Contents

Part I

Basic Management Configuration

Chapter 1

Switch management

1.1 Management options

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

1.1.1 Out-of-Band management

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

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

Step 1: Setting up the environment.

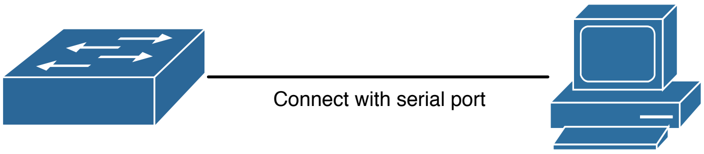


Figure 1.1: Out-of-band Management Configuration Environment

As shown in above, 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.
Serial port cable	One end attach to the RS-232 serial port, the other end to the Console port.
Switch	Functional Console port required.

Step 2: Starting the Terminal Emulation Software

Before you power on the switch, start the terminal emulation session so that you can see the output display from the power-on self-test(POST). The terminal-emulation software - frequently a

PC application such as Hyperterminal or PuTTY - makes communication between the switch and your PC or terminal possible.

1. Start the terminal-emulation program and open a session if you are using a PC or terminal.
2. Start a terminal-emulation session.
3. Configure the baud rate and character format of the PC or terminal to match the console port default characteristics:

- 9600 baud
- 8 data bits
- 1 stop bit
- No parity
- None (flow control)

Step 3: Entering switch CLI interface
Power on the switch, the following appears in the terminal-emulation window, that is the CLI configuration mode for Switch.

```
System is booting, please wait...



Bootrom version: 7.1.2

Creation date: Jun 21 2013 - 14:47:31


Testing RAM...
0x01000000 RAM OK.


Loading flash:/nos.img ...
## Booting kernel from Legacy Image at 82000100 ...
   Image Name:   Linux-2.6.21
   Created:      2013-06-21  11:45:11 UTC
   Image Type:   MIPS Linux Kernel Image (lzma compressed)
   Data Size:    6628641 Bytes = 6.3 MiB
   Load Address: 80001000
   Entry Point:  80210000
   Verifying Checksum ... OK
   Uncompressing Kernel Image ... OK

Starting kernel ...
```

```
BusyBox v1.19.3 (2012-06-14 09:58:25 CST) built-in shell (ash)
Enter 'help' for a list of built-in commands.

Current time is Sun Jan 01 00:00:00 2006

Orion Alpha A26 Series Switch Operating System
Software Version 7.0.3.1(R0073.0000)
Compiled Jun 21 19:21:22 2013

26 Ethernet/IEEE 802.3 interface(s)

Mac Addr f8-f0-82-00-11-22

Loading factory config ...

Orion Alpha A26>
```

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, or using HTTP, or using SNMP management software to configure the switch. 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.

Management via Telnet

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

1. Switch has an IPv4/IPv6 address configured;
2. The host IP address (Telnet client) and the switch's VLAN interface IPv4/IPv6 address is in the same network segment;
3. If 2) is not met, Telnet client can connect to an IPv4/IPv6 address of the switch via other devices, such as a router.

The switch is a Layer 2 switch that can be configured with several IP addresses, the configuration method refers to the relative chapter. 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(IPV4 address example):

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 VLAN1 interface IP address is

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 with the specified Telnet target.
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 that in the Console interface.

Management via HTTP

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

1. Switch has an IPv4/IPv6 address configured;
2. The host IPv4/IPv6 address (HTTP client) and the switch's VLAN interface IPv4/IPv6 address are in the same network segment;
3. If 2) is not met, HTTP client should connect to an IPv4/IPv6 address of the switch via other devices, such as a router.

Similar to management the switch via Telnet, as soon as the host succeeds to ping/ping6 an IPv4/IPv6 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 server function on the switch.

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

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

```
Switch>enable
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**;

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. Input the IPv6 address of the switch is http://[3ffe:506:1:2::3] and the address should draw together with the square brackets.

Step 3: Login to the switch.

Login to the Web configuration interface. Valid login name and password are required, otherwise the switch will reject HTTP 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 web 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>enable
Switch#config
Switch(config)#username admin privilege 15 password 0 admin
Switch(config)#authentication line web login local
```

Notice: When configure the switch, the name of the switch is composed with English letters.

Manage the Switch via SNMP Network Management Software

The necessities required by SNMP network management software to manage switches:

1. IP addresses are configured on the switch;
2. The IP address of the client host and that of the VLAN interface on the switch it subordinates to should be in the same segment;
3. If 2) is not met, the client should be able to reach an IP address of the switch through devices like routers;
4. SNMP should be enabled.

The host with SNMP network management software should be able to ping the IP address of the switch, so that, when running, SNMP network management software will be able to find it and implement read/write operation on it. Details about how to manage switches via SNMP network management software will not be covered in this manual.

1.2 CLI Interface

The switch provides three management interface for users: CLI (Command Line Interface) interface, Web interface, Snmp network management software. We will introduce the CLI interface and Web configuration interface in details, Web interface is familiar with CLI interface function and will not be covered.

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

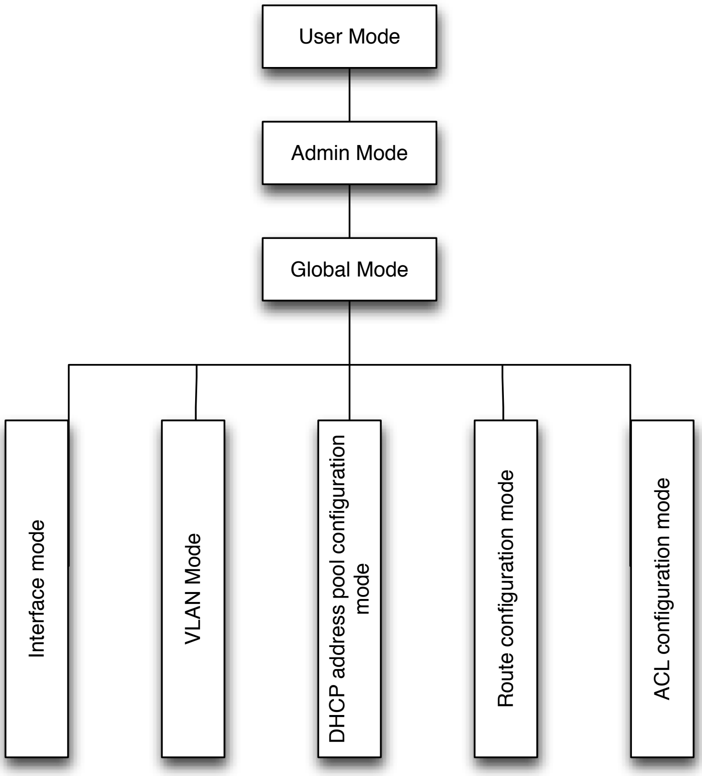


Figure 1.2: Shell Configuration Modes

1.2.1 Configuration Modes

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 exit 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.

Admin Mode

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

Under Admin Mode, 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.

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 and STP, etc. And the user can go further to Port Mode for configuration of all the interfaces.

Interface Mode

Use the interface command under Global Mode can enter the interface mode specified. Switch provides three interface type: 1. VLAN interface; 2. Ethernet port; 3. port-channel, accordingly the three interface configuration modes.

Interface Type	Entry	Operates	Exit
VLAN Interface	Type **interface vlan <Vlan-id>** command under Global Mode.	Configure switch IPs, etc	Use the **exit** command to return to Global Mode.
Ethernet Port	Type **interface ethernet <interface-list>** command under Global Mode.	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.	Configure port-channel related settings such as duplex mode, speed, etc.	Use the **exit** command to return to Global Mode.

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.

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.

ACL Mode

ACL type	Entry	Operates	Exit

Standard IP ACL Mode	Type **ip access-list standard** command under Global Mode.	Configure parameters for Standard IP ACL Mode.	Use the **exit** command to return to Global Mode.
Extended IP ACL Mode	Type **ip access-list extended** command under Global Mode.	Configure parameters for Extended IP ACL Mode.	Use the **exit** command to return to Global Mode.

1.2.2 Configuration Syntax

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

```
cmdtxt <variable> {enum1 | ... | enumN } [option1 | ... | optionN]
```

Conventions:
cmdtxt 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
textbf[option1 | … | optionN] indicate an optonal 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 version**, 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.
- **firewall { enable | disable }**, user can enter firewall enable or firewall disable for this command.
- **snmp-server community { ro | rw } <string>**, the followings are possible:

  ```
  snmp-server community ro <string>
  ```

  ```
  snmp-server community rw <string>
  ```

1.2.3 Shortcut Key Support

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

Key(s)	**Function**
BackSpace	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 this key to modify an entered command.
Right "→"	The cursor moves one character to the right. You can use this key to modify an entered command.
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.

1.2.4 Help Function

There are two ways in Switch for the user to access help information: the **help** command and the **?**.

Access to Help	**Usage and function**
Help	Under any command line prompt, type in **help** and press Enter will get a brief description of the associated help system.
"?"	1. Under any command line prompt, enter **?** to get a command list of the current mode and related brief description. 2. Enter a textbf? after the command keyword with an 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.

1.2.5 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.

1.2.6 Fuzzy Match Support

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

For example:

1. For command **show interfaces status ethernet1/1**, typing **sh in status ethernet1/1** will work.

2. However, for command **show running-config**, the system will report a **> Ambiguous command!** error if only **show r** is entered, as Shell is unable to tell whether it is **show run** or **show running-config**. Therefore, Shell will only recognize the command if **sh ru** is entered.

Chapter 2

Basic Switch Configuration

2.1 Basic Configuration

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

Command	Explanation
Normal User Mode / Admin Mode	
enable [<1-15>] disable	The User uses enable command to step into admin mode from normal user mode or modify the privilege level of the users. 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.
show privilege	Show privilege of the current users.
Except User Mode / Admin Mode	
end	Quit current mode and return to Admin mode when not at User Mode/ Admin Mode.
Admin Mode	
clock set <HH:MM:SS> [YYYY.MM.DD]	Set system date and time.
show version	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.
show cpu usage	Show CPU usage rate.
show cpu utilization	Show current CPU utilization rate.
show memory usage	Show memory usage rate.
Global Mode	
banner motd <LINE> no banner motd	Configure the information displayed when the login authentication of a telnet or console user is successful.

2.2 Telnet Management

2.2.1 Telnet

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. Switch can be either the Telnet Server or the Telnet client.

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

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

Telnet Configuration Task List

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

1. Configure Telnet Server

Command	Explanation
Global Mode	
telnet-server enable no telnet-server enable	Enable the Telnet server function in the switch: the no command disables the Telnet function.
username <user-name> [privilege <privilege>] [password [0 | 7] <password>] no username <username>	Configure user name and password of the telnet. The no form command deletes the telnet user authorization.
aaa authorization config-commands no aaa authorization config-commands	Enable command authorization function for the login user with VTY (login with Telnet and SSH). The no command disables this function. Only enabling this command and configuring command authorization manner, it will request to authorize when executing some command.
authentication securityip <ip-addr> no authentication securityip <ip-addr>	Configure the secure IP address to login to the switch through Telnet: the no command deletes the authorized Telnet secure address.
authentication securityipv6 <ipv6-addr> no authentication securityipv6 <ipv6-addr>	Configure IPv6 security address to login to the switch through Telnet; the no command deletes the authorized Telnet security address.

authentication ip access-class { <num-std> | <name> } no authentication ip access-class	Binding standard IP ACL protocol to login with Telnet/SSH/Web; the no form command will cancel the binding ACL.
authentication ipv6 access-class { <num-std> | <name> } no authentication ipv6 access-class	Binding standard IPv6 ACL protocol to login with Telnet/SSH/Web; the no form command will cancel the binding ACL.
authentication line { console | vty | web } login method1 [method2 …] no authentication line { console | vty | web } login	Configure authentication method list with telnet.
authentication enable method1 [method2 …] no authentication enable	Configure the enable authentication method list.
authorization line { console | vty | web } exec method1 [method2 …] no authorization line { console | vty | web } exec	Configure the authorization method list with telnet.
authorization line vty command <1-15> { local | radius | tacacs } (none |) no authorization line vty command <1-15>	Configure command authorization manner and authorization selection priority of login user with VTY (login with Telnet and SSH). The no command recovers to be default manner.
accounting line { console | vty } command <1-15> { start-stop | stop-only | none } method1 [method2…] no accounting line { console | vty } command <1-15>	Configure the accounting method list.
Admin Mode	
terminal monitor terminal no monitor	Display debug information for Telnet client login to the switch; the no command disables the debug information. show users Show the user information who logs in through telnet or ssh. It includes line number, user name and user IP.
clear line vty <0-31>	Delete the logged user information on the appointed line, force user to get down the line who logs in through telnet or ssh.

2. Telnet to a remote host from the switch

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

2.2.2 SSH

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.

SSH Server Configuration Task List

Command	Explanation
Global Mode	
ssh-server enable no ssh-server enable	Enable SSH function on the switch; the no command disables SSH function.
username <username> [privilege <privilege>] [password [0 | 7] <password>] no username <username>	Configure the username and password of SSH client software for logging on the switch; the no command deletes the username.
ssh-server timeout <timeout> no ssh-server timeout	Configure timeout value for SSH authentication; the no 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 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 terminal no monitor	Display SSH debug information on the SSH client side; the no command stops displaying SSH debug information on the SSH client side.
show crypto key	Show the secret key of ssh.
crypto key clear rsa	Clear the secret key of ssh.

Example of SSH Server Configuration

Example 1:

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)#username test privilege 15 password 0 test
```

In IPv6 networks, the terminal should run SSH client software which support IPv6, such as putty6. Users should not modify the configuration of the switch except allocating an IPv6 address for the local host.

2.3 Configure Switch IP Addresses

All Ethernet ports of switch are 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. Switch provides three IP address configuration methods:

- Manual
- BOOTP
- DHCP

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

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

2.3.1 Switch IP Addresses Configuration Task List

1. Enable VLAN port mode
2. Manual configuration
3. BOOTP configuration
4. DHCP configuration

1. Enable VLAN port mode

Command	Explanation
Global Mode	
interface vlan <vlan-id> no interface vlan <vlan-id>	Create VLAN interface (layer 3 interface); the no command deletes the VLAN interface.

2. Manual configuration

Command	Explanation
VLAN Interface Mode	
ip address <ip-address> <mask> [secondary] no ip address <ip-address> <mask> [secondary]	Configure IP address of VLAN interface; the no command deletes IP address of VLAN interface.
ipv6 address <ipv6-address / prefix-length> [eui-64] no ipv6 address <ipv6-address / prefix-length>	Configure IPv6 address, including aggregation global unicast address, local site address and local link address. The no command deletes IPv6 address.

3. BOOTP configuration

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

4. DHCP configuration

Command	Explanation
VLAN Interface Mode	
ip bootp-client enable no ip bootp-client enable	Enable the switch to be a DHCP client and obtain IP address and gateway address through DHCP negotiation; the no command disables the DHCP client function.

2.4 SNMP Configuration

2.4.1 Introduction to SNMP

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

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

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

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

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

NMS sends queries to the Agent with Get-Request, Get-Next-Request, Get-Bulk-Request and Set-Request messages; and the Agent, upon receiving the requests, replies with Get-Response message. On some special situations, like network device ports are on Up/Down status or the network topology changes, Agents can send Trap messages to NMS to inform the abnormal events. Besides, NMS can also be set to alert to some abnormal events by enabling RMON function. When alert events are triggered, Agents will send Trap messages or log the event according to the settings. Inform-Request is mainly used for inter-NMS communication in the layered network management.

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

VACM is used to classify the user's 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.

2.4.2 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.

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.

2.4.3 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).

2.4.4 SNMP Configuration

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
Global Mode	
snmp-server enabled no snmp-server enabled	Enable the SNMP Agent function on the switch; the no command disables the SNMP Agent function on the switch.

2. Configure SNMP community string

Command	Explanation
Global Mode	
snmp-server community { ro | rw } { 0 | 7 } <string> [access { <num-std> | <name> }] [ipv6-access { <ipv6-num-std> | <ipv6-name> }] [read <read-view-name>] [write <write-view-name>] no snmp-server community <string> [access { <num-std> | <name> }] [ipv6-access { <ipv6-num-std> | <ipv6-name> }]	Configure the community string for the switch; the no command deletes the configured community string.

3. Configure IP address of SNMP management station

Command	Explanation
Global Mode	

snmp-server securityip { <ipv4-address> | <ipv6-address> }
no snmp-server securityip { <ipv4-address> | <ipv6-address> }
	Configure IPv4/IPv6 security address which is allowed to access the switch on the NMS; the no command deletes the configured security 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
Global Mode	
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
Global Mode	
snmp-server user <use-string> <group-string> [{ authPriv | authNoPriv } auth { md5 | sha } <word>] [access { <num-std> | <name> }] [ipv6-access { <ipv6-num-std> | <ipv6-name> }] no snmp-server user <user-string> [access { <num-std> | <name> }] [ipv6-access { <ipv6-num-std> | <ipv6-name> }]	Add a user to a SNMP group. This command is used to configure USM for SNMP v3.

6. Configure group

Command	Explanation
Global Mode	
snmp-server group <group-string> { noauthnopriv | authnopriv | authpriv } [[read <read-string>] [write <write-string>] [notify <notify-string>]] [access { <num-std> | <name> }] [ipv6-access { <ipv6-num-std> | <ipv6-name> }] no snmp-server group <group-string> { noauthnopriv | authnopriv | authpriv } [access { <num-std> | <name> }] [ipv6-access { <ipv6-num-std> | <ipv6-name> }]	Set the group information on the switch. This command is used to configure VACM for SNMP v3.

7. Configure view

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

8. Configuring TRAP

Command	Explanation
Global Mode	
snmp-server enable traps no snmp-server enable traps	Enable the switch to send Trap message. This command is used for SNMP v1/v2/v3.

Command	Explanation
Global Mode	
snmp-server host { <host-ipv4-address> | <host-ipv6-address> } { v1 | v2c | { v3 { noauthnopriv | authnopriv | authpriv } } } <user-string> no snmp-server host { <host-ipv4-address> | <host-ipv6-address> } {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. The `no` form of this command cancels this IPv4 or IPv6 address.

snmp-server trap-source { <ipv4-address> | <ipv6-address> }
no snmp-server trap-source { <ipv4-address> | <ipv6-address> }
	Set the source IPv4 or IPv6 address which is used to send trap packet, the no command deletes the configuration.

9. Enable/Disable RMON

Command	Explanation
Global Mode	
rmon enable no rmon enable	Enable/disable RMON.

2.4.5 Typical SNMP Configuration Examples

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 enable
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 usertrap).

The configuration on the switch is listed below:

```
Switch(config)#snmp-server enable
Switch(config)#snmp-server host 1.1.1.5 v1 usertrap
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 authPriv auth md5 hellotst
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 enable
Switch(config)#snmp-server host 10.1.1.2 v3 authpriv tester
Switch(config)#snmp-server enable traps
```

Scenario 5: The IPv6 address of the NMS is **2004:1:2:3::2**; the IPv6 address of the switch (Agent) is **2004:1:2:3::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 enable
Switch(config)#snmp-server community rw private
Switch(config)#snmp-server community ro public
Switch(config)#snmp-server securityip 2004:1:2:3::2
```

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 6: 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 usertrap).

The configuration on the switch is listed below:

```
Switch(config)#snmp-server host 2004:1:2:3::2 v1 usertrap
Switch(config)#snmp-server enable traps
```

2.4.6 SNMP Troubleshooting

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

- Good condition of the physical connection.
- Interface and datalink layer protocol is Up (use the **'show interface'** command), and the connection between the switch and host can be verified by ping (use **'ping'** command).
- The switch enabled SNMP Agent server function (use **'snmp-server'** command)
- Secure IP for NMS (use **'snmp-server securityip'** command) and community string (use **'snmp-server community'** command) are correctly configured, as any of them fails, SNMP will not be able to communicate with NMS properly.

