displayed.

Example: Display all ports with lldp debug enabled.

Switch(config)#show debugging lldp
====BEGINNING OF   LLDP DEBUG SETTINGS====

debug lldp

debug lldp packets interface Ethernet1/1

debug lldp packets interface Ethernet1/2

debug lldp packets interface Ethernet1/3

debug lldp packets interface Ethernet1/4

debug lldp packets interface Ethernet1/5

=============END OF DEBUG SETTINGS==============

7.3.17 debug lldp

Command：**debug lldp**

　　　　　　no debug lldp

Function：Enable the debug information of LLDP function, the no operation of this command will disable the debug information of LLDP function.

Parameters：None.

Default：Disable the debug information of LLDP function.

Command Mode：Admin mode.

Usage Guide：When the debug switch is enabled, users can check the receiving and sending of packets and other information.

Example：Enable the debug switch of LLDP function on the switch.

Switch(config)#debug lldp

7.3.18 debug lldp packets

Command：**debug lldp packets interface ethernet *<IFNAME>***

　　　　　　no debug lldp packets interface ethernet *<IFNAME>*

Function：Display the message-receiving and message-sending information of LLDP on the port; the no operation of this command will disable the debug information switch.

Parameters：None.

Default：Disable the debug information on the port.

Command Mode：Admin mode.

Usage Guide：When the debug switch is enabled, users can check the receiving and

sending of packets and other information on the port.

Example：Enable the debug switch of LLDP function on the switch.

Switch(config)#debug lldp packets interface ethernet 1/1

%Jan 01 00:02:40 2006 LLDP-PDU-TX   PORT= ethernet 1/1

7.3.19 clear lldp remote-table

Command：**clear lldp remote-table**

Function：Clear the Remote-table on the port.

Parameters：None.

Default：Do not clear the entries.

Command Mode：Port configuration mode.

Usage Guide：Clear the Remote table entries on this port.

Example：
Switch(Config-If-Ethernet 1/1)#clear lldp remote-table

7.4 LLDP Function Typical Example
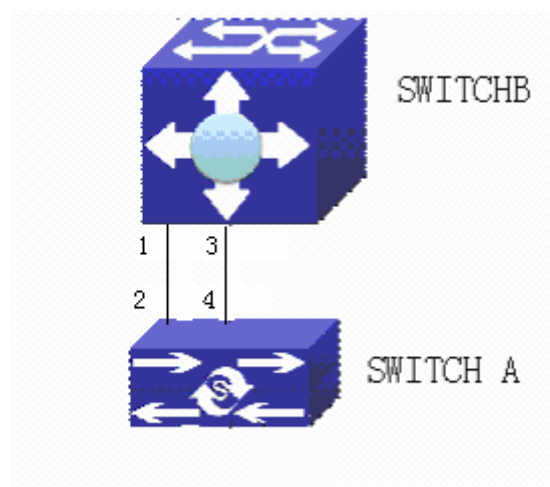
Fig 7-1 LLDP Function Typical Configuration Example

In the network topology graph above, the port 1,3 of SWITCH B are connected to port 2,4 of SWITCH A. Port 1 of SWITCH B is configured to message-receiving-only mode, Option TLV of port 4 of SWITCH A is configured as portDes and SysCap.

SWITCH A configuration task sequence:

SwitchA(config)#lldp enable

SwitchA(config)#interface ethernet 1/1

SwitchA(Config-If-Ethernet1/1)#lldp mode receive

SwitchA(Config-If-Ethernet1/1)#exit

SWITCH B configuration task sequence:

Switch B(config)#lldp enable

SwitchB(config)#interface ethernet 1/4

SwitchB(Config-If-Ethernet1/4)#lldp transmit optional tlv portdesc syscap

SwitchB(Config-If-Ethernet1/4)#exit

7.5 LLDP Function Troubleshooting Help

LLDP function is disabled by default. After enabling the global switch of LLDP, users can enable the debug switch "debug lldp" simultaneously to check debug information.

Using "show" function of LLDP function can display the configuration information in global or port configuration mode.

Chapter 8 Port Channel Configuration

8.1 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.
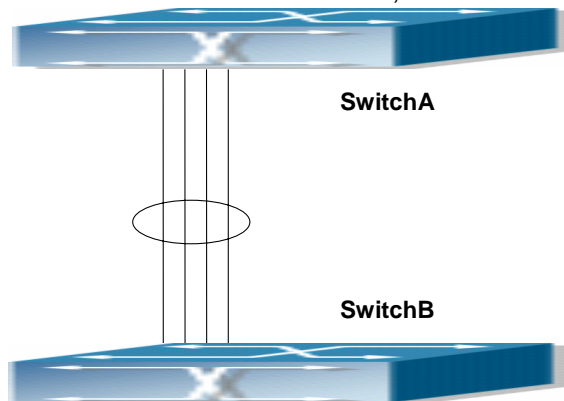
SwitchA

SwitchB

Fig   8-1   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.

ES4700 series 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 ES4700 series, 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. ES4700 series 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. ES4700 series 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.

8.2 Port Channel Configuration

8.2.1 Port Channel Configuration Task List

1. Create a port group
2. Add ports to the specified group from the Port Mode of respective ports
3. Enter port-channel configuration mode

1. Create 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
Port 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.

8.2.2 Command for port channel

8.2.2.1 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: Enable LACP debug.

Switch#debug lacp

8.2.2.2 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

8.2.2.3 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: Port 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-If-Ethernet1/1)#port-group 1 mode active

8.2.2.4 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)#

8.2.2.5 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 activety	.	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 activety          .                    .
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 activety	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".

8.3 Port Channel Example

Scenario 1: Configuring Port Channel in LACP.
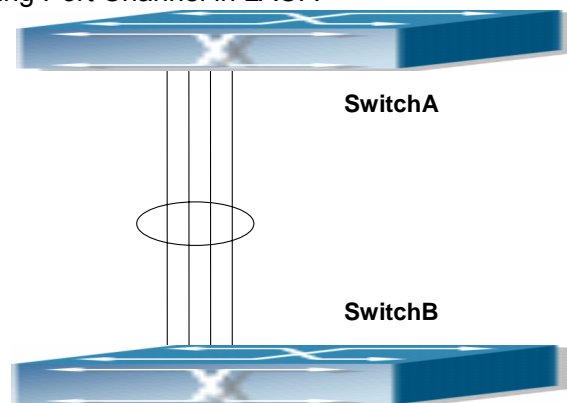
Fig   8-2   Configuring Port Channel in LACP

Example: The switches in the description below are all ES4700 series switches and as shown in the figure, ports 1, 2, 3, 4 of Switch 1 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 Switch 1 form an aggregated port named "Port-Channel1", ports 1, 2, 3, 4 of Switch 2 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.
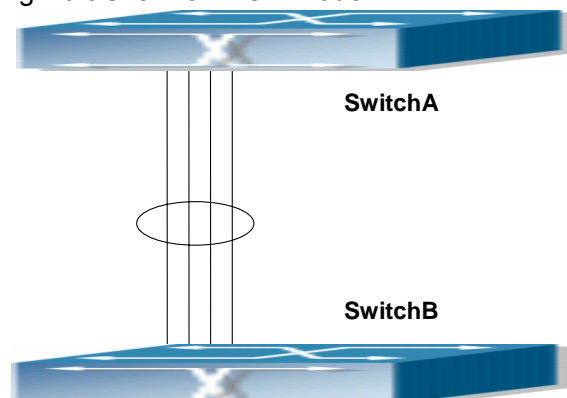
Fig   8-3   Configuring Port Channel in ON mode

Example: As shown in the figure, ports 1, 2, 3, 4 of Switch 1 are access ports that belong to vlan1. Add those four port to group1 in "on" mode. Ports 1, 2, 3, 4 of Switch 2 are access ports that also belong to vlan1, add the these four ports to group2 in "on" mode.

The configuration steps are listed below:

SwitchA#config

SwitchA (config)#interface eth 1/1

SwitchA (Config-If-Ethernet1/1)# port-group 1 mode on

SwitchA (Config-If-Ethernet1/1)#exit

SwitchA (config)#interface eth 1/2

SwitchA (Config-If-Ethernet1/2)# port-group 1 mode on

SwitchA (Config-If-Ethernet1/2)#exit

SwitchA (config)#interface eth 1/3

SwitchA (Config-If-Ethernet1/3)# port-group 1 mode on

SwitchA (Config-If-Ethernet1/3)#exit

SwitchA (Config-If-Ethernet1/4)# port-group 1 mode on

SwitchA (Config-If-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 Switch 1 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 Switch 1 and Switch 2 are aggregated in "on" mode and become an aggregated port respectively.

8.4 Port Channel Troubleshooting Help

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.

8.5 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.

8.5.1 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.

LACP port group configuration	
Group num(1-8)	1
Load balance mode	src-mac
Operation type	Add port group

8.5.2 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

LACP Port configuration	
group num	[▾]
Port	Ethernet1/1 ▾
Port mode	active ▾
Operation type	Add port to group ▾

Chapter 9 VLAN Configuration

9.1 VLAN Configuration

9.1.1 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 ES4700 series 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.
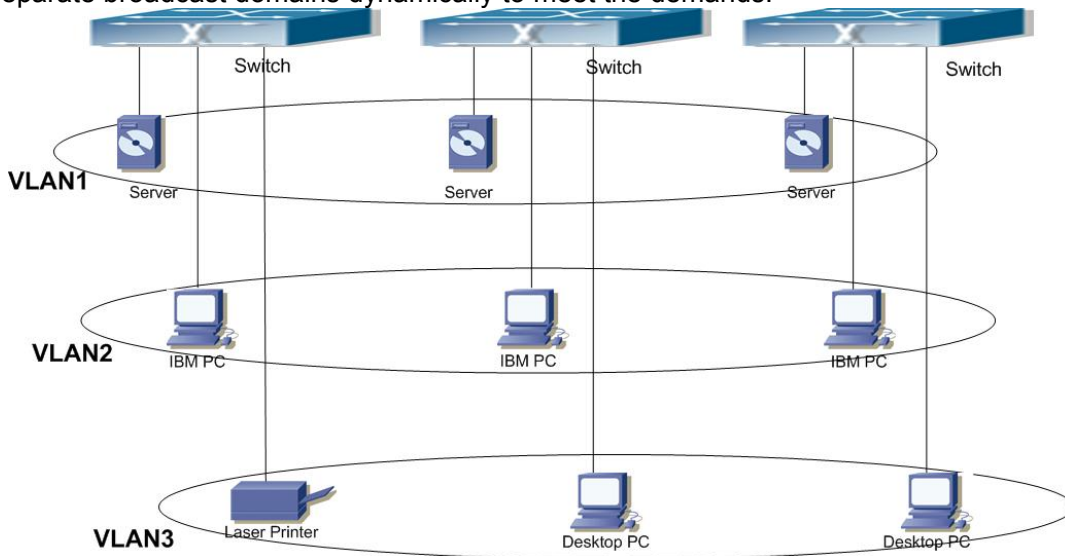
Fig 9-1 A VLAN network defined logically

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 ES4700 series. The chapter will describe the use and configuration of VLAN and GVRP in details.

9.1.2 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
Port mode	
switchport mode {trunk|access}	Set the current port as Trunk or Access port.

4. Set Trunk port

Command	Explanation
Port mode	
switchport trunk allowed vlan {WORD | all | add WORD | except WORD|remove WORD} **no switchport trunk allowed vlan**	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
Port mode	
switchport access vlan *<vlan-id>* **no switchport access vlan**	Add the current port to the specified VLAN. 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 deletes the 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.

9.1.3 Command for vlan Configuration

9.1.3.1 Vlan

Command: vlan <*vlan-id*>[name <*vlan-name*>]

no vlan <*vlan-id*>[name]

Function: Create VLANs 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, connect with";" and "-".

<*vlan-name*> is the name that creates 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 VLAN100-200 and enter the configuration mode for VLAN 100.

Switch(config)#vlan 100-200

Switch(config)#vlan 100

Switch(Config-Vlan100)#

9.1.3.2 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

Note:This will remove all the ports from vlan 100

Switch(Config-Vlan100)#exit

Switch(config)#vlan 200

Switch(Config-Vlan200)#private-vlan isolated

Note:This will remove all the ports from vlan 200

Switch(Config-Vlan200)#exit

Switch(config)#vlan 300

Switch(Config-Vlan300)#private-vlan community

Note:This will remove all the ports from vlan 300

Switch(Config-Vlan300)#exit

9.1.3.3 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

9.1.3.4 show vlan

Command: show vlan [brief| summary] [id <*vlan-id*>] [name <*vlan-name*>] [internal usage [id <vlan-id>| name <vlan-name>]] [private-vlan [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. **private-vlan** display the id、name、associate vlan and port information for private-vlan.

Command mode: Admin Mode and other configuration 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#show vlan summary

The max. vlan entrys: 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)

Switch(config)#show vlan private-vlan

VLAN	Name	Type	Asso VLAN	Ports	
100	VLAN0100	Primary	101 102	Ethernet6/9	Ethernet6/10
				Ethernet6/11	Ethernet6/12
				Ethernet6/13	
101	VLAN0101	Community	100	Ethernet6/9	Ethernet6/10
				Ethernet6/11	Ethernet6/12
				Ethernet6/13	
102	VLAN0102	Isolate	100	Ethernet6/9	

9.1.3.5 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: Port 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-If-Ethernet1/8)#switchport mode access

Switch(Config-If-Ethernet1/8)#switchport access vlan 100

Switch(Config-If-Ethernet1/8)#exit

9.1.3.6 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 slot 1 to VLAN100.

Switch(Config-Vlan100)#switchport interface ethernet 1/1;3;4-7;8

9.1.3.7 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: Port 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-If-Ethernet1/5)#switchport mode trunk

Switch(Config-If-Ethernet1/5)#exit

Switch(config)#interface ethernet 1/8

Switch(Config-If-Ethernet1/8)#switchport mode access

Switch(Config-If-Ethernet1/8)#exit

9.1.3.8 switchport trunk allowed vlan

Command: switchport trunk allowed vlan {WORD | all | add WORD | except WORD|remove WORD}

            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: WORD 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; "**add**" add assigned VIDs behind allow vlan; "**except**" all VID add to allow vlan except assigned VIDs; "**remove**" delet assigned allow vlan from allow vlan list.

Command mode: Port 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-If-Ethernet1/5)#switchport mode trunk

Switch(Config-If-Ethernet1/5)#switchport trunk allowed vlan 1;3;5-20

Switch(Config-If-Ethernet1/5)#exit

9.1.3.9 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: Port 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 command for VLAN forwarding.

Example: Set the native VLAN for a Trunk port to 100.

Switch(config)#interface ethernet 1/5

Switch(Config-If-Ethernet1/5)#switchport mode trunk

Switch(Config-If-Ethernet1/5)#switchport trunk native vlan 100

Switch(Config-If-Ethernet1/5)#exit

9.1.3.10 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: Port 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-If-Ethernet1/1)# no switchport ingress-filtering

9.1.4 Typical VLAN Application

Scenario:
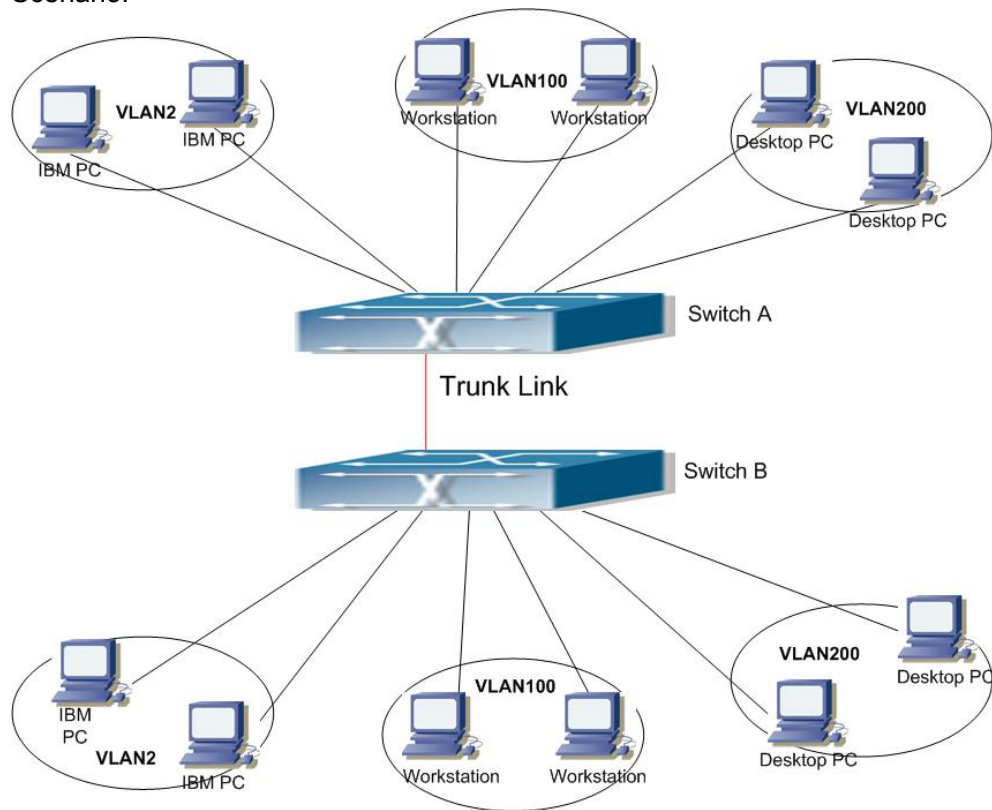
Fig 9-2 Typical VLAN Application Topology

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-If-Ethernet1/11)#switchport mode trunk

Switch(Config-If-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-If-Ethernet1/11)#switchport mode trunk

Switch(Config-If-Ethernet1/11)#exit

9.2 GVRP Configuration

9.2.1 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.

9.2.2 GVRP Configuration Task List

1. Configuring GARP Timer Parameters
2. Enable GVRP function

1. Configuring GARP Timer parameters.

Command	Explanation
Port 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 leaveall <*timer-value*> **no bridge-ext garp timer leaveall**	Configure the leave all timer for GARP.

2. Enable GVRP function

Command	Explanation
Port mode	
bridge-ext gvrp **no bridge-ext gvrp**	Enable/disable the GVRP function on current port.
Global Mode	
bridge-ext gvrp **no bridge-ext gvrp**	Enable/disable the GVRP function for the switch.

9.2.3 Command For GVRP

9.2.3.1 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 bridge-ext gvrp**" command disables the GVRP function globally or for the port**.**

Command mode: Port 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-If-Ethernet1/10)# bridge-ext gvrp

Switch(config)#exit

9.2.3.2 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

9.2.3.3 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: Port 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-If-Ethernet1/10)#bridge-ext garp timer hold 500

9.2.3.4 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: Port 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-If-Ethernet1/10)#bridge-ext garp timer join 1000

9.2.3.5 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: Port 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-If-Ethernet1/10)#bridge-ext garp timer leave 3000

9.2.3.6 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

9.2.3.7 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 and other configuration Mode.

Usage Guide: N/A.

Example: Display global GARP information.

Switch #show garp timer

9.2.3.8 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 and other configuration Mode.

Usage Guide: N/A.

Example: Display global GVRP information.

Switch#show gvrp configuration

---------------- Gvrp Information ------------------

Gvrp status : enable

Gvrp Timers(milliseconds)

LeaveAll   :   10000

9.2.4 Typical GVRP Application

Scenario:
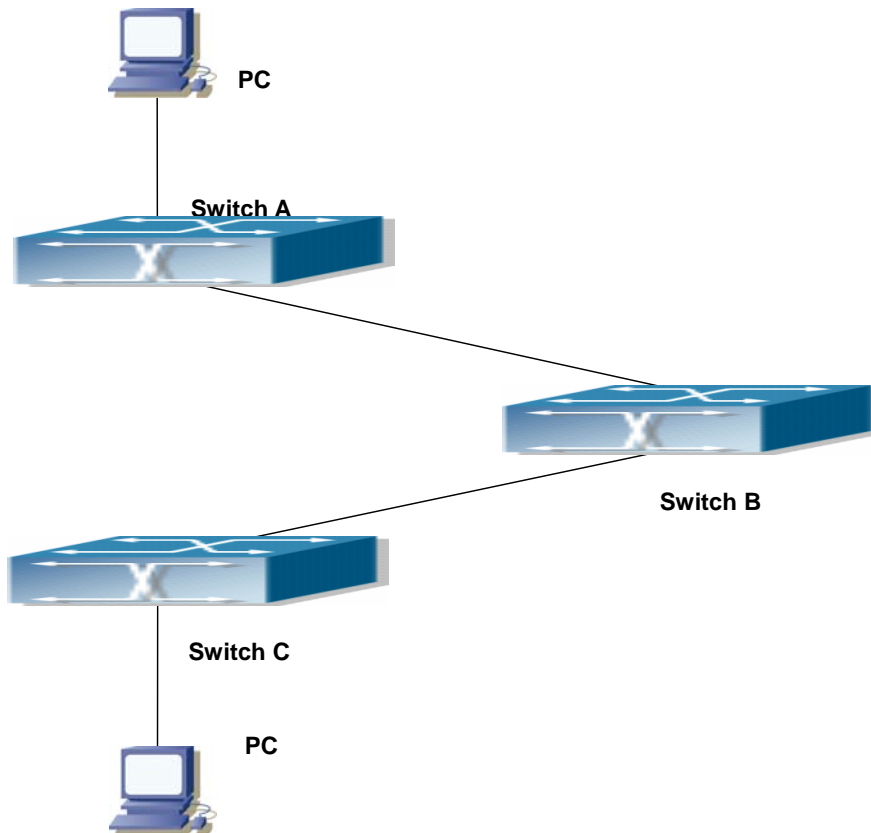
Fig 9-3 Typical GVRP Application Topology

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 slots 1 of 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-If-Ethernet1/11)#switchport mode trunk

Switch(Config-If-Ethernet1/11)# bridge-ext gvrp

Switch(Config-If-Ethernet1/11)#exit

Switch B:

Switch(config)# bridge-ext gvrp

Switch(config)#interface ethernet 1/10

Switch(Config-If-Ethernet1/10)#switchport mode trunk

Switch(Config-If-Ethernet1/10)# bridge-ext gvrp

Switch(Config-If-Ethernet1/10)#exit

Switch(config)#interface ethernet 1/11

Switch(Config-If-Ethernet1/11)#switchport mode trunk

Switch(Config-If-Ethernet1/11)# bridge-ext gvrp

Switch(Config-If-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-If-Ethernet1/11)#switchport mode trunk

Switch(Config-If-Ethernet1/11)# bridge-ext gvrp

Switch(Config-If-Ethernet1/11)#exit

9.2.5 GVRP Troubleshooting Help

☞ 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 ES4700 series. If GVRP is to be enabled, RSTP function for the ports must be disabled first.

9.3 Dot1q-tunnel Configuration

9.3.1 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.
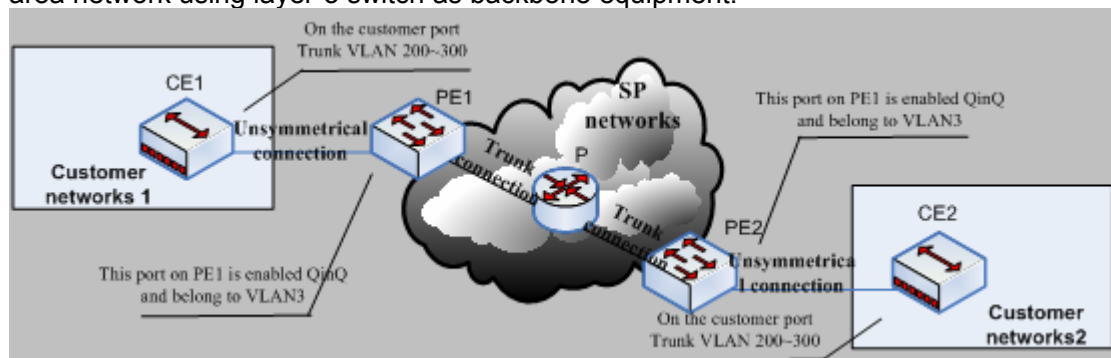
Fig 9-4 Dot1q-tunnel based Internetworking mode

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-tuunel provides the ISP internet the ability of supporting many client VLANs by only one VLAN of theirselves. 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 Switch will be provided in this section.

9.3.2 Dot1q-tunnel Configuration

9.3.2.1 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 {0x8100|0x9100|0x9200|<1-65535>}	Configure the type of protocol on the ports.

9.3.3 Dot1q-Tunnel Configuration Command

9.3.3.1 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. This command is mutex with dot1q-tunnel tpid.

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-If-Ethernet1/1)# dot1q-tunnel enable

Switch(Config-If-Ethernet1/1)# exit

9.3.3.2 dot1q-tunnel tpid

Command: dot1q-tunnel tpid {0x8100|0x9100|0x9200|<1-65535>}

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 0x8100.

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. This command is mutex with dot1q-tunnel enable.

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-If-Ethernet1/10)#switchport mode trunk

Switch(Config-If-Ethernet1/10)#dot1q-tunnel tpid 9100

Switch(Config-If-Ethernet1/10)#exit

9.3.3.3 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 and other configuration 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

9.3.4 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 Fig 6-4)
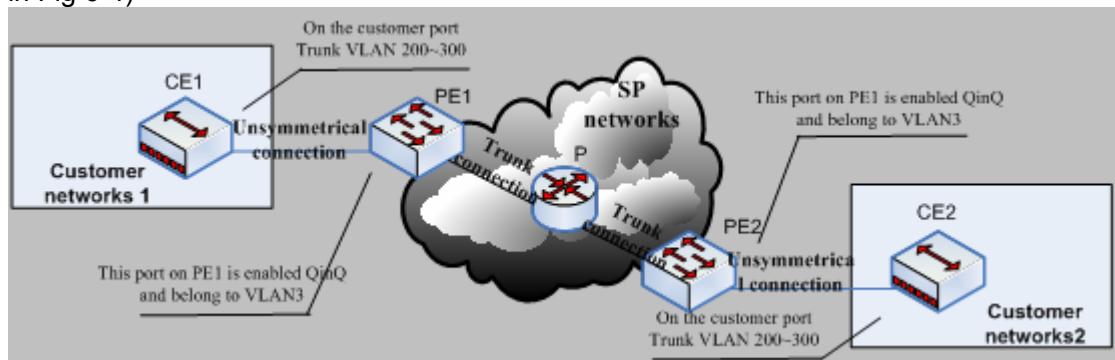
Configuration Item	Configuration Explanation
VLAN3	Port1 of PE1 and PE2.
dot1q-tunnel	Port1 of PE1 and PE2.

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-If-Ethernet1/1)# dot1q-tunnel enable

Switch(Config-If-Ethernet1/1)# exit

Switch(config)#interface ethernet 1/10

Switch(Config-If-Ethernet1/10)#switchport mode trunk

Switch(Config-If-Ethernet1/10)#dot1q-tunnel tpid 0x9100

Switch(Config-If-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-If-Ethernet1/1)# dot1q-tunnel enable

Switch(Config-If-Ethernet1/1)# exit

Switch(config)#interface ethernet 1/10

Switch(Config-If-Ethernet1/10)#switchport mode trunk

Switch(Config-If-Ethernet1/10)#dot1q-tunnel tpid 0x9100

Switch(Config-If-Ethernet1/10)#exit

Switch(config)#

9.3.5 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.

9.4 VLAN-translation Configuration

9.4.1 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.

9.4.2 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.

9.4.3 VLAN-translation Configuration Command

9.4.3.1 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 and other configuration 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

9.4.3.2 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

9.4.3.3 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

9.4.3.4 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

9.4.4 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 Fig 6-4)
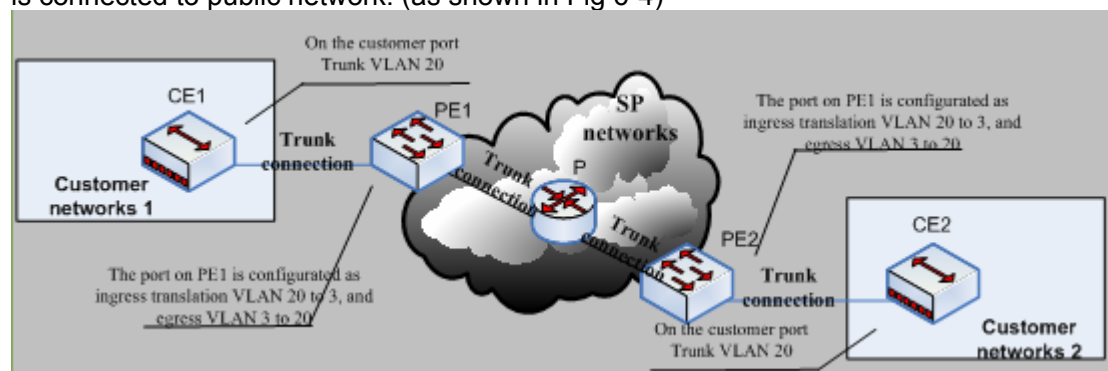
Configuration Item	Configuration Explanation
VLAN-translation	Port1 of PE1 and PE2.
Trunk port	Port1 and Port10 of PE1 and PE2.

Configuration procedure is as follows:

PE1、PE2:

Switch(config)#interface ethernet 1/1

Switch(Config-If-Ethernet1/1)#switchport mode trunk

Switch(Config-If-Ethernet1/1)# dot1q-tunnel enable

Switch(Config-If-Ethernet1/1)# vlan-translation enable

Switch(Config-If-Ethernet1/1)# vlan-translation 20 to 3 in

Switch(Config-If-Ethernet1/1)# vlan-translation 3 to 20 out

Switch(Config-If-Ethernet1/1)# exit

Switch(config)#interface ethernet 1/10

Switch(Config-If-Ethernet1/10)#switchport mode trunk

Switch(Config-If-Ethernet1/10)#exit

9.4.5 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.

9.5 Dynamic VLAN Configuration

9.5.1 Dynamic VLAN Introduction

The dynamic VLAN is named corresponding to the static VLAN (namely the port based VLAN). Dynamic VLAN supported by the ES4700 series 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.

9.5.2 Dynamic VLAN Configuration

9.5.2.1 Dynamic VLAN Configuration Task Sequence

1. Configure the MAC-based VLAN function on the port
2. Set the VLAN to MAC VLAN
3. Configure the correspondence between the MAC address and the VLAN
4. Configure the IP-subnet-based VLAN function on the port
5. Configure the correspondence between the IP subnet and the VLAN
6. Configure the correspondence between the Protocols and the VLAN
7. 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. Set the VLAN to MAC VLAN

Command	Explanation
Global Mode	
mac-vlan vlan *<vlan-id>* **no mac-vlan**	Configure the specified VLAN to MAC VLAN; the "**no mac-vlan** " command cancels the MAC VLAN configuration of this VLAN.

3. 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.

4. 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.

5. 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.

6. Configure the correspondence between the Protocols and the VLAN

Command	Explanation
Global Mode	
protocol-vlan mode {ethernetii etype *<etype-id>*|**llc {dsap** *<dsap-id>* **ssap** *<ssap-id>*}|**snap etype** *<etype-id>*} **vlan** *<vlan-id>* **no protocol-vlan {mode {ethernetii etype** *<etype-id>*|**llc {dsap** *<dsap-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.

7. 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.

9.5.2.2 Commands for Dynamic VLAN Configuration

9.5.2.2.1 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)#dynamic-vlan mac-vlan prefer

9.5.2.2.2 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)#dynamic-vlan subnet-vlan prefer

9.5.2.2.3 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

9.5.2.2.4 mac-vlan vlan

Command: mac-vlan vlan *<vlan-id>*

        no mac-vlan

Function: Configure the specified VLAN to MAC VLAN; the "**no mac-vlan** " command cancels the MAC VLAN configuration of this VLAN.

Parameter: *<vlan-id>* is the number of the specified VLAN.

Command Mode: Global Mode.

Default: No MAC VLAN is configured by default.

Usage Guide: Set specified VLAN for MAC VLAN, There can be only one MAC VLAN at the same time.

Example: Set VLAN100 to MAC VLAN.

Switch#config

Switch(config)#mac-vlan vlan 100

9.5.2.2.5 protocol-vlan

Command: protocol-vlan mode {ethernetii etype *<etype-id>*|llc {dsap *<dsap-id>* **ssap *<ssap-id>*}|snap etype *<etype-id>*} vlan *<vlan-id>***

no protocol-vlan {mode {ethernetii etype *<etype-id>*|llc {dsap ***<dsap-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;dsap-id is the access point of the destination service, the valid range is 0~255;ssap-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

9.5.2.2.6 show dynamic-vlan prefer

Command: show dynamic-vlan prefer

Function: Display the preference of the dynamic VLAN.

Parameter: None.

Command Mode: Admin Mode and other configuration Mode.

Usage Guide: Display the dynamic VLAN preference.

Example: Display current dynamic VLAN preference.

Switch#show dynamic-vlan prefer

IP Subnet Vlan

Mac Vlan/Voice Vlan

Protocol Vlan

9.5.2.2.7 show mac-vlan

Command: show mac-vlan

Function: Display the configuration of   MAC-based VLAN on the switch.

Parameter: None.

Command Mode: Admin Mode and other configuration 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

9.5.2.2.8 show mac-vlan interface

Command: show mac-vlan interface

Function: Display the ports at MAC-based VLAN.

Parameter: None.

Command Mode: Admin Mode and other configuration 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

9.5.2.2.9 show protocol-vlan

Command: show portocol-vlan

Function: Display the configuration of   Protocol-based VLAN on the switch.

Parameter: None.

Command Mode: Admin Mode and other configuration 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

9.5.2.2.10 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 and other configuration 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

9.5.2.2.11 show subnet-vlan interface

Command: show subnet-vlan interface

Function: Display the port at IP-subnet-based VLAN.

Parameter: None.

Command Mode: Admin Mode and other configuration 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

9.5.2.2.12 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

9.5.2.2.13 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

9.5.2.2.14 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

9.5.3 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.
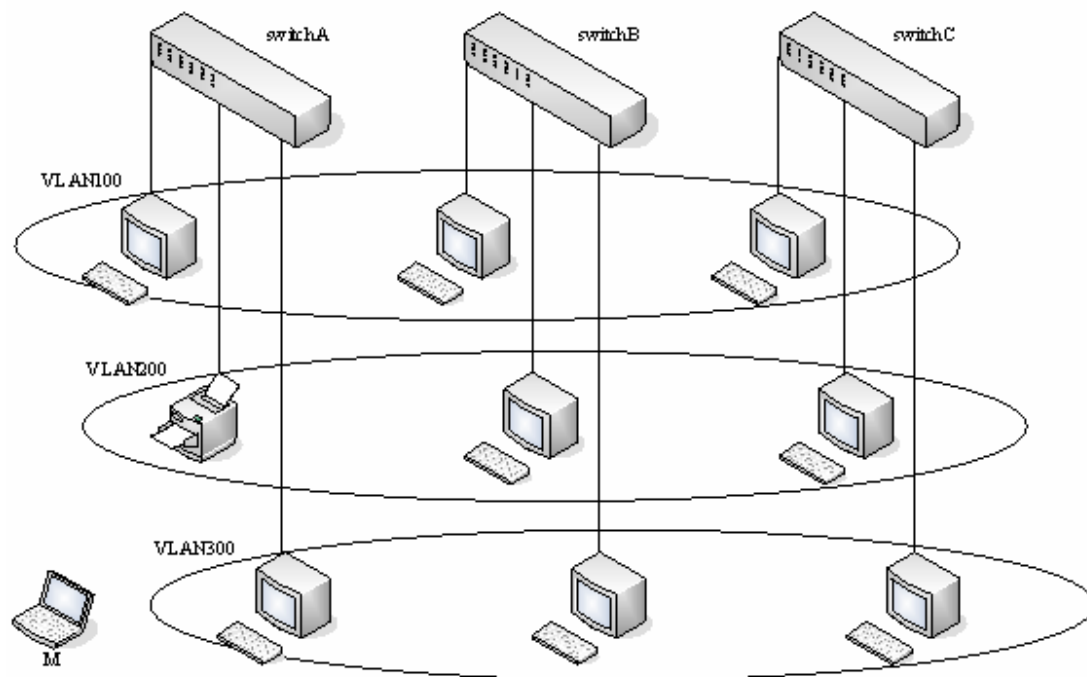
Figure 9-5Typical topology application of dynamic VLAN

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

9.5.4 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 go 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.

9.6 Voice VLAN Configuration

9.6.1 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.

9.6.2 Voice VLAN Configuration

9.6.2.1 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

9.6.2.2 Commands for Voice VLAN Configuration

9.6.2.2.1 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 and other configuration 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
----------------	---------------------	-----	--------
test	00-00-00-00-00-ff	0x80	7
NULL	00-00-00-00-00-11	0x80	5

9.6.2.2.2 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

9.6.2.2.3 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 0 priority 5 name test

9.6.2.2.4 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

9.6.3 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.
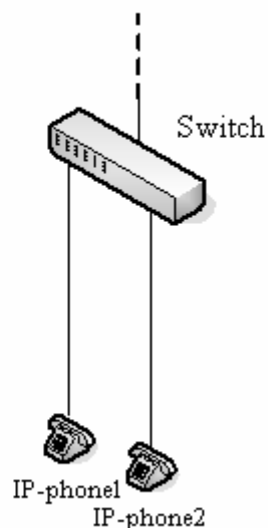
Fig 9-6 VLAN typical apply topology Figure

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

9.6.4 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 10 MAC Table Configuration

10.1 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.

10.1.1 Obtaining MAC Table

The MAC table can be built up staticly and dynamicly. 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.

MAC 00-01-11-11-11-11

MAC 00-01-33-33-33-33

MAC 00-01-22-22-22-22

MAC 00-01-44-44-44-44
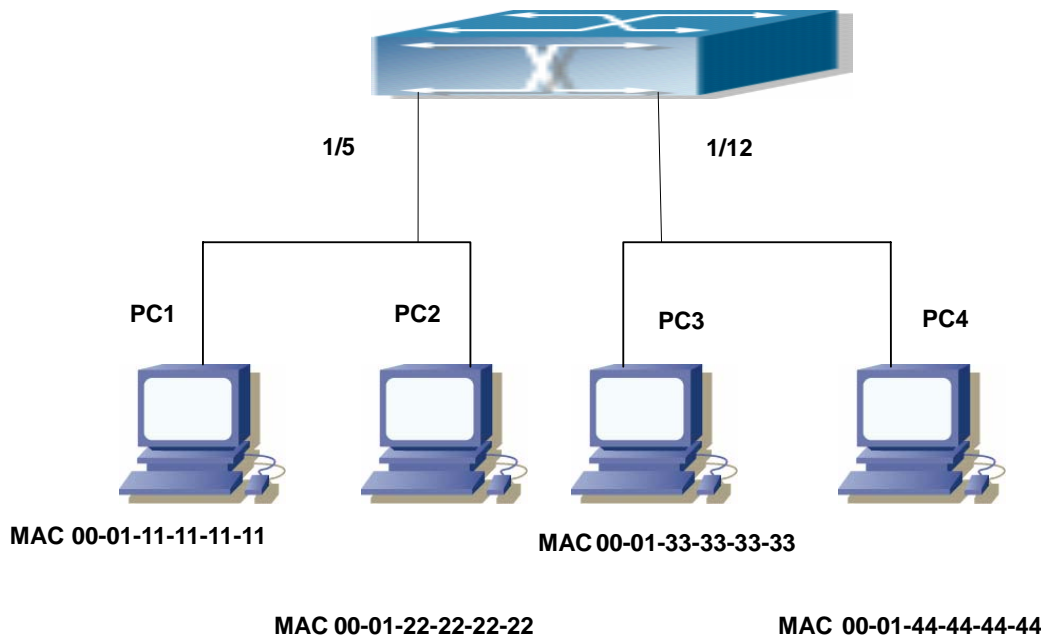
Fig10-1 MAC Table dynamic learning

The topology of the figure above: 4 PCs connected to ES4700 series, where PC1 and PC2 belongs to a same physical segment (same collision domain), the physical segment connects to port 1/5 of ES4700 series; PC3 and PC4 belongs to the same physical segment that connects to port 1/12 of ES4700 series.

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 sendsa 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 ES4700 series. Aging time can be modified in ES4700

series.

10.1.2 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 ES4700 series 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 ES4700 series 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.

3. 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.

10.2 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	blackhole} address** *<mac-addr>* **vlan** *<vlan-id>* **[interface [ethernet	portchannel]** *<interface-name>*]	**[source|destination|both]** **no mac-address-table {static	blackhole	dynamic} [address** *<mac-addr>*] **[vlan** *<vlan-id>*] **[interface [ethernet	portchannel]** *<interface-name>*]	Configure static MAC forwarding or filter entry.

10.3 Commands for MAC Address table configuration

10.3.1 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

10.3.2 mac-address-table

Command: mac-address-table {static | blackhole} address *<mac-addr>* vlan *<vlan-id>* [interface [ethernet | portchannel] *<interface-name>*] | [source|destination|both]

           no mac-address-table {static | blackhole | dynamic} [address *<mac-addr>*] [vlan *<vlan-id>*] [interface [ethernet | portchannel] *<interface-name>*]

Function: Add or modify static address entries and filter address entries. The "**no mac-address-table {static | blackhole | dynamic} [address *<mac-addr>*] [vlan *<vlan-id>*] [interface [ethernet | portchannel] *<interface-name>*]**" command deletes the two entries.

Parameter: static is the static entries; **blackhole** is filter entries, which is for discarding frames from specific MAC address, it can filter source address, destination address or the both; **dynamic** is dynamic address entries;*<mac-addr>* MAC address to be added or deleted;*<interface-name>* name of the port transmitting the MAC data packet;*<vlan-id>* is the vlan number. **Source** is based on source address filter; **destination** is based on destination address filter; **both** is based on source address and destination filter, the default is both.

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

10.3.3 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 and other configuration 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

10.4 Typical Configuration Examples
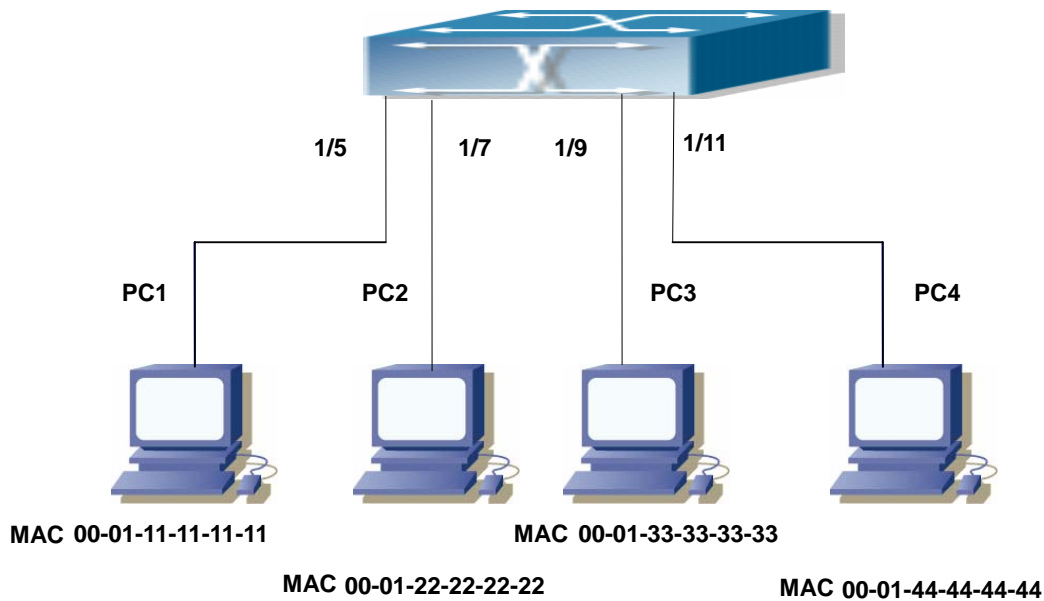
Fig 10-2 MAC Table typical configuration example

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

10.5 Troubleshooting Help

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 portand contact technical support for solution.

10.6 MAC Address Function Extension

10.6.1 MAC Address Binding

10.6.1.1 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.

10.6.1.2 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
Port mode	
port-security **no port-security**	Enable MAC address binding function for the port, when config the command, it will delete all the dynamic mac on the port and then begin to learn the new mac；the"**no port-security"** command disables the MAC address binding function for the port

2. Lock the MAC addresses for a port

Command	Explanation
Port mode	
port-security lock **no port-security lock**	Lock the port,when a port is locked, the MAC address learning function will be disabled.the "no port-security lock" command restores the MAC address learning function for the port.
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
Port 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.

10.6.1.3 Command For MAC Address Binding configuration

10.6.1.3.1 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

10.6.1.3.2 port-security

Command: port-security

        no port-security

Function: Enable MAC address binding function for the port, the "**no port-security**" command disables the MAC address binding function for the port.

Command mode: Port 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 1.

Switch(config)#interface ethernet 1/1

Switch(Config-If-Ethernet1/1)#port security

10.6.1.3.3 port-security lock

Command: port security lock

        no port-security lock

Function: Lock the port, when a port is locked, the MAC address learning function will be disabled ; the "**no port-security**" command restores the MAC address learning function for the port.

Command mode: Port Mode.

Default: Port security lock is not enabled by default.

Usage Guide: When config the command, you must make sure that there is dynamic mac on the interface,if there is no dynamic mac on the interface, the interface will down.

Example: Lock the port 1.

Switch(config)#interface ethernet 1/1

Switch(Config-If-Ethernet1/1)#port-security lock

10.6.1.3.4 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: Port 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-If-Ethernet1/1)# port-security convert

10.6.1.3.5 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: Port 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-If-Ethernet1/1)# port-security mac-address 00-03-0F-FE-2E-D3

10.6.1.3.6 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: Port 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-If-Ethernet1/1)# port-security maximum 4

10.6.1.3.7 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: Port 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-If-Ethernet1/1)# port-security timeout 30

10.6.1.3.8 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-If-Ethernet1/1)#port-security violation shutdown

10.6.1.3.9 show port-security

Command: show port-security

Function: Display the secure MAC addresses of the port.

Command mode: Admin Mode and other configuration 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

Security Port   MaxSecurityAddr   CurrentAddr   Security Action

----

Ethernet1/3   1   1   Protect

Max Addresses limit per port :128

Total Addresses in System :1

10.6.1.3.10 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 and other configuration 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.

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.

10.6.1.3.11 show port-security interface

Command: show port-security interface *<interface-id>*

Function: display the configuration of secure port.

Command mode: Admin Mode and other configuration 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 or not.
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 or not.

10.6.1.4 Binding MAC Address Binding Troubleshooting Help

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 11 MSTP Configuration

11.1 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.

11.1.1 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:
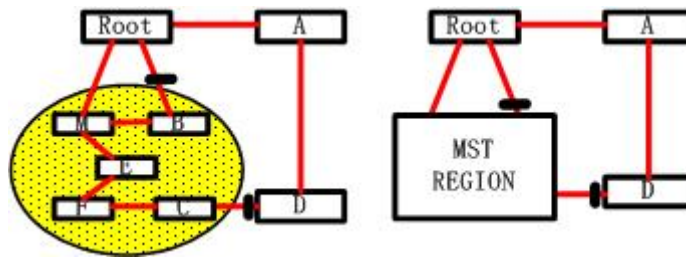
Fig 11-1 Example of CIST and MST Region

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.

11.1.1.1 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.

11.1.1.2 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.

11.1.2 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.

11.1.3 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.

11.2 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 Port mode	

spanning-tree **no spanning-tree**	Enable/Disable MSTP
Global Mode	
spanning-tree mode {mstp|stp} **no spanning-tree mode**	Set MSTP running mode
Port mode	
spanning-tree mcheck	Force port migrate 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
spanning-tree priority *<bridge-priority>* **no spanning-tree priority**	Configure the spanning-tree priority
Port 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>* rootguard **no spanning-tree mst *<instance-id>* rootguard**	Configure currently port whether running rootguard in specified instance, configure the rootguard port can't turn to root port.
spanning-tree rootguard **no spanning-tree rootguard**	Configure currently port whether running rootguard in instance 0, configure the rootguard port can't turn to root port.

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
Port 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
Port 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
Port 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 not more than one time every ten seconds. "no spanning-tree tcflush" restores to default setting,enable flush once the topology changes.
Port 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.

11.3 Command for MSTP

11.3.1 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

11.3.2 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

11.3.3 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

11.3.4 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

11.3.5 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

11.3.6 spanning-tree

Command: spanning-tree

    no spanning-tree

Function: Enable MSTP in global mode and in port mode; The command "**no spanning-tree**" is to disable MSTP.

Command mode: Global Mode and Port 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-If-Ethernet1/2)#no spanning-tree

11.3.7 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 CISCOequipments.

        auto: Auto identified packet format, which is determined by checking the format of the received packets.

Default: Auto 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 AUTO packet format is set by default in the concern of better compatibility with previous products and the leading companies.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-If-Ethernet1/2)#spanning-tree format standard

11.3.8 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

11.3.9 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

11.3.10 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: Port 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

11.3.11 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

11.3.12 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

11.3.13 spanning-tree mcheck

Command: spanning-tree mcheck

Function: Force the port to run in the MSTP mode.

Command mode: Port 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-If-Ethernet1/2)#spanning-tree mcheck

11.3.14 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

11.3.15 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 if 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)#

11.3.16 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: Port 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-If-Ethernet1/2)#spanning-tree mst 2 cost 3000000

11.3.17 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: Port 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-If-Ethernet1/2)#spanning-tree mst 1 port-priority 32

11.3.18 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

11.3.19 spanning-tree mst rootguard

Command: spanning-tree [mst *<instance-id>*]rootguard

          no spanning-tree [mst *<instance-id>*] rootguard

Function: Enable the rootguard function for specified instance, the rootguard function forbid the port to be MSTP root port. "no spanning-tree mst <instance-id> rootguard" disable the rootguard function.

Parameter:*<instance-id>*：MSTP instance ID.

Command mode: Port mode.

Default: Disable rootguard function.

Usage Guide: The command is used in port mode ,if the port is configured to be a rootguand port , it is forbidden to be a MSTP root port. If superior BPDU packet is received from a rootguard port, MSTP did not recalculate spanning-tree, and just set the status of the port to be root_inconsistent(blocked).If no superior BPDU packet is received from a blocked rootguard port, the port status will restore to be forwarding. The rootguard function can maintain a relative stable spanning-tree topology when a new switch is add to the network.

Example: Enable rootguard function for port 1/2 in instance 0.

Switch(config)#interface ethernet 1/2

Switch(Config-If-Ethernet1/2)#spanning-tree mst 0 rootguard

Switch(Config-If-Ethernet1/2)#

11.3.20 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: Port 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

11.3.21 spanning-tree priority

Command: spanning-tree priority *<bridge-priority>*

　　　　　no spanning-tree priority

Function: Configure the spanning-tree priority; The "**no spanning-tree priority**" command restores the default priority.

Parameter: *<bridge-priority>* is the priority of the bridging switch. Its value should be round times of 4096 between 0 and 61440, such as 0, 4096, 8192 … 61440.

Command Mode: Global Mode

Default: Priority is 32768.

Usage Guide: The bridge identifier can be altered by changing the priority of the switch. Further, the priority information can also be used for voting of the root bridge and the specified ports.

Example: Configure the priority is 4096.

Switch(config)#spanning-tree priority 4096

11.3.22 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: Port 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 cuase 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-If-Ethernet-1/2)#spanning-tree digest-snooping

11.3.23 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 not more than one time 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)#

11.3.24 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 not more than one time every ten seconds.

Default: Global configuration.

Command mode: Port 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-If-Ethernet-1/2)#spanning-tree tcflush disable

11.4 MSTP Example

The following is a typical MSTP application scenario:
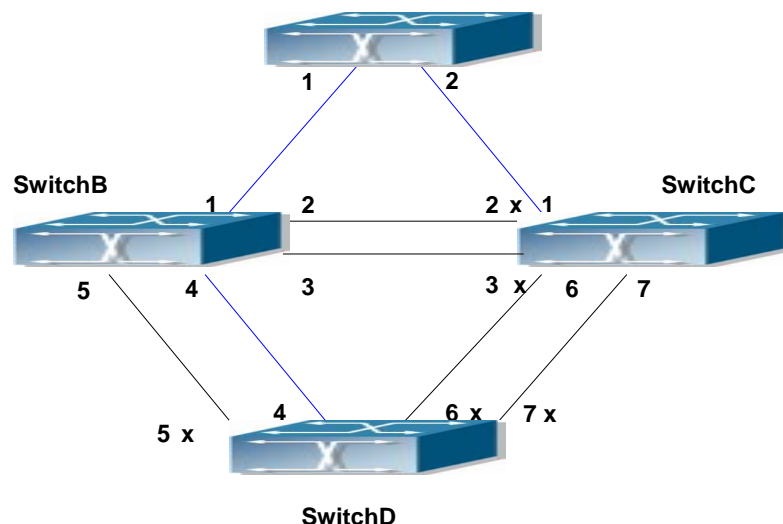
Fig 11-2Typical MSTP Application Scenario

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.
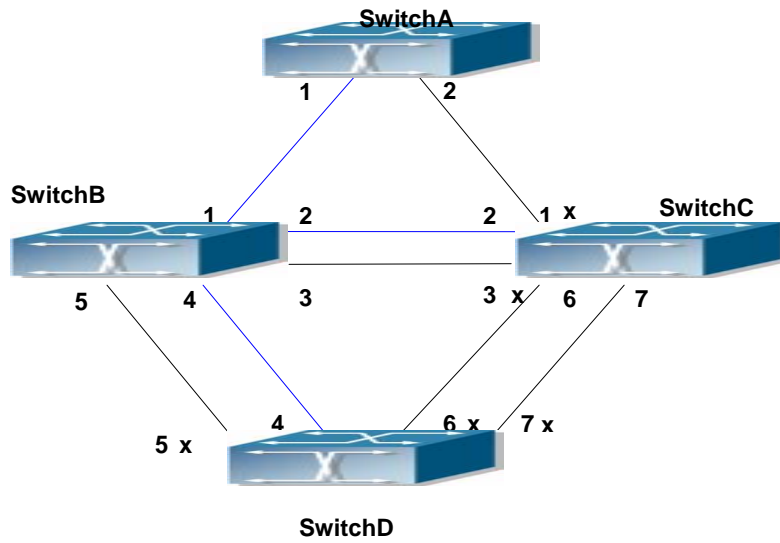
Fig 11-3 The Topology Of the Instance 0 after the MSTP Calculation
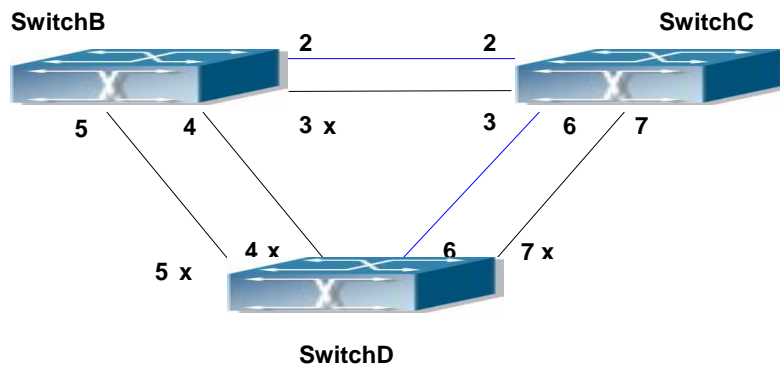
Fig 11-4 The Topology Of the Instance 3 after the MSTP Calculation
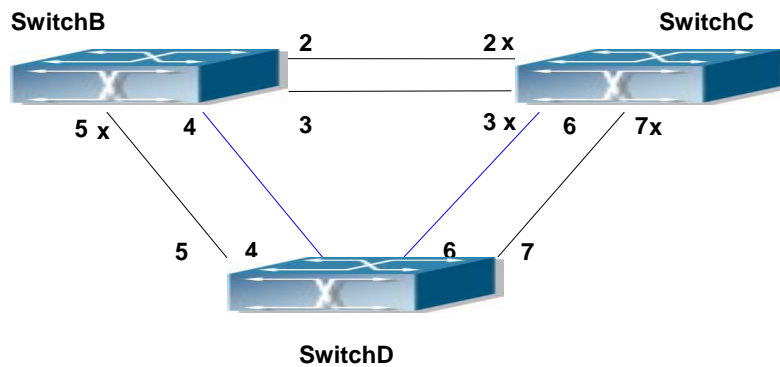
Fig 11-5 The Topology Of the Instance 4 after the MSTP Calculation

11.5 MSTP Troubleshooting Help

☞ 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.

11.5.1 Monitor And Debug Command

11.5.1.1 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

11.5.1.2 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

11.5.1.3 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)#

11.5.1.4 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

Switch#debug spanning-tree

Switch#debug spanning-tree bpdu rx interface e1/1

11.6 Web Management

Click "MSTP control" to enter MSTP control configuration mode to manage MSTP features for the switch.

11.6.1 MSTP field operation

Click "MSTP control" to enter MSTP field operation.

11.6.1.1 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.

Instance Config	
Instance Name	
VLAN name	

11.6.1.2 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.

Field Name Config	
Field Name	

11.6.1.3 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.

```
revision-level Config
revision-level      [                    ]
```

11.6.2 MSTP port operation

11.6.2.1 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.

```
PortFast Config
Port                 Ethernet1/1  ∨
```

11.6.2.2 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.

```
Port Priority Config
Port              Ethernet1/1  ∨
Instance Name     [                    ]
Priority          [                    ]
```

11.6.2.3 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.

```
Port Cost Config
Port              Ethernet1/1  ∨
Instance Name     [                    ]
Cost              [                    ]
```

11.6.2.4 MSTP mode

Click "MSTP control" to enter MSTP port operation, then "MSTP Mode".

Force switch port migrate to run under MSTP.

Force port 1/2 migrate to run under MSTP.

```
MSTP Mode
Port                 Ethernet1/1  ∨
```

11.6.2.5 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.

Link_Type Config	
Port	Ethernet1/1 ⌄
link type	auto ⌄

11.6.2.6 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.

MSTP Agreement Port Config	
Port	Ethernet1/1 ⌄

11.6.3 MSTP global control

11.6.3.1 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.

MSTP Global Agreement Port Config	
MSTP Global Config	Open Close

11.6.3.2 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.

Forward-time Config	
Forward-time	

11.6.3.3 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.

Hello_time Config	
Bridge Hello time	

11.6.3.4 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.

Max Age Time Config	
Max Age Time	

11.6.3.5 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.

Max Hop Time Config	
Max Hop Time	

11.6.3.6 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.

Priority Config	
Instance Name	
Priority	

11.6.4 Show MSTP setting

11.6.4.1 Instance information

Click MSTPL control, "show MSTP settings", enter "Instance Information".

Display MSTP and instances information.

Display Instance0 MSTP information.

```
Information Feedback Window

Name         00030f000007
Revision     0
Instance     Vlans Mapped
---------------------------------
00           1-4094
---------------------------------
```

11.6.4.2 MSTP field information

Click "MSTP control", "show MSTP setting", enter "MSTP Field Information".

Display effective MSTP field parameter configurations.

Chapter 12 Flow-based Redirection

12.1 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.

12.2 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>* **|***<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 < *IFNAME>* **| <** *IFNAME>* **]}**	Display the information of current flow-based redirection in the system/port

12.3 Command for Flow-based Redirection

12.3.1 access-group <aclname> redirect to interface ethernet

Command：**access-group** *<aclname>* **redirect to interface [ethernet** *<IFNAME>* **|<***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-If-Ethernet1/1)# access-group 1 redirect to interface ethernet 1/6

12.3.2 show flow-based-redirect

Command：**show flow-based-redirect {interface [ethernet <** *IFNAME>* **\| <** *IFNAME>* **]}**

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 **<IFNAME>**，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

12.4 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-If-Ethernet1/1)# access-group 1 redirect to interface ethernet 1/6

12.5 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 13 L3 Forward Configuration

ES4700 series supports Layer 3 forwarding which forwards Layer 3 protocol packets (IP packets) across VLANs. Such forwarding uses IP addresses, when a interface receives an IP packet, it will perform a lookup in its own routing table and decide the operation according to the lookup result. If the IP packet is destined to another subnet reachable from this switch, then the packet will be forwarded to the appropriate interface. ES4700 series can forward IP packets by hardware, the forwarding chip of ES4700 series 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 processed by the CPU in switch, the forwarding of traffic will be completely handled by hardware. As a result, forwarding efficiency can be greatly improved, even to wire speed.

13.1 Layer 3 Interface

13.1.1 Introduction to Layer 3 Interface

Layer 3 interface can be created on ES4700 series. 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 layer 2 ports which belong to the same VLAN, or contain no layer 2 ports. At least one of the Layer 2 ports contained in Layer 3 interface should be in UP state for Layer 3 interface in UP state, otherwise, Layer 3 interface will be in 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.

13.1.2 Layer 3 Interface Configuration Task List

1. Create Layer 3 Interface
2. Bandwidth for Layer 3 Interface configuration

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.

2. Bandwidth for Layer 3 Interface configuration

Command	Explanation
Port mode	
bandwidth *<bandwidth>* **no bandwidth**	Config the bandwidth for Layer 3 Interface. the "**no bandwidth**" command recovery the default value.

13.1.3 Command for Layer 3 Interface

13.1.3.1 interface vlan

Command: interface vlan *<vlan-id>*

        no interface vlan *<vlan-id>*

Function: Create 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 creating 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 port mode.

Example: Creating a VLAN interface (layer 3 interface).

Switch (config)#interface vlan 1

13.1.3.2 bandwidth

Command: bandwidth *<bandwidth>*

no bandwidth

Function: Config the bandwidth for Layer 3 Interface. the "**no bandwidth**" command recovery the default value. The bandwidth of interface vlan is used to protocol account but not control the bandwidth of port. For instance, it is use the interface bandwidth （cost=10^8/bandwidth） when OSPF account the link cost, so change the bandwidth can result in OSPF link cost changed.

Parameters: *<bandwidth>* is the bandwidth for interface vlan. Range from 1bits to 10000000000 bits. It is can use unit "k, m, g". There are no decimal numbers after conversion.

Command mode: Port mode

Default: The default bandwidth for interface vlan is 100,000,000bit.

Usage Guide: This command only can be used at interface vlan mode。 The conversion of unit: 1g=1,000m=1,000,000k=1,000,000,000bit.

Example: Config the bandwidth for vlan1 is 50,000,000bit.

Switch(Config-if-Vlan1)#bandwidth 50m

13.2 IP Configuration

13.2.1 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 addresses so that Internet can develop further.

The most important problem IPv6 has solved is to add the amount of IP addresses. 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 address 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 External 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.

13.2.2 IPv4 Configuration

Layer 3 interface can be configured as IPv4 interface, IPv6 interface, or both.

13.2.2.1 Ipv4 Address Configuration

1. Configure the IPv4 address of three-layer interface

1. Configure the IPv4 address of three-layer interface

Command	Explanation
Port 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.

13.2.2.2 Command For IPv4 Address

13.2.2.2.1 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 notation; ***<mask>*** is subnet mask, dotted decimal notation; **[secondary]** indicates that the IP address is configured as secondary IP address.

Command Mode: Port 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 primary IP address of VLAN interface; if optional parameter **secondary** is configured, then that means the IP address is the secondary IP address of VLAN. One VLAN interface can only have one primary IP address and more than one secondary IP addresses. Primary IP and Secondary IP all can be used on SNMP/Web/Telnet management. Furthermore, the switch also provides BOOTP/DHCP manner to get 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

13.2.3 IPv6 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 solicitation message number
    （2）   Configure send neighbor solicitation message interval
    （3）   Enable and disable router advertisement
    （4）   Configure router lifespan
    （5）   Configure router advertisement minimum interval
    （6）   Configure router advertisement maximum interval
    （7）   Configure prefix advertisement parameters
    （8）   Configure static IPv6 neighbor entries

（9） Delete all entries in IPv6 neighbor tabl

（10） Set the hoplimit of sending router advertisement

（11） Set the mtu of sending router advertisement

（12） Set the reachable-time of sending router advertisement

（13） Set the retrans-timer of sending router advertisement

（14） Set the flag representing whether information other than the address information will be obtained via DHCPv6

（15） set the flag representing whether the address information will be obtained via DHCPv6

3. IPv6 Tunnel configuration

（1） Create/Delete Tunnel

（2） Configure Tunnel Source

（3） Configure Tunnel Destination

（4） Configure Tunnel Next-Hop

（5） Configure Tunnel Mode

（6） Configure Tunnel Routing

13.2.3.1 IPv6 Address Configuration

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 advertisement, routing protocol, etc. The NO command disables IPv6 function.

(2). Configure interface IPv6 address

Command	Explanation
Interface Configuration Mode	

Command	Description
ipv6 address *<ipv6-address/prefix-length>* **[eui-64]** **no ipv6 address** *<ipv6-address/prefix-length>*	Configure IPv6 address, including aggregatable global unicast addresses, site-local addresses and link-local 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 solicitation 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 duplicate address detection. The NO command resumes default value (1).

（2）Configure Send Neighbor solicitation Message Interval

Command	Explanation
Interface Configuration Mode	

Command	Explanation
[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）Enable and disable router advertisement

Command	Explanation
Interface Configuration Mode	
[no] ipv6 nd suppress-ra	Forbid IPv6 Router Advertisement. The NO command enables IPv6 router advertisement.

（4）Configure Router Lifespan

Command	Explanation
Interface Configuration Mode	
[no] ipv6 nd ra-lifetime <*seconds*>	Configure Router advertisement Lifespan. The NO command resumes default value (1800 seconds).

（5）Configure router advertisement Minimum Interval

Command	Description
Interface Configuration Mode	
[no] ipv6 nd min-ra-interval <*seconds*>	Configure the minimum interval for router advertisement. The NO command resumes default value (200 seconds).

（6）Configure router advertisement Maximum Interval

Command	Explanation
Interface Configuration Mode	

Command	Explanation
[no] ipv6 nd max-ra-interval *<seconds>*	Configure the maximum interval for router advertisement. The NO command resumes default value (600 seconds).

（7）Configure prefix advertisement 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 advertisement parameters of router. The NO command cancels the address prefix of routing advertisement.

（8）Configure static IPv6 neighbor 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）Delete all entries in IPv6 neighbor table

Command	Explanation
Admin Mode	
clear ipv6 neighbors	Clear all static neighbor table entries

（10）Set the hoplimit of sending router advertisement

Command	Explanation
Interface Configuration Mode	
ipv6 nd ra-hoplimit <value>	Set the hoplimit of sending router advertisement.

（11）Set the mtu of sending router advertisement

Command	Explanation
Interface Configuration Mode	
ipv6 nd ra-mtu <value>	Set the mtu of sending router advertisement.

（12）Set the reachable-time of sending router advertisement

Command	Explanation
Interface Configuration Mode	
ipv6 nd reachable-time <seconds>	Set the reachable-time of sending router advertisement.

（13）Set the retrans-timer of sending router advertisement

Command	Explanation
Interface Configuration Mode	
ipv6 nd retrans-timer <seconds>	Set the retrans-timer of sending router advertisement.

（14）Set the flag representing whether information other than the address information will be obtained via DHCPv6.

Command	Explanation
Interface Configuration Mode	
ipv6 nd other-config-flag	Set the flag representing whether information other than the address information will be obtained via DHCPv6.

（15）Set the flag representing whether the address information will be obtained via DHCPv6

Command	Explanation
Interface Configuration Mode	
ipv6 nd managed-config-flag	Set the flag representing whether the address information will be obtained via DHCPv6.

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 Mode

Command	Explanation
Tunnel Configuration Mode	
[no] tunnel mode ipv6ip [6to4 | isatap]	Configure tunnel mode. The NO command clears tunnel mode.

（**6**）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.

13.2.3.2 Command For IPv6 Configuration

13.2.3.2.1 ipv6 enable

Command:[no] ipv6 enable

Function: This command enables functions such as Unicast IPv6 Data Packet Transmit, Neighbor Discovery, Router advertisement and Routing Protocol, etc.

Parameter: None

Command Mode: Global Mode

Default: IPv6 is disabled.

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

13.2.3.2.2 ipv6 address

Command:ipv6 address *<ipv6-address/prefix-length>* [eui-64]

 no ipv6 address *<ipv6-address/prefix-length>* [eui-64]

Function: Configure agregatable global unicast address, site-local address and link-local address for the interface

Parameter: Parameter *<ipv6-address>* is the prefix of IPv6 address, parameter *<prefix-length>* is the prefix length 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:IPv6 address prefix can not be multicast address or any other specific IPv6 address, and different layer 3 interfaces can not configure the same address prefix. For global unicast address, the prefix must be in the range from 2000:: to 3fff::, and the length of the prefix must be greater than or equal to 3. For site-local address and link-local address, the length of the prefix must be greater 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

13.2.3.2.3 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 route

Parameters: Parameter ***<ipv6-prefix>*** is the destination prefix of IPv6 static route, 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 name of interface from which to reach the destination, parameter ***<tunnel no>*** is the exit tunnel No. of tunnel route, parameter *<**precedence**>* is the weight of this route, the range is 1-255, the default is 1

Default: There is not any IPv6 static route which is configured by default.

Command Mode: Global Mode

Usage Guide: When the next hop IPv6 address is link-local address, the interface name must be specified. When the next hop IPv6 address is global aggregatable unicast address and site-local 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 route.

Example: Configure static route 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 route 2 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

13.2.3.2.4 ipv6 redirect

Command：ipv6 redirect

             no ipv6 redirect

Function：Enable IPv6 router redirect function. The no operation of this command will disable the function.

Parameters：None.

Command Mode：Global Mode.

Default Settings：IPv6 router redirect function is disabled by default.

Usage Guide：If router A, router B, and node C are on the same network link, and router

A forwards IPv6 packets from node C to router B, expecting router B to continue the forwarding, then router A will send an IPv6 ICMPv6 redirect message to node C-source of the packet, notifying it that the best next hop of this destination address is router B. By doing so, the forwarding overhead of router A will be decreased, so is the network transmission delay of node C.

Examples： Enable IPv6 router redirect function.

Switch(config)#ipv6 redirect

13.2.3.2.5 ipv6 nd dad attempts

Command:ipv6 nd dad attempts *<value>*

           no ipv6 nd dad attempts

Function: Set Neighbor Solicitation Message number sent in succession by interface when setting Duplicate Address Detection.

Parameter:*<value>* is the Neighbor Solicitation Message number sent in succession by Duplicate Address Detection, 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 Duplicate Address Detection, this command is used to configure the ND message number of Duplicate Address Detection to be sent, *value* being 0 means no Duplicate Address Detection is executed.

Example: The Neighbor Solicitation Message number sent in succession by interface when setting　Duplicate Address Detection is 3..

Switch(Config-if-Vlan1)# ipv6 nd dad attempts 3

13.2.3.2.6 ipv6 nd ns-interval

Command:ipv6 nd ns-interval *<seconds>*

           no ipv6 nd ns-interval

Function: Set the time interval of Neighbor Solicitation Message sent by the interface

Parameter: parameter *<seconds>* is the time interval of sending Neighbor Solicitation 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 Solicitation Message time interval to

be 8 seconds.

Switch(Config-if-Vlan1)#ipv6 nd ns-interval 8

13.2.3.2.7 ipv6 nd suppress-ra

Command:[no] ipv6 nd suppress-ra

Function:Prohibit router announcement.

Parameter: None

Command Mode: Interface Configuration Mode

Default: Router Announcement function is disabled.

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

13.2.3.2.8 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

13.2.3.2.9 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 3/4 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

13.2.3.2.10 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

13.2.3.2.11 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 link-local. Parameter **off-link** says the prefix specified by router announcement message is not assigned to link-local, the node which sends data to the address including this prefix consider link-local 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

13.2.3.2.12 ipv6 nd ra-hoplimit

Command: ipv6 nd ra-hoplimit <value>

Function: Set the hoplimit of sending router advertisement.

Parameters: <value> is the hoplimit of sending router advertisement, ranging from 1 to 255.

Command Mode： Interface Configuration Mode.

Default: The default hoplimit of sending router advertisement is 64.

Example: Set the hoplimit of sending router advertisement in interface vlan 1 as 128.

Switch#(Config-if-Vlan1)#ipv6 nd ra-hoplimit 128

13.2.3.2.13 ipv6 nd ra-mtu

Command: ipv6 nd ra-mtu <value>

Function: Set the mtu of sending router advertisement.

Parameters: <value> is the mtu of sending router advertisement, ranging from 0 to 1500.

Command Mode： Interface Configuration Mode.

Default: The default mtu of sending router advertisement is 1500.

Example: Set the mtu of sending router advertisement in interface vlan 1 as 500.

Switch#(Config-if-Vlan1)#ipv6 nd ra-mtu 500

13.2.3.2.14 ipv6 nd reachable-time

Command: ipv6 nd reachable-time <seconds>

Function: Set the reachable-time of sending router advertisement.

Parameters: <value> is the reachable-time of sending router advertisement, ranging from 0 to 3600000 milliseconds.

Command Mode： Interface Configuration Mode.

Default Settings: The default reachable-time of sending router advertisement is 30000 milliseconds.

Example: Set the reachable-time of sending router advertisement in interface vlan 1 as 100000 milliseconds.

Switch#(Config-if-Vlan1)#ipv6 nd reachable-time 100000

13.2.3.2.15 ipv6 nd retrans-timer

Command: ipv6 nd retrans-timer <seconds>

Function: Set the retrans-timer of sending router advertisement.

Parameters: <value> is the retrans-timer of sending router advertisement, ranging from 0 to 4294967295 milliseconds.

Command Mode： Interface Configuration Mode.

Default: The default retrans-timer of sending router advertisement is 1000 milliseconds.

Example: Set the reachable-time of sending router advertisement in interface vlan 1 as 10000 milliseconds.

Switch#(Config-if-Vlan1)#ipv6 nd retrans-timer 10000

13.2.3.2.16 ipv6 nd managed-config-flag

Command: ipv6 nd managed-config-flag

no ipv6 nd managed-config-flag

Function: Set the management address configuration flag of Router Advertisement as 1.

Parameters: None.

Command Mode： Interface Configuration Mode.

Default: The management address configuration flag of Router Advertisement is 0 by default.

Usage Guide ： When the management address configuration flag of Router Advertisement is 1, in order to obtain an address, the hosts receiving this router advertisement may use a stateless address autoconfiguration protocol, and also have to use a stateful address configuration protocol (like DHCPv6); when the flag is 0, the hosts receiving this router advertisement only use stateless autoconfiguration protocol to obtain an address.

Example： Set the management address flag of Router Advertisement.

Switch(Config-if-Vlan1)#ipv6 nd managed-config-flag

13.2.3.2.17 ipv6 nd other-config-flag

Command: ipv6 nd other-config-flag

no ipv6 nd other-config-flag

Function: Set other configuration flags of Router Advertisement as 1.

Parameters: None.

Command Mode： Interface Configuration Mode.

Default: Other configuration flags of Router Advertisement are 0 by default.

Usage Guide： When other configuration flags are 1, the hosts receiving this router advertisement have to use a stateful address configuration protocol (like DHCPv6) to obtain information other than it address (such as the DNS addresses).

Example： Set other configuration flags of Router Advertisement.