- If Trap function is required, remember to enable Trap (use **'snmp-server enable traps'** command). And remember to properly configure the target host IP address and community string for Trap (use **'snmp-server host'** command) to ensure Trap message can be sent to the specified host.
- If RMON function is required, RMON must be enabled first (use **'rmon enable'** command).
- Use **'show snmp'** command to verify sent and received SNMP messages; Use **'show snmp status'** command to verify SNMP configuration information; Use **'debug snmp packet'** to enable SNMP debugging function and verify debug information.

If users still can't solve the SNMP problems, Please contact our technical and service center.

2.5 Switch Upgrade

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

2.5.1 Switch System Files

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

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

The boot file is for initiating the switch, namely what we usually call the ROM update file (It can be compressed into IMG file if it is of large size). In switch, the boot file is allowed to save in ROM only. Switch mandates the name of the boot file to be **boot.rom**.

The update method of the system image file and the boot file is the same. The switch supplies the user with two modes of updating:

1. BootROM mode;
2. TFTP and FTP update at Shell mode.

This two update method will be explained in details in following two sections.

2.5.2 BootROM Upgrade

There is one method for BootROM upgrade: TFTP which can be configured at BootROM command.

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 TFTP server software installed and has the image file required for the upgrade.

Step 2:

Press **'Ctrl+b'** on switch boot up until the switch enters BootROM monitor mode. The operation result is shown below:

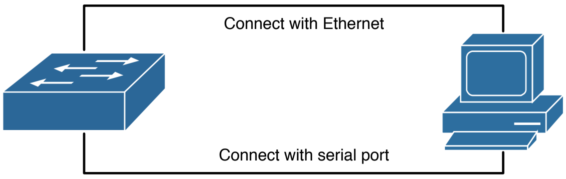


Figure 2.1: Typical topology for switch upgrade in BootROM mode

```
[Boot]:
```

Step 3:

Under BootROM mode, run **'setconfig'** to set the IP address and mask of the switch under BootROM mode and server IP address. Suppose the switch address is **192.168.1.2**, and PC address is **192.168.1.66**, and 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
[Boot]:
```

Step 4:

Enable TFTP server in the PC. Run TFTP server program. Before start downloading upgrade file to the switch, verify the connectivity between the server and the switch by ping from the switch. 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 update file boot.rom.

```
[Boot]: load boot.rom
Using switch device
TFTP from server 192.168.1.66; our IP address is 192.168.1.2
Filename 'boot.rom'.
Load address: 0x82000000
Loading: #################################################################
 ################################
done
Bytes transferred = 496240 (79270 hex)
[Boot]:
```

Step 5:

Execute write boot.rom in BootROM mode. The following saves the update file.

```
[Boot]: write boot.rom
File exists, overwrite? (Y/N)[N] y

Writing flash:/boot.rom......
Write flash:/boot.rom OK.

[Boot]:
```

Step 6:
The following is the configuration for the system update image file.

```
[Boot]: load nos.img
Using switch device
TFTP from server 192.168.1.66; our IP address is 192.168.1.2
Filename 'nos.img'.
Load address: 0x82000000
Loading: ###########
done
Bytes transferred = 51635 (c9b3 hex)
[Boot]:
```

Step 7:
Execute write nos.img in BootROM mode. The following saves the system update image file.

```
[Boot]: write nos.img
File exists, overwrite? (Y/N)[N] y

Writing flash:/nos.img.............................................
...............................................................
Write flash:/nos.img OK.

[Boot]:
```

Step 8:
After successful upgrade, execute run or reboot 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
  5399893   nos.img

1 file(s), 0 dir(s)

Total size:6995456 bytes , used size:5422080 bytes, free size:1573376 bytes
[Boot]:
```

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

```
[Boot]: boot img nos.img primary
flash:/nos.img will be used as the primary img file at the next time!

[Boot]: show boot-files
The primary img file : flash:/nos.img
The backup img file : flash:/nos.img

The startup-config file: NULL

[Boot]:
```

2.5.3 FTP/TFTP Upgrade

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

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

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

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

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

FTP/TFTP clients, as file list service as FTP server.

Here are some terms frequently used in FTP/TFTP.

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

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

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

System file: including system image file and boot file.

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

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

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

Start up configuration file: refers to the configuration sequence used in switch startup. Startup configuration file stores in nonvolatile storage, corresponding to the so-called configuration save. If the device does not support CF, the configuration file stores in FLASH only, if the device supports CF, the configuration file stores in FLASH or CF, if the device supports multi-config file, names the configuration file to be .cfg file, the default is startup.cfg. If the device does not support multi-config file, mandates the name of startup configuration file to be startup-config.

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

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

FTP/TFTP Configuration

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

FTP/TFTP Configuration Task List

1. FTP/TFTP client configuration

   (a) Upload/download the configuration file or system file.

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

2. FTP server configuration

(a) Start FTP server

(b) Configure FTP login username and password

(c) Modify FTP server connection idle time

(d) Shut down FTP server

3. TFTP server configuration

(a) Start TFTP server

(b) Configure TFTP server connection idle time

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

(d) Shut down TFTP server

1. FTP/TFTP client configuration
(a)FTP/TFTP client upload/download file

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

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

Command	Explanation
Admin Mode	
ftp-dir <ftpServerUrl>	For FTP client, server file list can be checked. FtpServerUrl format looks like: ftp://user:password@IPv4|IPv6 Address.

2. FTP server configuration
(a)Start FTP server

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

(b)Configure FTP login username and password

Command	Explanation
Global Mode	
ip ftp username <username> password [0 | 7] <password> no ip ftp username <username>	Configure FTP login username and password; this no command will delete the username and password.

(c)Modify FTP server connection idle time

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

3. TFTP server configuration

(a)Start TFTP server

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

(b)Modify TFTP server connection idle time

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

(c)Modify TFTP server connection retransmission time

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

FTP/TFTP Configuration Examples

The configuration is same for IPv4 address or IPv6 address. The example only for IPv4 address.

Fig 2 3 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 **'superuser'**. Place the `12_30_nos.img` file to the appropriate FTP server directory on the computer.

The configuration procedures of the switch are listed below:

```
Switch(config)#interface vlan 1
Switch(Config-if-Vlan1)#ip address 10.1.1.2 255.255.255.0
Switch(Config-if-Vlan1)#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 **'12_30_nos.img'** file to the appropriate TFTP server directory on the computer.

The configuration procedures of the switch are listed below:

```
Switch(config)#interface vlan 1
Switch(Config-if-Vlan1)#ip address 10.1.1.2 255.255.255.0
Switch(Config-if-Vlan1)#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 are listed below:

```
Switch(config)#interface vlan 1
Switch(Config-if-Vlan1)#ip address 10.1.1.2 255.255.255.0
Switch(Config-if-Vlan1)#no shut
Switch(Config-if-Vlan1)#exit
Switch(config)#ftp-server enable
Switch(config)#username Admin password 0 superuser
```

Computer side configuration:

Login to the switch with any FTP client software, with the username **'Switch'** and password **'superuser'**, 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 are listed below:

```
Switch(config)#interface vlan 1
Switch(Config-if-Vlan1)#ip address 10.1.1.2 255.255.255.0
Switch(Config-if-Vlan1)#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: Switch acts as FTP client to view file list on the FTP server. Synchronization conditions: The switch connects to a computer by an Ethernet port, the computer is a FTP server with an IP address of **10.1.1.1**; the switch acts as a FTP client, and the IP address of the switch management VLAN1 interface is **10.1.1.2**.

FTP Configuration:

PC side:

Start the FTP server software on the PC and set the username **'Switch'**, and the password **'superuser'**.

Switch:

```
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#copy ftp://Switch:superuser@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
...(some display omitted here)
show.txt
snmp.TXT
226 Transfer complete.
```

FTP/TFTP Troubleshooting

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

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

```
220 Serv-U FTP-Server v2.5 build 6 for WinSock ready...
331 User name okay, need password.
230 User logged in, proceed.
200 PORT Command successful.
```

```
nos.img file length = 1526021
read file ok
send file
150 Opening ASCII mode data connection for nos.img.
226 Transfer complete.
close ftp client.
```

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

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

- If the switch is upgrading system file or system start up file through FTP, the switch must not be restarted until **'close ftp client'** or **'226 Transfer complete.'** is displayed, indicating upgrade is successful, otherwise the switch may be rendered unable to start. If the system file and system start up file upgrade through FTP fails, please try to upgrade again or use the BootROM mode to upgrade.

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

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

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

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

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

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

Part II

Port Configuration

Chapter 3

Port Configuration

3.1 Introduction to Port

Switch contains Cable ports and Combo ports. The Combo ports can be configured to as either 1000GX-TX ports or SFP Gigabit fiber ports.

If the user needs to configure some network ports, he/she can use the **interface ethernet <interface-list>** command to enter the appropriate Ethernet port configuration mode, where **<interface-list>** stands for one or more ports. If **<interface-list>** contains multiple ports, special characters such as **';'** or **'-'** can be used to separate ports, **';'** is used for discrete port numbers and **'-'** is used for consecutive port numbers. Suppose an operation should be performed on ports 2,3,4,5 the command would look like: **interface ethernet 1/2-5**. Port speed, duplex mode and traffic control can be configured under Ethernet Port Mode causing the performance of the corresponding network ports to change accordingly.

3.2 Network Port Configuration Task List

1. Enter the network port configuration mode
2. Configure the properties for the network ports
   (a) Configure combo mode for combo ports
   (b) Enable/Disable ports
   (c) Configure port names
   (d) Configure port cable types
   (e) Configure port speed and duplex mode
   (f) Configure bandwidth control
   (g) Configure traffic control
   (h) Enable/Disable port loopback function
   (i) Configure broadcast storm control function for the switch
   (j) Configure scan port mode
   (k) Configure rate-violation control of the port

(l) Configure interval of port-rate-statistics

3. Virtual cable test

1. Enter the Ethernet port configuration mode

Command	Explanation
Global Mode	
interface ethernet <interface-list>	Enters the network port configuration mode.

2. Configure the properties for the Ethernet ports

Command	Explanation
Port Mode	
media-type { copper | copper-preferred-auto | fiber | sfp-preferred-auto }	Sets the combo port mode (combo ports only).
shutdown no shutdown	Enables/Disables specified ports.
description <string> no description	Specifies 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 by combo port and fiber port of switch.
speed-duplex { auto [10 [100 [1000]] [auto | full | half |]] | 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]] } | force10g-full } 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.
negotiation { on | off }	Enables/Disables the auto-negotiation function of 1000Base-FX ports.
bandwidth control <bandwidth> [both | receive | transmit] no bandwidth control	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.

storm-control { unicast | broadcast | multicast } <Kbits>	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.

switchport flood-control { bcast|mcast|ucast }
no switchport flood-control { bcast|mcast|ucast }
	Configure that switch does not transmit broadcast, unknown multicast or unknown unicast packets any more to the specified port; no command restores the default configuration.

port-scan-mode { interrupt | poll } no port-scan-mode	Configure port-scan-mode as interrupt or poll mode, the no command restores the default port-scan-mode.
rate-violation <200-2000000> [recovery <0-86400>] no rate-violation	Set the max packet reception rate of a port. If the rate of the received packet violates the packet reception rate, shut down this port and configure the recovery time, the default is 300s. The no command will disable the rate-violation function of a port.
switchport discard packet { all | untag } no switchport discard packet { all | untag }	Configure the port not to receive any packet or untag; the no command cancel the restriction of discard, it means the port is allowed to receive any packet or untag.
port-rate-statistics interval <interval-value>	Configure the interval of port-rate-statistics.

3. Virtual cable test

Command	Explanation
Admin Mode	
virtual-cable-test interface ethernet <interface-list>	Test virtual cables of the port.

3.3 Port Configuration Example

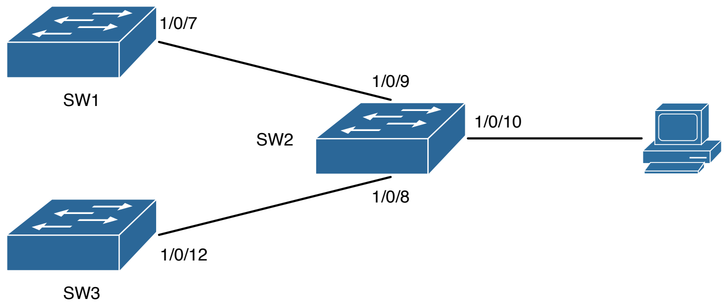


Figure 3.1: Port Configuration Example

No VLAN has been configured in the switches, default VLAN1 is used.

Switch	Port	Property
Switch1	1/7	Ingress bandwidth limit: 50 M
Switch2	1/8	Mirror source port
	1/9	100Mbps full, mirror source port
	1/10	1000Mbps full, mirror destination port
Switch3	1/12	100Mbps full

The configurations are listed below:
Switch1:

```
Switch1(config)#interface ethernet 1/7
Switch1(Config-If-Ethernet1/7)#bandwidth control 50000 both
```

Switch2:

```
Switch2(config)#interface ethernet 1/9
Switch2(Config-If-Ethernet1/9)#speed-duplex force100-full
Switch2(Config-If-Ethernet1/9)#exit
Switch2(config)#interface ethernet 1/10
Switch2(Config-If-Ethernet1/10)#speed-duplex force1g-full
Switch2(Config-If-Ethernet1/10)#exit
Switch2(config)#monitor session 1 source interface ethernet 1/8;1/9
Switch2(config)#monitor session 1 destination interface ethernet 1/10
```

Switch3:

```
Switch3(config)#interface ethernet 1/12
Switch3(Config-If-Ethernet1/12)#speed-duplex force100-full
Switch3(Config-If-Ethernet1/12)#exit
```

3.4 Port Troubleshooting

Here are some situations that frequently occurs in port configuration and the advised solutions:

- Two connected fiber interfaces won't link up if one interface is set to auto-negotiation but the other to forced speed/duplex. This is determined by IEEE 802.3.
- The following combinations are not recommended: enabling traffic control as well as setting multicast limiting for the same port; setting broadcast, multicast and unknown destination unicast control as well as port bandwidth limiting for the same port. If such combinations are set, the port throughput may fall below the expected performance.

Chapter 4

Port Isolation Function Configuration

4.1 Introduction to Port Isolation Function

Port isolation is an independent port-based function working in an inter-port way, which isolates flows of different ports from each other. With the help of port isolation, users can isolate ports within a VLAN to save VLAN resources and enhance network security. After this function is configured, the ports in a port isolation group will be isolated from each other, while ports belonging to different isolation groups or no such group can forward data to one another normally. No more than 16 port isolation groups can a switch have.

4.2 Task Sequence of Port Isolation

1. Create an isolate port group
2. Add Ethernet ports into the group
3. Display the configuration of port isolation

1. Create an isolate port group

Command	Explanation
Global Mode	
isolate-port group <WORD> no isolate-port group <WORD>	Set a port isolation group; the no operation of this command will delete the port isolation group.

2. Add Ethernet ports into the group

Command	Explanation
Global Mode	
isolate-port group <WORD> switchport interface [ethernet] <IFNAME> no isolate-port group <WORD> switchport interface [ethernet] <IFNAME>	Add one port or a group of ports into a port isolation group to isolate, which will become isolated from the other ports in the group; the no operation of this command will remove one port or a group of ports out of a port isolation group.

3. Display the configuration of port isolation

Command	Explanation
Admin Mode and Global Mode	
show isolate-port group [<WORD>]	Display the configuration of port isolation, including all configured port isolation groups and Ethernet ports in each group.

4.3 Port Isolation Function Typical Examples

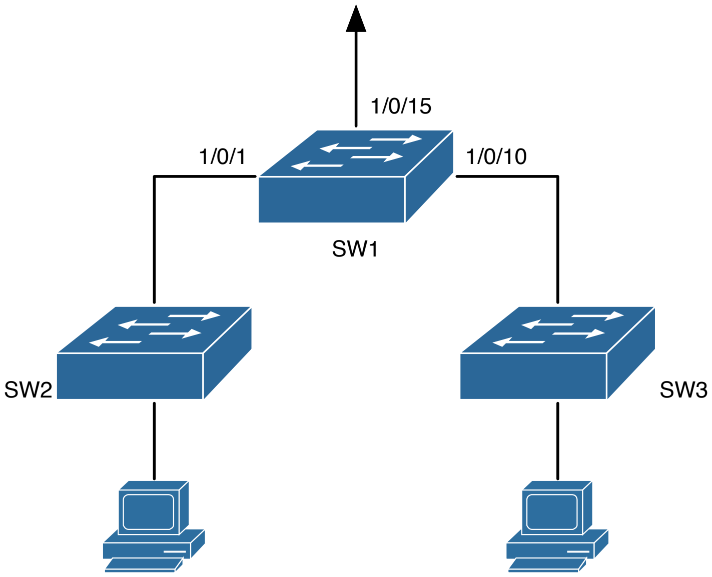


Figure 4.1: Typical example of port isolation function

The topology and configuration of switches are showed in the figure above, with e1/1, e1/10 and e1/15 all belonging to VLAN 100. The requirement is that, after port isolation is enabled on switch S1, e1/1 and e1/10 on switch S1 can not communicate with each other, while both of them can communicate with the uplink port e1/15. That is, the communication between any pair of downlink ports is disabled while that between any downlink port and a specified uplink port is normal. The uplink port can communicate with any port normally. The configuration of S1:

```
Switch(config)#isolate-port group test
Switch(config)#isolate-port group test switchport interface ethernet 1/1;1/10
```

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 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 the 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 the loopback-detection control mode (automatic recovery enabled or not)**

Command	Explanation
Global Mode	
loopback-detection control-recovery timeout <0-3600>	Configure the loopback-detection control mode (automatic recovery enabled or not) or recovery time.

5.3 Port Loopback Detection Function Example

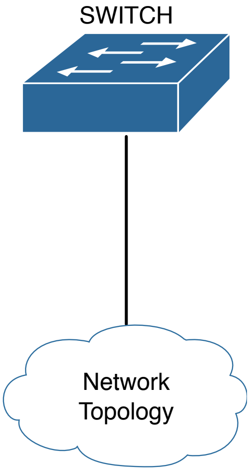


Figure 5.1: Typical example of port loopback detection function

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 corresponding relation between the spanning tree instance and the VLAN should be configured.