Switch(Config-if-Vlan1)#ipv6 nd other-config-flag

13.2.3.2.18 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, same to interface prefix, 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

13.2.3.2.19 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

13.2.3.2.20 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 link-local 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 Echos 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.

13.2.3.2.21 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

13.2.3.2.22 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

13.2.3.2.23 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 nexhop.

Example: Configure tunnel next hop 178.99.156.8

Switch {Config-if-Tunnel1}#tunnel nexthop 178.99.156.8

13.2.3.2.24 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

13.2.3.2.25 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

13.2.4 IP Configuration Examples

13.2.4.1 Configuration Examples of IPv4
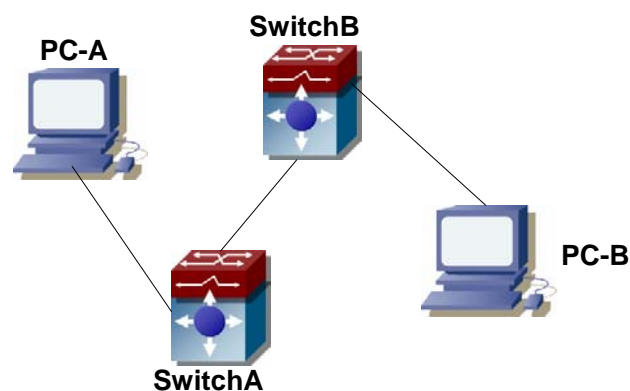
Fig 13-1   IPv4 configuration example

The user's configuration requirements are: Configure IPv4 address of different network segments on switchA and switchB, configure static routing and validate accessibility using ping function.

Configuration Description:

1、 Configure two vlans on SwitchA, namely, vlan1 and vlan2.

2、 Configure IPv4 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 vlan3.

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

13.2.4.2 Configuration Examples of IPv6

Example 1:
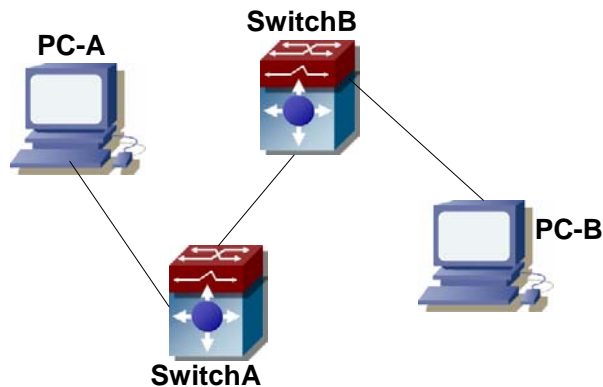
Fig 13-2 IPv6 configuration example

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 vlan3.

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:
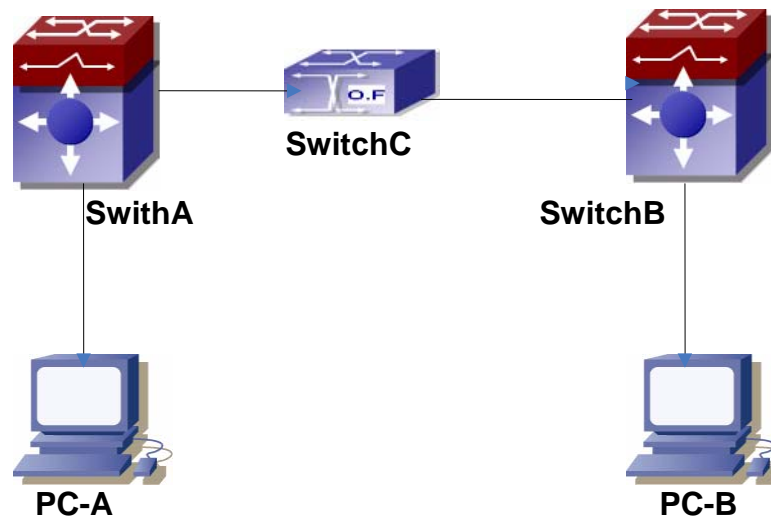
Fig   13-3 IPv6 Tunnel

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

13.2.5 IP Troubleshooting Help

IPv6 troubleshooting:

☞ IPv6 on-off 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 advertisement Interval.

☞ If the connected PC has not obtained IPv6 address, you should check the RA announcement switch (the default is turned off)

13.2.5.1 Monitor And Debug Command

13.2.5.1.1 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	Statistics of total ICMP packets received and classified information

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	Statistics of total ICMP packets sent and classified information
TCP statistics:	TCP packet statistics.
UDP statistics:	UDP packet statistics.

13.2.5.1.2 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: Enable 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

13.2.5.1.3 debug ipv6 packet

Command:[no] debug ipv6 packet

Function:IPv6 data packets receive/send debug message.

Parameter: None

Default: None

Command Mode: Admin Mode

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

13.2.5.1.4 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

13.2.5.1.5 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

13.2.5.1.6 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

Usage Guide: None

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

13.2.5.1.7 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 L3 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

13.2.5.1.8 show ipv6 route

Command:show ipv6 route [<*destination*>|<*destination* >/<*length*>| database| fib [local]| nsm [connected | static | rip| ospf | bgp | isis| kernel| database]|statistics]

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 kernal 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 -	Abbreviation display sign of every entry

connected, S - static, R - RIP, O - OSPF,I - IS-IS, B - BGP > - selected route, * - FIB route, p - stale info	
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.

13.2.5.1.9 show ipv6 neighbors

Command ： show ipv6 neighbors[{vlan|ethernet|tunnel}*interface-number| interface-name* | address *<ipv6address>*]

Function： Display neighbor table entry information.

Parameter： Parameter **{vlan|ethernet|tunnel}***interface-number|interface-name* specify the lookup based on interface.Parameter ***ipv6-address*** specifies the lookup based on IPv6 address.It displays the whole neighbor table entry if without parameter.

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	Port
State			
2002:ca60:c801:1:250:baff:fef2:a4f4	00-50-ba-f2-a4-f4	Vlan1	
Ethernet1/2	reachable		
3ffe:3240:800d:1::100	00-03-0f-01-27-86	Vlan1	
Ethernet1/3	reachable		
3ffe:3240:800d:1::8888	00-02-01-00-00-00	Vlan1	
Ethernet1/1	permanent		
3ffe:3240:800d:1:250:baff:fef2:a4f4	00-50-ba-f2-a4-f4	Vlan1	
Ethernet1/4	reachable		
3ffe:3240:800d:2::8888	00-02-01-00-01-01	Vlan2	
Ethernet1/16	permanent		
3ffe:3240:800d:2:203:fff:fefe:3045	00-03-0f-fe-30-45	Vlan2	
Ethernet1/15	reachable		
fe80::203:fff:fe01:2786	00-03-0f-01-27-86	Vlan1	

Ethernet1/5   reachable

fe80::203:fff:fefe:3045   00-03-0f-fe-30-45   Vlan2

Ethernet1/17   reachable

fe80::20c:ceff:fe13:eac1   00-0c-ce-13-ea-c1   Vlan12

Ethernet1/20   reachable

fe80::250:baff:fef2:a4f4   00-50-ba-f2-a4-f4   Vlan1

Ethernet1/6   reachable

IPv6 neighbour table: 11 entries

Displayed information	Explanation
IPv6 Addres	Neighbor IPv6 address
Link-layer Addr.	Neighbor MAC address
Interface	Exit interface name
Port	Exit interface name
State	Neighbor status (reachable、 statle、 delay、 probe、 permanent、 incomplete、 unknow)

13.2.5.1.10 show ipv6 traffic

Command:show ipv6 traffic

Function: Display IPv6 transmission data packets statistics information.

Parameter: None

Default Situation: None

Command Mode: Admin Mode

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

13.2.5.1.11 show ipv6 enable

Command:show ipv6 enable

Function: Display IPv6 transmission function on/off status

Parameter: None

Default: None

Command Mode: Admin Mode

Usage Guide:

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

13.2.5.1.12 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)

13.3 IP Forwarding

13.3.1 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 ES4700 series is done with the participation of hardware, and can achieve wire speed forwarding . In addition, flexible management is provided to adjust and monitor forwarding. ES4700 series 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.

13.3.2 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.

13.3.3 Command for IP Route Aggregation

13.3.3.1 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

13.4 URPF

13.4.1 Introduction to URPF

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.

In Source Address Spoofing attacks, attackers will construct a series of messages with fake source addresses. For applications based on IP address verification, such attacks may allow unauthorized users to access the system as some authorized ones, or even the administrator. Even if the response messages can't reach the attackers, they will also damage the targets.

1.1.1.8/8   2.2.2.1/8

Source IP：2.2.2.1/8

Router A   Router B   Router C
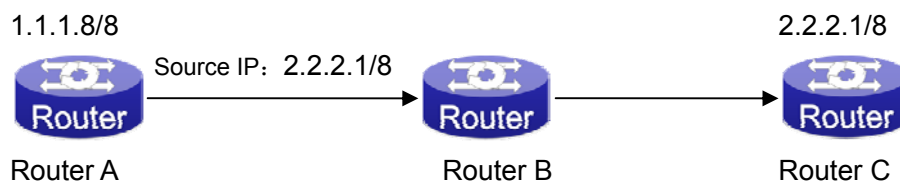
In the above figure, Router A sends requests to the server Router B by faking messages whose source address are 2.2.2.1/8 .In response, Router B will send the messages to the real "2.2.2.1/8". Such illegal messages attack both Router B and Router C. The application of URPF technology in the situation described above can avoid the attacks based on the Source Address Spoofing.

13.4.1.1 URPF Operating Mechanism

At present the UPRF relies on the ACL function provided by the switch chips.

Firstly, globally enable the URPF function to monitor the changes in the router table: create a corresponding URPF permit ACL rule for each router in the router table FIB. In URPF strict mode, the format of ACL rules is: the source address segments of inbound packets + the ingress interface VID of inbound packets. The source address segments of inbound packets are in correspondence with the destination address segments in the FIB router table entries, while the ingress interface VID of inbound packets with the egress interface VID in the FIB router table entries. In URPF loose mode, the format of ACL rules is the source address segments of inbound packets, which are in correspondence with destination address segments in the FIB router table entries.

After enabling URPF on the port: bind the port to RUPF rules, and create the default hardware for DENY ALL rule distribution.

The above operations will guarantee that, when data reach the port, only those match the rules can pass through it with all others dumped.

The present corresponding ACL rule privilege is low, not blocking all kinds of protocol packets; hence, enabling this function will not affect the normal operation of routing protocols of the switch.

13.4.2 URPF Configuration Task Sequence

1. Enable URPF
2. Enable URPF on port
3. Display and debug URPF relevant information

1. Globally enable URPF

Command	Explanation
Global mode	
urpf enable **no urpf enable**	Globally enable and disable URPF.

2. Enable URPF on port

Command	Explanation
Command	Explanation

Port mode	
**ip urpf enable {loose	strict} {allow-default-route }** **no ip urpf enable**	Enable and disable URPF on port.

3. Display and debug URPF relevant information

Command	Explanation
Admin mode	
debug l4driver urpf {notice |warning |error} **no debug l4driver urpf {notice	warning	error}**	Enable the URPF debug function to display error information if failures occur during the installation of URPF rules.
Admin and Config Mode	
show urpf	Display which interfaces have been enabled with URPF function.
show urpf rule ipv4 num interface {ethernet IFNAME |IFNAME}	Display the number of IPv4 rules bonded to the port.
show urpf rule ipv6 num interface {ethernet IFNAME |IFNAME}	Display the number of IPv6 rules bonded to the port.
show urpf rule ipv4 interface {ethernet IFNAME |IFNAME}	Display the details of IPv4 rules bonded to the port.
show urpf rule ipv6 interface {ethernet IFNAME |IFNAME}	Display the details of IPv6 rules bonded to the port.

13.4.3 Commands for URPF

13.4.3.1 urpf enable

Command: urpf enable

          no urpf enable

Function：Enable the global URPF function.

Command mode: Global Mode

Default：The URPF protocol module is disabled by default.

Example:

Switch(config)#urpf enable

13.4.3.2 ip urpf enable

Command：**ip urpf enable {loose | strict} {allow-default-route |}**

no ip urpf enable

Function：Enable the URPF function on the port.

Parameters：loose：the loose mode;

strict：the strict mode;

allow-default-route：allow the default route.

Command mode: Port Mode

Default：The URPF function is disabled on the port by default.

Usage Guide：Users should specify the mode: loose or strict.

Example:

Switch(config)#interface ethernet 1/4

Switch(Config-If-Ethernet1/4)#ip urpf enable strict

Switch(Config-If-Ethernet1/4)#interface ethernet 1/5

Switch(Config-If-Ethernet1/5)#ip urpf enable loose

Switch(Config-If-Ethernet1/5) #interface ethernet 1/6

Switch(Config-If-Ethernet1/6)#ip urpf enable loose allow-default-route

Switch(Config-If-Ethernet1/6)#interface ethernet 1/7

Switch(Config-If-Ethernet1/7)#ip urpf enable strict allow-default-route

13.4.3.3 show urpf rule ipv4 num

Command：**show urpf rule ipv4 num interface {ethernet IFNAME |IFNAME}**

Function：Display the number of IPv4 rules bonded to the port.

Parameters：IFNAME: specify the port name.

Command Mode：Admin and Config Mode

Examples：Display the number of IPv4 rules bonded to the port Ethernet1/4.

Switch#show urpf rule ipv4 num interface ethernet 1/4

13.4.3.4 show urpf rule ipv6 num

Command：**show urpf rule ipv6 num interface {ethernet IFNAME |IFNAME}**

Function：Display the number of IPv6 rules bonded to the port.

Parameters：IFNAME: specify the port name.

Command Mode：Admin and Config Mode

Example：Display the number of IPv6 rules bonded to the port Ethernet1/4.

Switch#show urpf rule ipv6 num interface ethernet 1/4

13.4.3.5 show urpf rule ipv4

Command：**show urpf rule ipv4 interface {ethernet IFNAME |IFNAME}**

Function：Display the details of IPv4 rules bonded to the port.

Parameters：IFNAME: specify the port name.

Command Mode：Admin and Config Mode

Usage Guide：Display the currently distributed rules.

Examples：Display the details of IPv4 rules bonded to the port Ethernet1/4.

Switch#show urpf rule ipv4 interface ethernet 1/4

13.4.3.6 show urpf rule ipv6

Command：**show urpf rule ipv6 interface {ethernet IFNAME |IFNAME}**

Function：Display the details of IPv6 rules bonded to the port.

Parameters：IFNAME: specify the port name.

Command Mode：Admin and Config Mode

Usage Guide：Display the currently distributed rules.

Examples：Display the details of IPv6 rules bonded to the port ethernet1/4.

Switch#show urpf rule ipv6 interface ethernet 1/4

13.4.3.7 show urpf

Command: show urpf

Function: Display which interfaces have been enabled with URPF function.

Command Mode: Admin and Config Mode

Example:

Switch#show urpf

13.4.3.8 debug l4driver urpf

Command：**debug l4driver urpf {notice| warning| error}**

               no debug l4driver urpf {notice| warning| error}

Function：Enable the URPF debug function to display error information if failures occur during the installation of URPF rules.

Command Mode: Admin Mode

Example:

Switch#debug l4driver urpf error

13.4.4 URPF Typical Example
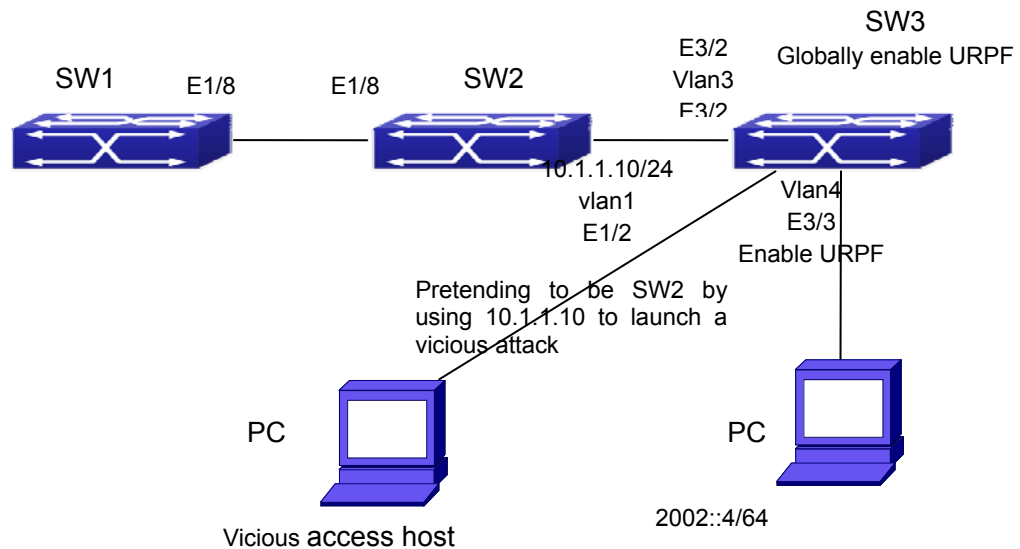
In the network, topology shown in the graph above, IP URPF function is enabled on SW3. When there is someone in the network pretending to be someone else by using his IP address to launch a vicious attack, the switch will drop all the attacking messages directly through the hardware FFP function.

Enable the URPF function in SW3 Ethernet3/3.

SW3 configuration task sequence:

Switch3#config

Switch3(config)#urpf enable

Switch3(config)#interface ethernet 3/3

Switch3(Config-If-Ethernet3/3)#ip urpf enable strict

13.4.5 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 whether there is a relative route in the FIB table. Only when one is found, can the ACL rules be distributed to the port.

☞ Check if the hardware ACL performance is full which lead to the newly generated route can not be applied with ACL rules.

☞ If all configurations are normal but URPF still can't operate as expected, please enable the URPF debug function and use the "show urpf" command and other

commands which display the rule number and details to observe whether the created URPF rules are correct, and send the result to the technology service center.

13.5 ARP

13.5.1 Introduction to ARP

ARP (Address Resolution Protocol) is mainly used to resolve IP address to Ethernet MAC address. ES4700 series supports both dynamic ARP and static ARP configuration. Furthermore, ES4700 series 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.

13.5.2 ARP Configuration Task List

1. Configure static ARP
2. Configure proxy ARP
3. Clear dynamic ARP
4. Clear the statistic information of ARP messages

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

4. Clear the statistic information of ARP message

Command	Explanation
Admin mode	
clear arp traffic	Clear the statistic information of ARP messages of the switch.

13.5.3 Command for ARP Configuration

13.5.3.1 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, at the same filed with interface 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: Port 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

13.5.3.2 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

13.5.3.3 clear arp traffic

Command：clear arp traffic
Function：Clear the statistic information of ARP messages of the switch. For box switches, this command will only clear statistics of APP messages received and sent from the current boardcard.
Command mode: Admin Mode
Example:
Switch#clear arp traffic

13.5.3.4 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: Port 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: Enable proxy ARP for VLAN 1.
Switch(Config-if-Vlan1)#ip proxy-arp

13.5.3.5 ARP Forwarding Troubleshooting Help

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 been 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.

13.5.3.6 Monitor And Debug Command

13.5.3.6.1 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: Enable 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.

13.5.3.6.2 show arp

Command: show arp [<*ipaddessr*>][<*vlan-id*>][<*hw-addr*>][type {static|dynamic}] [count] [vrf word]

Function: Displays the ARP table.

Parameters: < *ipaddessr* **>** 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; **word** is the specified vrf name.

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

ARP Unicast Items: 7, Valid: 7, Matched: 7, Verifying: 0, Incomplete: 0, Failed: 0, None: 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.
Valid	ARP entry number matching the filter conditions and attributing the legality states.

Matched	ARP entry number matching the filter conditions.
Verifying	ARP entry number at verifying again validity for Arp.
InCompleted	ARP entry number have ARP request sent without ARP reply.
Failed	ARP entry number at failed state.
None	ARP entry number at begin-found state.
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) port corresponding to the ARP entry.
Flag	Describes whether ARP entry is dynamic or static.

13.5.3.6.3 show arp traffic

Command：show arp traffic

Function：Display the statistic information of ARP messages of the switch. For box switches, this command will only show statistics of APP messages received and sent from the current boardcard.

Command mode: Admin and Config Mode

Usage Guide：Display statistics information of received and sent APP messages.

Example:

Switch#show arp traffic

ARP statistics:

   Rcvd: 10 request, 5 response

   Sent: 5 request, 10 response

Chapter 14 DHCP Configuration

14.1 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. Another 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:
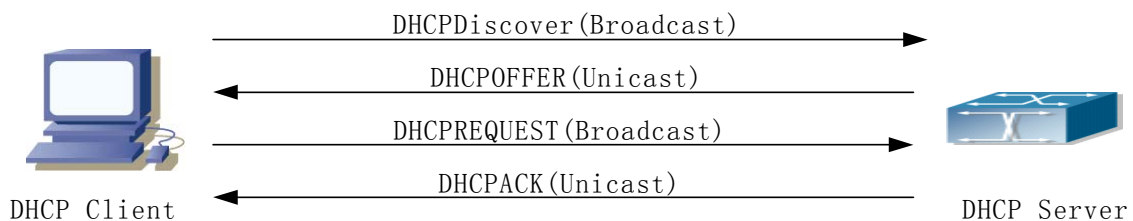
Fig   14-1   DHCP protocol interaction

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.

ES4700 series 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.

14.2 DHCP Server Configuration

14.2.1 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**	Enable 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>*	Configure 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**	Configure the address scope that can be allocated to the address pool
default-router **[**<*address1*>**[**<*address2*>**[**…<*address 8*>**]]]** **no default-router**	Configure default gateway for DHCP clients
dns-server **[**<*address1*>**[**<*address2*>**[**…<*address 8*>**]]]** **no dns-server**	Configure DNS server for DHCP clients
domain-name *<domain>* **no domain-name**	Configure Domain name for DHCP clients; the "**no domain-name**" command deletes the domain name.
netbios-name-server **[**<*address1*>**[**<*address2*>**[**…<*address 8*>**]]]** **no netbios-name-server**	Configure the address for WINS server
netbios-node-type ｛**b-node|h-node|m-node|p-node|**<*type-number*>｝ **no netbios-node-type**	Configure node type for DHCP clients
bootfile *<filename>* **no bootfile**	Configure the file to be imported for DHCP clients on boot up
next-server **[**<*address1*>**[**<*address2*>**[**…<*address 8*>**]]]** **no** **next-server** **[**<*address1*>**[**<*address2*>**[**…<*address 8*>**]]]**	Configure the address of the server hosting file for importing

Command	Explanation
option *<code>* **{ascii** *<string>* **| hex** *<hex>* **| ipaddress** *<ipaddress>***}** **no option** *<code>*	Configure the network parameter specified by the option code
lease **{infinite** **|** **[<days>][<hours>][<minutes>] }** **no lease**	Configure the lease period allocated to addresses in the address pool
ip dhcp excluded-address *<low-address>* **[***<high-address>***]** **no ip dhcp excluded-address** *<low-address>* **[***<high-address>***]**	Exclude 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**	Specify the hardware address when assigning address manually
host *<address>* **[***<mask>*** |** *<prefix-length>* **]** **no host**	Specify the IP address to be assigned to the specified client when binding address manually
client-identifier *<unique-identifier>* **no client-identifier**	Specify the unique ID of the user when binding address manually
client-name *<name>* **no client-name**	Configure 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**	Enable logging for DHCP address to detect address conflicts
Admin Mode	
clear ip dhcp conflict {*<address>***| all}**	Delete a single address conflict record or all conflict records

14.2.2 Commands for DHCP Server Configuration

14.2.2.1 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

14.2.2.2 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

14.2.2.3 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

14.2.2.4 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

14.2.2.5 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

14.2.2.6 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

14.2.2.7 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

14.2.2.8 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

14.2.2.9 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

14.2.2.10 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

14.2.2.11 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 32 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)#

14.2.2.12 ip dhcp conflict ping-detection enable

Command：ip dhcp conflict ping-detection enable

         no ip dhcp conflict ping-detection enable

Function：Enable ping-detection of conflict on DHCP server; the no operation of this command will disable the function.

Parameters：None.

Default：By default, ping-detection of conflict is disabled.

Command Mode：Global Mode.

Usage Guide：To enable Ping-detection of conflict, one should enable the log of conflict addresses, when which is disabled, so will the ping-detection of conflict. When a client is unable to receive Ping request (Echo Request) messages, (when blocked by firewall, for example), this function will check local ARP according to allocated IP: if a designated IP has a corresponding ARP, then an address conflict exists; otherwise, allocate it to the client.

Examples：Enable ping-detection of conflict.

Switch(config)#ip dhcp conflict ping-detection enable

Related Command：ip dhcp conflict logging, ip dhcp ping packets, ip dhcp ping timeout

14.2.2.13 ip dhcp ping packets

Command：ip dhcp ping packets *<request-num>*

         no ip dhcp ping packets

Function: Set the max number of Ping request (Echo Request) message to be sent in Ping-detection of conflict on DHCP server, whose default value is 2; the no operation of this command will restore the default value.

Parameters: *<request-num>* is the number of Ping request message to be sent in Ping-detection of conflict.

Default Settings：No more than 2 Ping request messages will be sent by default.

Command Mode：Global Mode.

Examples：Set the max number of Ping request (Echo Request) message to be sent in Ping-detection of conflict on DHCP server as 3.

Switch(config)#ip dhcp ping packets 3

Related Command：ip dhcp conflict ping-detection enable, ip dhcp ping timeout

14.2.2.14 ip dhcp ping timeout

Command：ip dhcp ping timeout *<timeout-value>*

          no ip dhcp ping timeout

Function: Set the timeout period (in ms) of waiting for a reply message (Echo Request) after each Ping request message (Echo Request) in Ping-detection of conflict on DHCP server, whose default value is 500ms. The no operation of this command will restore the default value.

Parameters: *<timeout-value>* is the timeout period of waiting for a reply message after each Ping request message in Ping-detection of conflict.

Default Settings： the timeout period is 500ms by default.

Command Mode： Global Mode.

Examples： Set the timeout period (in ms) of waiting for each reply message (Echo Request) in Ping-detection of conflict on DHCP server as 600ms.

Switch(config)#ip dhcp conflict timeout 600

Related Command：ip dhcp conflict ping-detection enable, ip dhcp ping packets

14.2.2.15 lease

Command:lease {infinite | [< days > [<hours > [<minutes >]]] }

          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 ES4700 series 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

14.2.2.16 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.

14.2.2.17 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

14.2.2.18 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

14.2.2.19 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

14.2.2.20 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

14.2.2.21 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. ES4700 series can only assign IP address for the DHCP clients and enable DHCP relay when DHCP server function is enabled.

Example: Enable DHCP server.

Switch(config)#service dhcp

14.2.2.22 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

14.2.2.23 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

14.2.2.24 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

14.2.2.25 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

14.3 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.
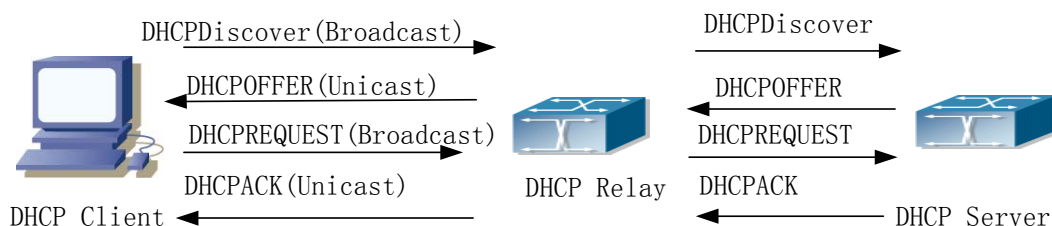
Fig 14-2 DHCP relay

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 DHCPREQUEST packet, DHCP relay forwards the packet to the DHCP server after processing.
4. On receiving DHCPREQUEST, the DHCP server responds with a DHCPACK packet via DHCP relay to the DHCP client.

14.3.1 DHCP Relay Configuration Task List

1. Enable DHCP relay.
2. Configure DHCP relay to forward DHCP broadcast packet.
3. 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.
Port 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. 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.

14.3.2 Commands for DHCP Relay Configuration

14.3.2.1 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: None.

Command mode: Global Mode

Usage Guide: The forwarding destination address is set in the "**ip helper-address**" command and described later.

Example: Setting DHCP packets to be forwarded to 192.168.1.5.

Switch(config)#ip forward-protocol udp boots

Switch(config)#interface vlan 1

Switch(Config-if-Vlan1)#ip helper-address 192.168.1.5

14.3.2.2 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:None.

Command mode: Port 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. 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>**. The combination of "**ip forward-protocol udp <port>**" command and this command should be used for configuration.

14.4 DHCP Configuration Example

Scenario 1:

Too save configuration efforts of network administrators and users, a company is using ES4700 series 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".

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

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.

Scenario 2:
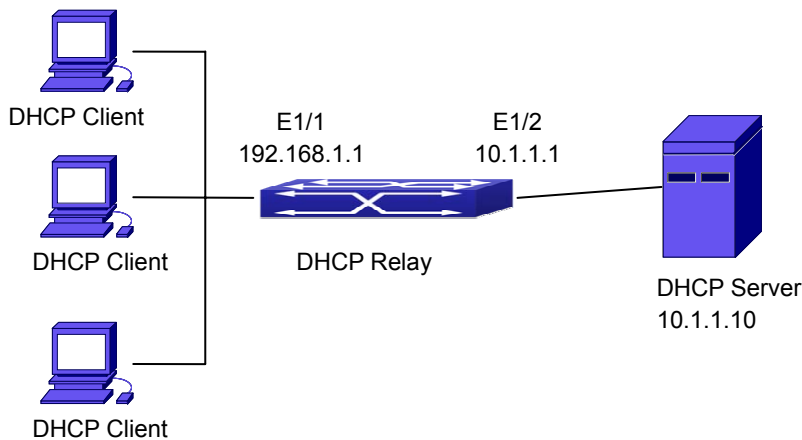
Fig 14-3 DHCP Relay Configuration

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 boots

Switch (config)#interface vlan 1

Switch (Config-if-Vlan1)#ip help-address 10.1.1.10

Switch (Config-if-Vlan1)#exit

Note: 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.

14.5 DHCP Troubleshooting Help

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 ES4700 series 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.

14.5.1 Commands for Monitor and Debug

14.5.1.1 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.

14.5.1.2 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.

14.5.1.3 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

14.6 Web Management

Click DHCP configuration. Users can configure DHCP on the switch.

14.6.1 DHCP server configuration

Click DHCP configuration, DHCP server configuration, The DHCP server configuration page is shown.

14.6.1.1 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; set Logging server port to 45, and then click Apply. The configuration is applied on the switch.

```
Enable DHCP
DHCP server status      Open  ▼
Conflict logging status Open  ▼
```

14.6.1.2 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

14.6.1.3 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)	

14.6.1.4 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)	

14.6.1.5 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)	

14.6.1.6 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; 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)	

14.6.1.7 DHCP network parameter configuration

Click DHCP configuration, DHCP server configuration, DHCP network parameter configuration. Users can specify DHCP network parameters; 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 ▾

14.6.1.8 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; 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.

DHCP manual address pool configuration

DHCP pool name	1 ▾
Hardware address	00-00-e2-3a-26-04
Client IP	10.1.128.160
Client network mask	255.255.255.0
User name(1-255 character)	00-00--e2-3a-26-04
	Add Remove

14.6.1.9 Excluded address

Click DHCP configuration, DHCP server configuration, Manual address pool configuration.Users can configure the exclusive addresses on the DCHP pool.10.1.128.1; 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.

Address allocation

Starting address	Ending address	Operation type
		Add address not for allocating dynamically ▾

14.6.1.10 DHCP packet statistics

Click DHCP configuration, DHCP server configuration, DHCP packet statistics. Users can display DHCP packet statistics.

14.6.1.11 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 forward UDP configuration

Port	69
	Reset Add Remove

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.

DHCP help-address configuration

IP address	192.168.1.5
L3 Interface	Vlan1 ▾
	Reset Add Remove

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.

Configure the relay policy to non-forward

| | Apply | Default |

14.6.2 DHCP debugging

Click DHCP configuration, DHCP debugging. Users can display DHCP debug information.

14.6.2.1 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.

Delete DHCP binding log	
Delete all binding log	⊙ Yes ○ No
IP Address	

14.6.2.2 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.

Delete DHCP conflict log	
Delete all conflict address	⊙ Yes ○ No
IP Address	

14.6.2.3 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.

Delete DHCP server statistics log

14.6.2.4 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
```

14.6.2.5 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 15 DHCPv6 Configuration

15.1 DHCPv6 introduction

DHCPv6 [RFC3315] is the IPv6 version for Dynamic Host Configuration Protocol (DHCP). It is a protocol that assigns IPv6 address as well as other network configuration parameters such as DNS address, and domain name to DHCPv6 client. DHCPv6 is a conditional auto address configuration protocol relative to IPv6. In the conditional address configuration process, DHCPv6 server assigns a complete IPv6 address to client, and provides DNS address, domain name and other configuration information, maybe the DHCPv6 packet can transmit through relay delegation, at last the binding of IPv6 address and client can be recorded by DHCPv6 server, all that can enhance the management of network. DHCPv6 server can also provide non state DHCPv6 service, that is only assigns DNS address and domain name and other configuration information but not assigns IPv6 address, it can solve the bug of IPv6 auto address configuration in non state. DHCPv6 can provide extend function of DHCPv6 prefix delegation, upstream route can assign address prefix to downstream route automatically, that achieve the IPv6 address auto assignment in levels of network environment, and resolved the problem of ISP and IPv6 network dispose.

There are three entites in the DHCPv6 protocol – the client, the relay and the server. The DHCPv6 protocol is based on the UDP protocol. The DHCPv6 client sends request messages to the DHCP server or DHCP relay with the destination port as 547. And the DHCPv6 server and relay send replying messages with the destination port as 546. The DHCPv6 client sends solicit or request messages with the multicast address – ff02::1:2 for DHCP relay and server.
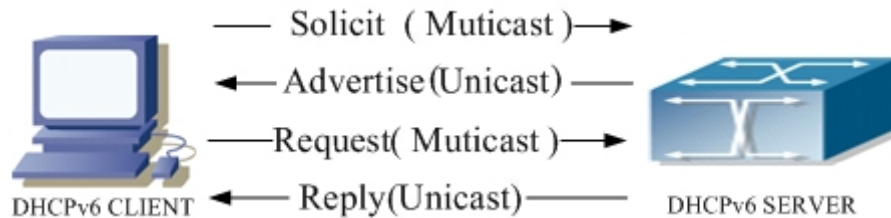
Fig 15-1 DHCPv6 negotiation

When a DHCPv6 client tries to request an IPv6 address and other configurations from the DHCPv6 server. The client has to find the location of the DHCP server, and then request configurations from the DHCP server.

1. In the time of located server, the DHCP client tries to find a DHCPv6 server by broadcasting a SOLICIT packet to all the DHCP delay delegation and server

with broadcast address as FF02::1:2.

2. Any DHCP server which receives the request, wil reply the client with an ADVERTISE message, which includes the identity of the server –DUID, and its priority.

3. It is possible that the client receives multiple ADVERTISE messages. The client should select one and reply it with an REQUEST message to request the address which is advertised in the ADVERTISE message.

4. The selected DHCP server then confirms the client about the IP address and any other configuration with the REPLY message.

The above four steps finish a Dynamic host configuration assignment process. However, if the DHCPv6 server and the DHCPv6 client are not in the same network, the server will not receive the DHCPv6 broadcast packets sent by the client, therefore no DHCPv6 packets will be sent to the client by the server. In this case, a DHCPv6 relay is required to forward such DHCPv6 packets so that the DHCPv6 packets exchange can be completed between the DHCPv6 client and server.

At the time this manual is written, DHCPv6 server, relay and prefix delegation client have been implemented on the switch. When the DHCPv6 relay receives any messages from the DHCP client, it will encapsulate the request in a relay forward packet and deliver it to the next DHCP relay or the DHCP server. The DHCPv6 messages coming from the server will be encapsulated as relay reply packets to the DHCPv6 relay. The relay then removes the encapsulation and deliver it the the DHCPv6 client or the next DHCPv6 relay in the network.

For DHCPv6 prefix delegation where DHCPv6 server is configured on the PE router and DHCPv6 client it configured on the CPE router, the CPE router is able to send address prefix allocation request to the PE router and get a pre-configured address prefix, but not set the adderss prefix manully. The protocol negotiation between the client and the prefix delegation client is quite similar to that when getting an DHCPv6 address. Then the CPE router divides the allocated prefix – whose lengh should be less than 64 characters, into 64 subnets. The divided address prefix will be advertised thourgh routing advertisement messages (RA) to the host directly connected to the client.

15.2 DHCPv6 server configuration

DHCPv6 server configuration task list as below：

1. To enable/disable DHCPv6 service
2. To configure DHCPv6 address pool
    （1） To achieve/delete DHCPv6 address pool
    （2） To configure parameter of DHCPv6 address pool

3. To enable DHCPv6 server function on port

1. To enable/disable DHCPv6 service

Command	Notes
Global Mode	
service dhcpv6 **no service dhcpv6**	To enable DHCPv6 service.

2. To configure DHCPv6 address pool.

（1）To achieve/delete DHCPv6 address pool.

Command	Notes
Global Mode	
ipv6 dhcp pool <*poolname*> **no ipv6 dhcp pool <*poolname*>**	To configure DHCPv6 address pool.

（2）To configure parameter of DHCPv6 address pool.

Command	Notes
DHCPv6 address pool Configuration Mode	
network-address **<*ipv6-pool-start-address*>** **{<*ipv6-pool-end-address*>** | **<*prefix-length*>} [eui-64]** **no network-address**	To configure the range of IPv6 address assignable of address pool.
dns-server <*ipv6-address*> **no dns-server <*ipv6-address*>**	To configure DNS server address for DHCPv6 client.
domain-name <*domain-name*> **no domain-name <*domain-name*>**	To configure DHCPv6 client domain name.
excluded-address <*ipv6-address*> **no excluded-address <*ipv6-address*>**	To exclude IPv6 address which isn't used for dynamic assignment in address pool.
lifetime {<*valid-time*> | infinity} **{<*preferred-time*> | infinity}** **no lifetime**	To configure valid time or preferred time of DHCPv6 address pool.

3. To enable DHCPv6 server function on port.

Command	Notes
Interface Configuration Mode	

ipv6 dhcp server *<poolname>* **[preference** *<value>***] [rapid-commit] [allow-hint]** **no ipv6 dhcp server**	To enable DHCPv6 server function on specified port, and binding the used DHCPv6 address pool.

15.3 DHCPv6 relay delegation configuration

DHCPv6 relay delegation configuration task list as below：

1. To enable/disable DHCPv6 service
2. To configure DHCPv6 relay delegation on port

1.To enable DHCPv6 service.

Command	Notes
Global Mode	
service dhcpv6 **no service dhcpv6**	To enableDHCPv6 service.

2.To configure DHCPv6 relay delegation on port.

Command	Notes
Interface Configuration Mode	
ipv6 dhcp relay destination **{ [***<ipv6-address>***] [interface** **{** *<interface-name>* **| vlan** *<1-4096>* **}] }** **no ipv6 dhcp relay destination** **{ [***<ipv6-address>***] [interface** **{** *<interface-name>* **| vlan** *<1-4096>* **}] }**	To specify the destination address of DHCPv6 relay transmit; The no form of this command delete the configuration.

15.4 DHCPv6 prefix delegation server configuration

DHCPv6 prefix delegation server configuration task list as below:

1. To enable/delete DHCPv6 service
2. To configure prefix delegation pool
3. To configure DHCPv6 address pool
    （1） To achieve/delete DHCPv6 address pool
    （2） To configure prefix delegation pool used by DHCPv6 address pool
    （3） To configure static prefix delegation binding
    （4） To configure other parameter of DHCPv6 address pool

4. To enable DHCPv6 prefix delegation server function on port

1.To enable/delete DHCPv6 service

Command	Notes
Global Mode	
service dhcpv6 **no service dhcpv6**	To enable DHCPv6 service.

2. To configure prefix delegation pool

Command	Notes
Global Mode	
ipv6 local pool *<poolname>* *<prefix/prefix-length>* *<assigned-length>* **no ipv6 local pool** *<poolname>*	To configure prefix delegation pool.

3.To configure DHCPv6 address pool

（1）To achieve/delete DHCPv6 address pool

Command	Notes
Global Mode	
ipv6 dhcp pool *<poolname>* **no ipv6 dhcp pool** *<poolname>*	To configure DHCPv6 address pool.

（2）To configure prefix delegation pool used by DHCPv6 address pool

Command	Notes
DHCPv6 address pool Configuration Mode	
prefix-delegation pool *<poolname>* **[lifetime {***<valid-time>* **|** **infinity}** **{***<preferred-time>* **| infinity}]** **no prefix-delegation pool** *<poolname>*	To specify prefix delegation pool used by DHCPv6 address pool, and assign usable prefix to client.

（3）To configure static prefix delegation binding

Command	Notes
DHCPv6 address pool Configuration Mode	

Command	Notes
prefix-delegation *<ipv6-prefix/prefix-length>* *<client-DUID>* [iaid *<iaid>*] [lifetime {*<valid-time>* | infinity} {*<preferred-time>* | infinity}] **no prefix-delegation** <ipv6-prefix/prefix-length> <client-DUID> [iaid <iaid>]	To specify IPv6 prefix and any prefix required static binding by client.

（4） To configure other parameter of DHCPv6 address pool

Command	Notes
DHCPv6 address pool Configuration Mode	
dns-server *<ipv6-address>* **no dns-server** *<ipv6-address>*	To configure DNS server address for DHCPv6 client.
domain-name *<domain-name>* **no domain-name** *<domain-name>*	To configure domain name for DHCPv6 client.

4. To enable DHCPv6 prefix delegation server function on port

Command	Notes
Interface Configuration Mode	
ipv6 dhcp server *<poolname>* **[preference** *<value>***] [rapid-commit] [allow-hint]** **no ipv6 dhcp server**	To enable DHCPv6 server function on specified port, and binding used DHCPv6 address pool.

15.5 DHCPv6 prefix delegation client configuration

DHCPv6 prefix delegation client configuration task list as below:

1.   To enable/disable DHCPv6 service
2.   To enable DHCPv6 prefix delegation client function on port

1.To enable/disable DHCPv6 service

Command	Notes
Global Mode	
service dhcpv6 **no service dhcpv6**	To enable DHCPv6 service.

2. To enable DHCPv6 prefix delegation client function on port

Command	Notes
Interface Configuration Mode	
ipv6 dhcp client pd *<prefix-name>* **[rapid-commit]** **no ipv6 dhcp client pd**	To enable client prefix delegation request function on specified port, and the prefix obtained associate with universal prefix configured.

15.6 DHCPv6 Configuration Command

15.6.1 clear ipv6 dhcp binding

Command：clear ipv6 dhcp binding [<*ipv6-address*>][pd <*ipv6-prefix/prefix-length*>]

Function: To clear one specified DHCPv6 assigned address or prefix binding record or all the IPv6 address and prefix binding records.

Parameter: *<ipv6-address>* is the specified IPv6 address with binding record; *<ipv6-prefix/prefix-length>* is the specified IPv6 prefix with binding record.To clear all IPv6 address and prefix binding record if there is no specified record.

Command Mode: Admin Mode.

Usage Guide: DHCPv6 IPv6 address and prefix binding information can be displayed through the command **show ipv6 dhcp binding**. If DHCPv6 client doesnot use the DHCPv6 allocated IPv6 address and prefix but when the life time of the IPv6 address doesnot end, the DHCPv6 server will not remove its bind for this address and prefix. In this situation, the address and prefix binding information can be removed manually though this command. And if no parameter is appended, this command will remove all the address and prefix binding information.

Example: To delete all binding record of IPv6 address and prefix.

Switch#clear ip dhcp binding

Relative Command：show ipv6 dhcp binding

15.6.2 clear ipv6 dhcp server statistics

Command：clear ipv6 dhcp server statistics

Function: To delete the statistics of DHCPv6 Server, and reset DHCPv6 server counter.

Parameter: None.

Command Mode: Admin Mode.

Usage Guide: Statistics about the DHCPv6 server can be displayed though the command **show ipv6 dhcp server statistics**. And these statistics can be reset with this command.

Example: To reset DHCPv6 Server counter.

Switch#clear ip dhcp server statistics

Relative Command：show ip dhcp server statistics

15.6.3 debug ipv6 dhcp client

Command：debug ipv6 dhcp client { event | packet }

            no debug ipv6 dhcp client { event | packet }

Function: To enable the debugging messages for protocol packets of DHCPv6 prefix delegation client. The no form of this command will disable the debugging information.

Default: Disabled.

Command Mode: Admin Mode.

Example: To enable the debugging messages.

Switch#debug ipv6 dhcp client packet

15.6.4 debug ipv6 dhcp detail

Command：debug ipv6 dhcp detail

            no debug ipv6 dhcp detail

Function: To display the debug information of all kinds of packets received or sent by DHCPv6, the no form of this command disabled this function.

Default: Disabled.

Command Mode: Admin Mode.

Example:

Switch#debug ipv6 dhcp detail

15.6.5 debug ipv6 dhcp relay packet

Command：debug ipv6 dhcp relay packet

            no debug ipv6 dhcp relay packet

Function: To enable the debugging information for protocol packets of DHCPv6 relay. The no form of this command will disable the debugging.

Default: Disabled.

Command Mode: Admin Mode.

Example:

Switch#debug ipv6 dhcp relay packet

15.6.6 debug ipv6 dhcp server

Command：debug ipv6 dhcp server { event | packet }

          no debug ipv6 dhcp server { event | packet }

Function: To enable the debugging information of DHCPv6 server. The no form of this command will disable the debugging.

Parameter: event is to enable debugging messages for DHCPv6 server events, such as address allocation.packet is for debugging messages of protocol packets of DHCPv6 server.

Default: Disabled.

Command Mode: Admin Mode.

Example:

Switch#debug ipv6 dhcp server packet

15.6.7 dns-server

Command：dns-server *<ipv6-address>*

          no dns-server *<ipv6-address>*

Function: To configure the IPv6 address of the DNS server for DHCPv6 clients. The no form of this command will remove the DNS configuration.

Parameter: *<ipv6-address>* is the IPv6 address of DNS Server.

Default: No configured address pool of DNS Server by default.

Command Mode: DHCPv6 address pool configuration mode.

Usage Guide: For each address pool, at most 3 DNS server can be configured. And the addresses of the DNS server must be valid IPv6 addresses.

Example: To configure the DNS Server address of DHCPv6 client as 2001:da8::1.

Switch(dhcp-1-config)#dns-server 2001:da8::1

15.6.8 domain-name

Command：domain-name *<domain-name>*

          no domain-name *<domain-name>*

Function: To configure domain name of DHCPv6 client; The no form of this command will delete the domain name.

Parameter: *<domain-name>* is the domain name, less than 32 characters.

Command Mode: DHCPv6 address pool configuration mode.

Default: The domain name parameter of address pool is not configured by default.

Usage Guide: At most 3 domain names can be configured for each address pool.

Example: To set the domain name of DHCPv6 client as digitalchina.com.cn.

Switch(dhcp-1-config)#domain-name digitalchina.com.cn

15.6.9 excluded-address

Command：excluded-address *<ipv6-address>*

  no excluded-address *<ipv6-address>*

Function: To configure the specified IPv6 address to be excluded from the address pool. The excluded address will not be allocated to any hosts. The no form of this command will remove the configuration.

Parameter: *<ipv6-address>* is the IPv6 address to be excluded from being allocated to hosts in the address pool.

Default: Disabled

Command Mode: DHCPv6 address pool configuration mode.

Usage Guide: This command is used to preserve the specified address from DHCPv6 address allocation.

Example: To configure to exclude 2001:da8:123::1 from DHCPv6 address allocation.

Switch(config)#excluded-address 2001:da8:123::1

15.6.10 ipv6 address

Command：ipv6 address *<prefix-name> <ipv6-prefix/prefix-length>*

  no ipv6 address *<prefix-name> <ipv6-prefix/prefix-length>*

Function: To configure the specified interface to use prefix delegation for address allocation. The no form of this command will disable the using of prefix delegation for address allocation.

Parameters: <prefix-name> is a string with its length no more than 32, designating the name of the address prefix defined in the prefix pool. **<ipv6-prefix/prefix-length>** is latter part of the IPv6 address excluding the address   prefix, as well as its length.

Command Mode: Interface Configuration Mode.

Default: No global address is configured for interfaces by default.

Usage Guide: The IPv6 address of an interface falls into two parts: **<prefix-name>** and **<ipv6-prefix>/<prefix-lengh>** . If routing advertisement has been enabled, the first 64 bits of the addresses will be advertised. The address generated by **<prefix-name>** and **<ipv6-prefix/prefix-length>** combination will be removed, and the advertising of the

prefix will be disabled. Only one **<ipv6-prefix/prefix-length>** can be configured for one prefix name.

Example: If the prefix name my-prefix designates 2001:da8:221::/48, then the following command will add the address 2001:da8:221:2008::2008 to interface vlan 1.

Switch(Config-if-Vlan1)#ipv6 address my-prefix 0:0:0:2008::2008/64

15.6.11 ipv6 dhcp client pd

Command：ipv6 dhcp client pd *<prefix-name>* **[rapid-commit]**

        no ipv6 dhcp client pd

Function: To configure DHCPv6 prefix delegation client for the specified interface. The no form of this command will disable the DHCPv6 prefix delegation client and remove the allocated address prefix.

Parameters: <prefix-name> is the string with its length no more than 32, which designates the name of the address prefix. **rapid-commit** is an optional parameter. If configured, and the prefix proxy also enables rapid-commmit, the prefix delegation server will reply the prefix delegation client with the REPLY message directly. And the prefix delegation request will be accomplished by exchanging messages once.

Command Mode: Interface Configuration Mode.

Default: DHCPv6 prefix delegation client is not enabled by default.

Usage Guide: This command is used to configure the prefix delegation client on the specified interface. An interface with prefix delegation client enabled will send SOLICIT packets to try to get address prefix from the server. If the prefix is retrieved correctly, the address prefix in the global address pool can be used by the **ipv6 address** command to generate a valid IPv6 address. This command is exclusive with **ipv6 dhcp server** and **ipv6 dhcp relay destination.** If the prefix delegation client is disabled for an interface, then the address prefix which is get from this interface through prefix delegation client, will be removed from the global address pool. Also the interface addresses which is generated by the prefix delegation client will be removed , and routing advertisement with the prefix will be disabled. If any general prefix has been configured by the ipv6 general-prefix command, the same prefix learnt from prefix delegation will be disgarded.

Example:

Switch(vlan-1-config)#ipv6 dhcp client pd ClientA rapid-commit

15.6.12 ipv6 dhcp client pd hint

Command：ipv6 dhcp client pd hint *<prefix|prefix-length>*

no ipv6 dhcp client pd hint *<prefix|prefix-length>*

Function：Designate the prefix demanded by the client and its length. The no operation of this command will delete that prefix and its length from the specified interface.

Parameters：<prefix|prefix-length> means the prefix demanded by the client and its length.

Command Mode：Interface Configure Mode.

Default Settings：There is no such configuration in the system by default.

Usage Guide：The system designates a prefix and its length on the interface for a client. If client prefix-proxy demanding function is enabled on the interface and hint function is enabled on the switch, the user will have prior claim to the prefix it demands and the prefix length when the server allocates them. Only one hint prefix is allowed in the system.

Examples：

Switch(vlan-1-config)#ipv6 dhcp client pd hint 2001::/48

15.6.13 ipv6 dhcp pool

Command：**ipv6 dhcp pool** *<poolname>*

no ipv6 dhcp pool *<poolname>*

Function: To configure the address pool for DHCPv6, and enter the DHCPv6 address pool configuration mode. In this mode, information such as the address prefix to be allocated, the DNS server addresses, and domain names, can be configured for the DHCPv6 client. The no form of this command will remove the configuration of the address pool.

Parameter: *<poolname>* is the address pool name of DHCPv6 with its length no more than 32.

Default: Any DHCPv6 address pool are not configured by default.

Command Mode: Global Mode.

Usage Guide: This command should be launched in global configuration mode, and falls in DHCPv6 address pool configuration mode if launched successfully. To remove a configured address pool, interface bindings related to the address pool, as well as the related address bindings will be removed.

Example: To define an address pool, named 1.

Switch(config)#ipv6 dhcp pool 1

Switch(dhcp-1-config)#

15.6.14 ipv6 dhcp relay destination

Command ：ipv6 dhcp relay destination { [*<ipv6-address>*] [interface { *<interface-name>* | vlan *<1-4096>* }] }

no ipv6 dhcp relay destination { [*<ipv6-address>*] [interface { *<interface-name>* | vlan *<1-4096>* }] }

Function: To configure the destination to which the DHCPv6 relay forwards the DHCPv6 requests from the clients. The destination should be the address of an external DHCPv6 relay or the DHCPv6 server. The no form of this command will remove the configuration.

Parameters: <ipv6-address> is the address of the destination to which the DHCPv6 relay forwards. **<interface-name>** or **vlan** is the interface name or vlan id which is used for forwarding of DHCPv6 requests. **<interface-name>** should be a lay 3 vlan name. And the vlan id is limited between 1 and 4096. If **<ipv6-addess>** is a global unicast address, the **interface** parameter should not be configured. If **<ipv6-address>** is an local address, the **interface** parameter is required be configured. The destination address for the DHCPv6 server will be the multicast address of ALL_DHCP_Servers – FF05::1:3, if the interface parameter is configured only.

Command Mode: Interface Configuration Mode.

Default: By default, destination address for DHCPv6 relay is not configured.

Usage Guide: This command is used to configure the DHCPv6 relay for the specified interface. The address should be the address of another DHCPv6 relay or the address DHCPv6 server. At most 3 relay addresses can be configured for an interface. To be mentioned, the DHCPv6 relay stops working only if all the relay destination address configurations have been removed.

Example:

Switch(vlan-1-config)#ipv6 dhcp relay destination 2001:da8::1

15.6.15 ipv6 dhcp server

Command：ipv6 dhcp server *<poolname>* [preference *<value>*] [rapid-commit] [allow-hint]

no ipv6 dhcp server

Function: This command configures the address pool which will be allocated by the DHCPv6 server through the specified interface. The no form of this command will remove the address pool configuration.

Parameters: <poolname> is a string with its length less than 32, which designates the name of the address pool which is associated with the specified interface. If the **rapid-commit** option has been specified, the DHCPv6 server send a REPLY packet to the client immediately after receiving the SOLICIT packet. If the **preference** option has been specified, **<value>** will be the priority of the DHCPv6 server, with its value allowed

between 0 and 255, and with 0 by defaut. The bigger the preference value is, the higher the priority of the DHCPv6 server. If the **allow-hint** option has been specified, the client expected value of parameters will be appended in its request packets.

Command Mode: Interface Configuration Mode.

Default: DHCPv6 address pool based on port is not configured by default.

Usage Guide: This command configure the DHCPv6 address pool which is applied by the DHCPv6 server for the specified interface, as well as optional parameters.

Example:

Switch(vlan-1-config)#ipv6 dhcp server PoolA preference 80 rapid-commit allow-hint

15.6.16 ipv6 general-prefix

Command：ipv6 general-prefix *<prefix-name> <ipv6-prefix/prefix-length>*

no ipv6 general-prefix *<prefix-name>*

Function: To define an IPv6 general prefix. The no form of this command will delete the configuration.

Parameter: *<prefix-name>* is a character string less than 32 characters, to used as IPv6 general prefix name. *<ipv6-prefix/prefix-length>* is defined as IPv6 general prefix.**Command Mode:** Global Mode.

Default: IPv6 general prefix is not configured by default.

Usage Guide: If IPv6 general prefix is configured, the interface will use the configured prefix for IPv6 address generating. Commonly, the general prefix is used for enterprise IPv6 prefix. And when entering an IPv6 address, users can simply add the address suffix of to the name of the general prefix. The configured address prefix will be reserved in the general address prefix pool. At most 8 general prefix can be configured at the same time. When trying to remove a configured general prefix name, the operation will fail if any interfaces used the configured prefix. Only one general prefix for an prefix name. The general prefix can not use the same prefix definition with prefixes learnt from prefix delegation.

Example: To set the prefix of 2001:da8:221::/48 to general prefix my-prefix.

Switch(config)#ipv6 general-prefix my-prefix 2001:da8:221::/48

15.6.17 ipv6 local pool

Command：ipv6 local pool *<poolname> <prefix/prefix-length> <assigned-length>*

no ipv6 local pool *<poolname>*

Function: To configure the address pool for prefix delegation. The no form of this command will remove the IPv6 prefix delegation configuration.

Parameters: <poolname> is the name for the IPv6 address pool of the prefix delegation. The length name string should be less than 32. **<prefix/prefix-length>** is the address prefix and its length of the prefix delegation. **<assigned-length>** is the length of the prefix in the address pool which can be retrieved by the clients. The assigned prefix length should be no less than the value of **<prefix-lengh>**.

Command Mode: Global Mode.

Default: No IPv6 prefix delegation address pool is configured by default.

Usage Guide: This command should be used with the **prefix delegation pool** command to allocate address prefixes to the clients. If IPv6 prefix delegation is removed, the associated **prefix delegation** command will be in-effective either.

15.6.18 lifetime

Command：lifetime {<*valid-time*> | infinity} {<*preferred-time*> | infinity}

          no lifetime

Function: To configure the life time for the addresses or the address prefixes allocated by DHCPv6. The no form of this command will restoer the default setting.

Parameters: <valid-time> and <preferred-time> are the valid life time and preferred life time respectively for the allocated IPv6 addresses in the local address pool. Its value is allowed to be between 1 and 31536000 in seconds. And **<preferred-time>** should never be bigger than **<valid-time>.** The **infinity** parameter means the life time is infinity.

Command Mode: DHCPv6 address pool configuration mode.

Default: The default valid life time and preferred life time are 2592000 seconds(30 days) and 604800 seconds(7 days) respectively.

Example: To configure the valid life time as 1000 seconds, and the preferred life time as 600 seconds.

Switch(config)#lifetime 1000 600

15.6.19 network-address

Command：network-address <*ipv6-pool-start-address*> {<*ipv6-pool-end-address*> | <*prefix-length*>} [eui-64]

          no network-address

Function: To configure the DHCPv6 address pool. The no form of this command will remove the address pool configuration.

Parameters: <ipv6-pool-start-adderss> is the start of the adderss pool. **<ipv6-pool-end-address>** is the end of the addresss pool. **<prefix-length>** is the length of the address prefix, which is allowed to be between 3 and 128, and 64 by default. The

size of the pool will be determined by **<prefix-length>** if it has been specified. **<ipv6-pool-end-address>** and **<prefix-length>** alternative options to determine the size of the IPv6 addresss pool. If **<prefix-length>** is 64 and the **eui-64** option has been configured, the DHCPv6 server will allocate IPv6 addresses according to the EUI-64 standard. Or the DHCPv6 server will be allocating addresses sequentially.

Default: No address pool is configured by default.

Command Mode: DHCPv6 address pool configuration mode.

Usage Guide: This command configures the address pool for the DHCPv6 server to allocate addresses. Only one address range can be configured for each address pool. To be noticed, if the DHCPv6 server has been enabled, and the length of the IPv6 address prefix has been configured, the length of the prefix in the address pool should be no less than the length of the prefix of the IPv6 address of the respective layer 3 interface in the switch.

Example: To configure the address range for address poo 1 as 2001:da8:123::100-2001:da8:123::200.

Switch(dhcp-1-config)#network-address 2001:da8:123::100 2001:da8:123::200

Relative Command：excluded-address

15.6.20 prefix-delegation

Command: prefix-delegation *<ipv6-prefix/prefix-length> <client-DUID>* [iaid *<iaid>*] [lifetime {*<valid-time>* | infinity} {*<preferred-time>* | infinity}]

 no prefix-delegation *<ipv6-prefix/prefix-length> <client-DUID>* [iaid *<iaid>*]

Function: To configure dedicated prefix delegation for the specified user. The no form of this command will remove the dedicated prefix delegation.

Parameters: ***<ipv6-prefix/prefix-length>*** is the length of the prefix to be allocated to the client. ***<client-DUID>*** is the DUID of the client. DUID with the type of DUID-LLT and DUID-LL are supported, the DUID of DUID-LLT type should be of 14 characters. ***<iaid>*** is the value to be appended in the IA_PD field of the clients' requests. ***<valid-time>*** and ***<preferred-time>*** are the valid life time and the preferred life time of the IPv6 address allocated to the clients respectively, in seconds, and its value is allowed between 1 and 31536000. However, ***<preferred-time>*** should never be bigger than ***<valid-time>***. If not configured, the default ***<valid-time>*** will be 2592000, while ***<preferred-time>*** will be 604800. The **infinity** parameter means the life time is infinity.

Command Mode: DHCPv6 address pool configuration mode.

Default: Disabled

Usage Guide: This command configures the specified IPv6 address prefix to bind with

the specified client. If no IAID is configured, any IA of any clients will be able get this address prefix. At most eight static binding address prefix can be configured for each address pool. For prefix delegation, static binding is of higher priority than the prefix address pool.

Example: The following command will allocate 2001:da8::/48 to the client with DUID as 0001000600000005000BBFAA2408, and IAID as 12.

Switch(dhcp-1-config)#prefix-delegation   2001:da8::/48
0001000600000005000BBFAA2408 iaid 12

15.6.21 prefix-delegation pool

Command: prefix-delegation pool *<poolname>* [lifetime{*<valid-time>* | infinity}{*<preferred-time>* | infinity}]

              no prefix-delegation pool *<poolname>*

Function: To configure prefix delegation name used by DHCPv6 address pool. The no form of this commands delete the configuration.

Parameters: *<poolname>* is the name of the address prefix pool, the length name string should be less than 32. *<valid-time>* and *<preferred-time>* are the valid life time and the preferred life time of the IPv6 address allocated to the clients respectively, in seconds, and its value is allowed between 1 and 31536000. However, *<preferred-time>* should never be bigger than *<valid-time>*. If not configured, the default *<valid-time>* will be 2592000, while *<preferred-time>* will be 604800. The **infinity** parameter means the life time is infinity.

Command Mode: DHCPv6 address pool configuration mode.

Default: The prefix delegation name used by DHCPv6 address pool is not configured.

Usage Guide: This command configures the name of the address prefix pool for address allocation. If configured, the addresses in the prefix address pool will be allocated to the clients. This command can be used in association with the **ipv6 local pool** command. For one address pool, only one prefix delegation pool can be bound. When trying to remove the prefix name configuration, the prefix delegation service of the server will be unavailable, if both the address pool is not associated with the prefix delegation pool and no static prefix delegation binding is enabled.

Example:

Switch(dhcp-1-config)#prefix-delegation pool abc

15.6.22 service dhcpv6

Command：service dhcpv6

no service dhcpv6

Function: To enable DHCPv6 server function; the no form of this command disables the configuration.

Parameter: None.

Default: Disabled.

Command Mode: Global Mode.

Usage Guide: The DHCPv6 services include DHCPv6 server function, DHCPv6 relay function, DHCPv6 prefix delegation function. All of the above services are configured on ports. Only when DHCPv6 server function is enabled, the IP address assignment of DHCPv6 client, DHCPv6 relay and DHCPv6 prefix delegation functions enabled can be configured on ports.

Example: To enable DHCPv6 server.

Switch(config)#service dhcpv6

15.6.23 show ipv6 dhcp

Command：show ipv6 dhcp

Function: To show the enable switch and DUID of DHCPv6 service.

Command Mode: Admin Mode.

Usage Guide: To show the enable switch and DUID of DHCPv6 service, this command only can support the DUID type of DUID-LLT. The DUID types are the same not only displayed but also required in client and server identifier options.

Example:

Switch#show ipv6 dhcp

DHCPv6 is enabled

DUID is <000100060000000500030f112233>

15.6.24 show ipv6 dhcp binding

Command：show ip dhcp binding [<*ipv6-address*> | pd <*ipv6-prefix/prefix-length*> | count]

Function: To show all the address and prefix binding information of DHCPv6.

Parameter: <*ipv6-address*> is the specified IPv6 address; count show the number of DHCPv6 address bindings. <*ipv6-prefix/prefix-length*> is the length of the prefix to be allocated to the client.

Command Mode: Admin Mode.

Usage Guide: To show all the address and prefix binding information of DHCPv6, include type, DUID, IAID, prefix, valid time and so on.

Example:

Switch#show ipv6 dhcp binding

Client: iatype IANA, iaid 0x0e001d92

DUID: 00:01:00:01:0f:55:82:4f:00:19:e0:3f:d1:83

IANA leased address: 2001:da8::10

Preferred lifetime 604800 seconds, valid lifetime 2592000 seconds

Lease obtained at %Jan 01 01:34:44 1970

Lease expires at %Jan 31 01:34:44 1970   (2592000 seconds left)

The number of DHCPv6 bindings is 1

15.6.25 show ipv6 dhcp interface

Command：show ipv6 dhcp interface [<*interface-name*>]

Function: To show the information for DHCPv6 interface.

Parameter: *<interface-name>* is the name and number of interface, if the*<interface-name>* parameter is not provided, then all the DHCPv6 interface information will be shown.

Command Mode: Admin Mode.

Usage Guide: To show the   information for DHCPv6 interface, include port mode (Prefix delegation client、DHCPv6 server、DHCPv6 relay)，and the relative conformation information under all kinds of mode.

Example:

Switch#show ipv6 dhcp interface vlan10

Vlan10 is in server mode

Using pool: poolv6

Preference value: 20

Rapid-Commit is disabled

Switch#show ipv6 dhcp interface vlan10

Vlan10 is in relay mode

Relay destination is <2001::1>

15.6.26 show ipv6 dhcp local pool

Command：show ipv6 dhcp local pool

Function: To show the statistic information of DHCPv6 prefix pool.

Command Mode: Admin Mode.

Usage Guide: To show the statistic information of DHCPv6 prefix pool, include the name

of prefix pool, the prefix and prefix length as well as assigned prefix length, the number of assigned prefix and information in DHCPv6 address pool.

Example:

Switch#show ipv6 dhcp pool binding

15.6.27 show ipv6 dhcp pool

Command：show ipv6 dhcp pool [<*poolname*>]

Function: To show the DHCPv6 address pool information.

Parameter: <*poolname*> is the DHCPv6 address pool name which configured already, and the length less than 32 chatacters.If the **<*poolname*>** parameter is not provided, then all the DHCPv6 address pool information will be shown.

Command Mode: Admin Mode.

Usage Guide: To display the configuration and dynamic assignment information for DHCPv6 address pool, include the name of DHCPv6 address pool, the prefix of DHCPv6 address pool, excluded address, DNS server configuration, relative prefix information and so on. To display assigned address binding number of address pool that is used as address assignment server. To display assigned prefix number of address pool that is used as prefix delegation server.

Example:

Switch#show ipv6 dhcp pool poolv6

15.6.28 show ipv6 dhcp statistics

Command：show ipv6 dhcp statistics

Function: To show the statistic of all kinds of DHCPv6 packets by DHCPv6 server.

Command Mode: Admin Mode.

Example:

Switch#show ipv6 dhcp server statistics

Address pools   1

Active bindings   0

Expiried bindings   0

Malformed message   0

Message   Recieved

DHCP6SOLICIT   0

DHCP6ADVERTISE   0

DHCP6REQUEST   0

DHCP6REPLY   0
DHCP6RENEW   0
DHCP6REBIND   0
DHCP6RELEASE   0
DHCP6DECLINE   0
DHCP6CONFIRM   0
DHCP6RECONFIGURE   0
DHCP6INFORMREQ   0
DHCP6RELAYFORW   0
DHCP6RELAYREPLY   0

Message   Send
DHCP6SOLICIT   0
DHCP6ADVERTISE   0
DHCP6REQUEST   0
DHCP6REPLY   0
DHCP6RENEW   0
DHCP6REBIND   0
DHCP6RELEASE   0
DHCP6DECLINE   0
DHCP6CONFIRM   0
DHCP6RECONFIGURE   0
DHCP6INFORMREQ   0
DHCP6RELAYFORW   0
DHCP6RELAYREPLY   0

Show information	Notes
Address pools	To configure the number of DHCPv6 address pools.
Active bindings	The number of auto assign addresses.
Expiried bindings	The number of expired bindings.
Malformed message	The number of malformed messages.
Message Recieved	The statistic of received DHCPv6 packets.
DHCP6SOLICIT	The number of DHCPv6 SOLICIT packets.
DHCP6ADVERTISE	The number of DHCPv6 ADVERTISE packets.
DHCPv6REQUEST	The number of DHCPv6 REQUEST packets.

DHCP6REPLY	The number of DHCPv6 REPLY packets.
DHCP6RENEW	The number of DHCPv6 RENEW packets.
DHCP6REBIND	The number of DHCPv6 REBIND packets.
DHCP6RELEASE	The number of DHCPv6 RELEASE packets.
DHCP6DECLINE	The number of DHCPv6 DECLINE packets.
DHCP6CONFIRM	The number of DHCPv6 CONFIRM packets.
DHCP6RECONFIGURE	The number of DHCPv6 RECONFIGURE packets.
DHCP6INFORMREQ	The number of DHCPv6 INFORMREQ packets.
DHCP6RELAYFORW	The number of DHCPv6 RELAYFORW packets.
DHCP6RELAYREPLY	The number of DHCPv6 RELAYREPLY packets.
Message Send	The statistic of sending DHCPv6 packets
DHCP6SOLICIT	The number of DHCPv6 SOLICIT packets.
DHCP6ADVERTISE	The number of DHCPv6 ADVERTISE packets.
DHCPv6REQUEST	The number of DHCPv6 REQUEST packets.
DHCP6REPLY	The number of DHCPv6 REPLY packets.
DHCP6RENEW	The number of DHCPv6 RENEW packets.
DHCP6REBIND	The number of DHCPv6 REBIND packets.
DHCP6RELEASE	The number of DHCPv6 RELEASE packets.
DHCP6DECLINE	The number of DHCPv6 DECLINE packets.
DHCP6CONFIRM	The number of DHCPv6 CONFIRM packets.
DHCP6RECONFIGURE	The number of DHCPv6 RECONFIGURE packets.
DHCP6INFORMREQ	The number of DHCPv6 INFORMREQ packets.
DHCP6RELAYFORW	The number of DHCPv6 RELAYFORW packets.

15.6.29 show ipv6 general-prefix

Command：show ipv6 general-prefix

Function: To show the IPv6 general prefix pool information.

Command Mode: Admin Mode.

Usage Guide: To show the IPv6 general prefix pool information, include the prefix number in general prefix pool, the name of every prefix, the interface of prefix obtained, and the prefix value.

Example:

Switch#show ipv6 general-prefix

15.7 Examples of DHCPv6 Configuration

Example1：

When deploying IPv6 networking, switches can be configured as DHCPv6 server in order to manage the allocation of IPv6 addresses. Both the stateful and the stateless DHCPv6 is supported.

Topology:

The access layer use SWITCH1 switch to connect users of dormitory buildings; Switch2 is configured as DHCPv6 relay delegation in primary aggregation layer; Switch3 is configured as DHCP server in secondary aggregation layer, and connected with backbone network or higher aggregation layers; The Windows Vista which be provided with DHCPv6 client must load on PC.
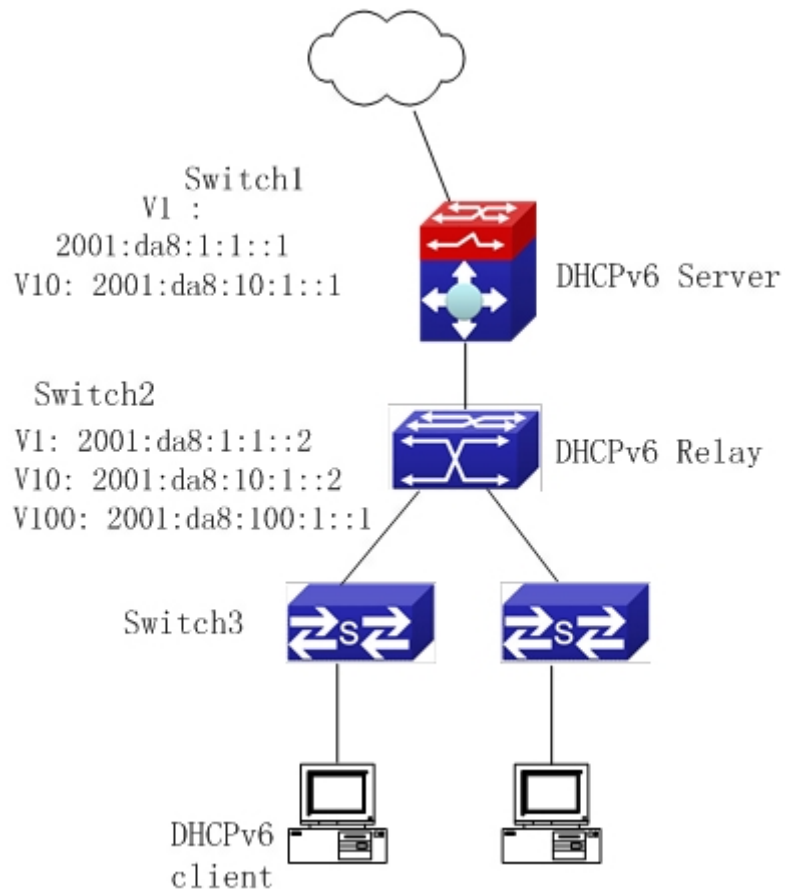
Usage guide:

Switch3 configuration：

Switch3>enable

Switch3#config

Switch3(config)#ipv6 enable

Switch3(config)#service dhcpv6

Switch3(config)#ipv6 dhcp pool EastDormPool

Switch3(dhcpv6-EastDormPool-config)#network-address 2001:da8:100:1::1 2001:da8:100:1::100

Switch3(dhcpv6-EastDormPool-config)#excluded-address 2001:da8:100:1::1

Switch3(dhcpv6-EastDormPool-config)#dns-server 2001:da8::20

Switch3(dhcpv6-EastDormPool-config)#dns-server 2001:da8::21

Switch3(dhcpv6-EastDormPool-config)#domain-name dhcpv6.com

Switch3(dhcpv6-EastDormPool-config)#lifetime 1000 600

Switch3(dhcpv6-EastDormPool-config)#exit

Switch3(config)#interface vlan 1

Switch3(Config-if-Vlan1)#ipv6 address 2001:da8:1:1::1/64

Switch3(Config-if-Vlan1)#exit

Switch3(config)#interface vlan 10

Switch3(Config-if-Vlan10)#ipv6 address 2001:da8:10:1::1/64

Switch3(Config-if-Vlan10)#ipv6 dhcp server EastDormPool preference 80

Switch3(Config-if-Vlan10)#exit

Switch3(config)#

Switch2 configuration：

Switch2>enable

Switch2#config

Switch2(config)#ipv6 enable

Switch2(config)#service dhcpv6

Switch2(config)#interface vlan 1

Switch2(Config-if-Vlan1)#ipv6 address 2001:da8:1:1::2/64

Switch2(Config-if-Vlan1)#exit

Switch2(config)#interface vlan 10

Switch2(Config-if-Vlan10)#ipv6 address 2001:da8:10:1::2/64

Switch2(Config-if-Vlan10)#exit

Switch2(config)#interface vlan 100

Switch2(Config-if-Vlan100)#ipv6 address 2001:da8:100:1::1/64

Switch2(Config-if-Vlan100)#no ipv6 nd suppress-ra

Switch2(Config-if-Vlan100)#ipv6 nd managed-config-flag

Switch2(Config-if-Vlan100)#ipv6 nd other-config-flag

Switch2(Config-if-Vlan100)#ipv6 dhcp relay destination 2001:da8:10:1::1

Switch2(Config-if-Vlan100)#exit

Switch2(config)#

Example2：

When the network operator is deploying IPv6 networks, network automatical configuration can be achieved through the prefix delegation allocation of IPv6 addresses, in stead of configuring manually for each switch.

1. To configure the switching or routing device which is connected to the client switch as DHCPv6 prefix delegation server. That is to setup a local database for the relationship between the allocated prefix and the DUID of the client switch.

2. To configure the switch as the prefix delegation client, and make the client switch to get IPv6 address prefix from the prefix delegation server, through a process which is much like the process of DHCPv6 address allocation.

3. The edge devices which receive the address prefix, send routing advertisement - RA messages, to the client hosts about the address prefix thourgh the interface which is connected to the hosts. Then the hosts get an valid IPv6 address through stateless auto configuration, while at the same time, the sateless DHCPv6 server will be configured for the interface, in order to provide

the DHCPv6 client with information such as DNS, and domain name, etc.

Network Topology:

The edge switch is Switch2. The interface connected to the trunk switch which is Switch1, is configured as the prefix delegation client. The interfaces connected to hosts, are configured as stateless DHCPv6 servers to provide the hosts with stateless information such as DNS and domain names. Also routing advertisement of stateless address allocation is enabled for the host interfaces. On Switch1, the prefix delegation server is configured, and routing advertisement of stateful adderss allocation is enabled. On the host side, DHCPv6 client capable operating system such Windows Vista should be installed.
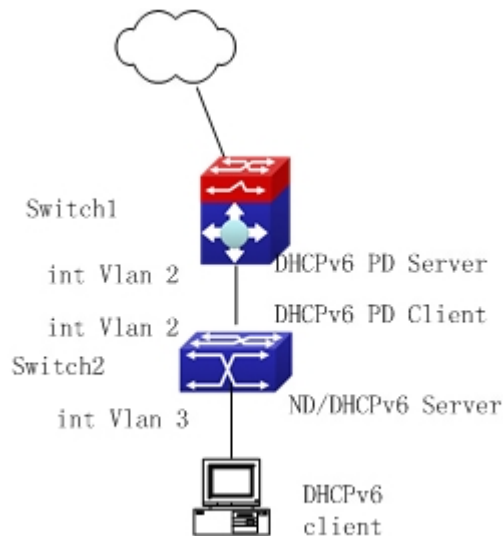
Usage guide:

Switch1 configuration

Switch1>enable

Switch1#config

Switch1(config)#ipv6 enable

Switch1(config)#interface vlan 2

Switch1(Config-if-Vlan2)#ipv6 address 2001:da8:1100::1/64

Switch1(Config-if-Vlan2)#exit

Switch1(config)#service dhcpv6

Switch1(config)#ipv6 local pool client-prefix-pool 2001:da8:1800::/40 48

Switch1(config)#ipv6 dhcp pool dhcp-pool

Switch1(dhcpv6-dhcp-pool-config)#prefix-delegation pool client-prefix-pool 1800 600

Switch1(dhcpv6-dhcp-pool-config)#exit

Switch1(config)#interface vlan 2

Switch1(Config-if-Vlan2)#ipv6 dhcp server dhcp-pool

Switch1(Config-if-Vlan2)#exit

Switch2 configuration

Switch2>enable

Switch2#config

Switch2(config)#ipv6 enable

Switch2(config)#service dhcpv6

Switch2(config)#interface vlan 2

Switch2(Config-if-Vlan2)#ipv6 dhcp client pd prefix-from-provider

Switch2(Config-if-Vlan2)#exit

Switch2(config)#interface vlan 3

Switch2(Config-if-Vlan3)#ipv6 address prefix-from-provider 0:0:0:1::1/64

Switch2(Config-if-Vlan3)#exit

Switch2(config)#ipv6 dhcp pool foo

Switch2(dhcpv6-foo-config)#dns-server 2001:4::1

Switch2(dhcpv6-foo-config)#domain-name edge-core.com

Switch2(dhcpv6-foo-config)#exit

Switch2(config)#interface vlan 3

Switch2(Config-if-Vlan3)#ipv6 dhcp server foo

Switch2(Config-if-Vlan3)#ipv6 nd other-config-flag

Switch2(Config-if-Vlan3)#no ipv6 nd suppress-ra

Switch2(Config-if-Vlan3)#exit

Switch2#

15.8 DHCPv6 Troubleshooting

If the DHCPv6 clients cannot obtain IPv6 addresses and other network parameters, the following procedures can be followed when DHCPv6 client hardware and cables have been verified ok.

☞ Verify the DHCPv6 server is running, start the related DHCP v6 server function if not running.

☞ If the DHCPv6 clients and servers are not in the same physical network, verify the router responsible for DHCPv6 packet forwarding has DHCPv6 relay function. If DHCPv6 relay is not available for the intermediate router, it is recommended to replace the router or upgrade its software to one that has a DHCPv6 relay function.

☞ Sometimes hosts are connected to the DHCPv6 enabled switches, but can not get IPv6 addresses. In this situation, it should be checked first whether the ports which the hosts are connected to, are connected with the port which the DHCPv6 server is connected to. If connected directly, it should be checked then whether the IPv6 address pool of the VLAN which the port belongs to, is in the same subnet with the address pool configure in the DHCPv6 server. If not connected directly, and any

layer 3 DHCPv6 relay is configured between the hosts and the DHCPv6 server, it should be checked first whether an valid IPv6 address has been configured for the switch interface which the hosts are connected to. If not configured, configure an valid IPv6 address. If configured, it should be checked whether the configured IPv6 address is in the same subnet with the DHCPv6 server. If not, please add it to the address pool.

Chapter 16 DHCP option 82 Configuration

16.1 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.

16.1.1 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    Len      Agent Information Field
+------+------+------+------+------+------+--...-+------+
|  82  |   N  |  i1  |  i2  |  i3  |  i4  |      |  iN  |
+------+------+------+------+------+------+--...-+------+
```