```
Switch(config)#spanning-tree
Switch(config)#spanning-tree mst configuration
Switch(Config-Mstp-Region)#instance 1 vlan 1
Switch(Config-Mstp-Region)#instance 2 vlan 2
Switch(Config-Mstp-Region)#
```

5.4 Port Loopback Detection Troubleshooting

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

Chapter 6

ULDP Function Configuration

6.1 Introduction to ULDP Function

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.

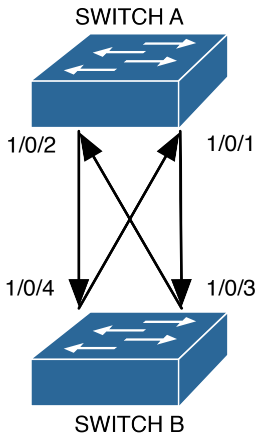


Figure 6.1: Fiber Cross Connection

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.

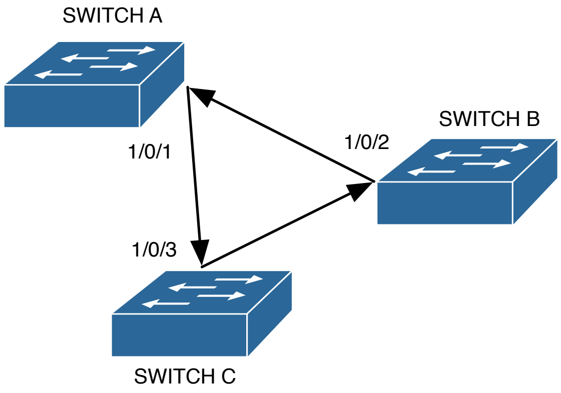


Figure 6.2: One End of Each Fiber Not Connected

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. Besides, ULDP provides the reset mechanism, when the port is disabled by ULDP, it can check again through reset mechanism. 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. Enable ULDP function globally
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 link
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. Enable ULDP function globally

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 link

Command	Explanation
Global Configuration Mode	
uldp manual-shutdown no uldp manual-shutdown	Configure the method to shut down unidirectional link.

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 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 reset, ranging from 30 to 86400 seconds. The value is 0 second by default.

8. **Reset the port shut down by ULDP**

Command	Explanation
Global configuration mode or port configuration mode	
uldp reset	Reset all ports in global configuration mode; Reset 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 information 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 can be received and sent on the specified port.

6.3 ULDP Function Typical Examples

In the network topology in Graph, 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
```

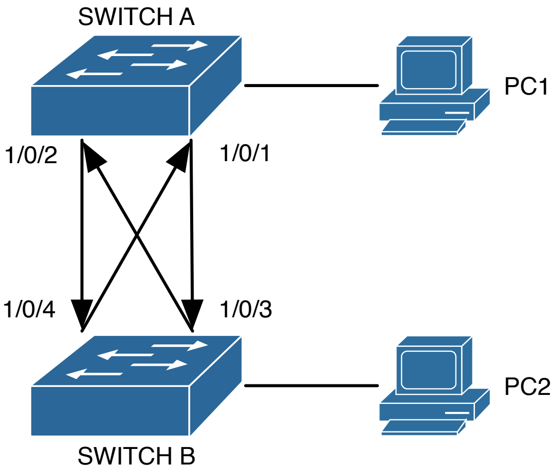


Figure 6.3: Fiber Cross Connection

```
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 ethernet1/3
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 shutted 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 shutted down!
    %Oct 29 11:09:50 2007 Unidirectional port Ethernet1/2 shutted 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 PC2.

```
    %Oct 29 11:09:50 2007 A unidirectional link is detected!  Port Ethernet1/3 need
to be shutted down!
    %Oct 29 11:09:50 2007 Unidirectional port Ethernet1/3 shutted down!
    %Oct 29 11:09:50 2007 A unidirectional link is detected!  Port Ethernet1/4 need
to be shutted down!
    %Oct 29 11:09:50 2007 Unidirectional port Ethernet1/4 shutted down!
```

6.4 ULDP Troubleshooting

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-channel, 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

LLDP Function Operation Configuration

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 of LLDP messages 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
Global 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, 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 configuration mode	
clear lldp remote-table	Clear Remote-table of the port.

7.3 LLDP Function Typical 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.

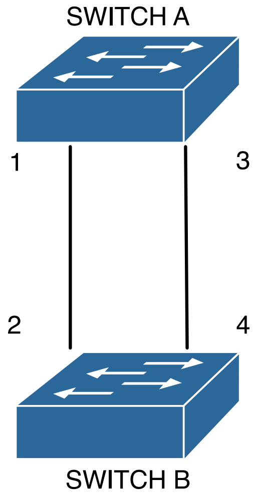


Figure 7.1: LLDP Function Typical Configuration Example

SWITCH A configuration task sequence:

```
SwitchA(config)# lldp enable
SwitchA(config)#interface ethernet 1/4
SwitchA(Config-If-Ethernet1/4)#lldp transmit optional tlv portDesc sysCap
SwitchA(Config-If-Ethernet1/4)exit
```

SWITCH B configuration task sequence:

```
SwitchB(config)#lldp enable
SwitchB(config)#interface ethernet1/1
SwitchB(Config-If-Ethernet1/1)#lldp mode receive
SwitchB(Config-If-Ethernet1/1)#exit
```

7.4 LLDP Function Troubleshooting

- 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.

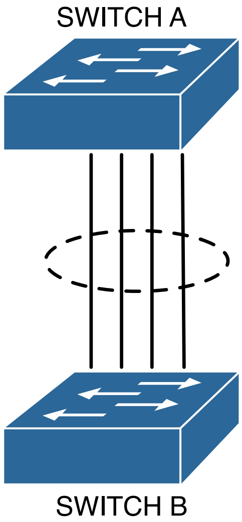


Figure 8.1: Port aggregation

As shown in the above, S1 is aggregated to a Port Channel, the bandwidth of this Port Channel is the total of all the four ports. If traffic from S1 needs to be transferred to S2 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.

Switch offers two 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, or are all Hybrid ports.
- If the ports are all TRUNK ports or Hybrid ports, then their **Allowed VLAN** and **Native VLAN** property should also be the same.

If Port Channel is configured manually or dynamically on switch, the system will automatically set the port with the smallest number to be Master Port of the Port Channel. If the spanning tree function is enabled in the switch, the spanning tree protocol will regard Port Channel as a logical port and send BPDU frames via the master port.

Port aggregation is closely related with switch hardware. Switch allow physical port aggregation of any two switches, maximum 14 groups and 8 ports in each port group are supported.

Once ports are aggregated, they can be used as a normal port. Switch have a built-in aggregation interface configuration mode, the user can perform related configuration in this mode just like in the VLAN and physical interface configuration mode.

8.2 Brief Introduction to LACP

LACP (Link Aggregation Control Protocol) is a kind of protocol based on IEEE802.3ad standard to implement the link dynamic aggregation. LACP protocol uses LACPDU (Link Aggregation Control Protocol Data Unit) to exchange the information with the other end.

After LACP protocol of the port is enabled, this port will send LACPDU to the other end to notify the system priority, the MAC address of the system, the priority of the port, the port ID and the operation Key. After the other end receives the information, the information is compared with the saving information of other ports to select the port which can be aggregated, accordingly, both sides can reach an agreement about the ports join or exit the dynamic aggregation group.

The operation Key is created by LACP protocol according to the combination of configuration (speed, duplex, basic configuration, management Key) of the ports to be aggregated.

After the dynamic aggregation port enables LACP protocol, the management Key is 0 by default. After the static aggregation port enables LACP, the management Key of the port is the same with the ID of the aggregation group.

For the dynamic aggregation group, the members of the same group have the same operation Key, for the static aggregation group, the ports of Active have the same operation Key.

The port aggregation is that multi-ports are aggregated to form an aggregation group, so as to implement the out/in load balance in each member port of the aggregation group and provides the better reliability.

8.2.1 Static LACP Aggregation

Static LACP aggregation is enforced by users configuration, and do not enable LACP protocol. When configuring static LACP aggregation, use **on** mode to force the port to enter the aggregation group.

8.2.2 Dynamic LACP Aggregation

1. The summary of the dynamic LACP aggregation

Dynamic LACP aggregation is an aggregation created/deleted by the system automatically, it does not allow the user to add or delete the member ports of the dynamic LACP aggregation. The ports which have the same attribute of speed and duplex, are connected to the same device, have the same basic configuration, can be dynamically aggregated together. Even if only one port can create the dynamic aggregation, that is the single port aggregation. In the dynamic aggregation, LACP protocol of the port is at the enable state.

2. The port state of the dynamic aggregation group

In dynamic aggregation group, the ports have two states: selected or standby. Both selected ports and standby ports can receive and send LACP protocol, but standby ports can not forward the data packets.

Because the limitation of the max port number in the aggregation group, if the current number of the member ports exceeds the limitation of the max port number, then the system of this end will negotiates with the other end to decide the port state according to the port ID. The negotiation steps are as follows:

Compare ID of the devices (the priority of the system + the MAC address of the system). First, compare the priority of the systems, if they are same, then compare the MAC address of the systems. The end with a small device ID has the high priority.

Compare the ID of the ports (the priority of the port + the ID of the port). For each port in the side of the device which has the high device priority, first, compare the priority of the ports, if the priorities are same, then compare the ID of the ports. The port with a small port ID is selected, and the others become the standby ports.

In an aggregation group, the port which has the smallest port ID and is at the selected state will be the master port, the other ports at the selected state will be the member port.

8.3 Port Channel Configuration Task List

1. Create a port group in Global Mode
2. Add ports to the specified group from the Port Mode of respective ports
3. Enter port-channel configuration mode
4. Set load-balance method for port-group
5. Set the system priority of LACP protocol
6. Set the port priority of the current port in LACP protocol
7. Set the timeout mode of the current port in LACP protocol

1. **Creating a port group**

Command	Explanation
Global mode	
port-group <port-group-number> no port-group <port-group-number>	Create or delete a port 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	Add the ports to the port group and set their mode.

3. **Enter port-channel configuration mode.**

Command	Explanation
Global mode	
interface port-channel <port-channel-number>	Enter port-channel configuration mode.

4. **Set load-balance method for port-group**

Command	Explanation
Aggregation port configuration mode	
load-balance { src-mac | dst-mac | dst-src-mac | src-ip | dst-ip | dst-src-ip }	Set load-balance for port-group.

5. **Set the system priority of LACP protocol**

Command	Explanation
Global mode	
lacp system-priority <system-priority> no lacp system-priority	Set the system priority of LACP protocol, the no command restores the default value.

6. **Set the port priority of the current port in LACP protocol**

Command	Explanation
Port mode	
lacp port-priority <port-priority> no lacp port-priority	Set the port priority in LACP protocol. The no command restores the default value.

7. Set the timeout mode of the current port in LACP protocol

Command	Explanation
Port mode	
lacp timeout { short | long } no lacp timeout	Set the timeout mode in LACP protocol. The no command restores the default value.

8.4 Port Channel Examples

Scenario 1: Configuring Port Channel in LACP.

The switches in the description below are all switch and as shown in the figure, ports 1, 2, 3, 4 of S1 are access ports and add them to group1 with active mode. Ports 6, 8, 9, 10 of S2 are access ports and add them to group2 with passive mode. All the ports should be connected with cables.

The configuration steps are listed below:

```
Switch1#config
Switch1(config)#interface ethernet 1/1-4
Switch1(Config-If-Port-Range)#port-group 1 mode active
Switch1(Config-If-Port-Range)#exit
Switch1(config)#interface port-channel 1
Switch1(Config-If-Port-Channel1)#

Switch2#config
Switch2(config)#port-group 2
Switch2(config)#interface ethernet 1/6
Switch2(Config-If-Ethernet1/6)#port-group 2 mode passive
Switch2(Config-If-Ethernet1/6)#exit
Switch2(config)#interface ethernet 1/8-10
Switch2(Config-If-Port-Range)#port-group 2 mode passive
Switch2(Config-If-Port-Range)#exit
Switch2(config)#interface port-channel 2
Switch2(Config-If-Port-Channel2)#
```

Configuration result:

Shell prompts ports aggregated successfully after a while, now ports 1, 2, 3, 4 of S1 form an aggregated port named **Port-Channel1**, ports 6, 8, 9, 10 of S2 form an aggregated port named **Port-Channel2**; can be configured in their respective aggregated port mode.

Scenario 2: Configuring Port Channel in ON mode.

As shown in the figure, ports 1, 2, 3, 4 of S1 are access ports and add them to group1 with **on** mode. Ports 6, 8, 9, 10 of S2 are access ports and add them to group2 with **on** mode.

The configuration steps are listed below:

```
Switch1#config
Switch1(config)#interface ethernet 1/1
Switch1(Config-If-Ethernet1/1)#port-group 1 mode on
```

```
Switch1(Config-If-Ethernet1/1)#exit
Switch1(config)#interface ethernet 1/2
Switch1(Config-If-Ethernet1/2)#port-group 1 mode on
Switch1(Config-If-Ethernet1/2)#exit
Switch1(config)#interface ethernet 1/3
Switch1(Config-If-Ethernet1/3)#port-group 1 mode on
Switch1(Config-If-Ethernet1/3)#exit
Switch1(config)#interface ethernet 1/4
Switch1(Config-If-Ethernet1/4)#port-group 1 mode on
Switch1(Config-If-Ethernet1/4)#exit

Switch2#config
Switch2(config)#port-group 2
Switch2(config)#interface ethernet 1/6
Switch2(Config-If-Ethernet1/6)#port-group 2 mode on
Switch2(Config-If-Ethernet1/6)#exit
Switch2(config)#interface ethernet 1/8-10
Switch2(Config-If-Port-Range)#port-group 2 mode on
Switch2(Config-If-Port-Range)#exit
```

Configuration result:

Add ports 1, 2, 3, 4 of S1 to port-group1 in order, and we can see a group in **on** mode is completely joined forcedly, switch in other ends won't exchange LACP PDU to complete aggregation. Aggregation finishes immediately when the command to add port 1/2 to port-group 1 is entered, port 1 and port 2 aggregate to be port-channel 1, when port 1/3 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, when port 1/4 joins port-group 1, port-channel 1 of port 1, 2 and 3 are ungrouped and re-aggregate with port 4 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 S1 and S2 are aggregated in **on** mode and become an aggregated port respectively.

8.5 Port Channel Troubleshooting

If problems occur when configuring port aggregation, please first check the following for causes.

- Ensure all ports in a port group have the same properties, i.e., whether they are in full-duplex mode, forced to the same speed, and have the same VLAN properties, etc. If inconsistency occurs, make corrections.
- Some commands cannot be used on a port in port-channel, such as arp, bandwidth, ip, ip-forward, etc.

Chapter 9

MTU Configuration

9.1 Introduction to MTU

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 1519-9000 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 discard the Jumbo frames sent to CPU in the packet receiving process.

9.2 MTU Configuration Task Sequence

1. Configure enable MTU function

Command	Explanation
Global mode	
mtu [<mtu-value>] no mtu enable	Configure the MTU size of JUMBO frame, enable the receiving/sending function of JUMBO frame. The no command disables sending and receiving function of MTU frames.

Chapter 10

EFM OAM Configuration

10.1 Introduction to EFM OAM

Ethernet is designed for Local Area Network at the beginning, but link length and network scope is extended rapidly while Ethernet is also applied to Metropolitan Area Network and Wide Area Network along with development. Due to lack the effectively management mechanism, it affects Ethernet application to Metropolitan Area Network and Wide Area Network, implementing OAM on Ethernet becomes a necessary development trend.

There are four protocol standards about Ethernet OAM, they are 802.3ah (EFM OAM), 802.3ag (CFM), E-LMI and Y.1731. EFM OAM and CFM are set for IEEE organization. EFM OAM works in data link layer to validly discover and manage the data link status of rock-bottom. Using EFM OAM can effectively advance management and maintenance for Ethernet to ensure the stable network operation. CFM is used for monitoring the whole network connectivity and locating the fault in access aggregation network layer. Compare with CFM, Y.1731 standard set by ITU (International Telecommunications Union) is more powerful. E-LMI standard set by MEF is only applied to UNI. So above protocols can be used to different network topology and management, between them exist the complementary relation.

EFM OAM (Ethernet in the First Mile Operation, Administration and Maintenance) works in data link layer of OSI model to implement the relative functions through OAM sublayer, figure is as bleow:

OAM protocol data units (OAMPDU) use destination MAC address 01-80-c2-00-00-02 of protocol, the max transmission rate is 10Pkt/s.

EFM OAM is established on the basis of OAM connection, it provides a link operation management mechanism such as link monitoring, remote fault detection and remote loopback testing, the simple introduction for EFM OAM in the following:

10.1.1 Ethernet OAM connection establishment

Ethernet OAM entity discovers remote OAM entities and establishes sessions with them by exchanging Information OAMPDUs. EFM OAM can operate in two modes: active mode and passive mode. One session can only be established by the OAM entity working in the active mode and ones working in the passive mode need to wait until it receives the connection request. After an Ethernet OAM connection is established, the Ethernet OAM entities on both sides exchange Information OAMPDUs continuously to keep the valid Ethernet OAM connection. If an Ethernet

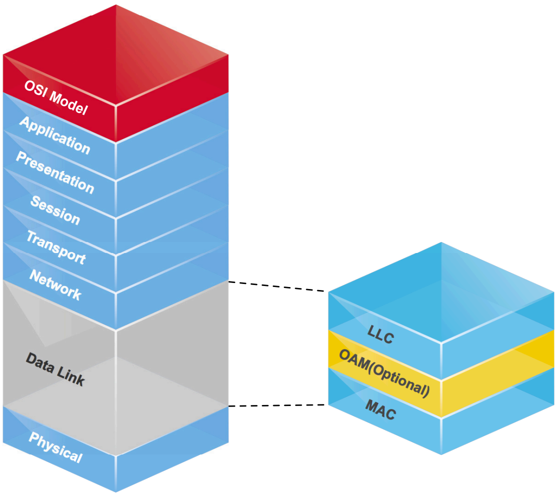


Figure 10.1: OAM location in OSI model

OAM entity receives no Information OAMPDU for five seconds, the Ethernet OAM connection is disconnected.

10.1.2 Link Monitoring

Fault detection in an Ethernet is difficult, especially when the physical connection in the network is not disconnected but network performance is degrading gradually. Link monitoring is used to detect and discover link faults in various environments. EFM OAM implements link monitoring through the exchange of Event Notification OAMPDUs. When detecting a link error event, the local OAM entity sends an Event Notification OAMPDU to notify the remote OAM entity. At the same time it will log information and send SNMP Trap to the network management system. While OAM entity on the other side receives the notification, it will also log and report it. With the log information, network administrators can keep track of network status in time.

The link event monitored by EFM OAM means that the link happens the error event, including Errored symbol period event, Errored frame event, Errored frame period event, Errored frame seconds event.

Errored symbol period event: The errored symbol number can not be less than the low threshold. (Symbol: the min data transmission unit of physical medium. It is unique for coding system, the symbols may be different for different physical mediums, symbol rate means the changed time of electron status per second.)

Errored frame period event: Specifying N is frame period, the errored frame number within the period of receiving N frames can not be less than the low threshold. (Errored frame: Receiving the errored frame detected by CRC.)

Errored frame event: The number of detected error frames over M seconds can not be less than the low threshold.

Errored frame seconds event: The number of error frame seconds detected over M seconds can not be less than the low threshold. (Errored frame second: Receiving an errored frame at least in a second.)

10.1.3 Remote Fault Detection

In a network where traffic is interrupted due to device failures or unavailability, the flag field defined in Ethernet OAMPDUs allows an Ethernet OAM entity to send fault information to its peer. As Information OAMPDUs are exchanged continuously across established OAM connections, an Ethernet OAM entity can inform one of its OAM peers of link faults through Information OAMPDUs. Therefore, the network administrator can keep track of link status in time through the log information and troubleshoot in time.

There are three kinds of link faults for Information OAMPDU, they are Critical Event, Dying Gasp and Link Fault, and their definitions are different for each manufacturer, here the definitions are as below:

Critical Event: EFM OAM function of port is disabled.

Link Fault: The number of unidirectional operation or fault can not be less than the high threshold in local. Unidirectional Operation means unidirectional link can not work normally on full-duplex link without autonegotiaction. EFM OAM can detect the fault and inform the remote OAM peers through sending Information OAMPDU.

Dying Gasp: There is no definition present. Although device does not generate Dying Gasp OAMPDU, it still receives and processes such OAMPDU sent by its peer.

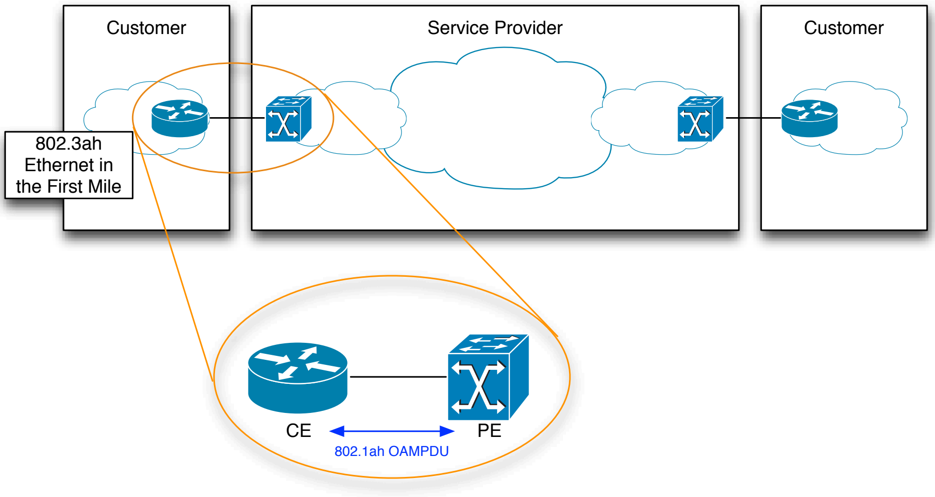


Figure 10.2: Typical OAM application topology

10.1.4 Remote loopback testing

Remote loopback testing is available only after an Ethernet OAM connection is established. With remote loopback enabled, operating Ethernet OAM entity in active mode issues remote loopback requests and the peer responds to them. If the peer operates in loopback mode, it returns all packets except Ethernet OAMPDUs to the senders along the original paths. Performing remote loopback testing periodically helps to detect network faults in time. Furthermore, performing remote loopback testing by network segments helps to locate network faults. Note: The communication will not be processed normally in remote loopback mode.

Typical EFM OAM application topology is in the following, it is used for point-to-point link and emulational IEEE 802.3 point-to-point link. Device enables EFM OAM through point-to-point connection to monitor the link fault in the First Mile with Ethernet access. For user, the connection between user to telecommunication is **the First Mile**, for service provider, it is **the Last Mile**.

10.2 EFM OAM Configuration

EFM OAM configuration task list

1. Enable EFM OAM function of port
2. Configure link monitor
3. Configure remote failure

Note: it needs to enable OAM first when configuring OAM parameters.

1. Enable EFM OAM function of port

Command	Explanation
Port mode	
ethernet-oam mode { active | passive }	Configure work mode of EFM OAM, default is active mode.
ethernet-oam no ethernet-oam	Enable EFM OAM of port, no command disables EFM OAM of port.
ethernet-oam period <seconds> no ethernet-oam period	Configure transmission period of OAMPDU (optional), no command restores the default value.
ethernet-oam timeout <seconds> no ethernet-oam timeout	Configure timeout of EFM OAM connection, no command restores the default value.

2. Configure link monitor

Command	Explanation
Port mode	
ethernet-oam link-monitor no ethernet-oam link-monitor	Enable link monitor of EFM OAM, no command disables link monitor.

ethernet-oam errored-symbol-period { threshold low <low-symbols> | window <seconds> }
no ethernet-oam errored-symbol-period { threshold low | window }
	Configure the low threshold and window period of errored symbol period event, no command resotores the default value. (optional)

ethernet-oam errored-frame-period { threshold low <low-frames> | window <seconds> }
no ethernet-oam errored-frame-period { threshold low | window }
	Configure the low threshold and window period of errored frame period event, no command resotores the default value.

Command	Explanation
Port mode	

ethernet-oam errored-frame { threshold low <low-frames> | window <seconds> }
no ethernet-oam errored-frame { threshold low | window }
	Configure the low threshold and window period of errored frame event, no command resotores the default value. (optional)

ethernet-oam errored-frame-seconds { threshold low <low-frame-seconds> | window <seconds> }
no ethernet-oam errored-frame-seconds {threshold low | window }
	Configure the low threshold and window period of errored frame seconds event, no command resotores the default value. (optional)

3. **Configure remote failure**

Command	Explanation
Port mode	
ethernet-oam remote-failure no ethernet-oam remote-failure	Enable remote failure detection of EFM OAM (failure means critical-event or link-fault event of the local), no command disables the function. (optional)
ethernet-oam errored-symbol-period threshold high { high-symbols | none } no ethernet-oam errored-symbol-period threshold high	Configure the high threshold of errored symbol period event, no command restores the default value. (optional)
ethernet-oam errored-frame-period threshold high { high-frames | none } no ethernet-oam errored-frame-period threshold high	Configure the high threshold of errored frame period event, no command restores the default value. (optional)
ethernet-oam errored-frame threshold high { high-frames | none } no ethernet-oam errored-frame threshold high	Configure the high threshold of errored frame event, no command restores the default value. (optional)
ethernet-oam errored-frame-seconds threshold high { high-frame-seconds | none } no ethernet-oam errored-frame-seconds threshold high	Configure the high threshold of errored frame seconds event, no command restores the default value. (optional)

10.3 EFM OAM Example

Example:

CE and PE devices with point-to-point link enable EFM OAM to monitor **the First Mile** link performance. It will report the log information to network management system when occurring fault event and use remote loopback function to detect the link in necessary instance

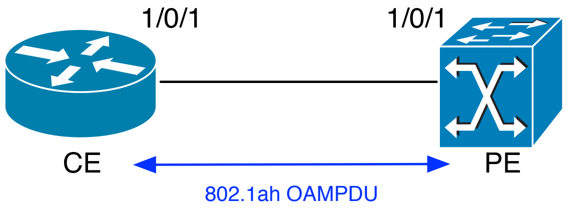


Figure 10.3: Typical OAM application topology

Configuration procedure: (Omitting SNMP and Log configuration in the following)
Configuration on CE:

```
CE(config)#interface ethernet1/1
CE(config-if-ethernet1/1)#ethernet-oam mode passive
CE(config-if-ethernet1/1)#ethernet-oam
CE(config-if-ethernet1/1)#ethernet-oam remote-loopback supported
```

Other parameters use the default configuration.
Configuration on PE:

```
PE(config)#interface ethernet 1/1
PE(config-if-ethernet1/1)#ethernet-oam
```

Other parameters use the default configuration.
Execute the following command when using remote loopback.

```
PE(config-if-ethernet1/1)#ethernet-oam remote-loopback
```

Execute the following command to make one of OAM peers exiting OAM loopback after complete detection.

```
PE(config-if-ethernet1/1)# no ethernet-oam remote-loopback
```

Execute the following command without supporting remote loopback.

```
CE(config-if-ethernet1/1)#no ethernet-oam remote-loopback supported
```

10.4 EFM OAM Troubleshooting

When using EFM OAM, it occurs the problem, please check whether the problem is resulted by the following reasons:

- Check whether OAM entities of two peers of link in passive mode. If so, EFM OAM connection can not be established between two OAM entities.
- Ensuring SNMP configuration is correct, or else errored event can not be reported to network management system.
- Link does not normally communicate in OAM loopback mode, it should cancel remote loopback in time after detect the link performance.
- Ensuring the used board supports remote loopback function.
- Port should not configure STP, MRPP, ULPP, Flow Control, loopback detection functions after it enables OAM loopback function, because OAM remote loopback function and these functions are mutually exclusive.

Chapter 11

Port Security

11.1 Introduction to Port Security

Port security is a MAC address-based security mechanism for network access controlling. It is an extension to the existing 802.1x authentication and MAC authentication. It controls the access of unauthorized devices to the network by checking the source MAC address of the received frame and the access to unauthorized devices by checking the destination MAC address of the sent frame. With port security, you can define various port security modes to make that a device learns only legal source MAC addresses, so as to implement corresponding network security management. After port security is enabled, the device detects an illegal frame, it triggers the corresponding port security feature and takes a pre-defined action automatically. This reduces user's maintenance workload and greatly enhances system security.

11.2 Port Security Configuration Task List

1. Basic configuration for Port Security

Command	Explanation
Port mode	
switchport port-security no switchport port-security	Configure port-security of the interface.
switchport port-security mac-address <mac-address> [vlan <vlan-id>] no switchport port-security mac-address <mac-address> [vlan <vlan-id>]	Configure the static security MAC of the interface.
switchport port-security maximum <value> [vlan <vlan-list>] no switchport port-security maximum <value> [vlan <vlan-list>]	Configure the maximum number of the security MAC address allowed by the interface.

Command	Explanation
Port mode	
switchport port-security violation { protect | restrict | shutdown } no switchport port-security violation	When exceeding the maximum number of the configured MAC addresses, MAC address accessing the interface does not belongs to this interface in MAC address table or a MAC address is configured to several interfaces in same VLAN, both of them will violate the security of the MAC address.

switchport port-security aging { static | time <value> | type { absolute | inactivity } }
no switchport port-security violation aging { static | time | type }
	Enable port-security aging entry of the interface, specify aging time or aging type.

Admin mode	
clear port-security { all | configured | dynamic | sticky } [[address <mac-addr> | interface <interface-id>] [vlan <vlan-id>]]	Clear the secure MAC entry of the interface.
show port-security [interface <interface-id>] [address | vlan]	Show port-security configuration.

11.3 Example of Port Security

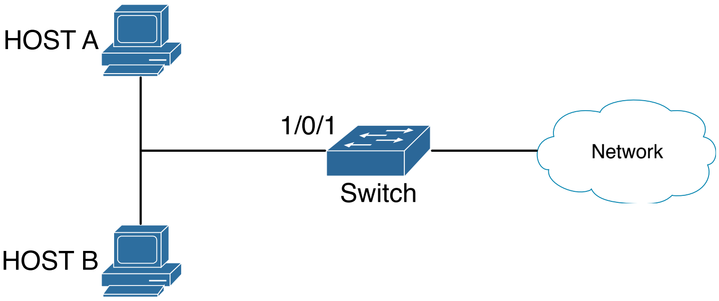


Figure 11.1: Typical topology chart for port security

When the interface enabled Port security function, configure the maximum number of the secure MAC addresses allowed by a interface to be 10, the interface allows 10 users to access the internet at most. If it exceeds the maximum number, the new user cannot access the internet, so that it not only limit the user's number but also access the internet safely. If configuring the maximum number of the secure MAC addresses as 1, only HOST A or HOST B is able to access the internet.

Configuration process:

```
#Configure the switch.
Switch(config)#interface Ethernet 1/0/1
Switch(config-if-ethernet1/0/1)#switchport port-security
Switch(config-if-ethernet1/0/1)#switchport port-security maximum 10
Switch(config-if-ethernet1/0/1)#exit
Switch(config)#
```

11.4 Port Security Troubleshooting

If problems occur when configuring Port Security, please check whether the problem is caused by the following reasons:

- Check whether Port Security is enabled normally
- Check whether the valid maximum number of MAC addresses is configured

Chapter 12

DDM Configuration

12.1 Introduction to DDM

12.1.1 Brief Introduction to DDM

DDM (Digital Diagnostic Monitor) makes the detailed digital diagnostic function standard in SFF-8472 MSA. It set that the parameter signal is monitored and make it to digitize on the circuit board of the inner module. After that, providing the demarcated result or the digitize measure result and the demarcate parameter which are saved in the standard memory framework, so as to expediently read by serial interface with double cables.

Normally, intelligent fiber modules support Digital Diagnostic function. Network management units is able to monitor the parameters (temperature, voltage, bias current, tx power and rx power) of the fiber module to obtain theirs thresholds and the real-time state of the current fiber module by the inner MCU of the fiber module. That is able to help the network management units to locate the fault in the fiber link, reduce the maintenance workload and enhance the system reliability.

DDM applications are shown in the following:

1. Module lifetime forecast

Monitoring the bias current is able to forecast the laser lifetime. Administrator is able to find some potential problems by monitoring voltage and temperature of the module.

1. High Vcc voltage will result in the breakdown CMOS, low Vcc voltage will result in the abnormity work.

2. High rx power will damage the receiving module, low rx power will result that the receiving module cannot work normally.

3. High temperature will result in the fast aging of the hardware.

4. Monitoring the received fiber power to monitor the capability of the link and the remote switch.

2. Fault location

In fiber link, locating the fault is important to the fast overload of the service, fault isolation is able to help administrator to fast locate the location of the link fault within the module (local module or remote module) or on the link, it also reduce the time for restoring the fault of the system.

Analyzing warning and alarm status of real-time parameters (temperature, voltage, bias current, tx power and rx power) can fast locate the fault through Digital Diagnostic function. Besides, the state of Tx Fault and Rx LOS is important for analyzing the fault.

3. Compatibility verification

Compatibility verification is used to analyze whether the environment of the module accords the data manual or it is compatible with the corresponding standard, because the module capability is able to be ensured only in the compatible environment. Sometimes, environment parameters exceed the data manual or the corresponding standard, it will make the falling of the module capability that result in the transmission error.

Environment is not compatible with the module are as below:

1. Voltage exceeds the set range
2. Rx power is overload or is under the sensitivity of the transceiver
3. Temperature exceeds the range of the running temperature

12.1.2 DDM Function

DDM descriptions are shown in the following:

1. Show the monitoring information of the transceiver

Administrator is able to know the current working state of the transceiver and find some potential problems through checking the real-time parameters (including TX power, RX power, Temperature, Voltage, Bias current) and querying the monitoring information (such as warning, alarm, real-time state and threshold, and so on). Besides, checking the fault information of the fiber module helps administrator to fast locate the link fault and saves the restored time.

2. Threshold defined by the user

For real-time parameters (TX power, RX power, Temperature, Voltage, Bias current), there are fixed thresholds. Because the user's environments are difference, the users is able to define the threshold (including high alarm, low alarm, high warn, low warn) to flexibly monitor the working state of the transceiver and find the fault directly.

The thresholds configured by the user and the manufacturer can be shown at the same time. When the threshold defined by the user is irrational, it will prompt the user and automatically process alarm or warning according to the default threshold. (the user is able to restore all thresholds to the default thresholds or restore a threshold to the default threshold)

Threshold rationality: high/low warn should be between high alarm and low alarm and high threshold should be higher than low threshold, namely, high alarm >= high warn >= low warn >= low alarm.

For fiber module, verification mode of the receiving power includes inner verification and outer verification which are decided by the manufacturer. Besides the verification mode of the real-time parameters and the default thresholds are same.

3. Transceiver monitoring

Besides checking the real-time working state of the transceiver, the user needs to monitor the detailed status, such as the former abnormity time and the abnormity type. Transceiver monitoring helps the user to find the former abnormity status through checking the log and query the last abnormity status through executing the commands. When the user finds the abnormity information of the fiber module, the fiber module information may be remonitored after processing the abnormity information, here, the user is able to know the abnormity information and renew the monitoring.

12.2 DDM Configuration Task List

DDM configuration task list:

1. Show the real-time monitoring information of the transceiver
2. Configure the alarm or warning thresholds of each parameter for the transceiver
3. Configure the state of the transceiver monitoring
   (a) Configure the interval of the transceiver monitoring
   (b) Configure the enable state of the transceiver monitoring
   (c) Show the information of the transceiver monitoring
   (d) Clear the information of the transceiver monitoring

1. Show the real-time monitoring information of the transceiver

Command	Explanation
User mode, admin mode and global mode	
show transceiver [interface ethernet <interface-list>][detail]	Show the monitoring of the transceiver.

2. Configure the alarm or warning thresholds of each parameter for the transceiver

Command	Explanation
Port mode	
transceiver threshold { default | { temperature | voltage | bias | rx-power | tx-power } { high-alarm | low-alarm | high-warn | low-warn } { <value> | default } }	Set the threshold defined by the user.

3. Configure the state of the transceiver monitoring

(a) Configure the interval of the transceiver monitoring

Command	Explanation
Global mode	
transceiver-monitoring interval <minutes> no transceiver-monitoring interval	Set the interval of the transceiver monitor. The no command sets the interval to be the default interval of 15 minutes.

(b)Configure the enable state of the transceiver monitoring

Command	Explanation
Port mode	
transceiver-monitoring { enable | disable }	Set whether the transceiver monitoring is enabled. Only the port enables the transceiver monitoring, the system records the abnormity state. After the port disables the function, the abnormity information will be clear.

(c)Show the information of the transceiver monitoring

Command	Explanation
Admin mode and global mode	
show transceiver threshold-violation [interface ethernet <interface-list>]	Show the information of the transceiver monitoring, including the last threshold-violation informatijon, the interval of the current transceiver monitoring and whether the port enables the transceiver monitoring.

(d)Clear the information of the transceiver monitoring

Command	Explanation
Admin mode	
clear transceiver threshold-violation [interface ethernet <interface-list>]	Clear the threshold violation of the transceiver monitor.

12.3 Examples of DDM

Example 1:

Ethernet 1/21 and Ethernet 1/23 are inserted the fiber module with DDM, Ethernet 1/24 is inserted the fiber module without DDM, Ethernet 1/22 does not insert any fiber module, show the DDM information of the fiber module.

a) Show the information of all interfaces which can read the real-time parameters normally, (No fiber module is inserted or the fiber module is not supported, the information will not be shown), for example:

```
Switch#show transceiver
Interface  Temp  Voltage(V)  Bias(mA)  RX Power(dBM)  TX Power(dBM)
1/21       33    3.31        6.11      -30.54(A-)     -6.01
1/23       33    5.00(W+)    6.11      -20.54(W-)     -6.02
```

b) Show the information of the specified interface. (N/A means no fiber module is inserted or does not support the fiber module), for example:

```
Switch#show transceiver interface ethernet 1/21-22;23
Interface  Temp  Voltage(V)  Bias(mA)  RX Power(dBM)  TX Power(dBM)
1/21       33    3.31        6.11      -30.54(A-)     -6.01
```

```
1/22       N/A   N/A         N/A       N/A            N/A
1/23       33    5.00(W+)    6.11      -20.54(W-)     -6.02
```

c) Show the detailed information, including base information, parameter value of the real-time monitoring, warning, alarm, abnormity state and threshold information, for example:

```
Switch#show transceiver interface ethernet 1/21-22;24 detail
Ethernet 1/21 transceiver detail information:
Base information:
SFP found in this port, manufactured by company, on Sep 29 2010.
Type is 1000BASE-SX, Link length is 550 m for 50um Multi-Mode Fiber.
Link length is 270 m for 62.5um Multi-Mode Fiber.
Nominal bit rate is 1300 Mb/s, Laser wavelength is 850 nm.
Brief alarm information:
RX loss of signal
Voltage high
RX power low
Detail diagnostic and threshold information:
                  Diagnostic                      Threshold
                  Realtime   High Alarm  Low Alarm  High Warn  Low Warn
                  ---------  ----------  ---------  ---------  --------
Temperature       33         70          0          70         0
Voltage(V)        7.31(A+)   5.00        0.00       5.00       0.00
Bias current(mA)  6.11(W+)   10.30       0.00       5.00       0.00
RX Power(dBM)    -30.54(A-)  9.00        -25.00     9.00       -25.00
TX Power(dBM)    -6.01       9.00        -25.00     9.00       -25.00

Ethernet 1/22 transceiver detail information: N/A

Ethernet 1/24 transceiver detail information:
Base information:
SFP found in this port, manufactured by company, on Sep 29 2010.
Type is 1000BASE-SX, Link length is 550 m for 50um Multi-Mode Fiber.
Link length is 270 m for 62.5um Multi-Mode Fiber.
Nominal bit rate is 1300 Mb/s, Laser wavelength is 850 nm.
Brief alarm information: N/A
Detail diagnostic and threshold information: N/A
```

Example 2:

Ethernet 1/21 is inserted the fiber module with DDM. Configure the threshold of the fiber module after showing the DDM information.

Step 1: Show the detailed DDM information.

```
Switch#show transceiver interface ethernet 1/21 detail
Ethernet 1/21 transceiver detail information:
Base information:

Brief alarm information:
```

```
RX loss of signal
Voltage high
RX power low
Detail diagnostic and threshold information:
                  Diagnostic                      Threshold
                  Realtime    High Alarm  Low Alarm  High Warn  Low Warn
                  ----------  ----------  ---------  ---------  ---------
Temperature       33          70          0          70         0
Voltage(V)        7.31(A+)    5.00        0.00       5.00       0.00
Bias current(mA)  6.11(W+)    10.30       0.00       5.00       0.00
RX Power(dBM)     -30.54(A-)  9.00        -25.00     9.00       -25.00
TX Power(dBM)     -13.01      9.00        -25.00     9.00       -25.00
```

Step 2: Configure the tx-power threshold of the fiber module, the low-warning threshold is -12, the low-alarm threshold is -10.00.