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.

16.1.2 option 82 Working Mechanism
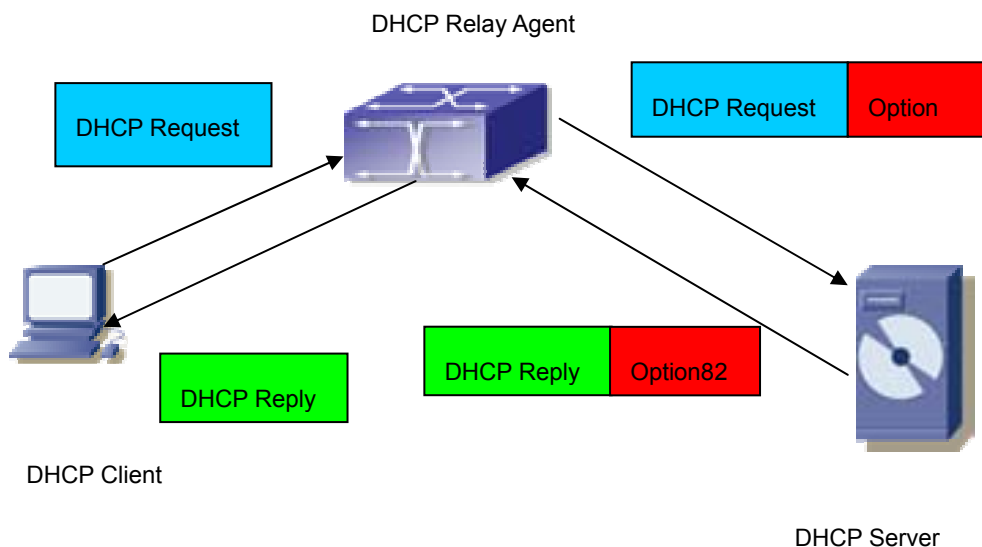
Fig 16-1 DHCP option 82 flow chart

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.

16.2 DHCP option 82 Configuration

16.2.1 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.

16.2.2 Command for DHCP option 82

16.2.2.1 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

16.2.2.2 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 DHCP 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

16.2.2.3 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

16.2.2.4 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

16.2.2.5 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

16.2.2.6 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

16.3 DHCP option 82 Application Examples
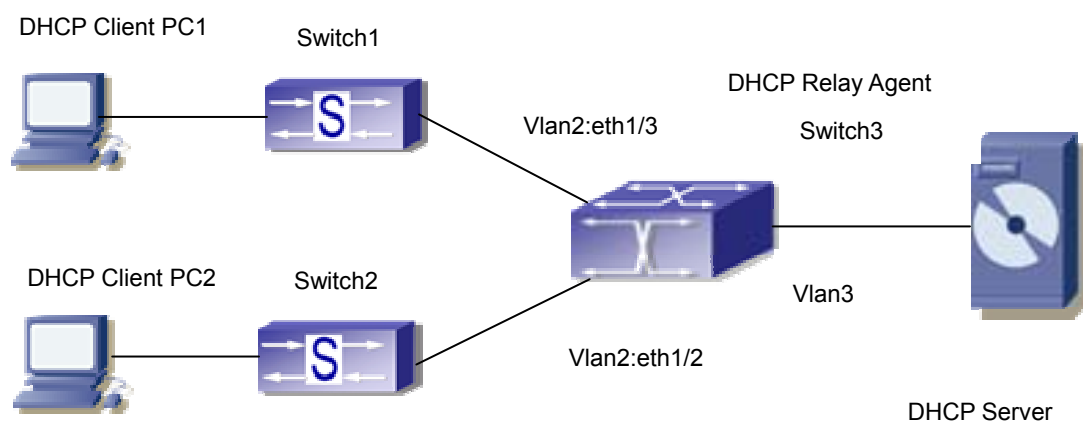
Fig 16-2 a DHCP option 82 typical application example

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.

16.4 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 17 DHCP snooping Configuration

17.1 Introduction to DHCP Snooping

DHCP Snooping means that the switch monitors the IP-getting process of DHCP CLIENT via DHCP protocol. It prevents DHCP attacks and illegal DHCP SERVER by setting trust ports and untrust ports. And the DHCP messages from trust ports can be forwarded without being verified. In typical settings, trust ports are used to connect DHCP SERVER or DHCP RELAY proxy, and untrust ports are used to connect DHCP CLINET. The switch will forward the DHCP request messages from untrust ports, but not DHCP reply ones. If any DHCP reply messages is received from a untrust port, besides giving an alarm, the switch will also implement designated actions on the port according to settings, such as "shutdown", or distributing a "blackhole". If DHCP Snooping binding is enabled, the switch will save binding information (including its MAC address, IP address, IP lease, VLAN number and port number) of each DHCP CLINET on untrust ports in DHCP snooping binding table With such information, DHCP Snooping can combine modules like dot1x and arp, or implement user-access-control independently.

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.

The Encryption of Private Messages: The communication between the switch and the inner network security management system TrustView uses private messages. And the users can encrypt those messages of version 2.

Add option82 Function: It is used with dot1x dhcpoption82 authentication mode. Different option 82 will be added in DHCP messages according to user's authentication status.

17.2 DHCP Snooping Configuration

17.2.1 DHCP Snooping Configuration Task Sequence

1. Enable DHCP Snooping
2. Enable DHCP Snooping binding function
3. Enable DHCP Snooping option82 function
4. Set the private packet version
5. Set DES encrypted key for private packets
6. Set helper server address
7. Enable DHCP Snooping binding ARP function
8. Set trusted ports
9. Enable DHCP Snooping binding DOT1X function
10. Enable DHCP Snooping binding USER function
11. Adding static list entries function
12. Set defense actions
13. Set rate limitation of DHCP messages
14. 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． Enable DHCP Snooping option82 function

Command	Explanation
Globe mode	
ip dhcp snooping information enable **no ip dhcp snooping information enable**	Enable or disable DHCP snooping option82 function.
ip dhcp snooping option82 enable **no ip dhcp snooping option82 enable**	To enable/delete DHCP option82 of dot1x in access switch.

4． Set the private packet version

Command	Explanation
Globe mode	
ip user private packet version two **no ip user private packet version two**	The switch choose private packet version two to communicate with Edge-Core inter security management background system.

5． Set DES encrypted key for private packets

Command	Explanation
Globe mode	
enable trustview key 0/7 <password> **no enable trustview key**	To configure/delete DES encrypted key for private packets,

6． Set HELPER SERVER address

Command	Explanation
Globe mode	

Command	Explanation
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

7. 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

8. 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.

9. 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

10. 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

11. 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

12. 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.

13. 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

14. 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

17.2.2 Command for DHCP Snooping Configuration

17.2.2.1 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.

17.2.2.2 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.

17.2.2.3 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.

17.2.2.4 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.

17.2.2.5 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.

17.2.2.6 enable trustview key

Command: enable trustview key 0/7 *<password>*

          no enable trustview key

Function: To configure DES encrypted key for private packets, this command is also the switch for the private packets encrypt and hash function enabled or not.

Parameter: *<password>* is character string length less than 16, which use as encrypted key. **0** for un-encrypted text for the password, while 7 for encrypted.

Command Mode: Global Mode.

Default: Disabled.

Usage Guide: The switch communicates with the DSCM management system through private protocols. By default these packets are not encrypted. In order to prevent spoofing, it can be configured to encrypt these packets. And at the same time, the same password should be configured on TrustView server.

Example：Enable encrypt or hash function of private message.

Switch(config)#enable trustview key 0 digitalchina

17.2.2.7 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

17.2.2.8 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

17.2.2.9 ip dhcp snooping binding user

Command：ip dhcp snooping binding user <mac> address <ipAddr> <mask> vlan <vid> interface [Ethernet] <ifname>

              no Ip 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

17.2.2.10 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

17.2.2.11 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

17.2.2.12 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

17.2.2.13 ip dhcp snooping binding user-control max-user

Command：**ip dhcp snooping binding user-control max-user** *<number>*

　　　　　　no ip dhcp snooping binding user-control max-user

Function：Set the max number of users allowed to access the port when enabling DHCP Snooping binding user funciton; the no operation of this command will restore default value.

Parameters：*<number>* the max number of users allowed to access the port, from 0 to 1024.

Command Mode：Port Mode

Default Settings：The max number of users allowed by each port to access is 1024.

Usage Guide：This command defines the max number of trust users distributed according to binding information, with ip DHCP Snooping binding user-contrl enabled on the port. By default, the number is 1024. Considering the limited hardware resources of the switch, the actual number of trust users distributed depends on the resource amount. If a bigger max number of users is set using this command, DHCP Snooping will distribute the binding informaiton of untrust users to hardware to be trust users as long as there is enough available resources. Otherwise, DHCP Snooping will change the distributed binging informaiton accordint to the new smaller max user number. When the number of distributed bingding informaiton entries reaches the max limit, no new dhcp will be able to become trust user or to access other network resouces via the switch.

Examples：Enable DHCP Snooping binding user function on Port ethernet1/1, setting the max number of user allowed to access by Port Ethernet1/1 as 5.

Switch(Config-If-Ethernet1/1)#ip dhcp snooping binding user-control max-user 5

Related Command：ip dhcp snooping binding user-control

17.2.2.14 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

17.2.2.15 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

17.2.2.16 ip dhcp snooping action

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

17.2.2.17 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

17.2.2.18 ip dhcp snooping information enable

Command：ip dhcp snooping information enable

         no ip dhcp snooping information enable

Function： This command will enable option 82 function of DHCP snooping on the switch, the no operation of this command will disable that function.

Parameters： None.

Default Settings： Option 82 function is disabled in DHCP snooping by default.

Command Mode： Global Mode.

Usage Guide： Only by implementing this command, can dhcp snooping add standard option 82 to dhcp request messages and forward the message. The format of suboption1 in option 82 (Circuit ID option) is standard vlan name plus physical port name, like "vlan1+ethernet1/12". That of cuboption2 in option 82 (remote ID option) is cpu mac of the switch, like "00030f023301". If a DHCP request message with option 82 options is received, DHCP snooping will replace those options in the message with its own. If a DHCP reply message with option 82 options is received, DHCP snooping will dump those options in the message and forward it. This command and "ip dhcp snooping option82 enable" command are mutually exclusive.

Examples： Enable option 82 function of DHCP snooping on the switch.

Switch(config)#ip dhcp snooping enable

Switch(config)#ip dhcp snooping binding enable

Switch(config)#ip dhcp snooping information enable

17.2.2.19 ip dhcp snooping option82 enable

Command: ip dhcp snooping option82 enable

      no ip dhcp snooping option82 enable

Function: To enable DHCP option82 of dot1x in access switch. After DHCP snooping monitored DHCP requires packets, add the option82 which can indicate user authentication state to the back of requires packet, and then deliver to DHCP relay.

Parameter: None.

Command Mode: Global Mode.

Default: Disabled.

Usage Guide: This command configures the DHCP snooping to append the option82 information for DHCP requests when dot1x dhcpoption82based authentication is applied. By default, for un-authenticated users, the switch appends to the option 82 field of the DHCP requests with the remote-id field as unauth, and the circuit-id field as the MAC address of the CPU port of the switch. The DHCP server allocates addresses based on the information provided by the option82 field. And users can retrieve different IP addresses before and after authentication. When this command is applied, DHCP relay should not be configured on the truck switch which is connected to the local access switch.

Example: Enable option82 function of dhcp snooping.

switch(config)#ip dhcp snooping option82 enable

17.2.2.20 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

17.2.2.21 ip user private packet version two

Command: ip user private packet version two

  no ip user private packet version two

Function: The switch choose private packet version two to communicate with Edge-Core inter security management background system.

Parameter: None.

Command Mode: Global Mode.

Default: The switch choose private packet version one to communicate with DCBI.

Usage Guide: If the DCBI access control system is applied, the switch should be configured to use private protocol of version one to communicate with the DCBI server. However, if TrustView is applied, version two should be applied.

Example: To configure the switch choose private packet version two to communicate with Edge-Core inter security management background system.

switch(config)#ip user private packet version two

Relative Command: ip user helper-address

17.2.2.22 show trustview status

Command: show trustview status

Function: To show all kinds of private packets state information, which sending or receiving from TrustView (inter security management background system) of Edge-Core.

Parameter: None.

Command Mode: Admin Mode.

Default: Disabled.

Usage Guide: This command can be used for debugging the communication messages between the switch and the TrustVie server. Messages such as protocol version notification, encryption negotiation, free resource and web URL redirection, and the number of forced log-off messages, as well as the number of forced accounting update messages, can be displayed.

Example:

Switch#show trustview status

Primary TrustView Server 200.101.0.9:9119

    TrustView version2 message inform successed

    TrustView inform free resource successed

    TrustView inform web redirect address successed

    TrustView inform user binding data successed

TrustView version2 message encrypt/digest enabled

Key: 08:02:33:34:35:36:37:38

Rcvd 106 encrypted messages, in which MD5-error 0 messages, DES-error 0 messages

Sent 106 encrypted messages

Free resource is 200.101.0.9/255.255.255.255

Web redirect address for unauthencated users is <http://200.101.0.9:8080>

Rcvd 0 force log-off packets

Rcvd 19 force accounting update packets

17.2.2.23 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

17.3 DHCP Snooping Typical Application
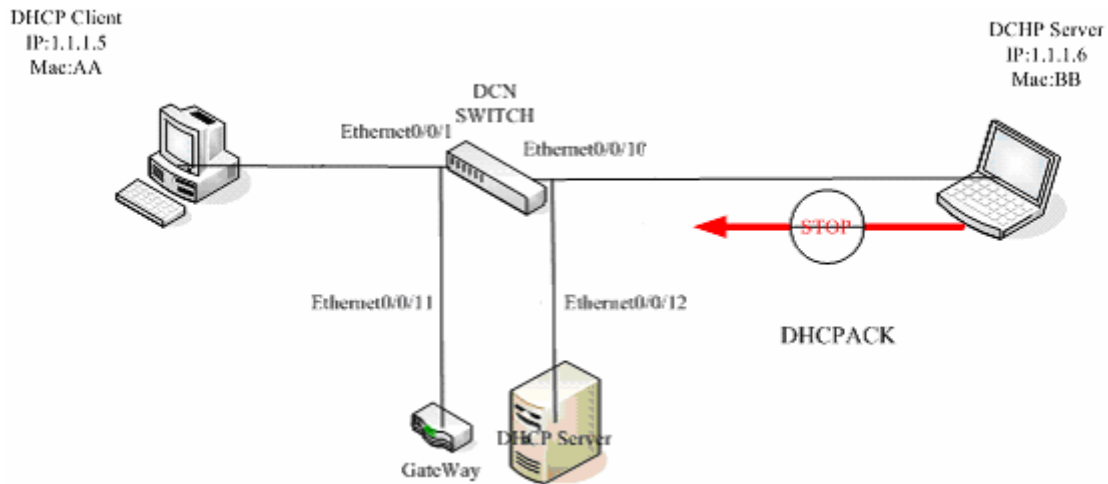
Fig 17-1 Sketch Map of TRUNK

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-If-Ethernet1/11)#ip dhcp snooping trust
switch(Config-If-Ethernet1/11)#exit
switch(config)#interface ethernet 1/12
switch(Config-If-Ethernet1/12)#ip dhcp snooping trust
switch(Config-If-Ethernet1/12)#exit
switch(config)#interface ethernet 1/1-10
switch(Config-Port-Range)#ip dhcp snooping action shutdown
switch(Config-Port-Range)#
```

17.4 DHCP Snooping Troubleshooting Help

17.4.1 Monitor And Debug Information

The "debug ip dhcp snooping" command can be used to monitor the debug information.

17.4.2 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 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 18 SNTP Configuration

18.1 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.
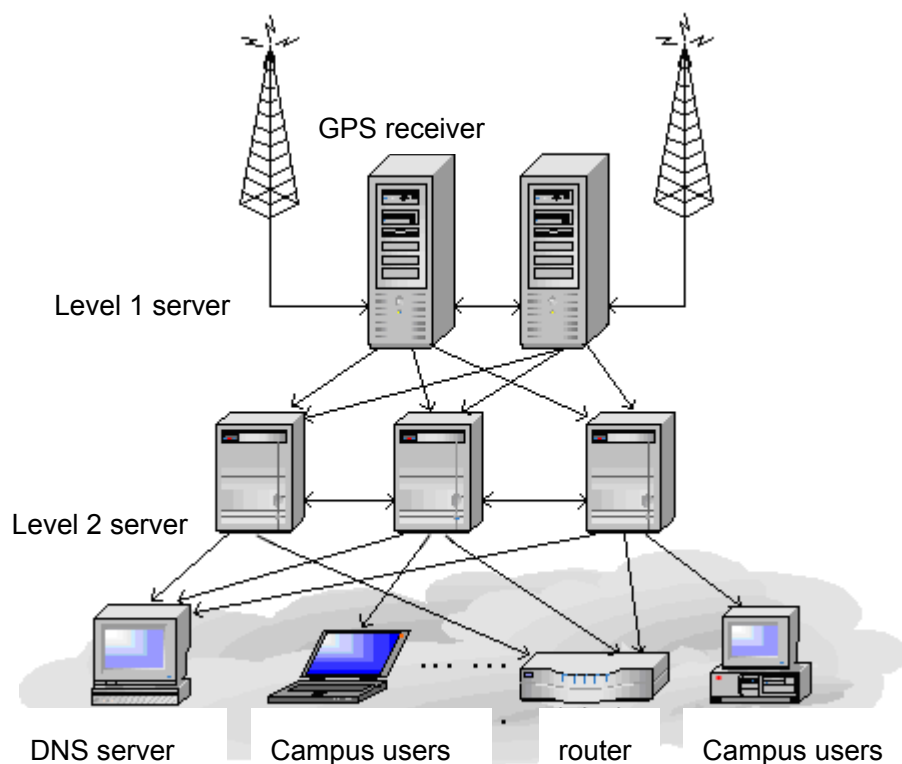
Fig 12-1 Working Scenario

ES4700 series 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.

18.2 Command for SNTP

18.2.1 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: UTC time.
Command Mode: Global Mode
Example: set the customer timezone 10 hours before-utc.
Switch(config)#clock timezone customer10 before-utc

18.2.2 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

18.2.3 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

18.2.4 debug sntp

Command:debug sntp {adjust | packet | select }

          no debug sntp {adjust | packet | 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 packet.

Switch#debug sntp packet

18.2.5 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

18.3 Typical SNTP Configuration Examples
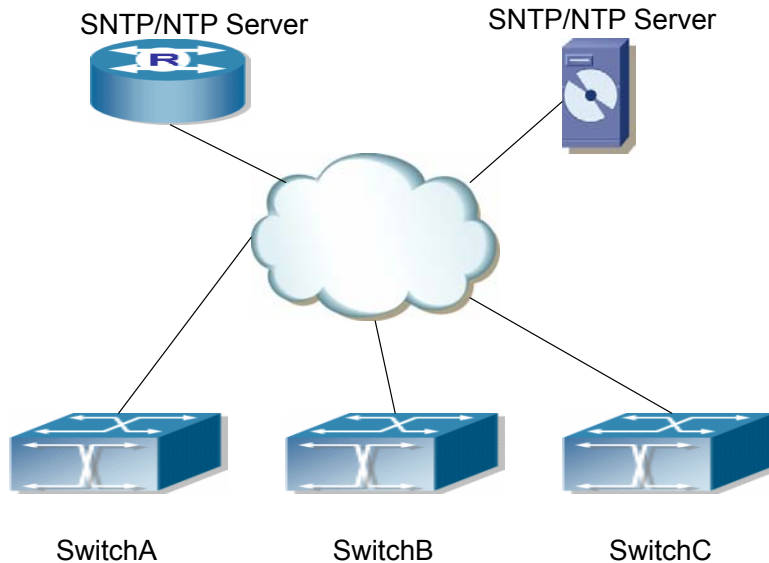
Fig 18-1Typical SNTP Configuration

All ES4700 series switches 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 ES4700 series 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 ES4700 series 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).

18.4 Web Management

Click "SNTP configuration" to open the switch SNTP configuration management list. Users may then make configuration to switch's SNTP settings.

18.4.1 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

18.4.2 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

18.4.3 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 .

Time difference configuration

Time zone	beijing
Time difference	⦿ after-utc ○ before-utc
Time value	8
Operation	Add

18.4.4 Show SNTP

Click "SNTP configuration", "Show sntp" to display the SNTP client current configuration and server status.

Information Feedback Window		
server address	version	last receive

Chapter 19 NTP function configuration

19.1 Introduction of NTP function

The NTP (network time protocol) synchronizes timekeeping spans WAN and LAN among distributed time servers and clients, it can get millisecond precision. The introduction of event, state, transmit function and action are defined in RFC 1305.

The purpose of using NTP is to keep consistent timekeeping among all clock-dependent devices within the network so that the devices can provide diverse applications based on the consistent time.

For a local system running NTP, its time can be synchronized by other reference sources and can be used as a reference source to synchronize other clocks, also can synchronize each other by transmit NTP packets.

19.2 NTP function configuration task list.

1. To enable NTP function

2. To configure NTP server function

3. To configure the max number of broadcast or multicast servers supported by the NTP client

4. To configure time zone

5. To configure NTP access control list

6. To configure NTP authentication

7. To specified some interface as NTP broadcast/multicast client interface

8. To configure some interface can't receive NTP packets

9. Display information

10. Dubug

1. To enable NTP function

Command	Notes
Global Mode	
ntp enable **ntp disable**	To enable or disable NTP function.

2. To configure NTP server function

Command	Notes
Global Mode	
ntp server {<*ip-address*>/<*ipv6-address*>} [version <*version_no*>] [key <*key-id*>] no ntp server {<*ip-address*> | <*ipv6-address*>}	To enable the specified time server of time source.

3. To configure the max number of broadcast or multicast servers supported by the NTP client

Command	Explication
Global Mode	
ntp broadcast server count <number> no ntp broadcast server count	Set the max number of broadcast or multicast servers supported by the NTP client. The no operation will cancel the configuration and restore the default value.

4. To configure time zone

Command	Notes
Global Mode	
ntp timezone <*name*> [{add | subtract}] [<*time_difference*>] no ntp timezone	To configure the time zone and time different with UTC for NTP client.

5. To configure NTP access control list

Command	Notes
Global Mode	
ntp access-group server <*acl*> no ntp access-group server <*acl*>	To configure NTP server access control list.

6. To configure NTP authentication

Command	Notes
Global Mode	

ntp authenticate	To enable NTP authentication function.
no ntp authenticate	
ntp authentication-key <*key-id*> md5 <*value*>	To configure authentication key for NTP authentication.
no ntp authentication-key <*key-id*>	
ntp trusted-key <*key-id*>	To configure trusted key.
no ntp trusted-key <*key-id*>	

7. To specified some interface as NTP broadcast/multicast client interface

Command	Notes
Interface Configuration Mode	
ntp broadcast client **no ntp broadcast client** **ntp multicast client** **no ntp multicast client** **ntp ipv6 multicast client** **no ntp ipv6 multicast client**	To configure specified interface to receive NTP broadcast packets. To configure specified interface to receive NTP multicast packets. To configure specified interface to receive IPv6 NTP multicast packets.

8. To configure some interface can't receive NTP packets

Command	Notes
Interface Configuration Mode	
ntp disable **no ntp disable**	To disable the NTP function.

9. Display information

Command	Notes
Admin Mode	
show ntp status **show ntp session** **[<*ip-address*>/<*ipv6-address*>]**	To display the state of time synchronize. To display the information of NTP session.

10. Debug

Command	Notes
Admin Mode	

debug ntp authentication **no debug ntp authentication**	To enable debug switch of NTP authentication.
debug ntp packets [send | receive] **no debug ntp packets [send | receive]**	To enable debug switch of NTP packet information.
debug ntp adjust **no debug ntp adjust**	To enable debug switch of time update information.
debug ntp sync **no debug ntp sync**	To enable debug switch of time synchronize information.
debug ntp events **no debug ntp events**	To enable debug switch of NTP event information.

19.3 NTP configuration command

19.3.1 ntp enable

Command: ntp enable

Function: To enable NTP function globally.

Parameter: None.

Default: Disabled.

Command Mode: Global Mode.

Usage Guide: None.

Example: To enable NTP function.

Switch(config)#ntp enable

19.3.2 ntp disable

Command: ntp disable

Function: To disable NTP function globally.

Parameter: None.

Default: Disabled.

Command Mode: Global Mode.

Usage Guide: None.

Example: To disable NTP function.

Switch(config)#ntp disable

19.3.3 ntp server

Command: ntp server {*<ip-address>*|*<ipv6-address>*} [version *<version_no>*] [key*<key-id>*]

no ntp server {*<ip-address>*|*<ipv6-address>*}

Function: To enable specified time server of time source. The no command is to delete specified time server of time source.

Parameter: ip-address：IPv4 address of time server.

ipv6-address：IPv6 address of time server.

version：The version information configured for server.

version_no：The version number of server, range between 1 to 4, by default is 4.

key：To configure key for server.

key-id：The key id.

Default: Disabled.

Command Mode: Global Mode.

Usage Guide: None.

Example: To configure time server address as 1.1.1.1 on switch:

Switch(config)#ntp server 1.1.1.1

19.3.4 ntp broadcast server count

Command：ntp broadcast server count <number>

no ntp broadcast server count

Function： Set the max number of broadcast or multicast servers supported by the NTP client. The no operation will cancel the configuration and restore the default value.

Parameters： number：1-100, the max number of broadcast servers.

Default： The default max number of broadcast servers is 50.

Command Mode: Global Mode.

Examples： Configure the max number of broadcast servers is 70 on the switch.

Switch(config)#ntp broadcast server count 70

19.3.5 ntp timezone

Command: ntp timezone *<name>* [{add | subtract}] [*<time_difference>*]

no ntp timezone

Function: To configure the time zone and time different with UTC for NTP client. The no command is to delete the configured time zone, restores the default value.

Parameter: name is the configured time zone, less than 16 characters.

add means the configured UTC time add time_difference.

Subtract means the configured UTC time subtract time_difference, add is by default, time_different range between 0 to 12, set to 8 is by default.

Default: The time different is set to 8 by default.

Command Mode: Global Mode.

Usage Guide: None.

Example: To configure the time zone to Beijing.

Switch#config

Switch(config)#ntp timezone beijing add 8

19.3.6 ntp access-group

Command: ntp access-group server *<acl>*

        no ntp access-group server *<acl>*

Function: To configure the access control list of NTP Server. The no command is to delete the access control list of NTP service.

Parameter: acl: ACL number, ranger between 1 to 99.

Default: Disabled.

Command Mode: Global Mode.

Usage Guide: None.

Example: To configure access control list 2 on the switch.

Switch(config)#ntp access-group server 2

19.3.7 ntp authenticate

Command: ntp authenticate

        no ntp authenticate

Function: To enable/disable NTP authentication function.

Parameter: None.

Default: Disabled.

Command Mode: Global Mode.

Usage Guide: None.

Example: To enable NTP authentication function.

Switch(config)# ntp authenticate

19.3.8 ntp authentication-key

Command: ntp authentication-key *<key-id>* md5 *<value>*

no ntp authentication-key *<key-id>*

Function: To enable NTP authentication function, and defined NTP authentication key. The no command is to delete the authentication key of NTP authentication.

Parameter: key-id：The id of key, range between 1 to 4294967295.

value：The value of key, range between 1 to 16 of ascii code.

Default: The authentication key of NTP authentication is not configured by default.

Command Mode: Global Mode.

Usage Guide: None.

Example: To define the authentication key of NTP authentication, the key id is 20, the md5 is abc.

Switch(config)#ntp authentication-key 20 md5 abc

19.3.9 ntp trusted-key

Command: ntp trusted-key *<key-id>*

no ntp trusted-key *<key-id>*

Function: To configure the trusted key. The no command is to delete the specified trusted key.

Parameter: key-id:The id of key, range between 1 to 4294967295.

Default: Trusted key is not configured by default.

Command Mode: Global Mode.

Usage Guide: None.

Example: To configure the specified key 20 to trusted key.

Switch(config)#ntp trusted-key 20

19.3.10 ntp disable

Command: ntp disable

no ntp disable

Function: To disable the NTP function on port.

Parameter: None.

Default: To enable NTP function on all ports.

Command Mode: Interface Configuration Mode.

Usage Guide: None.

Example: To delete the NTP function on VLAN interface.

Switch(config)#interface vlan 1

Switch(Config-if-Vlan1)#ntp disable

19.3.11 ntp broadcast client

Command: ntp broadcast client

        no ntp broadcast client

Function: To configure the specified port to receive NTP broadcast packets. The no command is to delete the specified port to receive NTP broadcast packets.

Parameter: None.

Default: Disabled.

Command Mode: Interface Configuration Mode.

Usage Guide: None.

Example: To enable the function of VLAN1 interface to receive NTP broadcast packets.

Switch(config)# interface vlan 1

Switch(Config-if-Vlan1)#ntp broadcast client

19.3.12 ntp multicast client

Command: ntp multicast client

        no ntp multicast client

Function: To configure the specified port to receive NTP multicast packets. The no command is to delete the specified port to receive NTP multicast packets.

Parameter: None.

Default: Disabled.

Command Mode: Interface Configuration Mode.

Usage Guide: None.

Example: To enable the function of VLAN1 interface to receive NTP multicast packets.

Switch(config)#interface vlan 1

Switch(Config-if-Vlan1)#ntp multicast client

19.3.13 ntp ipv6 multicast client

Command: ntp ipv6 multicast client

        no ntp ipv6 multicast client

Function: To configure the specified port to receive NTP multicast packets of IPv6. The no command is to configure the specified port not to receive NTP multicast packets of IPv6.

Parameter: None.

Default: Disabled.

Command Mode: Interface Configuration Mode.

Usage Guide: None

Example: To enable the function of VLAN1 interface to receive NTP multicast packets of IPv6.

Switch(config)#interface vlan 1

Switch(Config-if-Vlan1)#ntp ipv6 multicast client

19.3.14 debug ntp authentication

Command: debug ntp authentication

    no debug ntp authentication

Function: To display NTP authentication information, if the switch is enabled, and if the packets schlepped authentication information when the packet in sending or receiving process, then the key identifier will be printed out. The no command is to close the switch of displaying NTP authentication information.

Parameter: None.

Default: Disabled.

Command Mode: Admin Mode.

Usage Guide: None.

Example: To enable the switch of displaying NTP authentication information.

Switch(config)#debug ntp authentication

19.3.15 debug ntp packets

Command: debug ntp packets [send | receive]

    no debug ntp packets [send | receive]

Function: To enable/disable the debug switch of displaying NTP packets information.

Parameter: send：The debug switch of sending ntp packets.

    receive：The debug switch of receiving ntp packets.

  If there is no parameter, that means enable the sending and receiving switch of ntp packets in the same time.

Default: Disabled.

Command Mode: Admin Mode.

Usage Guide: None.

Example: To enable the debug switch of displaying NTP packets information.

Switch(config)#debug ntp packets

19.3.16 debug ntp adjust

Command: debug ntp adjust

        no debug ntp adjust

Function: To enable/disable the debug switch of displaying local time adjust information.

Parameter: None.

Default: Disabled.

Command Mode: Admin Mode.

Usage Guide: None.

Example: To enable the debug switch of displaying local time adjust information.

Switch(config)#debug ntp adjust

19.3.17 debug ntp sync

Command: debug ntp sync

        no debug ntp sync

Function: To enable/disable debug switch of displaying local time synchronization information.

Parameter: None.

Default: Disabled.

Command Mode: Admin Mode.

Usage Guide: None.

Example: To enable debug switch of displaying local time synchronization information.

Switch(config)#debug ntp sync

19.3.18 debug ntp events

Command: debug ntp events

        no debug ntp events

Function: To enable/disable debug switch of displaying ntp event, after that, if some server changed from available to unavailable or from unavailable to available, the received illegal packet events will be printed.

Parameter: None.

Default: Disabled.

Command Mode: Admin Mode.

Usage Guide: None.

Example: To enable debug switch of displaying local time synchronization information.

Switch(config)#debug ntp events

19.3.19 show ntp status

Command: show ntp status

Function: To display time synchronization status, include synchronized or not, layers, address of time source and so on.

Parameter: None.

Default: None.

Command Mode: Admin and Config Mode.

Usage Guide: None.

Example:

Switch#show ntp status

Clock status: synchronized

Clock stratum: 3

Reference clock server: 1.1.1.2

Clock offset: 0.010 s

Root delay: 0.012 ms

Root dispersion: 0.000 ms

Reference time: TUE JAN 03 01:27:24 2006

19.3.20 show ntp session

Command: show ntp session [<*ip-address*>|<*ipv6-address*>]

Function: To display the information of all ntp session or some one specific session, include server ID, server layer, the local offset according to server. (The symbol * means this server is the selected local time server)

Parameter: ip-address：The IPv4 address of some specific configured time server.

ipv6-address： The IPv6 address of some specific configured time server.

If no parameter , the session relative information of all servers will be displayed. (Include broadcast and multicast servers)

Default: None.

Command Mode: Admin and Config Mode.

Usage Guide: None.

Example:

Switch#show ntp session

	server	stream	type	rootdelay	rootdispersion	trustlevel
*	1.1.1.2	2	unicast	0.010s	0.002s	10
	2.2.2.2	3	unicast	0.005s	0.000s	10

19.4 Typical Example of NTP function

A client switch wanted to synchronize time with time server in network, there is two time server in network, the one is used as host, the other is used as standby, the connection and configuration as follows (The switch A and switch B are the switch or route which support NTP server, they can be cisco switch):
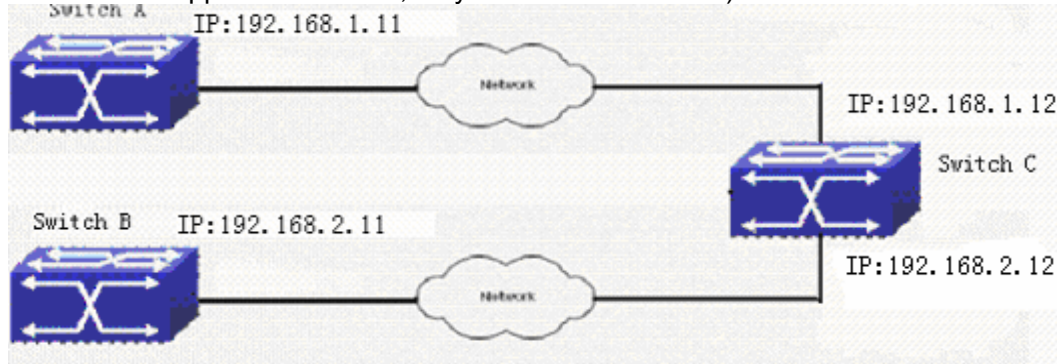
The configuration of switch C is as follows: (Switch A and Switch B may have the different command because of different companies, we not explain there, our switch are not support NTP server at present)

Switch C:

Switch(config)#ntp enable

Switch(config)#interface vlan 1

Switch(Config-if-Vlan1)# ip address 192.168.1.12 255.255.255.0

Switch(config)#interface vlan 2

Switch(Config-if-Vlan1)# ip address 192.168.2.12 255.255.255.0

Switch(config)#ntp server 192.168.1.11

Switch(config)#ntp server 192.168.2.11

19.5 NTP function troubleshooting

In configuration procedures, if there is error occurred, the system can give out the dubug information.

The NTP function disables by default, the show command can be used to display current configuration. If the configuration is right please use debug every relative debugging command and display specific information in procedure, and the function is configured right or not, you can also use "show" command to display the NTP running information, any questions please send the recorded message to the technical server center.

Chapter 20 DNSv4/v6 Configuration

20.1 DNS introduction

DNS (Domain name system) is a distributed database used by TCP/IP applications to translate domain names into corresponding IPv4/IPv6 addresses. With DNS, you can use easy-to-remember and signification domain names in some applications and let the DNS server translate them into correct IPv4/IPv6 addresses.

There are two types of DNS services, static and dynamic, which supplement each other in application. Each time the DNS server receives a name query it checks its static DNS database first before looking up the dynamic DNS database. Some frequently used addresses can be put in the static DNS database, the reduction the searching time in the dynamic DNS database would increase efficiency. The static domain name resolution means setting up mappings between domain names and IPv4/IPv6 addresses. IPv4/IPv6 addresses of the corresponding domain names can be found in the static DNS database when you use some applications. Dynamic domain name resolution is implemented by querying the DNS server. A user program sends a name query to the resolver in the DNS client when users want to use some applications with domain name, the DNS resolver looks up the local domain name cache for a match. If a match is found, it sends the corresponding IPv4/IPv6 address back to the switch. If no match is found, it sends a query to a higher DNS server. This process continues until a result, whether success or failure, is returned.

The Domain Name System (DNS) is a hierarchical naming system for computers, services, or any resource participating in the Internet. It associates various information with domain names assigned to such participants. Most importantly, it translates humanly meaningful domain names to the numerical (binary) identifiers associated with networking equipment for the purpose of locating and addressing these devices world-wide. An often used analogy to explain the Domain Name System is that it serves as the "phone book" for the Internet by translating human-friendly computer hostnames into IP addresses. For example, www.example.com translates to 208.77.188.166.

The Domain Name System makes it possible to assign domain names to groups of Internet users in a meaningful way, independent of each user's physical location. Because of this, World-Wide Web (WWW) hyperlinks and Internet contact information can remain consistent and constant even if the current Internet routing arrangements change or the participant uses a mobile device. Internet domain names are easier to remember than IP addresses such as 208.77.188.166(IPv4) or

2001:db8:1f70::999:de8:7648:6e8 (IPv6). People take advantage of this when they recite meaningful URLs and e-mail addresses without having to know how the machine will actually locate them.

The Domain Name System distributes the responsibility for assigning domain names and mapping them to Internet Protocol (IP) networks by designating authoritative name servers for each domain to keep track of their own changes, avoiding the need for a central register to be continually consulted and updated.

In general, the Domain Name System also stores other types of information, such as the list of mail servers that accept email for a given Internet domain. By providing a world-wide, distributed keyword-based redirection service, the Domain Name System is an essential component of the functionality of the Internet.

20.2 DNSv4/v6 Configuration Task List

1. To enable/disable DNS function
2. To configure/delete DNS server
3. To configure/delete domain name suffix
4. To delete the domain entry of specified address in dynamic cache
5. To enable DNS dynamic domain name resolution
6. Enable/disable DNS SERVER function
7. Configure the max number of client information in the switch queue
8. Configure the timeout value of caching the client information on the switch
9. Monitor and diagnosis of DNS function

1. To enable/disable DNS function

Command	Notes
Global Mode	
ip domain-lookup **no ip domain-lookup**	To enable/disable DNS dynamic lookup function.

2. To configure/delete DNS server

Command	Notes
Global Mode	
dns-server {*<ip-address>* / *<ipv6-address>*} [priority *<value>*] **no dns-server {*<ip-address>* / *<ipv6-address>*}**	To configure DNS server, the no form of this command deletes DNS server.

3. To configure/delete domain name suffix

Command	Notes
Command	Notes

Global Mode	
ip domain-list *\<WORD\>* **no ip domain-list *\<WORD\>***	To configure/delete domain name suffix

4. To delete the domain entry of specified address in dynamic cache

Command	Notes
Admin Mode	
clear dynamic-host {*\<ip-address\>* |*\<ipv6-address\>*|*all* }	To delete the domain entry of specified address in dynamic cache

5. To enable DNS dynamic domain name resolution

Command	Notes
Global Mode	
dns lookup {ipv4|ipv6} *\<hostname\>*	To enable DNS dynamic domain name resolution

6. Enable/disable DNS SERVER function

Command	Explanation
Global Mode	
ip dns server **no ip dns server**	Enable/disable DNS SERVER function.

7. Configure the max number of client information in the switch queue

Command	Explanation
Global Mode	
ip dns server queue maximum \<1-5000\> **no ip dns server queue maximum**	Configure the max number of client information in the switch queue.

8. Configure the timeout value of caching the client information on the switch

Command	Explanation
Global Mode	
ip dns server queue timeout \<1-100\> **no ip dns server queue timeout**	Configure the timeout value of caching the client information on the switch.

9. Monitor and diagnosis of DNS function

Command	Explanation
Admin Mode and Configuration Mode	
show dns name-server	To show the configured DNS server information.

show dns domain-list	To show the configured DNS domain name suffix information.
show dns dynamic-hosts	To show the dynamic domain name information of resolved by switch.
show dns config	Display the configured global DNS information on the switch.
show dns client	Display the DNS Client information maintained by the switch.
debug dns {all | packet [send | recv]| events} **no debug dns {all | packet [send | recv]| events|relay }**	To enable/disable DEBUG of DNS function.

20.3 Chapter DNSv4/v6 Configuration Tasks

20.3.1 clear dynamic-host

Command: clear dynamic-host {*<ip-address>*/*<ipv6-address>*\|all }
Function: To delete the domain entry of specified address or all address in dynamic cache.
Parameter: *<ip-address>* is the IP address, in dotted decimal notation; *<ipv6-address>* is the IPv6 address; **all** is to delete the domain entry of all address in dynamic cache.
Command Mode: Admin Mode.
Default: Disabled.
Usage Guide: This command is used to manually delete the domain name and address entry in dynamic cache, this command is much useful when domain name have lived long time in cache.
Example: To delete the address of 202.108.22.5 of domain entry.
Switch(config)#clear dynamic-host 202.108.22.5

20.3.2 ip domain-lookup

Command: ip domain-lookup
          no ip domain-lookup
Function: To enable/disable DNS function, whether the switch will send dynamic DNS domain queries to the real DNS server or not.

Parameter: None.

Command Mode: Global Mode.

Default: Disabled.

Usage Guide: This command is used to enable or disable the switch DNS dynamic query function. If DNS dynamic query function is enabled, the DNS server will resolve the host name and domain name to the IPv4 or IPv6 address for requests from the clients. If DNS is disabled, client applications will not be able to send any DNS requests to the DNS server. In this situation, only the static address resolution is available. For the address mapping in the resolve cache, which is learnt through DNS before, will be invalid after aging.

Example: To enable DNS function, can resolve the domain name dynamic.

Switch(config)# ip domain-lookup

20.3.3 dns-server

Command: dns-server {*<ip-address>*|*<ipv6-address>*} [priority *<value>*]

        no dns-server {*<ip-address>*|*<ipv6-address>*}

Function: To configure/delete DNS server.

Parameter: *<ip-address>* is the IP address, in dotted decimal notation, *<ipv6-address>* is the IPv6 address, *<value>* is the priority of DNS server, range between 0~255, 0 by default.

Command Mode: Global Mode.

Default: Disabled.

Usage Guide: This command is used for configure or delete DNS server, when need to enable dynamic domain name mapping, the switch will sending a domain name search request packet to configured DNS server, the DNS server can be configured no more than 6. The priority is the optional parameter, if priority is configured, the DNS server must be organized according to the order of priority, from high to low. That is the switch sending domain name search request to the server which have the biggest priority, so some DNS server with quick search speed and used frequently can be configured to highest priority. If priority is not configured, to search DNS server must according to the configuration order. When the switch serves as a DNS SERVER, the queries to the DNS SERVER won't follow the above privilege rule; instead, the requests will be sent to all configured servers at the same time.

Example: To configure the priority of DNS server as 200, the server's address is 10.1.120.241.

Switch(config)#dns-server 10.1.120.241 priority 200

20.3.4 ip domain-list

Command: ip domain-list <WORD>

         no ip domain-list <WORD>

Function: To configure/delete domain name suffix.

Parameter: <WORD> is the character string of domain name suffix, less than 63 characters.

Command Mode: Global Mode.

Default: Disabled.

Usage Guide: This command is used to configure or delete suffix of domain name, when the entered domain name is not integrity (such as sina), the switch can add suffix automatically, after that, address mapping can run. The domain name suffix can be configured no more than 6. The first configured domain name suffix will be added first.

Example: To configure domain name suffix of com.

Switch(config)#ip domain-list com

20.3.5 ip dns server

Command： ip dns server

         no ip dns server

Function： Enable/disable DNS SERVER function.

Parameter: None.

Command Mode: Global Mode.

Default: Disabled by default.

Usage Guide： After the DNS SERVER function is enabled, the switch will be able to receive and handle DNS Requests from the clients by looking up locally or forward the request to the real DNS server.

Example： Configure to enable the dns server function of the switch.

Switch(config)#ip dns server

20.3.6 ip dns server queue maximum

Command： ip dns server queue maximum <1-5000>

         no ip dns server queue maximum

Function： Configure the max number of client information in the switch queue.

Parameter： <1-5000> the value can be 1－5000.

Command Mode: Global Mode.

Default： The default client number is 3000.

Usage Guide：When receiving a DNS Request from a client, the switch will cache the client's information. But the number of client information in the queue should not exceed the configured maximum number; otherwise the client's request won't be handled.

Example：Set the max number of client information in the switch queue as 2000.

Switch(config)#ip dns server queue maximum 2000

20.3.7 ip dns server queue timeout

Command：**ip dns server queue timeout <1-100>**

　　　　　　no ip dns server queue timeout

Function：Configure the timeout value of caching the client information on the switch.

Parameters：<1-100> the value can be1－100s.

Command Mode: Global Mode.

Default：The default timeout value is 5s.

Usage Guide：When receiving a DNS Request from a client, the switch will cache the client's information. But the time of maintaining the client information should not exceed the configured maximum timeout value; otherwise the client's information will be cleared out.

Example：Configure the maximum timeout value of caching the client information on the switch as 10s.

Switch(config)#ip dns server queue timeout 10

20.3.8 dns lookup

Command: dns lookup {ipv4|ipv6} *<hostname>*

Function: To enable DNS dynamic domain name resolution.

Parameter: {ipv4|ipv6} means the IPv4 or IPv6 address look up, *<hostname>* is the resoluted dynamic host name, less than 63 characters.Command Mode: Global Mode.

Default: Disabled.

Usage Guide: This command is used to look up correspond address based on entered client name. It can look up both IPv4 and IPv6 address. This command only used for domain name mapping, it have no other application function. When command is running , interrupt is forbidding. If configured many servers and domain name suffix, longer time will be required for domain name mapping.

Example: To look up the IPv4 address of www.sina.com.

Switch(config)#dns lookup ipv4 www.sina.com

20.3.9 show dns name-server

Command: show dns name-server

Function: To display the information of configured DNS server.

Parameter: None.

Command Mode: Admin Mode and Configuration Mode.

Example:

Switch#show dns name-server

DNS NAME SERVER:

Address	Priority
10.1.120.231	100
10.1.180.85	80
2001::1	20

20.3.10 show dns domain-list

Command:show dns domain-list

Function: To display the suffix information of configured DNS domain name.

Parameter: None.

Command Mode: Admin Mode and Configuration Mode.

Example:

Switch#show dns domain-list

DNS DOMAIN LIST:

com.cn

edu.cn

20.3.11 show dns dynamic-hosts

Command: show dns dynamic-hosts

Function: To display the dynamic domain name information of resolute by switch.

Parameter: None.

Command Mode: Admin Mode and Configuration Mode.

Example:

Switch# show dns dynamic-hosts

Total number of dynamic host is 2

DNS HOST LIST：

Hostname	Address	Time to live	Type
www.sina.com.cn	202.108.33.32	168000	dynamic
www.ipv6.org	2001:6b0:1:	168060	dynamic

20.3.12 show dns config

Command：show dns config

Function： Display the configured global DNS information on the switch.

Parameter: None.

Command Mode: Admin and Configuration Mode.

Example:

Switch(config)#show dns config

ip dns server enable

ip domain-lookup enable

the maximum of dns client in cache is 3000, timeout is 5

dns client number in cache is 0

dns dynamic host in cache is 0

dns name server number is 1

dns domain-list number is 0

20.3.13 show dns client

Command：show dns client

Function： Display the DNS Client information maintained by the switch.