```
Switch#config
Switch(config)#interface ethernet 1/21
Switch(config-if-ethernet1/21)#transceiver threshold tx-power low-warning -12
Switch(config-if-ethernet1/21)#transceiver threshold tx-power low-alarm -10.00
```

Step 3: Show the detailed DDM information of the fiber module. The alarm uses the threshold configured by the user, the threshold configured by the manufacturer is labeled with the bracket. There is the alarm with **A-** due to -13.01 is less than -12.00.

```
Switch#show transceiver interface ethernet 1/21 detail
Ethernet 1/21 transceiver detail information:
Base information:

Brief alarm information:
RX loss of signal
Voltage high
RX power low
TX power low
Detail diagnostic and threshold information:
                  Diagnostic                        Threshold
                  Realtime    High Alarm  Low Alarm      High Warn  Low Warn
                  ----------  ----------  -------------  ---------  ---------
Temperature       33          70          0              70         0
Voltage(V)        7.31(A+)    5.00        0.00           5.00       0.00
Bias current(mA)  6.11(W+)    10.30       0.00           5.00       0.00
RX Power(dBM)     -30.54(A-)  9.00        -25.00         9.00       -25.00
TX Power(dBM)     -13.01(A-)  9.00        -12.00(-25.00) 9.00       -10.00(-25.00)
```

Example 3:

Ethernet 1/21 is inserted the fiber module with DDM. Enable the transceiver monitoring of the port after showing the transceiver monitoring of the fiber module.

Step 1: Show the transceiver monitoring of the fiber module. Both ethernet 1/21 and ethernet 1/22 do not enable the transceiver monitoring, its interval is set to 30 minutes.

```
Switch(config)#show transceiver threshold-violation interface ethernet 1/21-22
Ethernet 1/21 transceiver threshold-violation information:
Transceiver monitor is disabled. Monitor interval is set to 30 minutes.
The last threshold-violation doesn't exist.

Ethernet 1/22 transceiver threshold-violation information:
Transceiver monitor is disabled. Monitor interval is set to 30 minutes.
The last threshold-violation doesn't exist.
```

Step 2: Enable the transceiver monitoring of ethernet 1/21.

```
Switch(config)#interface ethernet 1/21
Switch(config-if-ethernet1/21)#transceiver-monitoring enable
```

Step 3: Show the transceiver monitoring of the fiber module. In the following configuration, ethernet 21 enabled the transceiver monitoring, the last threshold-violation time is Jan 02 11:00:50 2011, the detailed DDM information exceeding the threshold is also shown.

```
Switch(config-if-ethernet1/21)#quit
Switch(config)#show transceiver threshold-violation interface ethernet 1/21-22
Ethernet 1/21 transceiver threshold-violation information:
Transceiver monitor is enabled. Monitor interval is set to 30 minutes.
The current time is Jan 02 12:30:50 2011.
The last threshold-violation time is Jan 02 11:00:50 2011.
Brief alarm information:
RX loss of signal
RX power low
Detail diagnostic and threshold information:
                    Diagnostic                    Threshold
                  Realtime   High Alarm  Low Alarm    High Warn  Low Warn
                  ---------  ----------  -----------  ---------  ---------
Temperature       33         70          0            70         0
Voltage(V)        7.31       10.00       0.00         5.00       0.00
Bias current(mA)  3.11       10.30       0.00         5.00       0.00
RX Power(dBM)     -30.54(A-) 9.00        -25.00(-34)  9.00       -25.00
TX Power(dBM)     -1.01      9.00        -12.05       9.00       -10.00

Ethernet 1/22 transceiver threshold-violation information:
Transceiver monitor is disabled. Monitor interval is set to 30 minutes.
The last threshold-violation doesn't exist.
```

12.4 DDM Troubleshooting

If problems occur when configuring DDM, please check whether the problem is caused by the following reasons:

- Ensure that the transceiver of the fiber module has been inserted fast on the port, or else DDM configuration will not be shown.

- Ensure that SNMP configuration is valid, or else the warning event cannot inform the network management system.

- Because only some boards and box switches support SFP with DDM or XFP with DDM, ensure the used board and switch support the corresponding function.

- When using show transceiver command or show transceiver detail command, it cost much time due to the switch will check all ports, so it is recommended to query the monitoring information of the transceiver on the specified port.

- Ensure the threshold defined by the user is valid. When any threshold is error, the transceiver will give an alarm according to the default setting automatically.

Chapter 13

LLDP-MED

13.1 Introduction to LLDP-MED

LLDP-MED (Link Layer Discovery Protocol-Media Endpoint Discovery) based on 802.1AB LLDP (Link Layer Discovery Protocol) of IEEE. LLDP provides a standard link layer discovery mode, it sends local device information (including its major capability, management IP address, device ID and port ID) as TLV (type/length/value) triplets in LLDPDU (Link Layer Discovery Protocol Data Unit) to the direct connection neighbors. The device information received by the neighbors will be stored with a standard management information base (MIB). This allows a network management system to quickly detect and identify the communication status of the link.

In 802.1AB LLDP, there is no transmission and management about the voice device information. To deploy and manage voice device expediently, LLDP-MED TLVs provide multiple information, such as PoE (Power over Ethernet), network policy, and the location information of the emergent telephone service.

13.2 LLDP-MED Configuration Task Sequence

1. Basic LLDP-MED configuration

Command	Explanation
Port mode	
lldp transmit med tlv all no lldp transmit med tlv all	Configure the specified port to send all LLDP-MED TLVs. The no command disables the function.
lldp transmit med tlv capability no lldp transmit med tlv capability	Configure the specified port to send LLDP-MED Capability TLV. The no command disables the capability.
lldp transmit med tlv networkPolicy no lldp transmit med tlv networkPolicy	Configure the specified port to send LLDP-MED Network Policy TLV. The no command disables the capability.
lldp transmit med tlv extendPoe no lldp transmit med tlv extendPoe	Configure the specified port to send LLDP-MED Extended Power-Via-MDI TLV. The no command disables the capability.

Command	Explanation
Port mode	
lldp transmit med tlv inventory no lldp transmit med tlv inventory	Configure the port to send LLDP-MED Inventory Management TLVs. The no command disables the capability.
network policy { voice | voice-signaling | guest-voice | guest-voice-signaling | softphone-voice | video-conferencing | streaming-video | video-signaling } [status { enable | disable }] [tag { tagged | untagged }] [vid { <vlan-id> | dot1p }] [cos <cos-value>] [dscp <dscp-value>] no network policy { voice | voice-signaling | guest-voice | guest-voice-signaling | softphone-voice | video-conferencing | streaming-video | video-signaling }	Configure network policy of the port, including VLAN ID, the supported application (such as voice and video), the application priority and the used policy, and so on.
civic location { dhcp server | switch | endpointDev } <country-code> no civic location	Configure device type and country code of the location with Civic Address LCI format and enter Civic Address LCI address mode. The no command cancels all configurations of the location with Civic Address LCI format.
ecs location <tel-number> no ecs location	Configure the location with ECS ELIN format on the port, the no command cancels the configured location.
lldp med trap { enable | disable }	Enable or disable LLDP-MED trap for the specified port.
Civic Address LCI address mode	
{ description-language | province-state | city | county | street | locationNum | location | floor | room | postal | otherInfo } <address> no { description-language | province-state | city | county | street | locationNum | location | floor | room | postal | otherInfo }	Configure the detailed address after enter Civic Address LCI address mode of the port.
Global mode	
lldp med fast count <value> no lldp med fast count	When the fast LLDP-MED startup mechanism is enabled, it needs to fast send the LLDP packets with LLDP-MED TLV, this command is used to set the value of the fast sending packets, the no command restores the default value.

Command	Explanation
Admin mode	
show lldp	Show the configuration of the global LLDP and LLDP-MED.
show lldp [interface ethernet <IFNAME>]	Show the configuration of LLDP and LLDP-MED on the current port.
show lldp neighbors [interface ethernet <IFNAME>]	Show LLDP and LLDP-MED configuration of the neighbors.

13.3 LLDP-MED Example

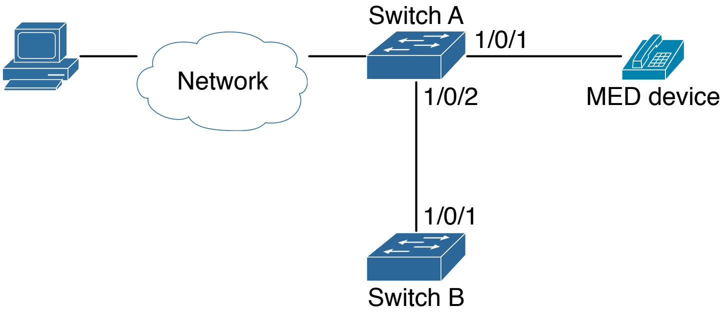


Figure 13.1: Basic LLDP-MED configuration topology

1) Configure Switch A

```
SwitchA(config)#interface ethernet1/0/1
SwitchA(Config-If-Ethernet1/0/1)#lldp enable
SwitchA(Config-If-Ethernet1/0/1)#lldp mode both
SwitchA(Config-If-Ethernet1/0/1)#lldp transmit med tlv capability
SwitchA(Config-If-Ethernet1/0/1)#lldp transmit med tlv network policy
SwitchA(Config-If-Ethernet1/0/1)#lldp transmit med tlv inventory
SwitchB(Config-If-Ethernet1/0/1)#network policy voice tag tagged vid 10 cos 5 dscp 15
SwitchA(Config-If-Ethernet1/0/1)#exit
SwitchA(config)#interface ethernet1/0/2
SwitchA(Config-If-Ethernet1/0/2)#lldp enable
SwitchA(Config-If-Ethernet1/0/2)#lldp mode both
```

2) Configure Switch B

```
SwitchB(config)#interface ethernet1/0/1
SwitchB(Config-If-Ethernet1/0/1)#lldp enable
SwitchB(Config-If-Ethernet1/0/1)#lldp mode both
SwitchB(Config-If-Ethernet1/0/1)#lldp transmit med tlv capability
SwitchB(Config-If-Ethernet1/0/1)#lldp transmit med tlv network policy
SwitchB(Config-If-Ethernet1/0/1)#lldp transmit med tlv inventory
SwitchB(Config-If-Ethernet1/0/1)#network policy voice tag tagged vid 10 cos 4
```

3) Verify the configuration

```
# Show the global status and interface status on Switch A.
SwitchA# show lldp neighbors interface ethernet 1/0/1
Port name : Ethernet1/0/1
Port Remote Counter : 1
TimeMark :20
ChassisIdSubtype :4
ChassisId :f8-f0-82-00-00-02
PortIdSubtype :Local
PortId :1
PortDesc :****
SysName :****
SysDesc :*****

SysCapSupported :4
SysCapEnabled :4

LLDP MED Information :
MED Codes:
(CAP)Capabilities, (NP) Network Policy
(LI) Location Identification, (PSE)Power Source Entity
(PD) Power Device, (IN) Inventory
MED Capabilities:CAP,NP,PD,IN
MED Device Type: Endpoint Class III
Media Policy Type :Voice
Media Policy :Tagged
Media Policy Vlan id :10
Media Policy Priority :3
Media Policy Dscp :5
Power Type : PD
Power Source :Primary power source
Power Priority :low
Power Value :15.4 (Watts)
Hardware Revision:
Firmware Revision:4.0.1
Software Revision:6.2.30.0
Serial Number:
Manufacturer Name:****
Model Name:Unknown
Assert ID:Unknown
IEEE 802.3 Information :
 auto-negotiation support: Supported
 auto-negotiation support: Not Enabled
 PMD auto-negotiation advertised capability: 1
 operational MAU type: 1
SwitchA# show lldp neighbors interface ethernet 1/0/2
Port name : interface ethernet 1/0/2
Port Remote Counter: 1
Neighbor Index: 1
Port name : Ethernet1/2
Port Remote Counter : 1
TimeMark :20
ChassisIdSubtype :4
ChassisId :f8-f0-82-00-00-02
PortIdSubtype :Local
PortId :1
PortDesc :Ethernet1/0/1
SysName :****
SysDesc :*****

SysCapSupported :4
SysCapEnabled :4
```

Explanation:

1. Both Ethernet2 of switch A and Ethernet1 of switch B are the ports of network connection device, they will not send LLDP packets with MED TLV information forwardly. Although configure Ethernet1 of switch B to send MED TLV information, it will not send the related MED information, that results the corresponding Remote table without the related MDE information on Ethernet2 of switch A.

2. LLDP-MED device is able to send LLDP packets with MED TLV forwardly, so the corresponding Remote table with LLDP MED information on Ethernet1 of switch A.

13.4 LLDP-MED Troubleshooting

If problems occur when configuring LLDP-MED, please check whether the problem is caused by the following reasons:

- Check whether the global LLDP is enabled.
- Only network connection device received LLDP packets with LLDP-MED TLV from the near MED device, it sends LLDP-MED TLV. If network connection device configured the command for sending LLDP-MED TLV, the packets also without LLDP-MED TLV sent by the port, that means no MED information is received and the port does not enable the function for sending LLDP-MED information.
- If neighbor device has sent LLDP-MED information to network connection device, but there is no LLDP-MED information by checking show lldp neighbors command, that means LLDP-MED information sent by neighbor is error.

Chapter 14

BPDU-Tunnel Configuration

14.1 Introduction to bpdu-tunnel

BPDU Tunnel is a Layer 2 tunnel technology. It allows Layer 2 protocol packets of geographically dispersed private network users to be transparently transmitted over specific tunnels across a service provider network.

14.1.1 bpdu-tunnel function

In MAN application, multi-branches of a corporation may connect with each other by the service provider network. VPN provided by the service provider enables the geographically dispersed networks to form a local LAN, so the service provider needs to provide the tunnel function, namely, data information generated by user's network is able to inextenso arrive at other networks of the same corporation through the service provider network. To maintain a local concept, it not only needs to transmit the data within the user's private network across the tunnel, but also transmit layer 2 protocol packets within the user's private network.

14.1.2 Background of bpdu-tunnel

Special lines are used in a service provider network to build user-specific Layer 2 networks. As a result, a user network is broken down into parts located at different sides of the service provider network. As shown in Figure, User A has two devices (CE 1 and CE 2) and both devices belong to the same VLAN. User's network is divided into network 1 and network 2, which are connected by the service provider network. When Layer 2 protocol packets cannot implement the passthrough across the service provider network, the user's network cannot process independent Layer 2 protocol calculation (for example, spanning tree calculation), so they affect each other.

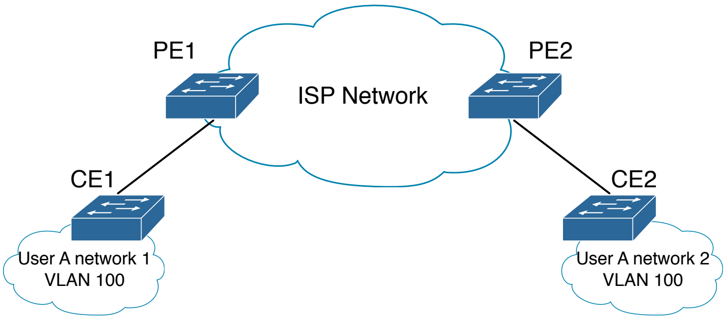


Figure 14.1: BPDU Tunnel application

14.2 bpdu-tunnel Configuration Task List

bpdu-tunnel configuration task list:

1. Configure tunnel MAC address globally
2. Configure the port to support the tunnel

1. Configure tunnel MAC address globally

Command	Explanation
Global mode	
bpdu-tunnel dmac <mac> no bpdu-tunnel dmac	Configure or cancel the tunnel MAC address globally.

2. Configure the port to support the tunnel

Command	Explanation
Port mode	

bpdu-tunnel { stp | gvrp | uldp | lacp | dot1x }
no bpdu-tunnel { stp | gvrp | uldp | lacp | dot1x }
	Enable the port to support the tunnel, the no command disables the function.

14.3 Examples of bpdu-tunnel

Special lines are used in a service provider network to build user-specific Layer 2 networks. As a result, a user network is broken down into parts located at different sides of the service provider network. As shown in Figure, User A has two devices (CE 1 and CE 2) and both devices belong to the same VLAN. User's network is divided into network 1 and network 2, which are connected by the service provider network. When Layer 2 protocol packets cannot implement the passthrough across the service provider network, the user's network cannot process independent Layer 2 protocol calculation (for example, spanning tree calculation), so they affect each other.

With BPDU Tunnel, Layer 2 protocol packets from user's networks can be passed through over the service provider network in the following work flow:

1. After receiving a Layer 2 protocol packet from network 1 of user A, PE 1 in the service provider network encapsulates the packet, replaces its destination MAC address with a specific multicast MAC address, and then forwards the packet in the service provider network.
2. The encapsulated Layer 2 protocol packet (called BPDU Tunnel packet) is forwarded to PE 2 at the other end of the service provider network, which de-encapsulates the packet, restores the original destination MAC address of the packet, and then sends the packet to network 2 of user A.

bpdu-tunnel configuration of edge switches PE1 and PE2 in the following:
PE1 configuration:

```
PE1(config)# bpdu-tunnel dmac 01-02-03-04-05-06
PE1(config-if-ethernet1/1)# bpdu-tunnel stp
PE1(config-if-ethernet1/1)# bpdu-tunnel lacp
PE1(config-if-ethernet1/1)# bpdu-tunnel uldp
PE1(config-if-ethernet1/1)# bpdu-tunnel gvrp
PE1(config-if-ethernet1/1)# bpdu-tunnel dot1x
```

PE2 configuration:

```
PE2(config)# bpdu-tunnel dmac 01-02-03-04-05-06
PE2(config-if-ethernet1/1)# bpdu-tunnel stp
PE2(config-if-ethernet1/1)# bpdu-tunnel lacp
PE2(config-if-ethernet1/1)# bpdu-tunnel uldp
PE2(config-if-ethernet1/1)# bpdu-tunnel gvrp
PE2(config-if-ethernet1/1)# bpdu-tunnel dot1x
```

14.4 bpdu-tunnel Troubleshooting

After port disables stp, gvrp, uldp, lacp and dot1x functions, it is able to configure bpdu-tunnel function.

Chapter 15

CFM-OAM Configuration

15.1 Overview

Since the Ethernet technology was naissance, it's simple and low-cost characteristics make it to become the dominant technology in the local area network.Recently, kilomega and million mega apply one after the other, this urges the network providers, facilities manufacturers and normalizer to advance the Ethernet technology to city and wide network.

Nevertheless, Ethernet is a LAN technology constitutionally. For the need of outlying inspection, SLA (service level protocol) testing are not imminent in the LAN environment, therefore the tradition Ethernet does not has the OMA function which is required by the network provider. Other than that, the tradition Ethernet has 10 seconds or the shortest 1 second linkage failure rearrange time is not acceptable by the network providers. Therefore, less than 50 millisecond failure rearrange time is also a big challenge for the city network Ethernet.

After several Ethernet OMA standards (for example, IEEE 802.3ah, IEEE802.1ag and ITU Y.1731) come out, OAM is not the indication weakness of the Ethernet.Using the IEEE802.1agas example, this also go by the name of connection failure management (CFM) standard, it provides the port to port network inspection and operation tools. It can execute the tasks such as MAC Ping, L2 Trace Route etc in the huge L2 Ethernet. It will simplify the failure elimination and SLA inspection in the operation of Ethernet. At the same time, the defined CCM (continuous inspection information) in the OMA standard in Ethernet can actualize undergo the protection rearrange lower than 50 millisecond. The shortest CCM sending time in the standard is 3.3 milliseconds. Three continuous losing CCM message will cause the main link declare invalidation and using the backup link to replace. CFM's effective is built up base on the reasonable dispose of network and configuration.

15.1.1 Ethernet OAM Protocol Criterion

About the Ethernet OAM, there are 4 protocol standard: 802.3ah (the first mile Ethernet, short form called EFM), 802.1ag (connection failure management, the short form called CFM), E-LMI (the local port of Ethernet), Y.1731 (failure and performance inspection), constitute by different group, the corresponding relationship as following:

- **IEEE 802.3ah:** Ethernet Link OAM (EFM OAM)
- **IEEE 802.1ag:** Connectivity Fault Management (CFM)

- **ITU-Y.1731:** OAM functions and mechanisms for Ethernet based network
- **MEF E-LMI:** Ethernet Local Management Interface

EFM OAM and CFM as the constitute to set the IEEE, EFM OAM working data link layer, as shown in Figure 15.1, can discover and manage the lower layer's data links effectively. Also, we can use EFM OAM technology to increase the management and maintenance ability, in order to maintain the stability of operation. CFM is the network level of Ethernet OAM technology, mainly use for the connect pool layer and responds for inspecting the connectedness of the network, orientating the failure of network connectedness. Y.1731 is establish by the ITU, the international telecom union, it's function is much bigger than CFM. Can also say that the function which perform by CFM is the subset of Y.1731. E-LMI is established by the MEF; only apply for UNI (the user boundary and the provider boundary that is faced by the user).

15.2 CFM OAM Basic Concept

802.1ag divide the whole network (customer, provider, operator) into different MD (Maintenance Domain). In each of the maintenance domains, it wills contrapose the MD provided service for maintenance management. On these services, there will have a lot of node point facilities. The core idea of the service of 802.1ag is inspecting the involved or all node points, so that it can discover the failure parts. The point that participates in maintenance inspection is called MP (Maintenance Point), the bridge of port that configure on the maintenance point.

15.2.1 Maintenance Domain

The network can be logically divided into different layers from internal to external; it is called MD (Maintenance Domain). The maintenance domain can be nesting but not across. Each of the vindicator can only see it own maintenance domain. The lower level of maintenance can provide the service to the border upon upper layer. Then, it can separate the vindicator e.g. operator and the user clearly. It can orientate the network problem more convenient.

In the network can contains of multi maintenance domain, each of the maintenance domain locates in particular level, totally there are 8 levels. The higher the level, the range of maintenance is higher. The higher level can nesting into lower level of domain. In the reality, CFM usually applies for the following situation. At this moment, it will divide into customer domain, service provider domain, operator domain etc.

Except the level, each of the MD has the global unique MD Name, which uses for label that MD.

15.2.2 Maintenance Set

Each of the service instances in the maintenance domain is a MA (Maintenance Association). One MD usually provide several service instances externally, 802.1ag is one to one management maintenance and inspect the failure of MA. Each of the MA will have a unique name in the MD. In the network, service instance usually mark by vlanId. And MA is corresponding to the services instances. Therefore, there is a linkage between MA and vlanId. One MA corresponds to one vlanId, at the same time, protocol allows many vlanId manage and maintain by one MA. In these

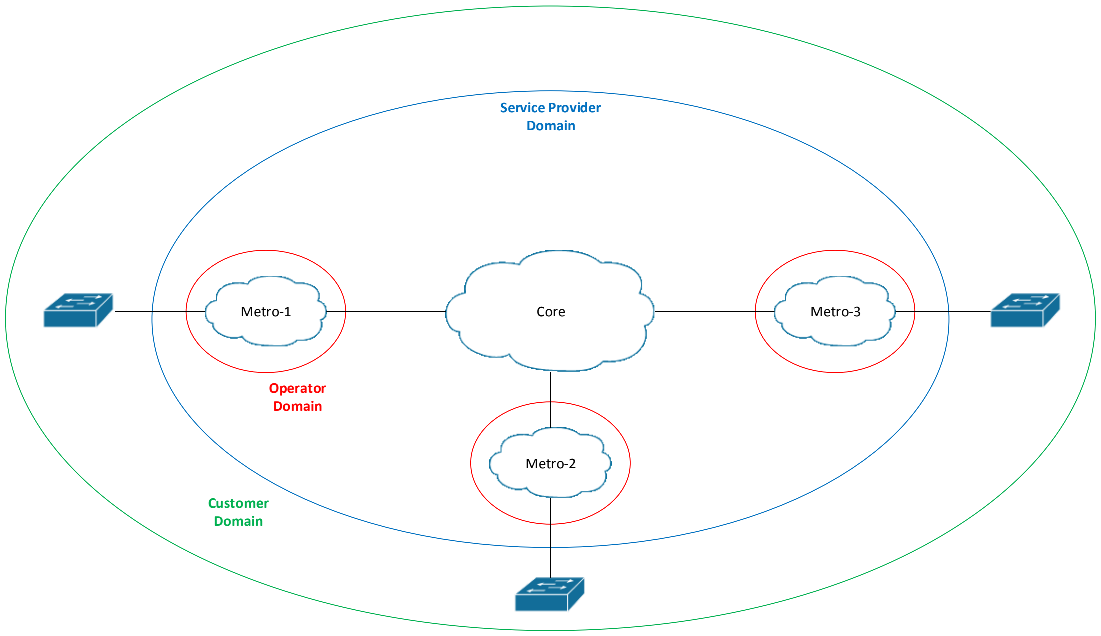


Figure 15.1: Maintenance Domain

vlanIds, there is a vlan that is a primary vlan. In the MD, there is an uncertainty of one vlanId corresponds to multi MA situation, therefore leave out of account for this moment. All in all, md and primary vlan Id is the unique label of MA.

15.2.3 Maintenance Base Point

It is belong to certain maintenance service, the boundary of the service, which is configured on the port. MEP responds for initiating all CFM messages (CCM,LTM,LBM), the protocol behaviours and the status are mainly occur in the MEP. MEP is divided into UP MEP and DOWN MEP. In the bridge, if MEP is sending and receiving the MA corresponding CFM messages from Lan, then this MEP is Down MEP; if the MEP is sending and receiving the MA corresponding CFM messages from Bridge Relay, then it is the Up MEP. Shown as following Figure:

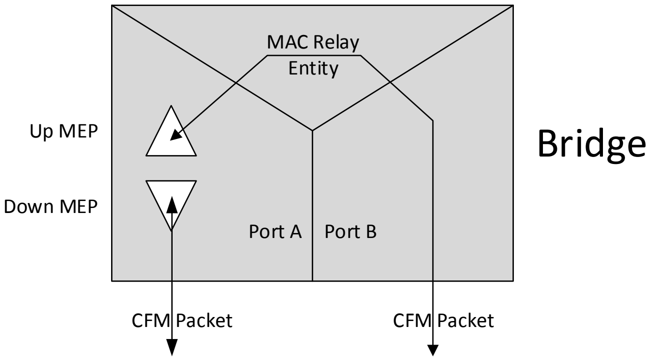


Figure 15.2: The difference between Down MEP and Up MEP

In more easy word, MEP sending and receiving the CFM messages from the local port is the Down MEP; in contrast, it is the Up MEP. MEP inherits the attributes of MD and MA that is located. It means the MD level and vlan Id. Maintenance base point is the only one label in the MA, it can be called MEPID.

15.2.4 Maintenance Mid-Point

It is belongs to certain maintenance service, the mid-point of maintenance service, and configures on the port. MIP cannot send the CFM messages actively; it can only receive the messages from the respond, sending Reply and transmit. It is not in charge of inspection and report failure, but it will assist MEP to undergo the failure inspection. MIP inherits the attributes of MD and MA that is located. It means the MD level and vlan Id.

MIP is not configured directly, it develops according to certain rules of system. In the port, each of the maintenance can only have one MIP. The following is the MIP rules:

none: Not build up the MIP node

default: If there is not a higher level of MEP on the port, and at the same time, lower level of MIP does not exist, then it will build up MIP on particular port at this level.

explicit: If there is not a higher level of MEP on the port, but at the same time, lower level of MEP exists and lower level of MIP does not exist, then it will build up MIP on particular port at this level.

defer: Whether build up the MIP node, the build rules will be determine by the configured rules of MD in the MA.

15.3 Introduction of CFM OAM Function

802.1ag provides 5 different functions: Fault detection, Fault verification and isolation, Path discovery, Fault notification and Fault recovery. Thereinto, Fault recovery need to execute with other protocols together.

15.3.1 Inspection of Failure

Maintenance base point (MEP) will send the CCM messages to Remote MEP in the same maintenance collection (MA) periodically. At the same time, it also receives other outlying point CCM message. If it cannot receive the CCM message in 3 months, then it will regards as occur failure in the link and report. The process is shown as follow:

CCM messages can also be sent to other MEP in the same MA, it is the group messages. The last 3 bit of the group broadcast address represent different maintenance domain level, thus it can more easy to tackle with hardware.For the lower level of MEP, after it receive higher level of messages, the hardware can accord to group broadcast MAC address and VLAN to undergo the transmitting directly.

The inspection of failure of the periodically sending CCM messages as follow:

- MEP cannot receive the CCM message on time, represent there is a failure occur in the MA;
- MEP checking the received CCM messages, it can find out the disagreement failure of the sending time interval;

- MEP received the failure MEPID or MAID, represent there is exist of internal configuration failure in MA or cross connection failure;
- MEP receive the lower level of the CCM messages, represent there is exist of internal configuration failure in MA or cross connection failure;
- MEP receive the CCM message which carries MAC status information, can investigate the outside failure of MA;

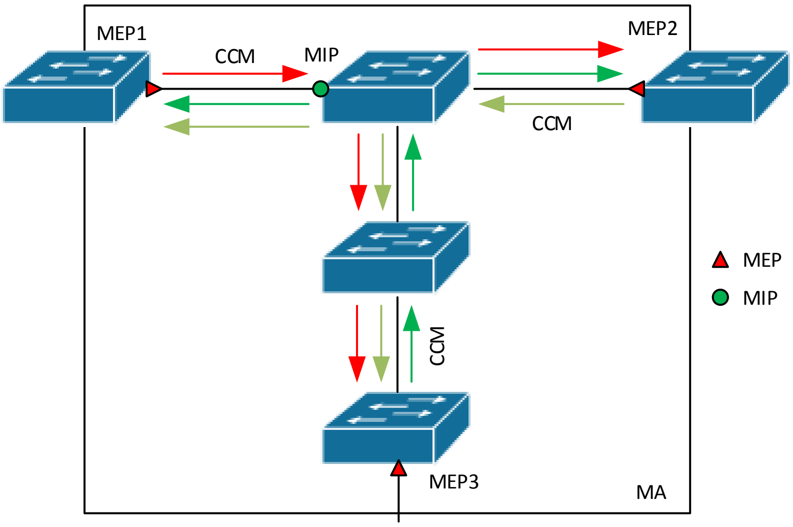


Figure 15.3: Connectedness inspection sketch map

15.3.2 Path Discovery

MEP and MIP will through the Linktrace to complete. The function of 802.1ag Linktrace is more or less the same with IP Traceroute. Through send the testing messages and receive replay messages to check the path of destination facilities or orientate the failure point. The processes as follow: MEP send LTM to the target MP (MEP or MIP), each of the MIP after receiving the LTM will also send a LTR to source MEP. And then, transmit the LTM messages, until the LTM arrive to destination MP or cannot transmit at all. Source MEP according to feedback LTR to confirm the status of the linkage, and obtains the paths to target MAC. It shows in the Figure 15.4.

LTM destination MAC address is the group broadcast address. The last 3 bit in the group broadcast address represents the level of different maintenance domain. LTR is the one way messages, the destination address as the LTM source MAC address.

15.3.3 Confirmation and Orientation of Failure

It can be actualizing by the 802.1ag Linktrace function that mention above. Also it can be actualizing by 802.1ag Loopback function as well. The circulation function is more or less the same with IP Ping, through out the sending of testing messages and receiving the replay messages to

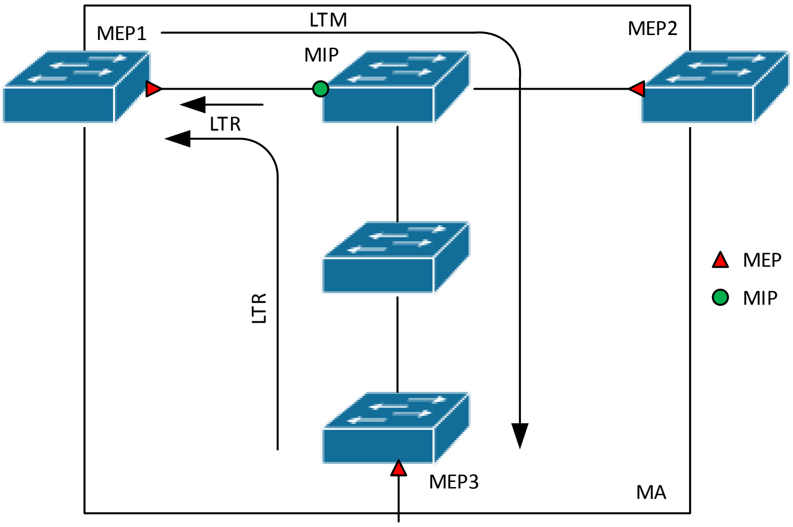


Figure 15.4: Path discovery sketch map

detect whether it can arrive to the destination facility. The idiographic processes as follow: MEP sending the one way broadcast message (LBM), the destination address of the message is the outlying MP. Once the middle facility receive the LBM will then transmit, and the outlying MP will sending the replay message (LBR) to the source MEP after it receive the LBM. The source MEP can accord this to determine whether the outlying MP can arrive or not. As shown in the following Figure 15.5.

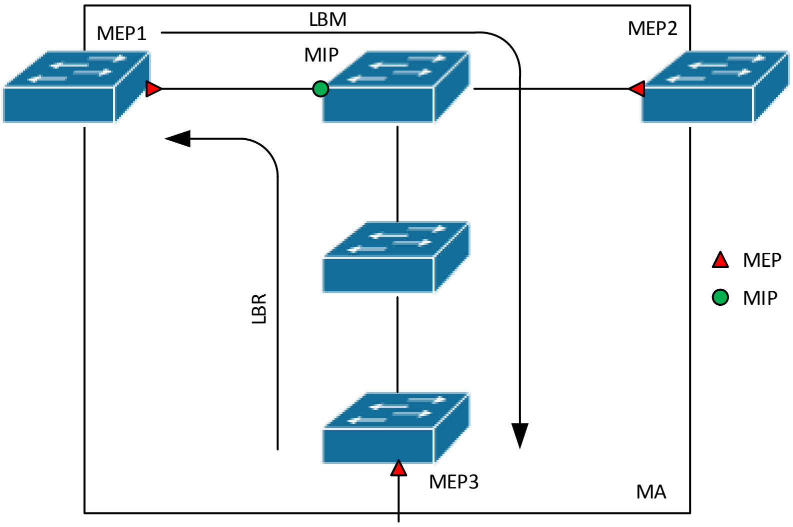


Figure 15.5: the figure of circulation function

15.3.4 Inform of Failure

After CFM inspects the failure of linkage, there are several of methods to tackle with:

- After checking the linkage failure, MEP will send the SNMP TRAP message to the management node, and inform failure occurred;
- After checking the linkage failure, MEP will send the records to the facility log book, and the administrators can discover the problem after checking it;
- After checking the linkage failure, will cooperate with others automatic protect protocol such as APS etc to undergo recovery. CFM will inform the occurrence of failure to these protocols, and confer switching the linkage automatically.

15.4 CFM OAM Basic Function Configuration

15.4.1 The Design of CFM Management Topology

Before the execution of CFM OAM function, need to perform the following layout in the network:

1. Need to divide the levels in the maintenance domain in the whole network, to confirm each level of boundaries in the domain.
2. Confirm the name of each maintenance domain, the name of different facilities is the same in the same maintenance domain.
3. According to the VLAN that is need to inspect, and confirm the maintenance services in different maintenance domains.
4. Confirm each of the name of all maintenance services, the name of different facilities is the same in the same maintenance service in the domain.
5. Confirm different facilities are the same in the same maintenance base point table in the same maintenance service of same domain.
6. Can maintenance the maintenance base point under the rules of the port in the maintenance domain and boundary of services. And maintenance the mid-point in the non- boundary or port.

Therefore require for the following data:

Serial number	Data
1	MD name and level
2	MA name, MA related VLAN ID
3	MEP ID, the name of the port that is connected to MEP, types of MEP
4	RMEP ID
5	MIP develop rules
6	The time interval that sending and detecting CCM news from MEP in MA

15.4.2 CFM OAM Configuration Task List

1. Select to enable CFM OAM function mode
2. Enable CFM OAM function globally
3. Enable y1731 function globally (selectable)
4. Create MD
5. Create MA
6. Create MEP
7. Configure RMEP
8. Create MIP (selectable)
9. Enable the failure confirmation function (selectable)
10. Configure CC sending and detecting
11. Check the configuration result of CFM

1. Select to enable CFM OAM function mode

Command	Explanation
Global mode	
ethernet cfm mode { hw | sw | auto } no ethernet cfm mode	Select the mode of enabling CFM OAM; it is only used before enabling CFM OAM function. No command recovers to be the default of auto.

2. Enable CFM OAM function globally

Command	Explanation
Global mode	
ethernet cfm global no ethernet cfm global	Enable CFM OAM function globally. No command disables this function.

3. Enable y1731 function globally (selectable)

Command	Explanation
Global mode	
ethernet cfm y1731 global no ethernet cfm y1731 global	Open the Y1731 function. After initial this function, the switch will enter into the y1731 mode. The messages are sending and decoding in the Y1731 format. Notice: It need to use the ethernet cfm global command before using this command, otherwise, it cannot be function. No command disables it.

4. Create MD

Command	Explanation
Global mode	
ethernet cfm domain < domain-name > level < level-id > no ethernet cfm domain < domain-name >	Build up MD: enter into the MD configuration mode. If the MD is created successfully, the level will not be allowed to modify. No command deletes the created MD.
MD Configuration Mode	
id { mac-address XX-XX-XX-XX-XX-XX domain-number < domain-number > | dns < dns-name > | null } no id	Configure MDID. Domain-name which is configured by the name of maintenance domain will use the command of ethernet cfm domain will not be fill in the message. Fill in the MDID and ma name will create MAID; the total length of MAID is 44. The length cannot be existed; otherwise, it will have error. No command deletes the configured id.

5. Create MA

Command	Explanation
MD Configuration Mode	
service { < ma-name > | number < ma-num > | pvlan < vlan-id > } { port | pvlan < vlan-id > } [vlan < WORD >] [direction down] no service { < ma-name > | number < ma-num > | pvlan < vlan-id > }	Build up MA. Configure the property of UP/DOWN of MA and enter into MA mode. One service can related to one or more vlan. If MA is created successfully, the association vlan and UP/DOWN property will not be allowed to modify. If there is need to modify, delete the MA first and create it again.One switch can configure maximum 512 MA. No command deletes the created MA.

6. Create MEP

Command	Explanation
MA Configuration Mode	
mep mepid < WORD > no mep mepid [< WORD >]	Using this command to build up the permit configured MEP table in the maintenance collection. No command deletes the created MEP.
Port Mode	
ethernet cfm mep < mepid > domain < domain-name > service { < ma-name > | number < ma-num > | pvlan < vlan-id > } no ethernet cfm mep < mepid > domain < domain-name > service { < ma-name > | number < ma-num > | pvlan < vlan-id >]}	Build up MEP on port. The MEP property has been formed when creating the MA. If MA is UP/DOWN property, all MEP points in this MA are UP-DOWN property. No command deletes the created MEP.

7. Configure RMEP

Command	Explanation
MA Configuration Mode	
continuity-check receive rmep <mep-id> [active time < time >] no continuity-check receive rmep <mep-id>	Open CCM message receiving function and build up rmep in MA. If the mepid in an MA has been configured as MEP, it cannot be configured as RMEP. No command deletes the configured RMEP.

8. Create MIP (selectable)

Command	Explanation
MD Configuration Mode; MA Configuration Mode	
mip auto-create [lower-mep-only | none] no mip auto-create	Configure the automatic MIP in the maintenance collection's domain. As default, there is no rule of configuring the mid point; and it does not carry the sender-id. No command deletes the MIP.
Global Mode	
ethernet cfm mip auto-create level < level-id > vlan < WORD > [lower-mep-only] [sender-id chassis] no mip auto-create	Build up the MIP configuration on the layer that does not relate to MA. As default, there is no rule of configuring the mid point; and it does not carry the sender-id. No command deletes the MIP.

9. Enable the failure confirmation function (selectable)

Command	Explanation
Global mode	
ethernet cfm alarm { delay < mseconds > | notification { all | error-xcon | mac-remote-error-xcon | none | remote-error-xcon | xcon } | reset < mseconds > } no ethernet cfm alarm { delay | notification { all | error-xcon | mac-remote-error-xcon | none | remote-error-xcon | xcon } | reset }	Enable the function of error alarm. No command recovers to be default.
ethernet cfm logging no ethernet cfm logging	Open the log record function. If alarm is occur, it means that has already recorded or inform out of order. No command disables this function.
ethernet cfm snmp-server enable traps no ethernet cfm snmp-server enable traps	Having the snmp notification during the alarm. If the set up is success, it will have the snmp notification during the alarm. No command disables this function.

10. **Configure CC sending and detecting**

Command	Explanation
MA Configuration Mode	
continuity-check enable no continuity-check enable	Using this command to open the maintenance point of CCM message sending and receiving functions. No command cancels the local CCM packets sending and detection.
continuity-check interval < interval-value > no continuity-check interval	Configure the time interval value for sending message from MEP to CCM. Under the software mode, the minimum sending cycle is 100ms (interval value=3) and under the hardware mode, the minimum sending cycle is 3.3ms (interval value=1). No command recovers to be 1s (interval value=4).

11. **Check the configuration result of CFM**

Command	Explanation
Admin Mode	
show ethernet cfm domain { < domain_name > | brief }	Display the configured information of maintenance domain.
show ethernet cfm service [domain < domain-name > [service { ma-name | number < ma-num > | pvlan < vlan-id > }]]	Display the configured information of the maintenance collection.
show ethernet cfm maintenance-points local [detail] [mep | mip] [domain < domain-name > | interface { ethernet | } <IFNAME>]	Display the attribute and the operation information of the maintenance basepoint.
show ethernet cfm maintenance-points remote detail (mac XX-XX-XX-XX-XX-XX | domain WORD (service ((WORD)|(number <0-65535>)|(pvlan <1-4094>))) mepid <1-4094>)	Display the attribute and the operation information for the outlaying maintenance base point.
show ethernet cfm maintenance-points remote (domain WORD (service (WORD|number <0-65535>|pvlan <1-4094>) (mepid <1-4094>|)|)|)	Display the attribute and operation information of outlaying maintenance base point.
show ethernet cfm statistic [domain < domain-name > [service { ma-name | number < ma-num > | pvlan < vlan-id > }]]	Display the message sending statistics information in the CFM of the facility.

15.5 CFM OAM Failure Confirmation

15.5.1 The Confirmation of Management topology

Before execute the failure confirmation, please ensure to finish the configuration of CFM OAM function.

The following data are needed to the inspection of failure manually:

Serial number	Data
1	MD name
2	MA name
3	Destination MEP ID or MAC
4	The require number, size and overtime of sending message from the loop-back function.
5	The TTL value of linktrace function which need to send

15.5.2 Implement Loopback Function

Under the admin mode, implement the commands:

Command	Explanation
Admin Mode	
ping ethernet [target-mep < mepid > | target-mac < mac-address >] domain < domain-name > service < ma-name > | number < ma-num > | pvlan < vlan-id > [number < number >] [packetsize < size >] [timeout < timeout >]	Open the circulate function. Send LBM messages and receiving LBR message from a particular maintenance point to the other points. Under the default stage, this function is closed. If enter into target-mep-id, it cannot searching the corresponding mac address. If it cannot find, it will display error. If you enter the mac address, then will according to this address for the circulation. If it is a domain-name, then it require opening the y1731function, then sending the group broadcast LBM message.

15.6 CFM OAM Failure Orientation

15.6.1 Management topology Confirmation

Before execute the confirmation of failure, please ensure the completion of CFM OAM function configuration.

To testing the failure manually need to prepare the following data:

Serial number	Data
1	MD name
2	MA name
3	Destination MEP ID or MAC
4 (selectable)	The largest run after reading
5 (selectable)	Only enquire for FDB; or need to enquire both FDB and MIP data for undergo the failure confirmation
6 (selectable)	MEP ID that initiates LTM

15.6.2 CFM OAM Failure Orientation Task List

1. Implement linktrace function

Command	Explanation
Admin Mode	
traceroute ethernet { target-mep < target-mep-id > | target-mac < mac-address > } {domain < domain-name > service { < ma-name > | number < ma-num > | pvlan < vlan-id > }} [fdb-only | source < mepid >]] [ttl < ttl-value >]	Check the path from the appointed maintaining point to the target point. As default, ttl=64 and inquiry FDB and MIP database.

2. Configure auto-linktrace function (selectable)

Command	Explanation
MA Configuration Mode	
traceroute ethernet auto no traceroute ethernet auto	Enable the function of sending the link track packets automatically. Enable the function of sending the link track packets automatically. As default, this function is disabled. **Notice:** After enabled this function, when the maintaining point does not receive the CCM packets from the distant point in 3.5 sending cycles of CCM packets, judge that the connection to the distant point is wrong, then send LTM packet (the target of this LTM packet is the distant maintaining point, the TTL field in LTM packet is the maximum value of 255) to locate the error through detecting the responded LTR packet. No command disables this function.
Global Mode	
ethernet cfm auto-traceroute cache { size < size-value > | hold-time <minutes> } no ethernet cfm auto-traceroute cache { size | hold-time }	Configure saving the size of automatic LT detection result or over time result. As default, The buffer just records the 5 least automatic detection result, the overtime as 100minutes. No command recovers to be default.

3. View the result of auto-linktrace

Command	Explanation
Admin Mode	
show ethernet cfm traceroute-reply auto [domain < domain_name > [service { ma-name | number < ma-num > | pvlan < vlan-id > }]]	Display the result of the automatic LT. If there is no appointed domain, then it will display all the automatic LT result in the facilities. If there is no appointed ma, then it will display particular domain's automatic LT result in the facilities.

15.7 ULPP Linkage (Selectable)

15.7.1 ULPP Linkage Task List

1. Configure ulpp linkage

- Configure with the topology and ensure CC function is running normally.
- Configure the ULPP function first.
- ULPP linkage is just with down MEP.
- The vlan associated with linkage MEP must be in the protection vlan of the relevant ULPP group.

Command	Explanation
Port Mode	
switchport ulpp group <group-id> track cfm cc level <level-value>	Configure ulpp group member port to associate with cfm cc detection. When ulpp group member port received the matching cfm information (timeout or recover), conduct the association.

2. Check the result of ULPP linkage configuration

Command	Explanation
Admin Mode	
show ulpp group <word>	Check the result of ULPP association configuration. If the configuration is successful, the level of MD in Track-cfm-level will be shown.

15.7.2 Example of ULPP linkage application

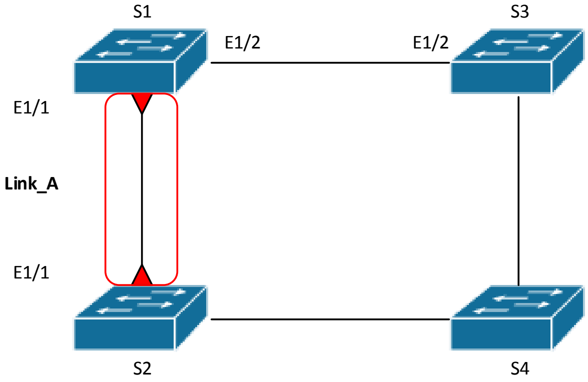


Figure 15.6: ULPP linkage application Figure

1. The consider path of configuration:
Using the following path of configuration to configure the ULPP linkage function:

- Build up the VLAN, and adding the related ports to corresponding VLAN.
- Build up the MD link_A in S1, S2 and the level is 4
- Build up and configure MA1 in customer_A (MA1 and VLAN1 related)
- Configure corresponding MEP and RMEP in the S1 and S2
- Build up the ulpp group1 in S1 and configure the main and assist port
- Configure corresponding flush receiving port to S2 and S3
- Configure linkage port in the S1

2. Steps of Configuration
(1) Build up VLAN, and adding the related ports to corresponding VLAN
(2) Build up the MD link_A and corresponding MEP and RMEP in S1 and S2