Parameter: None.

Command Mode: Admin and Configuration Mode.

Example:

Switch(config)#show dns client

DNS REQUEST LIST:

Total number of dns request is 2

Address	Request Id
192.168.11.141	1
192.168.11.138	2

20.3.14 debug dns

Command: debug dns {all | packet [send | recv]| events |relay}

no debug dns {all | packet [send | recv]| events |relay}

Function: To display the application dubug information of DNS domain name resolution,

the no form of this command disables the dubug display.

Parameter: None.

Command Mode: Admin Mode.

Example:

Switch#debug dns all

Switch#ping host www.sina.com.cn

%Jan 01 00:03:13 2006 domain name www.sina.com.cn is to be parsed!

%Jan 01 00:03:13 2006 Dns query type is A!

  %Jan 01 00:03:13 2006 Connect dns server 10.1.120.241 ......

ping www.sina.com.cn [202.108.33.32]

Type ^c to abort.

Sending 5 56-byte ICMP Echos to 202.108.33.32, timeout is 2 seconds.

%Jan 01 00:03:15 2006 Host:www.sina.com.cn   Address:202.108.33.32

.....

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

20.4 Typical Examples of DNS
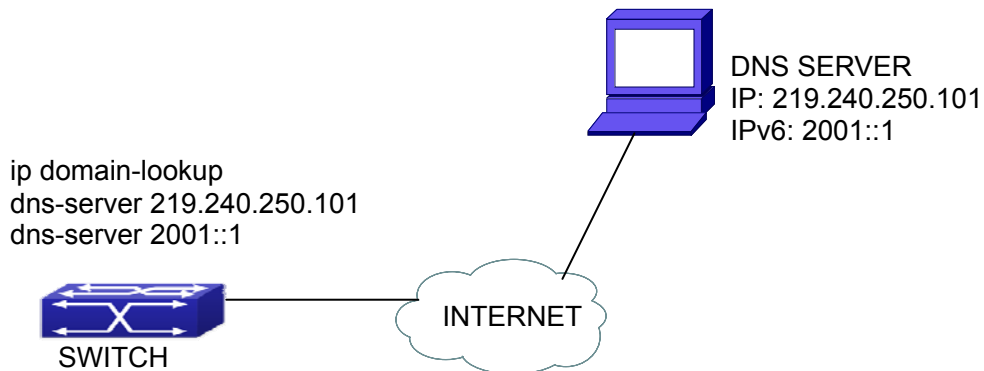
Fig 20-1 DNS CLIENT typical environment

    As shown in fig, the switch connected to DNS server through network, if the switch want to visit sina Website, it needn't to know the IPv4/IPv6 address of sina Website, only need is to record the domain name of sina Website is www.sina.com.cn. The DNS server can resolute out the IPv4/IPv6 address of this domain name and send to switch, then the switch can visit sina Website correctly. The switch is configured as DNS client, basic configurations are as below: first to enable DNS dynamic domain name resolution function on switch, and configure DNS server address, then with some kinds of tools such as PING, the switch can get corresponding IPv4/IPv6 address with dynamic domain name resolution function.
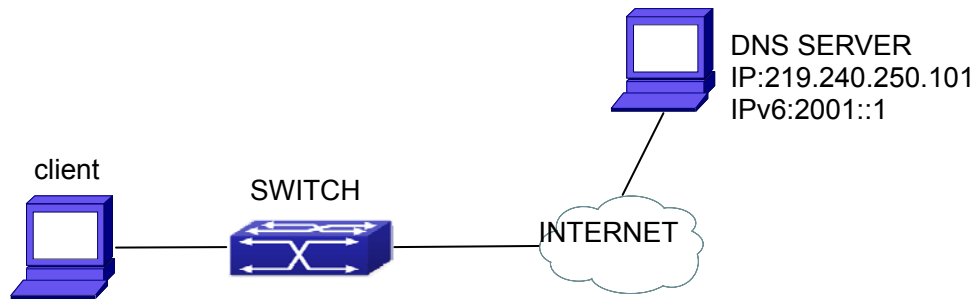
Fig 20-2 DNS SERVER typical environment

The figure above is an application of DNS SERVER. Under some circumstances, the client PC doesn't know the real DNS SERVER, and points to the switch instead. The switch plays the role of a DNS SERVER in two steps: Enable the global DNS SERVER function, configure the IP address of the real DNS server. After the DNS SERVER function is globally enabled, the switch will look up its local cache when receiving a DNS request from a client PC. If there is a domain needed by the local client, it will directly answer the client's request; otherwise, the switch will relay the request to the real DNS server, pass the reply from the DNS Server to the client and record the domain and its IP address for a faster lookup in the future.

Switch configuration for DNS CLIENT:
Switch(config)# ip domain-lookup
Switch(config)# dns-server 219.240.250.101
Switch(config)# dns-server 2001::1
Switch#ping host www.sina.com.cn
Switch#traceroute host www.sina.com.cn
Switch#telnet host www.sina.com.cn

Switch configuration for DNS SERVER:
Switch(config)# ip domain-lookup
Switch(config)# dns-server 219.240.250.101
Switch(config)# dns-server 2001::1
Switch(config)# ip dns server

20.5 DNS Troubleshooting

In configuring and using DNS, the DNS may fail due to reasons such as physical connection failure or wrong configurations. The user should ensure the following:
✧ First make sure good condition of the TACACS+ server physical connection;

✧ Second all interface and link protocols are in the UP state (use "show interface" command);

✧ Then please make sure that the DNS dynamic lookup function is enabled (use the "ip domain-lookup" command) before enabling the DNS CLIENT function. To use DNS SERVER function, please enable it (use the "ip dns server" command);

✧ Finally ensure configured DNS server address (use "dns-server" command), and the switch can ping DNS server.

✧ If the DNS problem remain unsolved, please use debug dns all and other debugging command and copy the DEBUG message within 3 minutes, send the recorded message to the technical server center.

Chapter 21 ARP Scanning Prevention Function Configuration

21.1 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.

21.2 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>*]	Set the trust attributes of IP
no anti-arpscan trust ip *\<ip-address>* [*\<netmask>*]	

5. Configure automatic recovery time

Command	Explanation
Global configuration mode	
anti-arpscan recovery enable	Enable or disable the automatic recovery function
no anti-arpscan recovery enable	
anti-arpscan recovery time *\<seconds>*	Set automatic recovery time
no anti-arpscan recovery time	

6. Display relative information of debug information and ARP scanning

Command	Explanation
Global configuration mode	
anti-arpscan log enable	Enable or disable the log function of ARP scanning prevention
no anti-arpscan log enable	
anti-arpscan trap enable	Enable or disable the SNMP Trap function of ARP scanning prevention
no anti-arpscan trap enable	
**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>***	Enable or disable the debug switch of ARP scanning prevention
**no debug anti-arpscan *\<port	ip>***	

21.3 Command for ARP Scanning Prevention

21.3.1 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： When remotely managing a switch with a method like telnet, users should set the uplink port as a Super Trust port before enabling anti-ARP-scan function, preventing the port from being shutdown because of receiving too many ARP messages. After the anti-ARP-scan function is disabled, this port will be reset to its default attribute, that is, Untrust port.

Example： Enable the ARP scanning prevention function of the switch.

Switch(config)#anti-arpscan enable

21.3.2 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： 10 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

21.3.3 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

21.3.4 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.

When remotely managing a switch with a method like telnet, users should set the uplink port as a Super Trust port before enabling anti-ARP-scan function, preventing the port from being shutdown because of receiving too many ARP messages. After the anti-ARP-scan function is disabled, this port will be reset to its default attribute, that is, Untrust port.

Example：Set port ethernet 4/5 of the switch as a trusted port

Switch(config)#interface ethernet4/5

Switch(Config-if-ethernet 4/5)# anti-arpscan trust port

21.3.5 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 192.168.1.0/24 as trusted IP

Switch(config)#anti-arpscan trust ip 192.168.1.0 255.255.255.0

21.3.6 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

21.3.7 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

21.3.8 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

21.3.9 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

21.3.10 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

21.3.11 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 the debug function for ARP scanning prevention of the switch.

Switch(config)#debug anti-arpscan

21.4 ARP Scanning Prevention Typical Examples
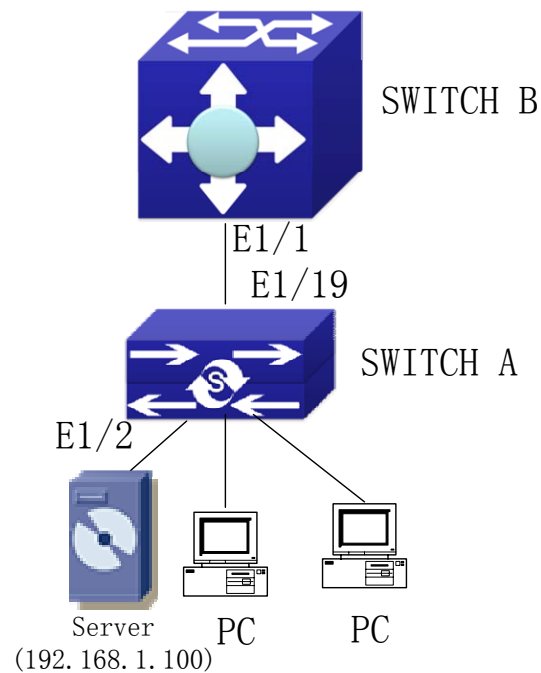
Fig 21-1 ARP scanning prevention typical configuration example

In the network topology above, port E1/1 of SWITCH B is connected to port E1/19 of SWITCH A, the port E1/2 of SWITCH A is connected to file server (IP address is 192.168.1.100), 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 192.168.1.0 255.255.255.0

SwitchA(config)#interface ethernet1/2

SwitchA (Config-If-Ethernet1/2)#anti-arpscan trust port

SwitchA (Config-If-Ethernet1/2)#exit

SwitchA(config)#interface ethernet1/19

SwitchA (Config-If-Ethernet1/19)#anti-arpscan trust supertrust-port

Switch A(Config-If-Ethernet1/19)#exit

SWITCHB configuration task sequence:

Switch B(config)# anti-arpscan enable

SwitchB(config)#interface ethernet1/2

SwitchB (Config-If-Ethernet1/2)#anti-arpscan trust port

SwitchB (Config-If-Ethernet1/2)exit

21.5 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 22 Prevent ARP, ND Spoofing Configuration

22.1 Overview

22.1.1 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.

22.1.2 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.

22.1.3 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 switchs, 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 maded 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.

22.2 Prevent ARP, ND Spoofing configuration

22.2.1 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 Port 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 Port mode	
ip arp-security learnprotect no lp 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 Port 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 Port mode	
clear ip arp dynamic clear ipv6 nd dynamic	Clear dynamic ARP, ND

22.3 Commands For Preventing ARP, ND Spoofing

22.3.1 ip arp-security updateprotect

Command：**ip arp-security updateprotect**

              no ip arp-security updateprotect

Function：Forbid ARP table automatic update, the ARP packets conflicting with current ARP item (e.g. with same IP but different MAC or port) will be droped, the others will be received to update aging timer or creat a new item; so, the current ARP item keep unchanged and the new item can still be learned. The "no ip arp-security updateprotect" command re-enables ARP table automatic update.

Parameter：None.

Default：ARP table automatic update.

Command Mode：Global Mode/ Interface configuration.

Example：Switch(Config-if-Vlan1)#ip arp-security updateprotect

Switch(config)#ip arp-security updateprotect

22.3.2 ipv6 nd-security updateprotect

Command：**ipv6 nd-security updateprotect**

 no ipv6 nd-security updateprotect

Function：Forbid ND automatic update function of IPv6 Version, the "no ipv6 nd-security updateprotect " command re-enables ND automatic update function.

Parameter：None

Default：ND update normally

Command Mode：Global Mode/ Interface configuration

Example：Switch(Config-if-Vlan1)#ipv6 nd -security updateprotect

Switch(config)#ipv6 nd -security updateprotect

22.3.3 ip arp-security learnprotect

Command：**ip arp-security learnprotect**

 no ip arp-security learnprotect

Function：Forbid ARP learning function of IPv4 Version, all the ARP packets will be droped; so, the current dynamic ARP item will age out, and no new ARP item will learned, the "no ip arp-security learnprotect " command re-enables ARP learning function.The "ip arp-security convert" is suggested to be used before this command.

Parameter：None

Default：ARP learning enabled.

Command Mode：Global Mode/ Interface configuration

Example：Switch(Config-if-Vlan1)# ip arp-security learnprotect

Switch(config)# ip arp-security learnprotect

22.3.4 ipv6 nd-security learnprotect

Command：**ipv6 nd-security learnprotect**

 no ipv6 nd-security learnprotect

Function：Forbid ND learning function of IPv6 Version, the "no ipv6 nd-security learning " command re-enables ND learning function.

Parameter：None

Default：ND learning enabled.

Command Mode：Global Mode/ Interface configuration

Example：Switch(Config-if-Vlan1)#ipv6 nd -security learnprotect

Switch(config)#ipv6 nd -security learnprotect

22.3.5 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

22.3.6 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

22.3.7 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

22.3.8 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

22.4 Prevent ARP, ND Spoofing Example
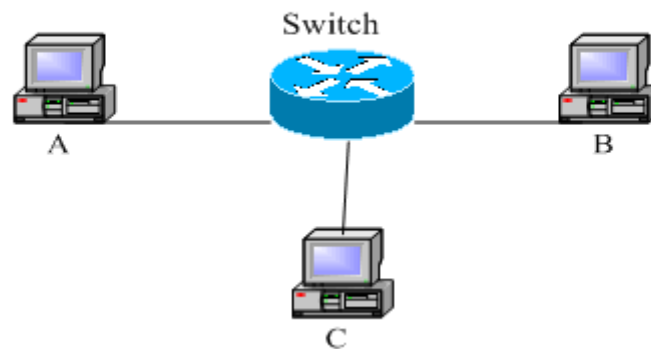
Fig 22-1 Prevent ARP ,ND Spoofing

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 23 ARP GUARD Configuration

23.1 ARP GUARD Introduction

There is serious security vulnerability in the design of ARP protocol, which is any network device, can send ARP messages to advertise the mapping relationship between IP address and MAC address. This provides a chance for ARP cheating. Attackers can send ARP REQUEST messages or ARP REPLY messages to advertise a wrong mapping relationship between IP address and MAC address, causing problems in network communication. The danger of ARP cheating has two forms: 1. PC4 sends an ARP message to advertise that the IP address of PC2 is mapped to the MAC address of PC4, which will cause all the IP messages to PC2 will be sent to PC4, thus PC4 will be able to monitor and capture the messages to PC2; 2. PC4 sends ARP messages to advertise that the IP address of PC2 is mapped to an illegal MAC address, which will prevent PC2 from receiving the messages to it. Particularly, if the attacker pretends to be the gateway and do ARP cheating, the whole network will be collapsed.
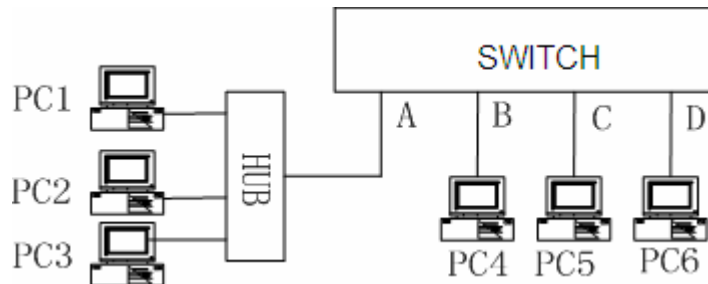
Fig 23-1 ARP GUARD schematic diagram

We utilize the filtering entries of the switch to protect the ARP entries of important network devices from being imitated by other devices. The basic theory of doing this is that utilizing the filtering entries of the switch to check all the ARP messages entering through the port, if the source address of the ARP message is protected, the messages will be directly dropped and will not be forwarded.

ARP GUARD function is usually used to protect the gateway from being attacked. If all the accessed PCs in the network should be protected from ARP cheating, then a large number of ARP GUARD address should be configured on the port, which will take up a big part of FFP entries in the chip, and as a result, might affect other applications. So this will be improper. It is recommended that adopting FREE RESOURCE related accessing scheme. Please refer to relative documents for details.

23.2 ARP GUARD Configuration Task List

1. Configure the protected IP address

Command	Explanation
Port configuration mode	
arp-guard ip <addr> **no arp-guard ip <addr>**	Configure/delete ARP GUARD address

23.3 Command For ARP GUARD

23.3.1 arp-guard ip

Command：arp-guard ip <addr>

no arp-guard ip <addr>

Function： Add a ARP GUARD address.

Parameters：<addr> is the protected IP address, in dotted decimal notation.

Command Mode： Port configuration mode.

Default： There is no ARP GUARD address by default.

Usage Guide： After configuring the ARP GUARD address, the ARP messages received from the ports configured ARP GUARD will be filtered. If the source IP addresses of the ARP messagse match the ARP GUARD address configured on this port, these messages will be judged as ARP cheating messages, which will be directly dropped instead of sending to the CPU of the switch or forwarding. 16 ARP GUARD addresses can be configured on each port.

Example： Configure the ARP GUARD address on port Ethernet1/1 as 100.1.1.1.

switch(config)#interface Ethernet1/1

switch(Config-If-Ethernet 1/1)#arp-guard ip 100.1.1.1

Chapter 24 Arp local proxy Configuration

24.1 Introduction to Arp local proxy function

In a real application environment, the switches in the aggregation layer are required to implement local arp proxy function to avoid arp cheating. This function will restrict the forwarding of arp messages in the same vlan and thus direct the L3 forwarding of the data flow through the switch.

PC1   **PC2**
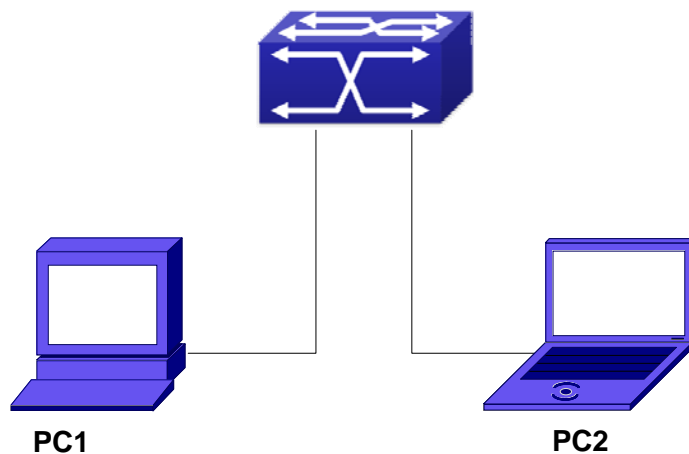
As shown in the figure above, PC1 wants to send an IP message to PC2, the overall procedure goes as follows (some non-arp details are ignored)

1. since PC1 does not have the arp of PC2, it sends and broadcasts ARP request.

2. Receiving the arp message, the switch hardware will send the arp request to CPU instead of forwarding this message via hardware, according to new arp handling rules.

3. With local arp proxy enabled, the switch will send arp reply message to PC1 (to fill up its mac address)

4. After receiving the arp reply, PC1 will create arp, send an IP message, and set the destination MAC of the Ethernet head as the MAC of the switch.

5. After receiving the ip message, the switch will search the router table (to create router cache) and distribute hardware entries.

6. If the switch has the arp of PC2, it will directly encapsulate the Ethernet head and send the message (the destination MAC is that of PC2)

7. if the switch does not have the arp of PC2, it will request it and then send the ip message.

This function should cooperate with other security functions. When users configure

local arp proxy on an aggregation switch while configuring interface isolation function on the layer-2 switch connected to it, all ip flow will be forwarded on layer 3 via the aggregation switch. And due to the interface isolation, arp messages will not be forwarded within the vlan, which means other PCs will not receive it.

24.2 arp local proxy function configuration task list

1) Enable arp local proxy function

1) Enable arp local proxy function

Command	Explanation
Interface vlan mode	
ip local proxy-arp **no ip local proxy-arp**	Enable or disable arp local proxy function.

24.3 Arp local proxy command

24.3.1 ip local proxy-arp

Command：**ip local proxy-arp**

　　　　　　no ip local proxy-arp

Function：Enable/disable the local arp proxy function of a specified interface.

Parameters：None.

Default Settings：This function is disabled on all interfaces by default.

Command Mode：Interface vlan Mode.

User Guide：This function is disabled on all interfaces by default, and differs from the original proxy-arp in that this function acts as an arp proxy inside the same layer-3 interface and thus directs the layer-3 forwarding of the switch.

Example：Enable the local arp proxy function of interface vlan1.

Switch(Config-if-Vlan1)# ip local proxy-arp

24.4 Typical examples of arp local proxy function

As shown in the following figure, S1 is a medium/high-level layer-3 switch supporting

arp local proxy, S2 is layer-2 access switches supporting interface isolation.

Considering security, interface isolation function is enabled on S2. Thus all downlink ports of S2 is isolated from each other, making all arp messages able to be forwarded through S1. if arp local proxy is enabled on S1, then all interfaces on S1 isolate arp while S1 serves as an arp proxy. As a result, IP flow will be forwarded at layer 3 through S1 instead of S2.
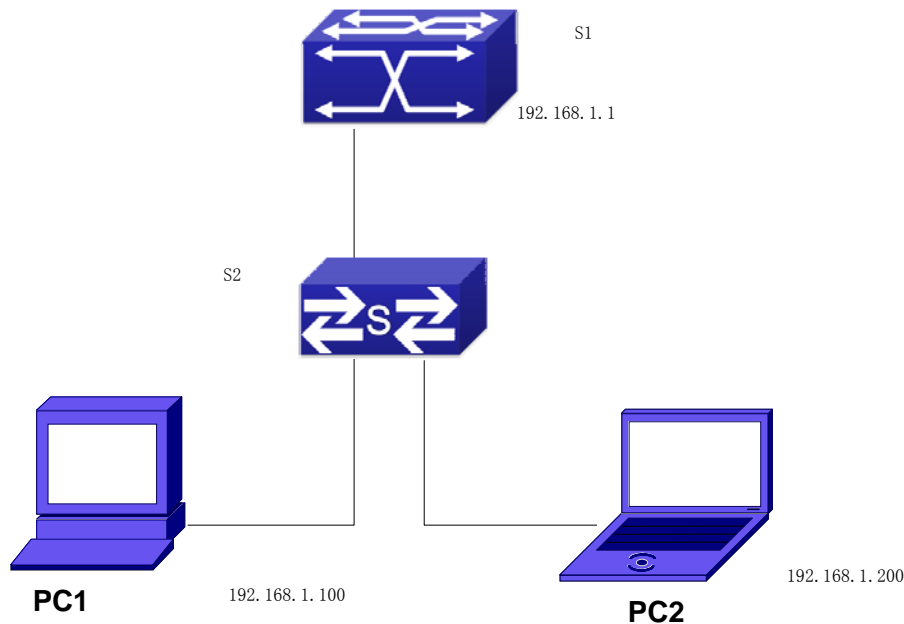
We can configure as follows:

Switch(config)#interface vlan 1

Switch(Config-if-Vlan1)#ip address 192.168.1.1 255.255.255.0

Switch(Config-if-Vlan1)#ip local proxy-arp

Switch(Config-if-Vlan1)#exit

24.5 Help on arp local proxy function troubleshooting

Arp local proxy function is disabled by default. Users can view the current configuration with display command. With correct configuration, by enabling debug of arp, users can check whether the arp proxy is normal and send proxy arp messages.

In the process of operation, the system will show corresponding prompts if any operational error occurs.

Chapter 25 Gratuitous ARP Configuration

25.1 Introduction to Gratuitous ARP

Gratuitous ARP is a kind of ARP request that is sent by the host with its IP address as the destination of the ARP request.

The basic working mode for Edge-Core switches is as below: The Layer 3 interfaces of the switch can be configured to advertise gratuitous ARP packets periodicly or the switch can be configured to enable to send gratuitous ARP packets in all the interfaces globally.

The purpose of gratuitous ARP is as below:

1. To reduce the frequency that the host sends ARP request to the switch. The hosts in the network will periodically send ARP requests to the gateway to update the MAC address of the gateway. If the switch advertises gratuitous ARP requests, the host will not have to send these request. This will reduce the frequency the hosts' sending ARP requests for the gateway's MAC address.

2. Gratuitous ARP is a method to prevent ARP cheating. The switch's advertising gratuitous ARP request will force the hosts to update its ARP table cache. Thus, forged ARP of gateway cannot function.

25.2 Gratuitous ARP Configuration Task List

1. To enable gratuitous ARP and configure the interval to send gratuitous ARP request
2. To display configurations about gratuitous ARP

1. To enable gratuitous ARP and configure the interval to send gratuitous ARP request

Command	Notes
Global configuration mode and Interface configuration mode.	
ip gratuitous-arp (<*5-1200*>|) **no ip gratuitous-arp**	To enable gratuitous ARP and configure the interval to send gratuitous ARP request.

2. To display configurations about gratuitous ARP

Command	Notes
All modes	
show ip gratuitous-arp (interface vlan <1-4094>|)	To display configurations about gratuitous ARP

25.3 Gratuitous ARP Command

25.3.1 ip gratuitous-arp

Command: **ip gratuitous-arp [<*interval-time*>]**

     no ip gratuitous-arp

Function: To enabled gratuitous arp, and specify update interval for gratuitous ARP. The no form of this command will disable the gratuitous ARP configuration.

Parameters: *<interval-time>* is the update interval for gratuitous ARP with its value limited between 5 and 1200 seconds and with default value as 300 seconds.

Command Mode: Global configuration mode and interface configuration mode.

Default: Gratuitous ARP is disabled by default.

Usage Guide: When configuring gratuitous ARP in global configuration mode, all the Layer 3 interfaces in the switch will be enabled to send gratuitous ARP request. If gratuitous ARP is configured in interface configuration mode, then only the specified interface is able to send gratuitous ARP requests.

  When configuring the gratuitous ARP, the update interval configuration from interface configuration mode has higher preference than that from the global configuration mode.

Example:

1) To enable gratuitous ARP in global configuration mode, and set the update interval to be 400 seconds.

Switch>enable

Switch#config

Switch(config)#ip gratuitous-arp 400

2) To enable gratuitous ARP for interface vlan 10 and set the update interval to be 350 seconds.

Switch(config)#interface vlan 10

Switch(Config-if-Vlan10)#ip gratuitous-arp 350

25.3.2 show ip gratuitous-arp

Command: show ip gratuitous-arp [interface vlan *<vlan-id>*]

Function: To display configuration information about gratuitous ARP.

Parameters: *<vlan-id>*is the VLAN IDThe valid range for <vlan-id> is between 1 and 4094.

Command Mode: All the configuration modes.

Usage Guide: In all the configuration modes, the command **show ip gratuitous arp** will display information about the gratuitous ARP configuration in global and interface configuration mode.

The command **show ip gratuitous-arp interface vlan *<vlan-id>*** will display information about the gratuitous ARP configuration about the specified VLAN interface.

Example:

1) To display information about gratuitous ARP configuration in both global and interface configuration modes.

Switch#show ip gratuitous-arp

Gratuitous ARP send is Global enabled, Interval-Time is 300(s)

Gratuitous ARP send enabled interface vlan information:

Name	Interval-Time(seconds)
Vlan1	400
Vlan10	350

2) To display gratuitous ARP configuration about interface vlan 10.

Switch#show ip gratuitous-arp interface vlan 10

Gratuitous ARP send interface Vlan10 information:

Name	Interval-Time(seconds)
Vlan10	350

25.4 Gratuitous ARP Configuration Example
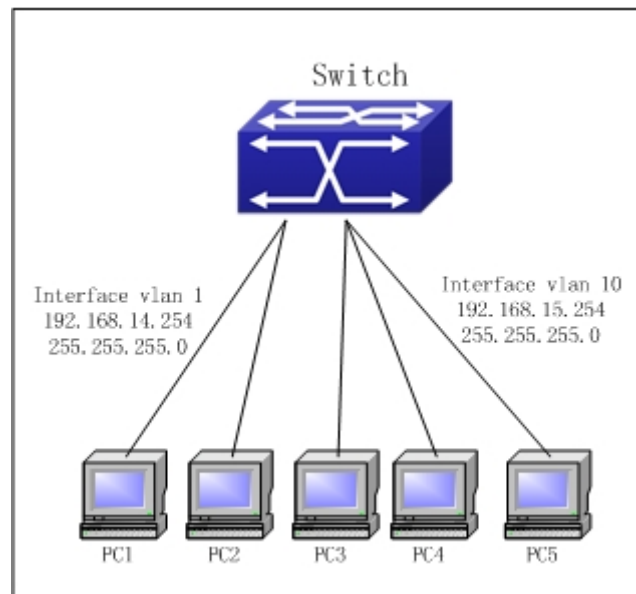
Fig 25-1 Gratuitous ARP Configuration Example

For the network topology shown in the figure above, interface vlan 10 whose IP address is 192.168.15.254 and network address mask is 255.255.255.0 in the Switch system. Three PCs – PC3, PC4, PC5 are connected to the interface. The IP address of interface vlan 1 is 192.168.14.254, its network address mask is 255.255.255.0. Two PCs – PC1 and PC2, are connected to this interface. Gratuitous ARP can be enabled through the following configuration:

1. To configure two interfaces to use gratuitous ARP at one time.
Switch(config)#ip gratuitous-arp 300
Switch(config)#exit

2. To configure gratuitous ARP specifically for only one interface at one time.
Switch(config)#interface vlan 10
Switch(Config-if-Vlan10)#ip gratuitous-arp 300
Switch(Config-if-Vlan10)#exit
Switch(config) #exit

25.5 Gratuitous ARP Trouble Shooting

Gratuitous ARP is disabled by default. And when gratuitous ARP is enabled, the debugging information about ARP packets can be retrieved through the command debug arp send.

If gratuitous ARP is enabled in global configuration mode, it can be disabled only in global configuration mode. If gratuitous ARP is configured in interface configuration mode, the configuration can only be disabled in interface configuration mode either.

If gratuitous ARP is configured in both global and interface configuration mode, and update interval is specified in both configuration modes, the switch take the value which is configured in interface configuration mode.

Chapter 26 IGMP Snooping

26.1 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.

ES4700 series provides IGMP Snooping and is able to send a query from the switch so that the user can use ES4700 series in IP multicast.

26.2 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
ip igmp snooping vlan *<vlan-id>* report souce-address *<A.B.C.D>* **no ip igmp snooping vlan *<vlan-id>***	Configure forward report source-address for IGMP, the "**no ip igmp snooping vlan *<vlan-id>* report source-address**"

report source-address	command restores the default setting.

26.3 Command For IGMP Snooping

26.3.1 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

26.3.2 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: To configure IGMP Snooping on specified vlan, the global IGMP Snooping should be first enabled. Disable IGMP Snooping on specified vlan with the "no ip igmp snooping vlan <vlan-id>" command.

Example: Enable IGMP Snooping for VLAN 100 in Global Mode.

Switch(config)#ip igmp snooping vlan 100

26.3.3 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: Enable immediate-leave function of the IGMP Snooping in specified vlan; the"no" form of this command disables the immediate-leave function of the IGMP Snooping.

Example: Enable the IGMP fast leave function for VLAN 100.

Switch(config)#ip igmp snooping vlan 100 immediate-leave

26.3.4 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

26.3.5 ip igmp snooping vlan limit

Command:　ip igmp snooping vlan *<vlan-id>* limit {group *<g_limit>* | source

　　　　　***<s_limit>*}**

　　　　　no ip igmp snooping vlan *<vlan-id>* limit

Function: Configure the max group count of vlan and the max source count of every group. The "**no ip igmp snooping vlan *<vlan-id>* limit**" command cancels this configuration.

Parameter: *<vlan-id>* is the VLAN number.

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, IGMP 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 IGMP is in operation, please make this configuration in accordance with the IGMP configuration as possible.

Example: Switch(config)#ip igmp snooping vlan 2 limit group 300

26.3.6 ip igmp snooping vlan mrouter-port interface

Command:ip igmp snooping vlan *<vlan-id>* mrouter-port interface [*<ehternet>*|*<port-channel>*]*<ifname>*

        no ip igmp snooping vlan *<vlan-id>* mrouter-port interface [*<ehternet>*|*<port-channel>*]*<ifname>*

Function: Configure static mrouter port of vlan. The no form of the command cancels this configuration

Parameter: *vlan-id*: ranging between <1-4094>

    ehternet: 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 [*<ehternet>*|*<port-channel>*]*<ifname>***" command.

Example: Switch(config)#ip igmp snooping vlan 2 mrouter-port interface ethernet1/1

26.3.7 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

26.3.8 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

26.3.9 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: 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

26.3.10 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: ranging between <2-10>

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

26.3.11 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: 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

26.3.12 ip igmp snooping vlan static-group

Command：ip igmp snooping vlan <vlan-id> static-group <A.B.C.D> [source < A.B.C.D >] interface [ethernet | port-channel] <IFNAME>

no ip igmp snooping vlan <vlan-id> static-group <A.B.C.D> [source < A.B.C.D >]interface [ethernet | port-channel] <IFNAME>

Function：Configure static-group on specified port of the vlan. The no form of the command cancels this configuration.

Parameter: ***vlan-id***: ranging between <1-4094>

A.B.C.D: the address of group or source

ethernet: Name of Ethernet port

> *port-channel*: Port aggregation
>
> *ifname*: Name of interface

Command Mode: Global mode

Default: No configuration by default.

Usage Guide: When a group is a static while also a dynamic group, it should be taken as a static group. Deleting static group can only be realized by the no form of the command.

Example:

Switch(config)#ip igmp snooping vlan 1 static-group 224.1.1.1 source 192.168.1.1 interface ethernet1/1

26.3.13 ip igmp snooping vlan report source-address

Command: ip igmp snooping vlan *<vlan-id>* report source-address *<A.B.C.D>*

> **no ip igmp snooping vlan *<vlan-id>* report source-address**

Function: Configure forward report source-address for IGMP, the "**no ip igmp snooping vlan *<vlan-id>* report source-address**" command restores the default setting.

Parameter: *vlan-id*: vlan id range<1-4094>

> ***A.B.C.D:*** IP address, can be 0.0.0.0.

Command Mode: Global Mode

Default: Disabled

Usage Guide: Default configuration is recommended here. If IGMP snooping needs to be configured, the source address for forwarded IGMP messages can be 0.0.0.0. If it is required by the upstream that IGMP messages should use the same network address, the source address of IGMP messages should be configured to be the same with upstream.

Example:

Switch(config)#ip igmp snooping vlan 2 report source-address 10.1.1.1

26.4 IGMP Snooping Example

Scenario 1. IGMP Snooping function
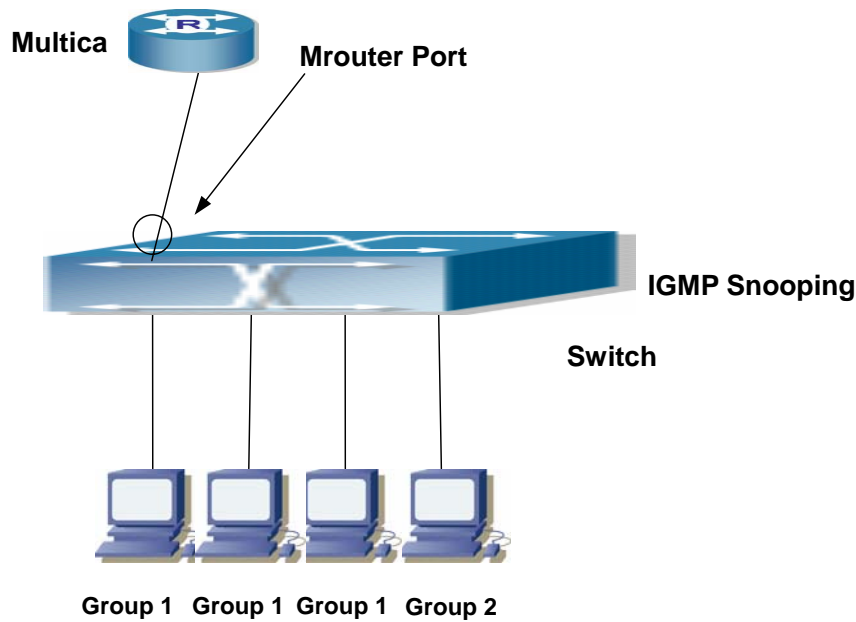
Fig 26-1   Enabling IGMP Snooping function

Example: As shown in the above figure, a VLAN 100 is configured in the switch and includes ports 1, 2, 6, 10 and 12 on slot 1. 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 Mrouter 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. L2-general-querier
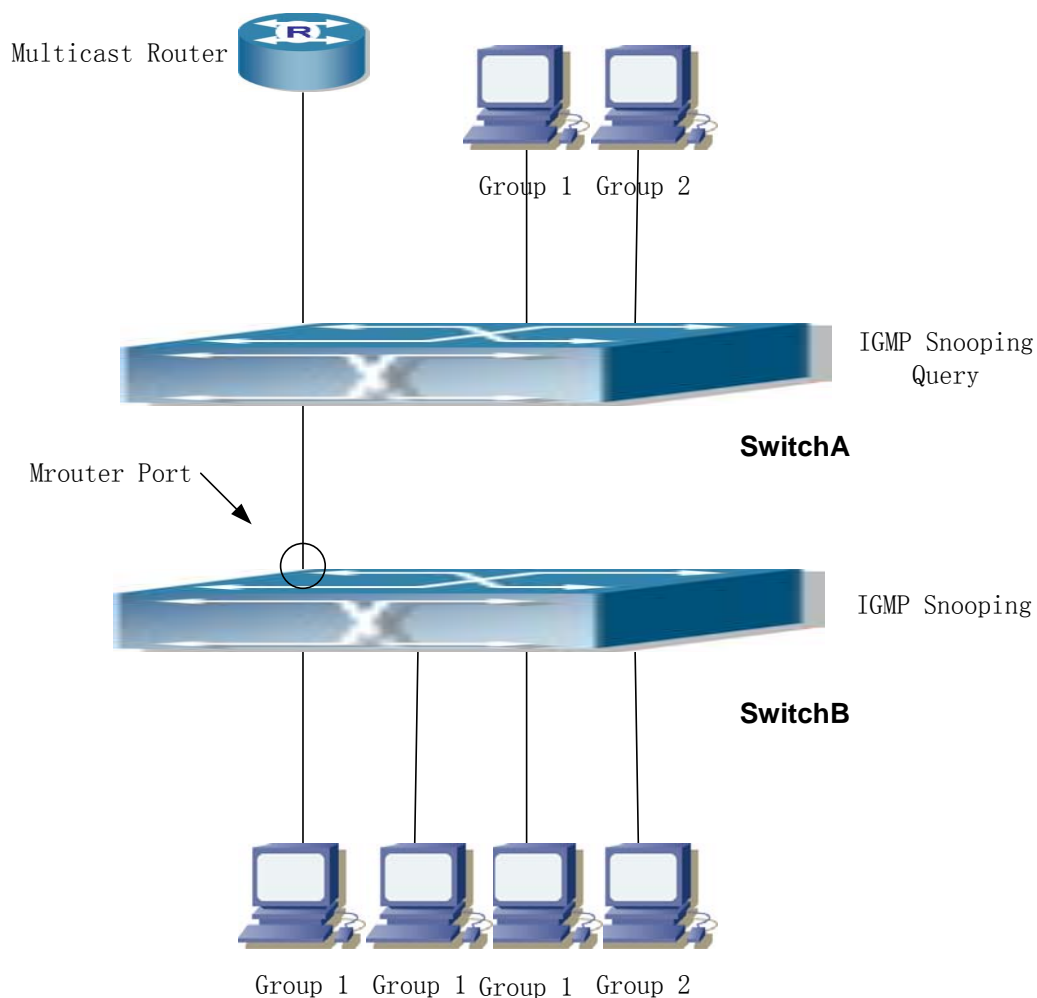
Fig 26-2 The switches as IGMP Queries

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 vlan 60
SwitchA(config)#ip igmp snooping vlan 60 L2-general-querier

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.

26.5 IGMP Snooping Troubleshooting Help

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:

1. Make sure correct physical connection.
2. Activate IGMP Snooping on whole config mode (use ip igmp snooping)
3. Config IGMP Snooping at VLAN on whole config mode (use ip igmp snooping vlan <vlan-id>)
4. Make sure one VLAN is configured as L2 common checker in same mask, or make sure configured static mrouter.
5. 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.

26.5.1 Monitor And Debug Command

26.5.1.1 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", downsending hardware entries message with "mfc", and all debugging messages with "all".

26.5.1.2 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 fo 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 reponse 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 reponse 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

26.5.1.3 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 Ethernet1/1

Chapter 27 VRRP Configuration

27.1 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.

27.2 VRRP 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>*	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

Port 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

27.3 Commands For VRRP

27.3.1 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_interva*> is the interval for sending VRRP packets in seconds, ranging from 1 to 10.

Default: The default <*adver_interva*> 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

27.3.2 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

27.3.3 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]

27.3.4 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

27.3.5 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

27.3.6 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

27.3.7 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

27.3.8 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

27.3.9 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

27.3.10 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

  Vrld <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

Vrld <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

27.3.11 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

27.4 Example Of VRRP

As shown in the figure below, SwitchA and SwitchB are Layer 3 Ethernet Switches in the same group and provide redundancy for each other.
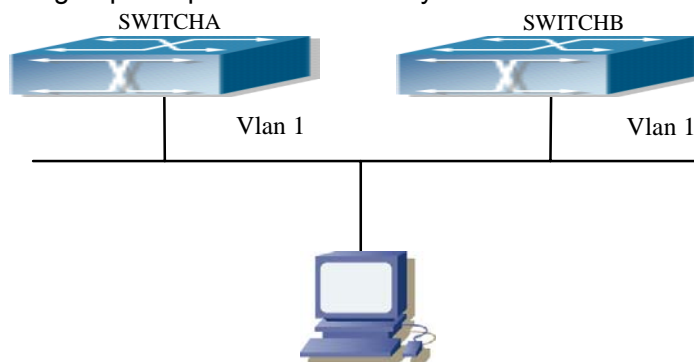
Fig 27-1 VRRP Network Topology

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

27.5 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.

27.6 Web Management

Click "VRRP control" to enter VRRP control configuration mode to manage VRRP features for the switch.

27.6.1 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.

Creat VRRP Number	
Creat VRRP Number	1

27.6.2 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 1. Click Remove to remove the Dummy IP address from Virtual Router number 1.