```
# Build up the link_A in S1 and configure corresponding MEP and RMEP
Switch(config)#ethernet  cfm domain link_A level 4
Switch(config-ecfm)#service MA1 pvlan 1 direction down
Switch(config-ecfm-srv)#mep mepid 1-2
Switch(config-ecfm-srv)#continuity-check enable
Switch(config-ecfm-srv)#continuity-check receive rmep 2
Switch(config-ecfm-srv)#exit
Switch(config-ecfm)exit
Switch(config)#interface ethernet 1/1
Switch(config-if-ethernet1/1)#ethernet cfm mep 1 domain link_A service MA1
```

Using the same method to build up the link_A in S2 and configure corresponding MEP and RMEP

(3) Build up the ulpp group 1 in S1 and protect vlan1

```
# Build up the ulpp group 1 in S1 and open the grabbing mode to protect vlan
Switch(config)#spanning-tree mst configuration
Switch(config-mstp-region)#instance 1 vlan 1
Switch(config-mstp-region)#exit
Switch(config)#ulpp group 1
Switch(ulpp-group-1)#protect vlan-reference-instance 1
Switch(ulpp-group-1)#flush enable mac-vlan
Switch(ulpp-group-1)#preemption mode
# configure the 1/1 in S1 to become the master port, and the 1/2 as slave port
Switch(config)#interface ethernet 1/1
Switch(config-if-ethernet1/1)#ulpp group 1 master
Switch(config)#interface ethernet 1/2
Switch(config-if-ethernet1/2)#ulpp group 1 master
# Configure the receiving port 1/1 in S2 to receive flush message
Switch(config-if-ethernet1/1)#ulpp flush enable mac-vlan
```

Using the same method to configure the receiving port 1/2 in S3 to receive flush message
(4) Configure ulpp linkage in the S1

```
# Configure ulpp linkage in the 1/1 port in S1
Switch(config-if-ethernet1/1)#switchport ulpp group 1 track cfm level 4
```

3. Checking the configuration result

```
# Checking the ulpp linkage configuration result in S1
Switch(config)#show ulpp group 1
ULPP group 1 information:
Description:
Preemption mode: ON
Preemption delay: 30s
Control VLAN: 1
Flush packet: MAC MAC-VLAN  ARP
Protected VLAN: Reference Instance 1
Member          Role        State        Track-cfm-level
-----------------------------------------------------------------------------------

Ethernet1/1     MASTER      FORWARD             4
Ethernet1/2     SLAVE       STANDBY             -
-----------------------------------------------------------------------------------
# if the CFM checking the CC is overtime, then it will inform the ULPP function to
# undergo the switching of main and assist ports:
%Jan 01 00:12:19 2012 ULPP: ULPP group 1:Master port Ethernet1/3 receives cfm event
        type:CFM_ALARM_RMEP_CCM vlan:1 level:4.
%Jan 01 00:12:19 2006 ULPP: ULPP group 1:Master port Ethernet1/3 change state to down,
        Slave port Ethernet1/1 change state to forwarding.
%Jan 01 00:12:21 2006 CFM:A CFM_ALARM_RMEP_CCM of Interface Ethernet1/3 is detected.
```

15.8 Example of Configuration Application

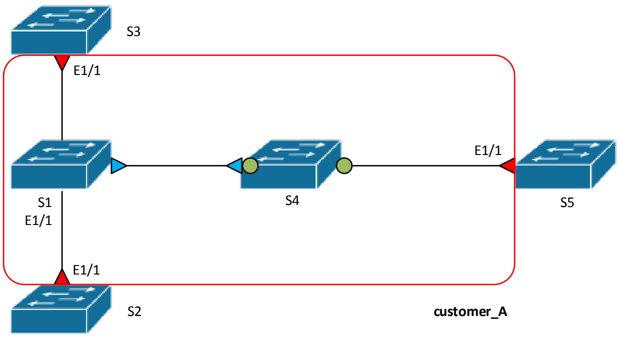


Figure 15.7: MD, MA, MEP and MIP configuration figure

The following Figure 15.7 is the CFM configuration application illustration, in order to actualize the inspection of the status of linkage, can follow the steps as shown below to undergo the configuration.

1. The consider path of configuration

Using the following path of configuration to configure the Ethernet CFM basic function:

- Build up the VLAN, and adding the related ports to corresponding VLAN.
- Build up the customer_A on the facilities S1, S2, S3, S4, S5 , the level of customer_A is 6.
- Build up and configure MA1 in customer_A (MA1 and VLAN1 related)
- Build up operator_A in the facilities S1, S5, the level of operator_A is 3
- Build up and configure MA2 in operator_A (MA2 and VLAN2 related)
- Build up local and outlying MEP in the MA1 of customer_A in the S1, S2, S3, and S4
- Build up MIP in the customer_A of S4
- Configure local and outlying MEP in the MA2 of customer_A in the S1, S5
- Initial the sending and receiving function of CCM information

2. Steps of Configuration

(1) Build up VLAN, and adding the related ports to corresponding VLAN

(2) Open the Global CFM function and build up customer_A and configure MA1

```
# Build up the customer_A in S1, and configure the UP direction MA1
Switch(config)#ethernet cfm global
Switch(config)#ethernet cfm domain customer_A level 6
Switch(config-ecfm)#service MA1 pvlan 1
```

(3) Build up the customer_A and configure the MA1 on the S2, S3, S4, and S5

```
# Build up the customer_A in S2, and configure the Down direction MA2
Switch(config)#ethernet cfm global
Switch(config)#ethernet cfm domain customer_A level 6
Switch(config-ecfm)#service MA1 pvlan 1 direction down
```

Using the same method to build up the MD and MA on other facilities

(4) Build up local and outlying MEP in the MA1 of customer_A in the S1, S2, S3, and S4, also build up the MIP in S5.

```
# Build up MEP list as 1-4 in the MA1 of S1, configure RMEP2-4, and build up
# the Etherne1/1 on MEP1.
Switch(config-ecfm-srv)#mep mepid 1-4
Switch(config-ecfm-srv)#continuity-check receive rmep 2-4
Switch(config-ecfm-srv)exit
Switch(config-ecfm)exit
Switch(config)#interface ethernet 1/1
Switch(config-if-ethernet1/1)#ethernet cfm mep 1 domain customer_A service MA1
# Build up MEP list as 1-4 in the MA1 of S2, configure RMEP1; 3-4, and build
# up the Etherne1/1 on MEP2.
Switch(config-ecfm-srv)#mep mepid 1-4
Switch(config-ecfm-srv)#continuity-check receive rmep 1;3-4
Switch(config-ecfm-srv)exit
Switch(config-ecfm)exit
Switch(config)#interface ethernet 1/1
Switch(config-if-ethernet1/1)#ethernet cfm mep 2 domain customer_A service MA1
# Build up MEP list as 1-4 in the MA1 of S3, configure RMEP1; 2; 4, and build
# up the Etherne1/1 on MEP3.
Switch(config-ecfm-srv)#mep mepid 1-4
Switch(config-ecfm-srv)#continuity-check receive rmep 1;2;4
Switch(config-ecfm-srv)exit
Switch(config-ecfm)exit
Switch(config)#interface ethernet 1/1
Switch(config-if-ethernet1/1)#ethernet cfm mep 3 domain customer_A service MA1
# Build up MEP list as 1-4 in the MA1 of S4, configure RMEP1-3, and build up
# the Etherne1/1 on MEP3.
Switch(config-ecfm-srv)#mep mepid 1-4
Switch(config-ecfm-srv)#continuity-check receive rmep 1-3
Switch(config-ecfm-srv)exit
Switch(config-ecfm)exit
Switch(config)#interface ethernet 1/1
Switch(config-if-ethernet1/1)#ethernet cfm mep 4 domain customer_A service MA1
```

Using the default rules to build up MIP in the MA1 on S5

```
Switch(config-ecfm-srv)#mip auto-create
```

(5) Build up operator_A and configure MA2 on S1 and S5

```
#Build up operator_A on S1and configure MA2, the types as port
Switch(config)#ethernet cfm domain operator_A  level 3
Switch(config-ecfm)#service MA2 port direction down
```

Using the same method (S5) mention above to build up operator_A and MA2
(6) Build up local and outlying MEP in the MA2 of operator_A in the S1 and S5

```
# Build up MEP list as 1-2 in the S1, configure RMEP2, and build up the
# Etherne1/2 on MEP1.
Switch(config-ecfm-srv)#mep mepid 1-2
Switch(config-ecfm-srv)#continuity-check receive rmep 2
Switch(config-ecfm-srv)exit
Switch(config-ecfm)exit
Switch(config)#interface ethernet 1/2
Switch(config-if-ethernet1/1)#ethernet cfm mep 1 domain customer_A service MA2
# Build up MEP list as 1-2 in the S2, configure RMEP1, and build up the
# Etherne1/2 on MEP2.
Switch(config-ecfm-srv)#mep mepid 1-2
Switch(config-ecfm-srv)#continuity-check receive rmep 1
Switch(config-ecfm-srv)exit
Switch(config-ecfm)exit
Switch(config)#interface ethernet 1/2
Switch(config-if-ethernet1/1)#ethernet cfm mep 2 domain customer_A service MA2
```

(7) Initial the sending and receiving function of CCM information in S1, S2, S3, S4 in MA1

```
# Initial the sending and receiving function of CCM information in S1in MA1
Switch(config-ecfm-srv)#continuity-check receive enable
```

Other facilities using the same method to initial the CC function.