```
VRRP Dummy Ip Config
Choose Vrid              1
VRRP Dummy Ip Config   192.168.2.100
```

27.6.3 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.

Notice:Before Interface,please first delete the Virtual IP on the Interface

```
VRRP Port
Choose Vrid         1
Interface           23
```

27.6.4 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.

Notice:Before enable VRRP,please finish the setting of Virtual IP and Interface

```
VRRP Enable
Choose Vrid         1
```

27.6.5 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".

```
VRRP Preempt
Choose Vrid         1
VRRP Preempt        True
```

27.6.6 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.

VRRP Priority	
Choose Vrid	1
Priority	255

27.6.7 Configure VRRP 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.

VRRP Interval	
Choose Vrid	1
Interval Time	3

27.6.8 Configure VRRP Circuit

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.

VRRP Circuit	
Choose Vrid	1
Circuit Port	23
Priority Decrease Num	100

27.6.9 Configure VRRP Authentication Mode.

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 28 IPv6 VRRPv3 Configuration

28.1 VRRPv3 Introduction

VRRPv3 is a virtual router redundancy protocol for IPv6. It is designed based on VRRP(VRRPv2) in IPv4 environment. The following is a brief introduction to it.

In a network based on TCP/IP protocol, in order to guarantee the communication between the devices which are not physically connected, routers should be specified. At present there are two most commonly used methods to specify routers: one is to study dynamically via routing protocols(such as internal routing protocols RIP and OSPF); the other is to configure statically. Running dynamical routing protocol on each terminal is unrealistic, since most operating systems for client end do not support dynamical routing protocol, even if they do, they are limited by the overheads of management, convergence, security and many other problems. So the common method is to adopt static routing configuration on terminal IP devices, which usually means specify one or more default gateway for terminal devices. Static routing simplifies the management of network and reduces the communication overheads of terminal devices, but it still has a disadvantage: if the router acting as the default gateway breaks, the communication of all the hosts which use this gateway as their next hop host. Even if there are more than one default gateways, before rebooting the terminal devices, they can not switch to the new gateway. Adopting virtual router redundancy protocol(VRPR) can effectively avoid the flaws of statically specifying gateways.

In VRRP protocol, there are two groups of import concepts: VRRP routers and virtual routers, master routers and backup routers. VRRP routers are routers running VRRP, which are physical entities; virtual routers are the ones created by VRRP, which are logical concepts. A group of VRRP routers cooperate to comprise a virtual router, which acts outwardly as a logical router with a unique fixed IP address and MAC address. The routers belonging to the same VRRP group play two mutually exclusive roles at the same time: master routers and backup routers. One VRRP group can only have one master router other but one or more backup routers/ VRRPv3 protocol uses selection policy to select a master router from the router group to take charge of responding ND(Neighbor Discovery) neighbor request messages(ARP in IPv4) and forwarding IP data packets, while the other routers in the group will be in a state of waiting as backups. When the master router has a problem for some season, the backup router will be updated to the master router after a delay of a few seconds. Since this switch is very fast and does not need to change IP address or MAC address, it will be transparent to terminal user

systems.

In IPv6 environment, the hosts in a LAN usually learn the default gateway via neighbor discovery protocol(NDP), which is implemented based on regularly receiving advertisement messages from routers. The NDP of IPv6 has a mechanism called Neighbor Unreachability Detection, which checks whether a neighbor node is failed by sending unicast neighbor request messages to it. In order to reduce the overheads of sending neighbor request messages, these messages are only sent to those neighbor nodes which are sending flows, and are only sent if there is no instruction of UP state of the router in a period of time. In Neighbor Unreachability Detection, if adopting default parameters, it will take about 38 seconds to detect an unreachable router, which is a delay not ignorable for users and might cause a time-out in some transport protocols. Compared with NDP, VRRP provides a fast default gateway switch. In VRRP, backup routers can take up the unavailable master router in about 3 seconds(default parameter), and this process needs no interaction with hosts, which means being transparent to hosts.

28.1.1 The Format of VRRPv3 Message

VRRPv3 has its own message format. VRRP messages are used to communicate the priority of routers and the state of Master in the backup group, they are encapsulated in IPv6 messages to send, and are sent to the specified IPv6 multicast address. The format of VRRPv3 message is shown in Graph 1. The source address of the IPv6 message encapsulating the VRRPv3 message is the local address of the outbound interface of the message, and the destination address of it is the IPv6 multicast address(the multicast allocated to VRRPv3 is FF02:0:0:0:0:0:0:12). The number of hops should be limited to 255, and the next message head is 112(representing a VRRP message).

The meaning of each field in a VRRPv3 message is shown as follows:

Version: The version of VRRPv3, whose value is 3.

Type：The type of VRRP messages. There is only one type：ADVERTISEMENT, and its value is 1;

Virtual Rtr ID：The ID of the virtual router

Priority：Priority, ranging from 0 to 255;

Count IPv6 Addr：The number of IPv6 addresses in a VRRPv3 message, the minimum of which is 1;

Rsvd：Reserved field, whose value is 0;

Adver Int：The advertisement interval of VRRPv3 messages, in seconds;

Checksum：The checksum, taking account of the whole VRRPv3 message and an

552

IPv6 psuedohead (please refer to RFC2460 for details);

IPv6 Address(es)：one or more IPv6 addresses related to the virtual router, the number of which is the same with "Count IPv6 Addr", and the first one of which should be the virtual IPv6 address of the virtual router.
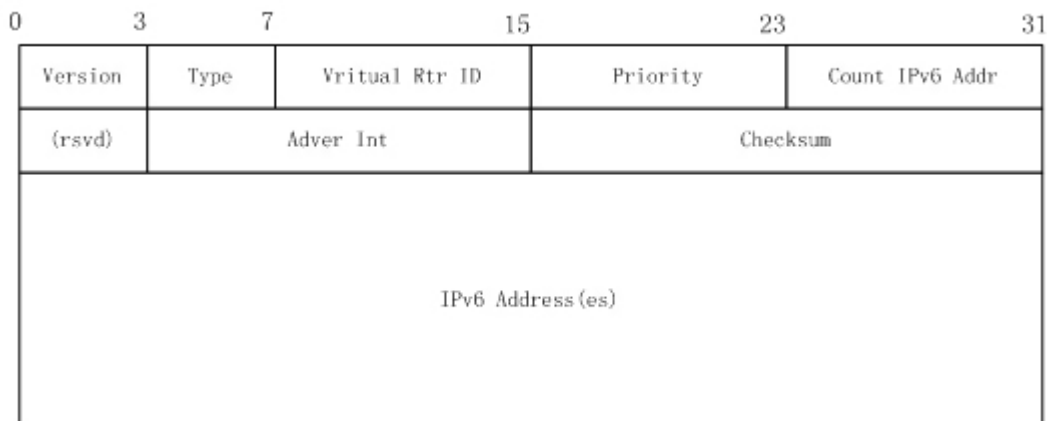
Fig 28-1 VRRPv3 message

28.1.2 VRRPv3 Working Mechanism

The working mechanism of VRRPv3 is the same with that of VRRPv2, which is mainly implemented via the interaction of VRRP advertisement messages. It will be briefly described as follows:

Each VRRP router has a unique ID: VRIP, ranging from 1 to 255. This router has a unique virtual MAC address outwardly, and the format of which is 00-00-5E-00-02-{VRID} (the format of virtual MAC address in VRRPv2 is 00-00-5E-00-01-{VRID}). Master router is in charge of using this MAC address to respond to ND neighbor request (it is ARP request in VRRPv2). Thus, no matter what switch is made, the terminal devices will get the same IP and MAC address all the time, reducing the affection that the switch causes on terminal devices.

There is only one kind of VRRP control message: VRRP advertisement. It uses IP multicast data packets to encapsulate, and the format of multicast addresses is FF02:0:0:0:0:0:XXXX:XXXX. In order to keep a consistence with the multicast address in VRRPv2 (224.0.0.18), the multicast addresses used by VRRPv3 advertisement messages can be FF02:0:0:0:0:0:0:12, and the advertisement is limited within the same LAN. Thus, different VRIDs are guaranteed to be used repeatedly in different networks. In order to reduce the overheads of network bandwidth, only master routers can send VRRP advertisement messages regularly. Backup routers will start a new round of VRRP selection if it hasn't received a VRRP advertisement in 3 advertisement intervals in a row or if it receives an advertisement with a priority of 0.

In a VRRP router group, the master router is selected according to priority. The range of priority in VRRP protocol is 0-255. If the IP address of a VRRP router is the same to that of the virtual router interface, then the virtual router will be called the IP address owner in the VRRP group. The IP address owner automatically has the highest priority: 255. The priority of 0 is usually used when the IP address owner gives up the role of master. The range of priority can be configured is 1-254. The configuration rule of priority can be set according to the speed and cost of the link, the performance and reliability of the router and other management policies. In the selection of the master router, the virtual router with high priority will win. So, if there is an IP owner in the VRRP group, it will always be the master router. For the candidate routers having the same priority, selection will be done according to the magnitude of IP addresses (the bigger IP address takes precedence). VRRP also provides a preemptive priority policy. If such policy is configured, the backup router with higher priority will preempt the role of new master router over the current master router with lower priority.

In order to avoid the fault of returning a physical MAC address when Pinging virtual IP, it is regulated that virtual IP can not be the real IP of the interface. Thus, all the interfaces participating of the backup group selection will be backups by default.

28.2 VRRPv3 Configuration Task Sequence

1. Create/delete the virtual router (necessary)
2. Configure the virtual IPv6 address and interface of VRRPv3 (necessary)
3. Enable/disable the virtual router (necessary)
4. Configure VRRPv3 assistant parameters (optional)
   （1）Configure VRRPv3 preempt mode
   （2）Configure VRRPv3 priority
   （3）Configure the VRRPv3 advertisement interval
   （4）Configure the monitor interface of VRRPv3

1. Create/delete the virtual router

Command	Explanation
Global configuration mode	
router ipv6 vrrp <*vrid*> **no router ipv6 vrrp <*vrid*>**	Create/delete the virtual router

2. Configure the virtual IPv6 address and interface of VRRPv3

Command	Explanation
VRRPv3 protocol mode	

virtual-ipv6 *<ipv6-address>* interface {Vlan *<ID>* | *IFNAME* } **no virtual-ipv6 interface**	Configure the virtual IPv6 address and interface of VRRPv3, the no operation of this command will delete the virtual IPv6 address and interface

3. Configure the VRRPv3 advertisement interval

Command	Explanation
VRRPv3 protocol mode	
enable	Enable the virtual router
disable	Disable the virtual router

4. Configure the monitor interface of VRRPv3

(1) Configure VRRPv3 preempt mode

Command	Explanation
VRRPv3 protocol mode	
preempt-mode {true| false}	Configure VRRPv3 preempt mode

(2) Configure VRRPv3 priority

Command	Explanation
VRRPv3 protocol mode	
priority *< priority >*	) Configure VRRPv3 priority

(3) Configure the VRRPv3 advertisement interval

Command	Explanation
VRRPv3 protocol mode	
advertisement-interval <time>	Configure the VRRPv3 advertisement interval (in cent seconds)

(4) Configure the monitor interface of VRRPv3

Command	Explanation
VRRPv3 protocol mode	
circuit-failover {vlan *<ID>*| *IFNAME*} *<value_reduced>* **no circuit-failover**	Configure the monitor interface of VRRPv3, the no operation of this command will delete the monitor interface.

28.3 IPv6 VRRPv3 Configuration Commands

28.3.1 advertisement-interval

Command：advertisement-interval *<adver_interval>*

Function： Configure the advertisement interval of VRRPv3.

Parameters: *<adver_interval>*is the interval of sending VRRPv3 advertisement messages, in centiseconds, ranging from 100 to 1000, and has to be a multiple of 100.

Command Mode： VRRPv3 protocol mode.

Default： *<adver_interval>* is 100 centi seconds (1 second) by default.

Usage Guide: The Master in a VRRPv3 backup group will send a VRRPv3 message to notify other routers (layer-three switches) in the group that it is working normally at intervals. This interval is *adver_interval*. If the Backup hasn't received any VRRPv3 message from Master over a certain period of time (the length of the time is *master_down_interval*), it will assume that the master is not working normally and will change the state of itself to Master.

Uses can use this command to adjust the interval of VRRPv3 advertisement messages sent by Master. For the members in the same backup group, this attribute should have same value. For Backup, the value of its *master_down_interval* should be two times more than *adver_interval*. If the network flow is too big or different routers (or layer-three switches) have different timers, *master_down_interval* might has a time-out, which will cause a state change as a result. This kind of situation can be solved by prolonging *adver_interval* or setting a longer preempts delay time.

Example： Configure the VRRPv3 advertisement interval as 300 centiseconds.

Switch(config-router)#advertisement-interval 300

28.3.2 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: VRRPv3 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

28.3.3 debug ipv6 vrrp

Command：**debug ipv6 vrrp [all | events | packet [recv | send]]**

            no debug ipv6 vrrp [all | events | packet [recv | send]]

Function：Display the state change, message receiving and sending of a VRRPv3 backup group, the no operation of this command will disable the display of DEBUG.

Parameters：None.

Command Mode：Admin mode.

Example：

Switch#debug ipv6 vrrp

Jan 01 01:03:13 2006 NSM: VRRP6 SEND[Hello]: Advertisement sent for vrid=[1], virtual-ip=[fe80::2]

Jan 01 01:03:14 2006 NSM: VRRP6 SEND[Hello]: Advertisement sent for vrid=[1], virtual-ip=[fe80::2]

Jan 01 01:03:15 2006 NSM: VRRP6 SEND[Hello]: Advertisement sent for vrid=[1], virtual-ip=[fe80::2]

28.3.4 disable

Command：**disable**

Function：Disable VRRPv3 virtual router.

Parameters：None.

Command Mode：VRRPv3 protocol mode.

Default：There is no configuration by default.

Usage Guide：Disable the corresponding virtual router session. Only after disabling the virtual router, can the relative configuration parameters be changed.

Examples：Disable the VRRPv3 virtual router whose ID is 10.

Switch(config)#router ipv6 vrrp 10

Switch(config-router)#disable

28.3.5 enable

Command：enable

Function： Enable VRRPv3 virtual router.

Parameters： None.

Command Mode： VRRPv3 protocol mode.

Default： There is no configuration by default.

Usage Guide： Start the corresponding virtual router session. Only the interface of the enabled router (or the layer-three switch can actually join the backup group. Before enabling the virtual router, the virtual IPv6 address and interface of VRRPv3 should be configured.

Example： Enable the VRRPv3 virtual router whose ID is 10.

Switch(config)#router ipv6 vrrp 10

Switch(config-router)#enable

28.3.6 preempt-mode

Command：preempt-mode {true| false}

Function： Configure the preempt mode of VRRPv3.

Parameters： None.

Command Mode： VRRPv3 protocol mode.

Default： It is VRRPv3 protocol mode by default.

Usage Guide： If it is needed that a router (or a layer-three switch) with higher priority can the role of master router, the preempt mode needs to be configured.

Example： Configure VRRPv3 as non-preempt mode.

Switch(config-router)#preempt-mode false

28.3.7 priority

Command：priority <*value*>

Function： Configure the priority of VRRPv3.

Parameters： <*value*> is the priority, whose range is 1～254.

Command Mode： VRRPv3 protocol mode.

Default： Backup routers（or layer-three switches）all have a priority of 100, the priority of IP address owners are all 255 in the backup group they belong to.

Usage Guide： Priority decides the state of a router (or a layer-three Ethernet switch) in a backup group. The higher the priority is, the more possible the router can be a Master. The configurable priority ranges from 1 to 254, while the priority of 255 is reserved to the

IP address owner. The priority of 0 has special usage, which is when disabling a VRRP session, Master will send an advertisement message with a priority of 0. When Backup receives such advertisement message, it will start a new round of Master selection. When there are two or more routers (or layer-three switches) in one backup group have the same priority, the router with biggest local link IPv6 address has higher priority.

Example：Configure the priority of VRRPv3 as 150

Switch(config-router)#priority 150

28.3.8 router ipv6 vrrp

Command：**router ipv6 vrrp** *<vrid>*

no router ipv6 vrrp *<vrid>*

Function：Create/delete a VRRPv3 virtual router.

Parameters：*<vrid>* is the ID of the virtual router, the valid range is 1 to 255.

Command Mode：Global mode.

Default：There is no configuration by default.

Usage Guide：This command is used to create/delete a VRRPv3 virtual router. The virtual router is uniquely specified by the virtual router ID and the related virtual IPv6 address. Only after creating a virtual router, relative configuration can be set on it. Considering the stability, the number of configurable virtual routers should not be more than 32.

Example：Configure a virtual router whose ID is10.

Switch(config)#router ipv6 vrrp 10

28.3.9 show ipv6 vrrp

Command：**show ipv6 vrrp [**_<vrid>_**]**

Function：Display the state and configuration information of VRRPv3 backup group.

Parameters：*<vrid>*is the ID of the virtual router, whose range is 1～255. No parameter means to display the state and configuration infomation of all backup gorups.

Command Mode：Executive mode.

Example：

Switch#show ipv6 vrrp

VrId 1

 State is Master

 Virtual IPv6 is fe80::2 (Not IPv6 owner)

 Interface is Vlan1

 Configured priority is 150, Current priority is 150

Advertisement interval is 100 centi seconds

Preempt mode is TRUE

Circuit failover interface Vlan1, Priority Delta 3, Status UP

VrId 10

State is Initialize

Virtual IPv6 is fe80::3 (Not IPv6 owner)

Interface is Vlan2

Priority is 100

Advertisement interval is 300 centi seconds

Preempt mode is TRUE

Circuit failover interface Vlan2, Priority Delta 10, Status UP

Display	Explanation
State	State;
Virtual IPv6	Virtual IPv6 address;
Interface	Interface name;
Priority	Priority;
Advertisement interval	The interval of VRRPv3 advertisement messages.
Preempt	Preempt mode.
Circuit failover interface	Monitor interface information.

28.3.10 virtual-ipv6 interface

Command：**virtual-ipv6 *<ipv6-address>* interface {Vlan *<ID>*| *IFNAME*}**

no virtual-ipv6 interface

Function：Configure the virtual IPv6 address and interface of VRRPv3.

Parameters：*<ipv6-address>*is the virtual IPv6 address, which has to be an IPv6 local link address.

{Vlan *<ID>*| *IFNAME*} is the interface name.

Command Mode：VRRPv3 protocol mode.

Default：There is no configuration by default.

Usage Guide：This command is used to add an IPv6 address and interface to an existing backup group. The no operation of this command will delete the virtual IPv6 address and interface of the specified backup group. The virtual IPv6 address is the link local unicast address. There can only be one virtual IPv6 address in a backup group. In order to avoid the fault of returning physical MAC address when Pinging virtual IPv6 address, it is regulated that the virtual IPv6 address should not be the real IPv6 address of the

interface. Thus, the interfaces of all VRRPv3 backup groups are Backup by default, and need to select a Master within the backup groups

Example: Configure the virtual IPv6 address of the backup group as fe80::2, the interface is vlan1.

Switch(config-router)# virtual-ipv6 fe80::2 interface vlan 1

28.4 VRRPv3 Typical Examples
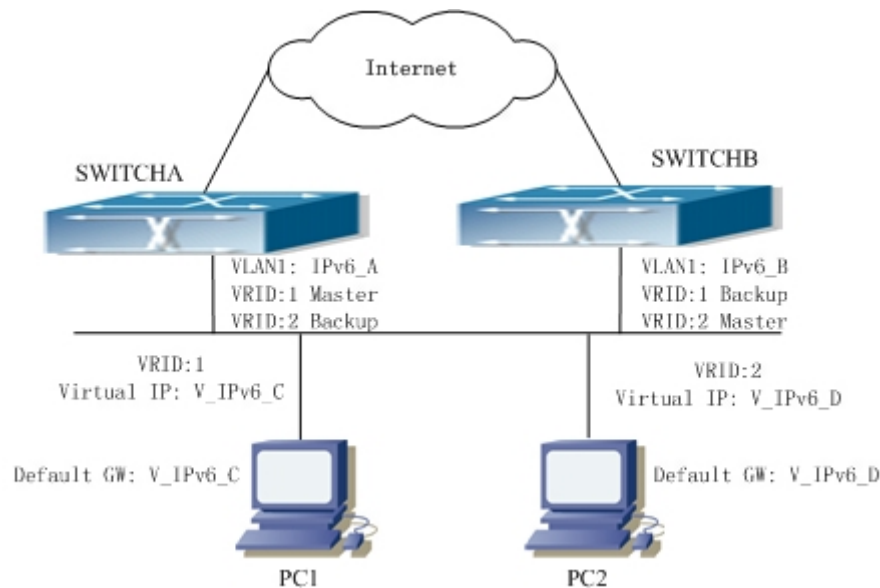
Fig 28-2 VRRPv3 Typical Network Topology

As shown in graph 2, switch A and switch B are backups to each other, switch A is the master of backup group 1 and a backup of backup group 2. Switch B is the master of backup group 2 and a Backup of backup group 1. The IPv6 addresses of switch A and switch B are "IPv6_A" and "IPv6_b" respectively (it is recommended that IPv6_A and IPv6_B are in the same segment), the virtual IPv6 address of backup group 1 and backup group are "V_IPv6_C" and "V_IPV6_D" respectively, and the default IPv6 gateway address are configured as "V_IPv6_C" and "V_IPv6_D" respectively (in reality, the IPv6 gateway address of hosts are usually learnt automatically via router advertisements, thus, the IPv6 next hop of the hosts will have some randomness). Doing this will not only implement router backup but also the flow sharing function in the LAN.

The configuration of switchA:

SwitchA(config)#ipv6 enable

SwitchA(config)#interface vlan 1

SwitchA(config)#router ipv6 vrrp 1

SwitchA(config-router)#virtual-ipv6 fe80::2 interface vlan 1

SwitchA(config-router)#priority 150

SwitchA(config-router)#enable

SwitchA(config)#router ipv6 vrrp 2

SwitchA(config-router)#virtual-ipv6 fe80::3 interface vlan 1

SwitchA(config-router)#enable

The configuration of switchB:

SwitchB(config)#ipv6 enable

SwitchB(config)#interface vlan 1

SwitchB(config)#router ipv6 vrrp 2

SwitchB(config-router)#virtual-ipv6 fe80::3 interface vlan 1

SwitchB(config-router)#priority 150

SwitchB(config-router)#enable

SwitchB(config)#router ipv6 vrrp 1

SwitchB(config-router)#virtual-ipv6 fe80::2 interface vlan 1

SwitchB(config-router)#enable

28.5 VRRPv3 Troubleshooting Help

When configuring and using VRRPv3 protocol, it might operate abnormally because of incorrect physical connections and configuration. So, users should pay attention to the following points:

☞ First, the physical connections should be correct;

☞ Next, the interface and link protocol are UP (use show ipv6 interface command);

☞ And then, make sure that IPv6 forwarding function is enabled (use ipv6 enable command)

☞ Besides, make sure that VRRPv3 protocol is enable on the interface;

☞ Check whether the time of timer in different routers (or layer-three Ethernet switches) within the same backup group is the same;

☞ Check whether the virtual IPv6 addresses in the same backup group is the same;

Chapter 29 MRPP Configuration

29.1 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.
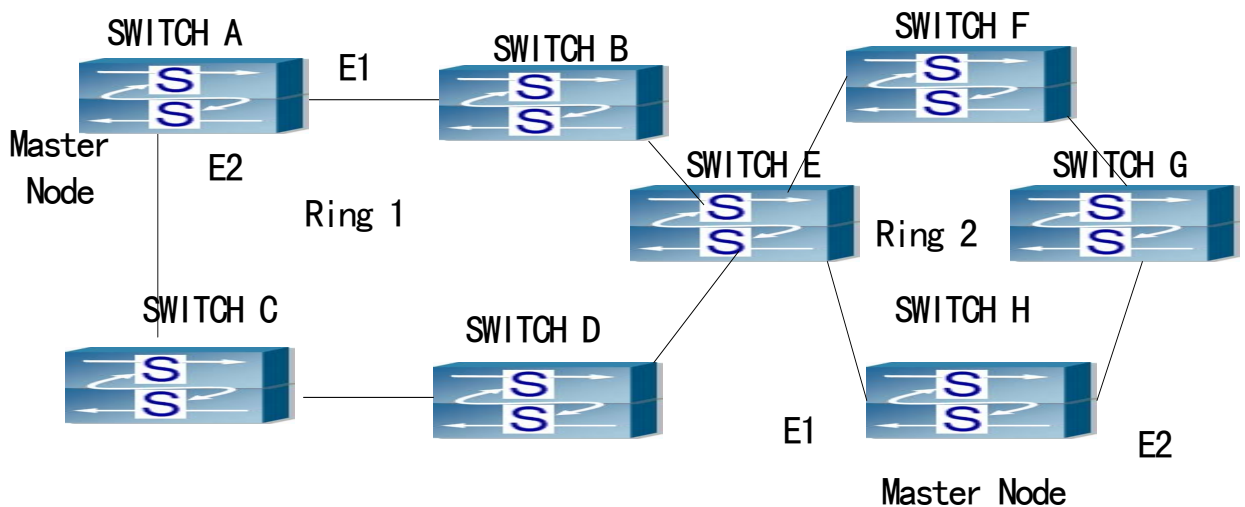
29.1.1 Conception Introduction

Fig 29-1MRPP 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.

29.1.2 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.

29.1.3 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.

29.2 MRPP Configuration Task Sequence

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.
**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
Interface Mode	
mrpp ring *<ring-id>* primary-port no mrpp ring *<ring-id>* primary-port	Specify MRPP ring primary-port.
mrpp ring *<ring-id>* secondary-port no mrpp ring *<ring-id>* secondary-port	Specify secondary of 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

29.3 Commands For MRPP

29.3.1 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

29.3.2 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.

The mrpp enable command must be start before the control-vlan command be used. If primary port, secondary port, node-mode and enable commands all be configured after control-vlan, the mrpp-ring function enabled.

Example： Configure control VLAN of mrpp ring 4000 is 4000.

Switch(config)# mrpp ring 4000

Switch(mrpp-ring-4000)#control-vlan 4000

29.3.3 debug mrpp

Command :debug mrpp

                no debug mrpp

Function： Open MRPP debug information; "no description" command disables MRPP debug inforamation

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

29.3.4 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 if the other command have configured, the MRPP ring enabled.

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)# node-mode master

Switch(mrpp-ring-4000)#fail-timer 18

Switch(mrpp-ring-4000)#hello-timer 6

Switch(mrpp-ring-4000)#enable

Switch(mrpp-ring-4000)#exit

Switch(config)#in ethernet 1/1

Switch(config-If-Ethernet1/1)#mrpp ring 4000 primary-port

Switch(config)#in ethernet 1/3

Switch(config-If-Ethernet1/3)#mrpp ring 4000 secondary-port

29.3.5 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

29.3.6 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

29.3.7 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

29.3.8 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 itcreate 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

29.3.9 mrpp port-scan-mode

Command: mrpp port-scan-mode {interrupt|pool}

            no mrpp port-scan-mode

Function: Set the scan mode of the mrpp port as "interrupt" or "pool".

Parameter: interrupt: the interrupt mode; pool: the pool mode.

Command Mode: Global Mode

Default : The default scan mode is active pool.

Example:

Switch(config)#mrpp enable

Switch(config)#mrpp port-scan-mode interrupt

29.3.10 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

29.3.11 mrpp ring primary-port

Command: mrpp ring *<ring-id>* primary-port

no mrpp ring *<ring-id>* primary-port

Function: Specify MRPP ring primary-port.

Parameter: *<ring-id>* is the ID of MRPP ring, range is <1-4094>.

Command Mode: Interface 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.

The mrpp enable command must be start before the control-vlan command be used. If primary port, secondary port, node-mode and enable commands all be configured after control-vlan, the mrpp-ring function enabled.

Example: Configure the primary of MRPP ring 4000 to Ethernet 1/1.

Switch(Config)# in ethernet 1/1

Switch(config-If-Ethernet1/1)#mrpp ring 4000 primary-port

29.3.12 mrpp ring secondary-port

Command: mrpp ring < *ring-id* > secondary-port

no mrpp ring < *ring-id* > secondary-port

Function: Specify secondary of MRPP ring.

Parameter: *<ring-id>* is the ID of MRPP ring, range is <1-4094>.

Command Mode: Interface 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.

The mrpp enable command must be start before the control-vlan command be used. If primary port, secondary port, node-mode and enable commands all be configured after control-vlan, the mrpp-ring function enabled.

Example: Configure secondary port of MRPP ring to 1/3.

Switch(Config)#in ethernet 1/3

Switch(config-If-Ethernet1/3)#mrpp ring 4000 secondary-port

29.3.13 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

29.3.14 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

29.4 MRPP typical scenario
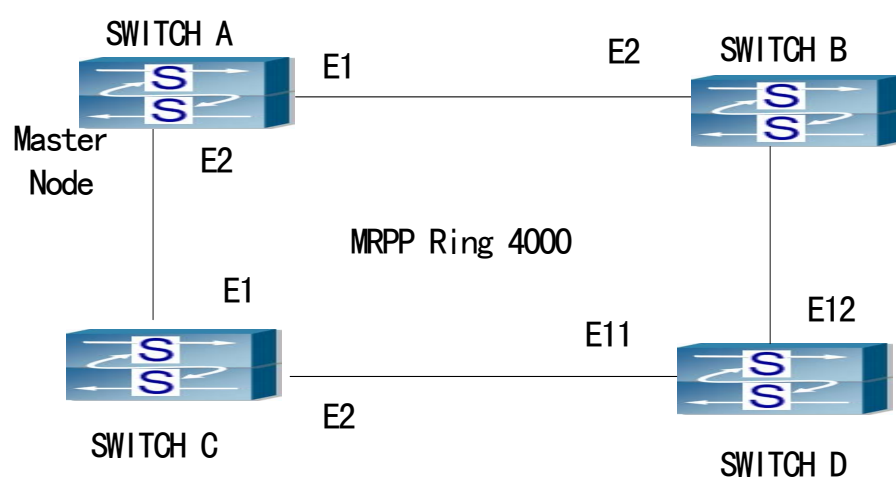
Fig   29-2 MRPP typical configuration scenario 1

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)#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)#interface ethernet 1/1

Switch(config-If-Ethernet1/1)#mrpp ring 4000 primary-port

Switch(config-If-Ethernet1/1)# interface ethernet 1/2

Switch(config-If-Ethernet1/2)#mrpp ring 4000 secondary-port

Switch(config-If-Ethernet1/2)#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)#enable

Switch(MRPP-ring-4000)#exit

Switch(config)#interface ethernet 1/1

Switch(config-If-Ethernet1/1)#mrpp ring 4000 primary-port

Switch(config-If-Ethernet1/1)# interface ethernet 1/2

Switch(config-If-Ethernet1/2)#mrpp ring 4000 secondary-port

Switch(config-If-Ethernet1/2)#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)#enable

Switch(MRPP-ring-4000)#exit

Switch(config)#interface ethernet 1/1

Switch(config-If-Ethernet1/1)#mrpp ring 4000 primary-port

Switch(config-If-Ethernet1/1)# interface ethernet 1/2

Switch(config-If-Ethernet1/2)#mrpp ring 4000 secondary-port

Switch(config-If-Ethernet1/2)#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)#enable

Switch(MRPP-ring-4000)#exit

Switch(config)#interface ethernet 1/1

Switch(config-If-Ethernet1/1)#mrpp ring 4000 primary-port

Switch(config-If-Ethernet1/1)# interface ethernet 1/2

Switch(config-If-Ethernet1/2)#mrpp ring 4000 secondary-port

Switch(config-If-Ethernet1/2)#exit

Switch(config)#

29.5 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 30 Cluster Configuration

30.1 Introduction To Cluster

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

30.2 Cluster Management Configuration Sequence

1. Enable or disable cluster function
2. Create cluster

1) Configure private IP address pool for member switches of the cluster

2) Create or delete cluster

3) Add or remove a member switch

3. Configure attributes of the cluster in the commander switch

1) Enable or disable automatically adding cluster members

2) Set automatically added members to manually added ones

3) Set or modify the time interval of keep-alive messages on switches in the cluster.

4) Set or modify the max number of lost keep-alive messages that can be tolerated

5) Clear the list of candidate switches maintained by the switch

4. Configure attributes of the cluster in the candidate switch

1) Set the time interval of keep-alive messages of the cluster

2) Set the max number of lost keep-alive messages that can be tolerated in the cluster

5. Remote cluster network management

1) Remote configuration management

2) Remotely upgrade member switch

3) Reboot member switch

6. Manage cluster network with web

1) Enable http

7. Manage cluster network with snmp

1) Enable snmp server

1.Enable or disable cluster

Command	Explanation
Global Mode	
cluster run[key <WORD>][vid <VID>] **no cluster run**	Enable or disable cluster function in the switch

2.Create a cluster

Command	Explanation
Global Mode	
cluster ip-pool<*commander-ip*> **no cluster ip-pool**	Configure the private IP addressed pool for cluster member devices
cluster commander [<cluster_name>] **no cluster commander**	Create or delete a cluster
cluster member {candidate-sn <candidate-sn> | mac-address <mac-addr> [id <member-id>]} **no cluster member {id <member-id> | mac-address <mac-addr>}**	Add or remove a member switch

3.Configure attributes of the cluster in the commander switch

Command	Explanation
Global Mode	
cluster auto-add **no cluster auto-add**	Enable or disable adding newly discovered candidate switch to the cluster
cluster member auto-to-user	Change automatically added members into manually added ones
cluster keepalive interval <second> **no cluster keepalive interval**	Set the keep-alive interval of the cluster
cluster keepalive loss-count <int> **no cluster keepalive loss-count**	Set the max number of lost keep-alive messages that can be tolerated in the cluster.
clear cluster nodes [nodes-sn <candidate-sn-list> | mac-address <mac-addr>]	Clear nodes in the list of candidate switches maintained by the switch

4. Configure attributes of the cluster in the candidate switch

Command	Explanation
Global Mode	
cluster keepalive interval <second> **no cluster keepalive interval**	Set the keep-alive interval of the cluster
cluster keepalive loss-count <int> **no cluster keepalive loss-count**	Set the max number of lost keep-alive messages that can be tolerated in the clusters

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 commander switch.
cluster reset member [id <member-id> | mac-address <mac-addr>]	In the commander switch, this command is used to reset the member switch.
cluster update member <member-id> <src-url> <dst-filename>[ascii|binary]	In the commander switch, this command is used to remotely upgrade the member switch.It can only upgrade nos.img file.

6. Manage cluster network with web

Command	Explanation
Global Mode	
ip http server	Enable http function in commander switch and member switch. Notice: must insure the http function be enabled in member switch when commander switch visiting member switch by web. The commander switch visit member switch via beat member node in member cluster topology.

7. Manage cluster network with snmp

Command	Explanation
Global Mode	
snmp-server enable	Enable snmp server function in commander switch and member switch. Notice: must insure the snmp server function be enabled in member switch when commander switch visiting member switch by snmp. The commander switch visit member switch via configure character string <commander-community>@sw<member id>.

30.3 Commands For Cluster

30.3.1 cluster run

Command: cluster run[key <WORD>][vid <VID>]

        no cluster run

Function: Enable cluster function; the "**no cluster run**" command disables cluster function.

Parameter：key：all keys in one cluster should be the same, no longer than 16 characters.

        vid：vlan id of the cluster, whose range is 1-4094.

Command mode: Global Mode

Default: Cluster function is disabled by default, key: NULL(\0) vid：1.

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. It is recommended that users allocate an exclusive vlan for cluster（such as vlan100）

Note：Routing protocols should be disabled on the layer-3 interface where cluster vlan locates to avoid broadcasting private route of the cluster.

Example: Disable cluster function in the local switch.

Switch (config)#no cluster run

30.3.2 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.

Parameters：*commander-ip* ：cluster IP address pool for allocating internal IP addresses of the cluster commander-ip is the head address of the address pool, of which the valid format is 10.x.x.x, in dotted-decimal notation; the address pool should be big enough to hold 128 members, which requires the last byte of addresses to be less than 126（254 – 128 = 126）。IP address pool should never be changed with commander configured. The change can only be done after the "no cluster commander" command being executed.

Command mode: Global Mode

Default: The default address pool is 10.254.254.1.

Usage Guide：When candidate switches becomes cluster members, the commander switch allocates a private IP address to each member for the communication within the cluster, and thus to realized its management and maintenance of cluster members. This command can only be used on non-commander switches. Once the cluster established, users can not modify its IP address pool. The NO command of this command will restore the address pool back to default value, which is 10.254.254.1.

Example: Set the private IP address pool used by cluster member devices as 10.254.254.10

Switch(config)#cluster ip-pool 10.254.254.10

30.3.3 cluster commander

Command: cluster commander *<cluster-name>*

       no cluster commander

Function: Set the switch as a commander switch, and create a cluster.

Parameter: *<cluster-name>* is the cluster's name, no longer than 32 characters.

Command mode: Global Mode

Default: Default setting is no commander switch. cluster_name is null by default.

Usage Guide：This command sets the role of a switch as commander switch and creates a cluster, which can only be executed on non commander switches. The cluster_name cannot be changed after the switch becoming a commander, and "no cluster commander" should be executed first to do that. The no operation of this command will cancel the

commander configuration of the switch.

Example: Set the current switch as the commander switch and name the cluster as admin.

Switch(config)#cluster commander admin

30.3.4 cluster member

Command: cluster member {nodes-sn <candidate-sn-list> | mac-address <mac-addr> [id <member-id>]}

           no cluster member {id <member-id> | mac-address <mac-addr>}

Function：On a commander switch, manually add candidate switches into the cluster created by it.

Parameters：nodes-sn：all cluster member switches as recorded in a chain list, each with a node sn which can be viewed by "show cluster candidates" command. One or more candidates can be added as member at one time. The valid range of candidate-sn-list is 1~256.

    mac-address：the CPU mac of candidate switches

    member-id：A member id can be specified to a candidate as it becomes a member, ranging from 1 to 128, increasing from 1 by default.

    nodes-sn is the automatically generated sn, which may change after the candidate becomes a member. Members added this way will be actually treated as those added in mac-addr mode with all config files in mac-addr mode.

    If more than one switch is added as member simultaneously, no member-id is allowed; neither when using nodes-sn mode.

Default：None.

Command Mode：Global Mode

Usage Guide：After executing this command, the switch will add those identified in *<nodes-sn>* or *<mac-address>*into the cluster it belongs to. One or more candidates are allowed at one time, linked with '-' or ';'. A switch can only be member or commander of one cluster, exclusively. Attempts to execute the command on a non commander switch will return error. The no operation of this command will delete the specified member switch, and turn it back to a candidate.

Example: In the commander switch, add the candidate switch which has the sequence number as 1. In the commander switch, add the switch whose the mac address is 11-22-33-44-55-66 to member, and the member-id is 5.

Switch(config)#cluster member nodes-sn 1

Switch(config)#cluster member mac-address 11-22-33-44-55-66 id 5

30.3.5 cluster auto-add

Command: cluster auto-add

        no cluster auto-add

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**" 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.

Usage Guide：After enabling this command on a commander switch, candidate switches will be automatically added as members.

Example: Enable the auto adding function in the commander switch.

Switch(config)#cluster auto-add

30.3.6 cluster member auto-to-user

Command：**cluster member auto-to-user**

Function：all members will be deleted when configuring no cluster auto-add. Users need to change automatically added members to manually added ones to keep them.

Parameter：None.

Default：None.

Command Mode：Global Mode.

Usage Guide：Execute this command on a switch to change automatically added members to manually added ones.

Example: change automatically added members to manually added ones.

Switch(config)#cluster member auto-to-user

30.3.7 cluster keepalive interval

Command: cluster keepalive interval *<second>*

        no cluster keepalive interval

Function：Configure the time interval of keepalive messages within the cluster.

Parameters：<second>: keepalive time interval, in seconds, ranging from 3 to 30.

Default：The default value is 30 seconds.

Command Mode：Global Configuration Mode

Usage Guide：After executing this command on a commander switch, the value of the parameter will be distributed to all member switches via the TCP connections between

the commander and members.

After executing it on a non commander switch, the configuration value will be saved but not used until the switch becomes a commander. Before that, its keepalive interval is the one distributed by its commander.

Commander will send DP messages within the cluster once in every keepalive interval. Members will respond to the received DP messages with DR messages.

The no operation of this command will restore the keepalive interval in the cluster back to its default value.

Example: Set the keepalive interval in the cluster to 10 seconds.

Switch(config)#cluster keepalive interval 10

30.3.8 cluster keepalive loss-count

Command: cluster keepalive loss-count*<loss-count>*

     no cluster keepalive loss-count

Function：Configure the max number of lost keepalive messages in a cluster that can be tolerated.

Parameters：loss-count：the tolerable max number of lost messages, ranging from 1 to 10.

Default：The default value is 3.

Command Mode：Global Configuration Mode

Usage Guide：After executing this command on a commander switch, the value of the parameter will be distributed to all member switches via the TCP connections between the commander and members.

After executing it on a non commander switch, the configuration value will be saved but not used until the switch becomes a commander. Before that, its loss-count value is the one distributed by its commander.

commander calculates the loss-count after sending each DP message by adding 1 to the loss-count of each switch and clearing that of a switch after receiving a DR message from the latter. When a loss-count reaches the configured value (3 by default) without receving any DR message, the commander will delete the switch from its candidate chain list.

If the time that a member fails to receive DP messages from the commander reaches loss-count, it will change its status to candidate.

The no operation of this command will restore the tolerable max number of lost keepalive messages in the cluster back to its default value: 3.

Example: Set the tolerable max number of lost keepalive messages in the cluster to 5.

Switch(config)#cluster keepalive loss-count 5

30.3.9 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>* commander the member id allocated by commander to each member, whose range is 1～128.

Command mode: Admin Mode

Usage Guide： After executing this command, users will remotely login to a member switch and enter Admin Mode on the latter. Use exit to quit the configuration interface of the member. Because of the use of internal private IP, telnet authentication will be omitted on member switches.This command can only be executed on commander switches.

Example: In the commander switch, enter the configuration interface of the member switch with mem-id 1.

Switch#rcommand member 1

30.3.10 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. This command can only be executed on member switches.

Example: In the member switch, enter the configuration interface of the commander switch.

Switch#rcommand commander

30.3.11 cluster update member

Command: cluster update member *<member-id> <src-url> <dst-filenamel>* **[ascii | binary]**

Function: Remotely upgrade member switches from the commander switch

Parameters： member-id：ranging from 1 to 128. Use hyphen "-" or semicolon "；" to specify more than one member;

   src-url：the location of source files to be copied;

dst-filename：the specified filename for saving the file in the switch flash;

ascii means that the file transmission follows ASCII standard; binary means that the file transmission follows binary standard, which is de default mode.

when src-url is a FTP address, its form will be: ftp://<username>:<password>@<ipadress>/<filename>，in which <username> is the FTP username <password> is the FTP password <ipadress> is the IP address of the FTP server,<filename> is the name of the file to be downloaded via FTP.

when src-url is a TFTP address, its form will be: tftp://<ipadress>/<filename>，in which <ipadress>is the IP address of the TFTP server <filename> is the name of the file to be downloaded via.

Special keywords used in filename：

Keywords	source or destination address
startup-config	start the configuration file
nos.img	system file

Command mode: Admin Mode

Usage Guide：The commander distributes the remote upgrade command to members via the TCP connections between them, causing the number to implement the remote upgrade and reboot. Trying to execute this command on a non-commander switch will return errors. If users want to upgrade more than one member, these switches should be the same type to avoid boot failure induced by mismatched IMG files.

Example: Remotely upgrade a member switch from the commander switch, with the member-id being 1 ， src-ul being ftp:// admin:admin @192.168.1.1/nos.img, and dst-url being nos.img

Switch#cluster update member 1 ftp:// admin:admin @192.168.1.1/nos.img nos.img

30.3.12 cluster reset member

Command: cluster reset member [id*<member-id>*|mac-address*<mac-addr>*]

Function: In the commander switch, this command can be used to reset the member switch.

Parameter: member-id：ranging from 1 to 128. Use hyphen "-" or semicolon "；" to specify more than one member; if no value is provided, it means to reboot all member switches.

Default： Boot all member switches.

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 1.

Switch#cluster reset member 1

30.3.13 clear cluster nodes

Command: clear cluster nodes [nodes-sn<candidate-sn-list>|mac-address <mac-addr>]

Function：Clear the nodes in the candidate list found by the commander switch.

Parameters: candidate-sn-list：sn of candidate switches, ranging from 1 to 256. More than one candidate can be specified.

mac-address：mac address of the switches (including all candidates, members and other switches).

Default：No parameter means to clear information of all switches.

Command Mode：Admin Mode.

Usage Guide：After executing this command, the information of this node will be deleted from the chain list saved on commander switch. In 30 seconds, the commander will recreate a cluster topology and re-add this node. But after being readded, the candidate id of the switch might change. The command can only be executed on commander switches

Example: Clear all candidate switch lists found by the commander switch.

Switch#clear cluster nodes

30.4 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
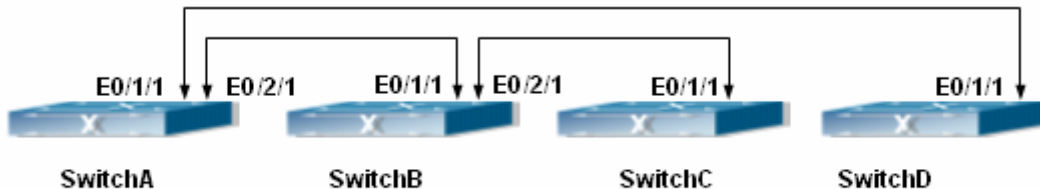
Fig 30-1 Examples of Cluster

Configuration Procedure

1. Configure the command switch

Configuration of SwitchA

Switch(config)#cluster run

Switch(config)#cluster ip-pool 10.254.254.30

Switch(config)#cluster commander 5526

Switch(config)#cluster auto-add

2. Configure the member switch

Configuration of SwitchB-SwitchD

Switch(config)#cluster run

30.5 Cluster Administration Troubleshooting

30.5.1 Cluster Debugging and Monitoring Command

30.5.1.1 show cluster

Command: show cluster

Function: Display cluster information of the switch.

Command Mode: Admin and Config Mode

Example: Execute this command on switches of different roles.

----in a commander----------------------------

Switch#show cluster

Status: Enabled

Cluster VLAN: 1

Role: commander

IP pool: 10.254.254.1

Cluster name: MIS_zebra

Keepalive interval: 30

Keepalive loss-count: 3

Auto add: Disabled

Number of Members: 0

Number of Candidates: 3

----in a member ----------------------------

Switch#show cluster

Status: Enabled

Cluster VLAN: 1

Role: Member

Commander Ip Address: 10.254.254.1

Internal Ip Address: 10.254.254.2

Commamder Mac Address: 00-12-cf-39-1d-90

---- a candidate ---------------------------

Switch#show cluster

Status: Enabled

Cluster VLAN: 1

Role: Candidate

---- disabled ---------------------------

Switch#show cluster

Status: Disabled

30.5.1.2 show cluster members

Command: show cluster members [id <member-id> | mac-address <mac-addr>]

Function: Display member information of a cluster. This command can only apply to commander switches.

Parameters：member-id: member id of the switch.

mac-addr: the CPU mac addresses of member switches.

Default：No parameters means to display information of all member switches.

Command Mode: Admin and Config Mode

Usage Guide： Executing this command on a commander switch will display the configuration information of all cluster member switches.

Example：Execute this command on a commander switch to display the configuration information of all and specified cluster member switches.

Switch#show cluster members

Member From : User config(U); Auto member (A)

ID	From	Status	Mac	Hostname	Description	Internal IP
xxx	x	xxxxxxxxxx12	xx-xx-xx-xx-xx-xx	xxxxxxxxxx12	xxxxxxxxxx12	xxx.xxx.xxx.xxx
1	U	Inactive	00-01-02-03-04-05	MIS_zebra	ES3528SPF	10.254.254.2
2	A	Active	00-01-02-03-04-05	MIS_bison	ES3528M	10.254.254.3
3	U	Active	00-01-02-03-04-05	SRD_jaguar	ES3528M	10.254.254.4
4	A	Inactive	00-01-02-03-04-05	HRD_puma	ES3528M	10.254.254.5

Switch#show cluster members id 1

Cluster Members:

ID: 1

Member status: Inactive member   (user_config)

IP Address: 10.254.254.2

MAC Address: 00-01-02-03-04-06

Description: ES3528M-SFP

Hostname: DSW102

30.5.1.3 show cluster candidates

Command: show cluster candidates [nodes-sn<candidate-sn-list> | mac-address <mac-addr>]

Function: Display the statistic information of the candidate member switches on the command switch

Parameter：candidate-sn-list：candidate switch sn, ranging from 1 to 256. More than one switch can be specified.

mac-address： mac address of the candidate switch

Default：No parameters means to display information of all member switches.

Command Mode: Admin and Config Mode

Usage Guide: Executing this command on the switch will display the information of the candidate member switches.

Example：Display configuration information of all cluster candidate switches.
Switch#show cluster candidates

Cluster Candidates:

SN   Mac   Description   Hostname

--- ---------------- ---------------------- -----------------------

xxx xx-xx-xx-xx-xx-xx xxxxxxxxxxxxxxxxxxxxxxx24 xxxxxxxxxxxxxxxxxxxxxx24

   1 00-01-02-03-04-06 ES3528M

   2 01-01-02-03-04-05 ES3528M   MIS_zebra

30.5.1.4 show cluster topology

Command: show cluster topology [root-sn<starting-node-sn> | nodes-sn <node-sn-list> | mac-address <mac-addr>]

Function：Display cluster topology information. This command only applies to commander switches.

Parameters：starting-node-sn：the starting node of the topology.

node-sn-list：the switch node sn.

mac-addr：the CPU mac address of the switch.

No parameters means to display all topology information.

Command Mode：Admin and Config Mode

Usage Guide：Executing this command on the commander switch will display the topology information with its starting node specified.

Example：Execute this command on the commander switch to display the topology

information under different conditions.

Switch#show cluster topology
Role: commander(CM);Member(M);Candidate(CA);Other commander(OC);Other member(OM)

LV	SN	Description	Hostname	Role	MAC_ADDRESS	Upstream local-port	Upstream remote-port	leaf node
==	==	===========	===========	==	================	============	============	=
x	xxx	xxxxxxxxxx12	xxxxxxxxxx12	xx	xx-xx-xx-xx-xx-xx	xxxxxxxxxx12	xxxxxxxxxx12	x
1	1	ES4626H	LAB_SWITCH_1	CM	01-02-03-04-05-01	-root-	-root-	-
	2	ES4626H	LAB_SWITCH_2	M	01-02-03-04-05-02	eth 1/1	eth 1/2	N
	3	ES4626H	LAB_SWITCH_3	CA	01-02-03-04-05-03	eth 1/1	eth 1/3	Y
	4	ES4626H	LAB_SWITCH_4	CA	01-02-03-04-05-04	eth 1/1	eth 1/4	Y
....								
2	2	ES4626H	LAB_SWITCH_2	M	01-02-03-04-05-02	eth 1/1	eth 1/2	-
	5	ES3528M	LAB_SWITCH_1	OC	01-02-03-04-05-13	eth 1/1	eth 1/2	Y
	6	ES3528M	LAB_SWITCH_1	OM	01-02-03-04-05-14	eth 1/1	eth 1/3	Y

Switch#show cluster topology root-sn 2

Role: commander(CM);Member(M);Candidate(CA);Other commander(OC);Other member(OM)

SN	Description	Hostname	Role	MAC_ADDRESS	Upstream local-port	Upstream remote-port	leaf node
==	===========	===========	==	================	============	============	=
* 2	ES4626H	LAB_SWITCH_2	M	01-02-03-04-05-02	eth 1/1	eth 1/2	-
5	ES3528M	LAB_SWITCH_1	OC	01-02-03-04-05-13	eth 1/1	eth 1/2	Y
6	ES3528M	LAB_SWITCH_1	OM	01-02-03-04-05-14	eth 1/1	eth 1/3	Y

Switch#show cluster topology nodes-sn 2

Toplogy role: Member

Member status: Active member (user-config)

SN: 2

MAC Address: 01-02-03-04-05-02

Description: ES4626H

Hostname   : LAB_SWITCH_2

Upstream local-port: eth 1/1

Upstream node: 01-02-03-04-05-01

Upstream remote-port:eth 1/2

Upstream speed: 100full

Switch#

Switch#show cluster topology mac-address 01-02-03-04-05-02

Toplogy role: Member

Member status: Active member (user-config)

SN: 2

MAC Address: 01-02-03-04-05-02

Description: ES4626H

Hostname   : LAB_SWITCH_2

Upstream local-port: eth 1/1

Upstream node: 01-02-03-04-05-01

Upstream remote-port:eth 1/2

Upstream speed: 100full

30.5.1.5 debug cluster

Command: debug cluster {statemachine | application| tcp }

**   no debug cluster {statemachine | application| tcp }**

Function：Enable the application debug of cluster; the no operation of this command will disable that.

Parameters：statemachine: print debug information when the switch status changes.

          Application: print debug information when there are users trying to configure the switch after logging onto it via SNMP, WEB.

          tcp: the tcp connection information between the commander members.

Default：None.

Command Mode：Admin Mode

Usage Guide：None.

Example：Enable the debug information of status change on the switch.

Swtich#debug cluster statemachine

30.5.1.6 debug cluster packets

Command: debug cluster packets {DP | DR | CP}{receive|send}

**   no debug cluster packets {DP | DR | CP}{receive|send}**

Parameters：DP：discovery messages

          DR：responsive messages

          CP：command messages

          receive：receive messages

          send: send messages.

Default：None.

Command Mode：Admin Mode

Usage Guide：Enable the debug information of cluster messages. After enabling classification, all DP, DR and CP messages sent or received in the cluster will be printed.

Example：Enable the debug information of receiving DP messages.

Switch#debug cluster packets DP receive

30.5.2 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) is enabled. If the ports connected the command switch and member switch belongs to the cluster vlan.

☞ Whether the connection between the command switch and the member switch is correct. We can use the debug command to check if the command and the member switches can receive and process related cluster admin packets correctly.