```
# Initial the sending and receiving function of CCM information in S1 and S5 in MA
Switch(config-ecfm-srv)#continuity-check receive enable
```

(8) To check the configuration of maintenance base point of MA1 in customer_A of S1

```
Switch#show ethernet cfm maintenance-points local detail mep domain customer_A
Mepid:1
Port:Ethernet1/1                    Active:1
Domain Name: customer_A
Service Name:MA1
Level:6
Vlan:1                                    Direction:Up
------------------------------------------------------------------------------
CCM:
CC Send:Enable
CC Received:Enable                        Interval:1(s)
```

15.9 CFM Troubleshooting

Undergo the configuration, using the CFM-OAM, it will occur errors and do not operate normally due to physical connection, configuration error.

- Ensure the whole link connection is normal, and the MA needed related vlan is existed.

1. Configuration Failure

- Ensure the system open the global OAM function, otherwise, it will failure to configure any related OAM commands
- Illegal configured MA/MD name:
  - **MD name:** 1∼43 characters straing.It can be formed by letter, number, underline and the first and the last character cannot be underline.

  - **MA name:** 1∼43 characters straing.It can be formed by letter, number, underline and the first and the last character cannot be underline. The sum of MA and the domain name cannot excess than 44 characters.

- In the same level, a primary vlan can only be related by one MA.
- MD level, MA related pvlan and UP/DOWN attribute cannot be changed after develop
- Need to build up the MEP ID before configure the MEP and RMEP
- MEP ID in one MA , after configured as MEP, the nit cannot be change to configure RMEP
- he DOWN attribute of MA in one facility can only allow existing one MEP; one UP attribute MA can allow to exist of several of MEP, but it cannot allow to configure several identical MA MEP to the same port.

2. Cannot build up the CC connection

- Through the show ethernet cfm to checking, ensure both port's level, MD name, MA name, MA related pvlan are the same.
- Ensure the configuration of RMEP of this port is same with the configured MEP ID at the other port.
- Ensure this port and the other port opened the CC sending and checking function
- Ensure the CCM sending period is the same for two port
- Configured the down mep on the port, then mep will receive the message from this port. If it configured the up mep, then the mep will receive the messages from others ports. Please ensure that the up mep configuration is on the non-receiving port.
- The port that is blocking by STP protocol cannot receiving, sending, replying the CFM messages. If it is configured as MEP, then even if that port was blocked by the STP protocol, it can still sending and receiving CCM messages. Only the second layer Ethernet port can support the CFM function.
- MEP and MIP can configure on the port channel, but at the same time, port channel configured MEP and MIP will ineffective on the members. If you want to increase the CFM MEP and MIP port to port channel, then that port's MEP and MIP will ineffective as well. If you want to recover the MEP and MIP on the port, then need to delete the port-channel from this port.

3. Cannot create the MIP point

- Ensure the develop rules of MIP is correct
  - **Default rules:** If there is not a higher level of MEP on the port, and at the same time, lower level of MIP does not exist, then it will build up MIP on particular port at this level.
  - **Explicit rules:** If there is not a higher level of MEP on the port, but at the same time, lower level of maintenance mid-point does not exist, then it will build up the mid-point depends on whether there is a maintenance base point on lower level.

- It will only develop the MIP as the port status as UP; one port bases on one vlan to develop only one MIP; lower MIP point will have higher priority to develop.
- A DOWN attribute MA is only need to configure on the port, if there is configured the MEP point in the port, then it cannot develop the MIP, even if there is configured the port-channel, it will cause the MEP ineffective. MIP cannot develop in the MA.

If it cannot solve the problem of CFM OAM after checking, then please using the debug ethernet cfm etc command, and copy the DEBUG information (3 minutes), and then sending to the technical center of our company.

Part III

VLAN and MAC Table Configuration

Chapter 16

VLAN Configuration

16.1 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 switch is implemented following IEEE 802.1Q.

The key idea of VLAN technology is that a large LAN can be partitioned into many separate broadcast domains dynamically to meet the demands.

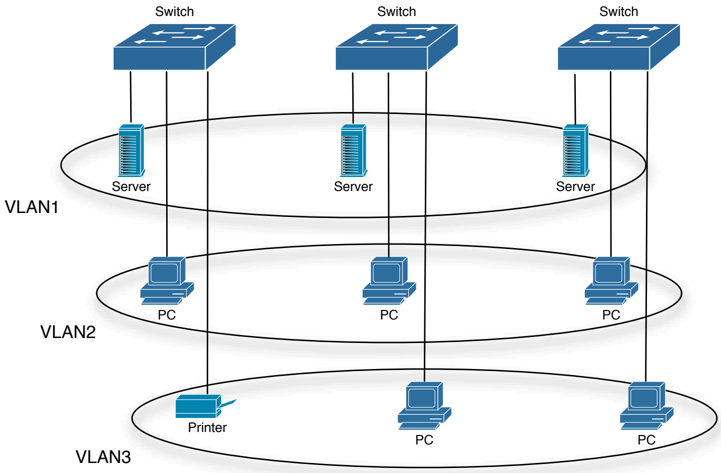


Figure 16.1: A VLAN network defined logically

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

Switch Ethernet Ports can works in three kinds of modes: Access, Hybrid and Trunk, each mode has a different processing method in forwarding the packets with tagged or untagged.

The ports of Access type only belongs to one VLAN, usually they are used to connect the ports of the computer.

The ports of Trunk type allow multi-VLANs to pass, can receive and send the packets of multi-VLANs. Usually they are used to connect between the switches.

The ports of Hybrid type allow multi-VLANs to pass, can receive and send the packets of multi-VLANs. They can be used to connect between the switches, or to a computer of the user.

Hybrid ports and Trunk ports receive the data with the same process method, but send the data with different method: Hybrid ports can send the packets of multi-VLANs without the VLAN tag, while Trunk ports send the packets of multi-VLANs with the VLAN tag except the port native VLAN.

The switch implements VLAN and GVRP (GARP VLAN Registration Protocol) which are defined by 802.1Q. The chapter will explain the use and the configuration of VLAN and GVRP in detail.

16.2 VLAN Configuration Task List

1. Create or delete VLAN
2. Set or delete VLAN name
3. Assign Switch ports for VLAN
4. Set the switch port type
5. Set Trunk port
6. Set Access port
7. Set Hybrid port
8. Enable/Disable VLAN ingress rules globally
9. Configure Private VLAN
10. Set Private VLAN association
11. Specify internal VLAN ID

1. Create or delete VLAN

Command	Explanation
Global mode	
vlan WORD no vlan WORD	Create/delete VLAN or enter VLAN Mode

2. Set or delete VLAN name

Command	Explanation
VLAN mode	
name <vlan-name> no name	Set or delete VLAN name.

3. Assigning Switch ports for VLAN

Command	Explanation
VLAN mode	
switchport interface <interface-list> no switchport interface <interface-list>	Assign Switch ports to VLAN.

4. Set the Switch Port Type

Command	Explanation
Port mode	
switchport mode { trunk | access | hybrid }	Set the current port as Trunk, Access or Hybrid port.

5. 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.

6. 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.

7. Set Hybrid port

Command	Explanation
Port mode	
switchport hybrid allowed vlan { WORD | all | add WORD | except WORD | remove WORD } { tag | untag } no switchport hybrid allowed vlan	Set/delete the VLAN which is allowed by Hybrid port with tag or untag mode.
switchport hybrid native vlan <vlan-id> no switchport hybrid native vlan	Set/delete PVID of the port.

8. Disable/Enable VLAN Ingress Rules

Command	Explanation
Global mode	
vlan ingress enable no vlan ingress enable	Enable/Disable VLAN ingress rules.

9. 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 private VLAN.

10. Set Private VLAN association

Command	Explanation
VLAN mode	
private-vlan association <secondary-vlan-list> no private-vlan association	Set/delete Private VLAN association.

11. Specify internal VLAN ID

Command	Explanation
Global mode	
vlan <2-4094> internal	Specify internal VLAN ID.

16.3 Typical VLAN Application

Scenario:

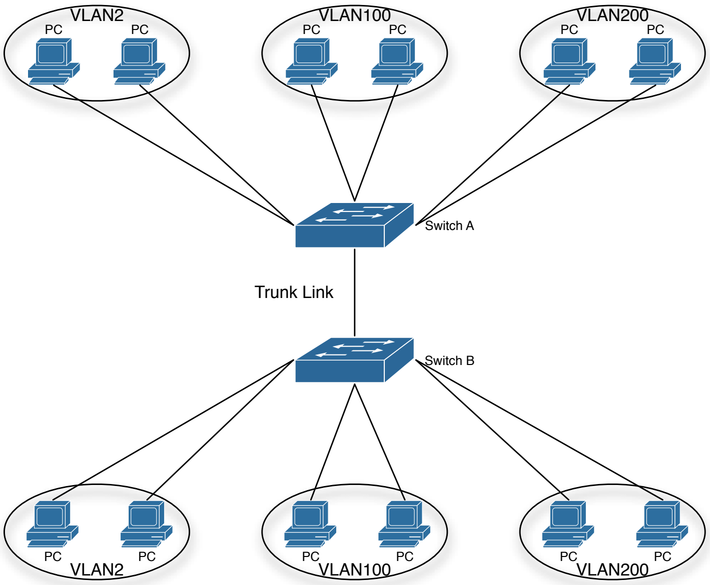


Figure 16.2: Typical VLAN Application Topology

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 are 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 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
```

16.4 Typical Application of Hybrid Port

Scenario:

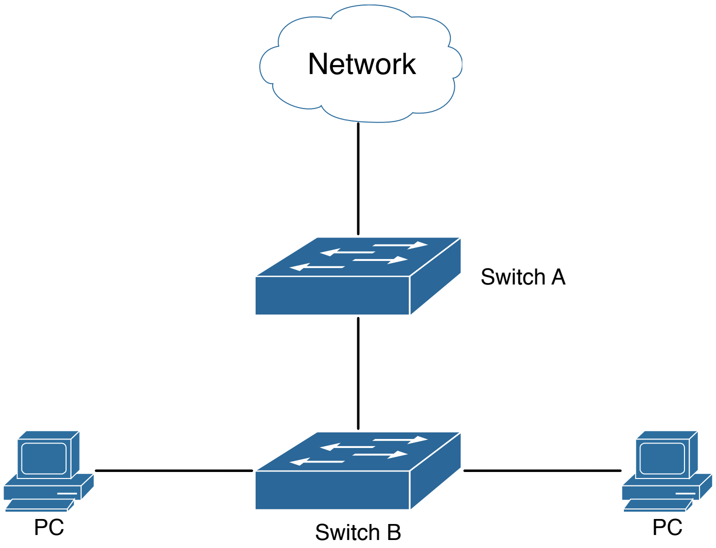


Figure 16.3: Typical Application of Hybrid Port

PC1 connects to the interface Ethernet 1/7 of SwitchB, PC2 connects to the interface Ethernet 1/9 of SwitchB, Ethernet 1/10 of SwitchA connect to Ethernet 1/10 of SwitchB.

It is required that PC1 and PC2 can not mutually access due to reason of the security, but PC1 and PC2 can access other network resources through the gateway SwitchA. We can implement this status through Hybrid port.

Configuration items are as follows:

Port	Type	PVID	the VLANs are allowed to pass
Port 1/10 of Switch A	Access	10	Allow the packets of VLAN 10 to pass with untag method.
Port 1/10 of Switch B	Hybrid	10	Allow the packets of VLAN 7, 9, 10 to pass with untag method.
Port 1/7 of Switch B	Hybrid	7	Allow the packets of VLAN 7, 10 to pass with untag method.
Port 1/9 of Switch B	Hybrid	9	Allow the packets of VLAN 9, 10 to pass with untag method.

The configuration steps are listed below:
Switch A:

```
Switch(config)#vlan 10
Switch(Config-Vlan10)#switchport interface ethernet 1/10
```

Switch B:

```
Switch(config)#vlan 7;9;10
Switch(config)#interface ethernet 1/7
Switch(Config-If-Ethernet1/7)#switchport mode hybrid
Switch(Config-If-Ethernet1/7)#switchport hybrid native vlan 7
Switch(Config-If-Ethernet1/7)#switchport hybrid allowed vlan 7;10 untag
Switch(Config-If-Ethernet1/7)#exit
Switch(Config)#interface Ethernet 1/9
Switch(Config-If-Ethernet1/9)#switchport mode hybrid
Switch(Config-If-Ethernet1/9)#switchport hybrid native vlan 9
Switch(Config-If-Ethernet1/9)#switchport hybrid allowed vlan 9;10 untag
Switch(Config-If-Ethernet1/9)#exit
Switch(Config)#interface Ethernet 1/10
Switch(Config-If-Ethernet1/10)#switchport mode hybrid
Switch(Config-If-Ethernet1/10)#switchport hybrid native vlan 10
Switch(Config-If-Ethernet1/10)#switchport hybrid allowed vlan 7;9;10 untag
Switch(Config-If-Ethernet1/10)#exit
```

Chapter 17

GVRP Configuration

17.1 Introduction to GVRP

GVRP, i.e. GARP VLAN Registration Protocol, is an application of GARP (Generic Attribute Registration Protocol). GARP is mainly used to establish an attribute transmission mechanism to transmit attributes, so as to ensure protocol entities registering and deregistering the attribute. According to different transmission attributes, GARP can be divided to many application protocols, such as GMRP and GVRP. Therefore, GVRP is a protocol which transmits VLAN attributes to the whole layer 2 network through GARP protocol.

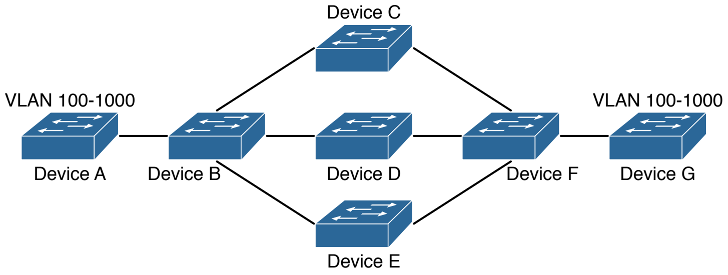


Figure 17.1: a typical application scene

A and G switches are not directly connected in layer 2 network; BCDEF are intermediate switches connecting A and G. Switch A and G configure VLAN100-1000 manually while BCDEF switches do not. When GVRP is not enabled, A and G cannot communicate with each other, because intermediate switches without relevant VLANs. However, after GVRP is enabled on all switches, its VLAN attribute transmission mechanism enables the intermediate switches registering the VLANs dynamically, and the VLAN in VLAN100-1000 of A and G can communicate with each other. The VLANs dynamically registered by intermediate switches will be deregistered when deregistering VLAN100-1000 of A and G switches manually. So the same VLAN of two unadjacent switches can communicate mutually through GVRP protocol instead of configuring each intermediate switch manually for achieving the purpose of simplifying VLAN configuration.

17.2 GVRP Configuration Task List

GVRP configuration task list:

1. Configure GVRP timer
2. Configure port type
3. Enable GVRP function

1. Configure GVRP timer

Command	Explanation
Global mode	
garp timer join <200-500> garp timer leave <500-1200> garp timer leaveall <5000-60000> no garp timer (join | leave | leaveAll)	Configure leaveall, join and leave timer for GVRP.

2. Configure port type

Command	Explanation
Port mode	
gvrp no gvrp	Enable/disable GVRP function of port.

3. Enable GVRP function

Command	Explanation
Global mode	
gvrp no gvrp	Enable/disable the global GVRP function of port.

17.3 Example of GVRP

GVRP application:

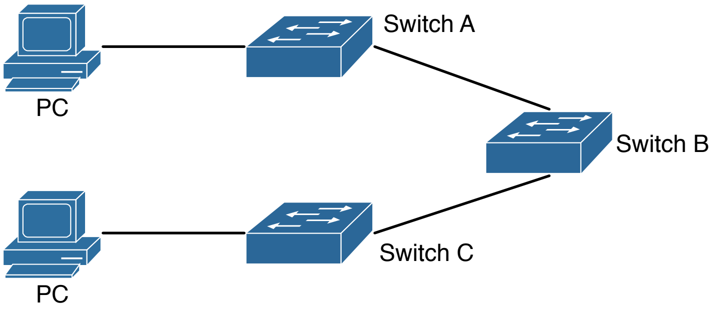


Figure 17.2: Typical GVRP Application Topology

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 two workstations 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 two workstations 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.

The configuration steps are listed below:

Switch A:

```
Switch(config)#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)#gvrp
Switch(Config-If-Ethernet1/11)#exit
```

Switch B:

```
Switch(config)#gvrp
Switch(config)#interface ethernet 1/10
Switch(Config-If-Ethernet1/10)#switchport mode trunk
Switch(Config-If-Ethernet1/10)#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)#gvrp
Switch(Config-If-Ethernet1/11)#exit
```

Switch C:

```
Switch(config)#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)#gvrp
Switch(Config-If-Ethernet1/11)#exit
```

17.4 GVRP Troubleshooting

The GARP counter setting for Trunk ports in both ends of Trunk link must be the same, otherwise GVRP will not work normally. It is recommended to avoid enabling GVRP and RSTP at the same time in switch. If GVRP needs to be enabled, RSTP function for the ports must be disabled first.

Chapter 18

MAC Table Configuration

18.1 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.

18.1.1 Obtaining MAC Table

The MAC table can be built up statically and dynamically. Static configuration is to set up a mapping between the MAC addresses and the ports; dynamic learning is the process in which the switch learns the mapping between MAC addresses and ports, and updates the MAC table regularly. In this section, we will focus on the dynamic learning process of MAC table.

The topology of the figure above: 4 PCs connected to switch, where PC1 and PC2 belongs to a same physical segment (same collision domain), the physical segment connects to port 1/5 of switch; PC3 and PC4 belongs to the same physical segment that connects to port 1/12 of switch.

The initial MAC table contains no address mapping entries. Take the communication of PC1 and PC3 as an example, the MAC address learning process is as follow:

1. When PC1 sends message to PC3, the switch receives the source MAC address 00-01-11-11-11-11 from this message, the mapping entry of 00-01-11-11-11-11 and port 1/5 is added to the switch MAC table.

2. At the same time, the switch learns the message is destined to 00-01-33-33-33-33, as the MAC table contains only a mapping entry of MAC address 00-01-11-11-11-11 and port1/5, 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).

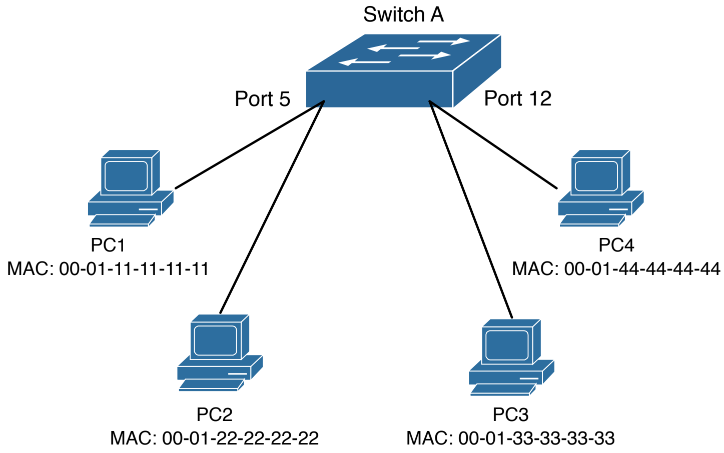


Figure 18.1: MAC Table dynamic learning

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 -port1/12.

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 in 300 to 2*300 seconds (ie, in single to double aging time). The 300 seconds here is the default aging time for MAC address entry in switch. Aging time can be modified in switch.

18.1.2 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 switch have learnt the MAC address of PC1 and PC3, and the user manually configured the mapping relationship for PC2 and PC4 to ports. The MAC table of switch will be:

MAC Address	Port number	Entry added by
00-01-11-11-11-11	1/5	Dynamic learning
00-01-22-22-22-22	1/5	Static configuration
00-01-33-33-33-33	1/12	Dynamic learning
00-01-44-44-44-44	1/12	Static configuration

1. Forward data according to the MAC table

If PC1 sends a message to PC3, the switch will forward the data received on port 1/5 from port 1/12.

2. Filter data according to the MAC table

If PC1 sends a message to PC2, the switch, on checking the MAC table, will find PC2 and PC1 are in the same physical segment and filter the message (i.e. drop this message).

Three types of frames can be forwarded by the switch:

- Broadcast frame
- Multicast frame
- Unicast frame

The following describes how the switch deals with all the three types of frames:

- **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.
- **Multicast frame:** For the unknown multicast, the switch will broadcast it in the same vlan, but the switch only forwards the multicast frames to the multicast group's port if IGMP Snooping function or the static multicast group has been configured.
- **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.

18.2 Mac Address Table Configuration Task List

1. Configure the MAC address aging-time
2. Configure static MAC forwarding or filter entry
3. Clear dynamic address table

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 | static-multicast | blackhole } address <mac-addr> vlan <vlan-id > [interface ethernet <interface-name>] | [source | destination | both] no mac-address-table { static | static-multicast | blackhole | dynamic } [address <mac-addr>] [vlan <vlan-id>] [interface ethernet <interface-name>]	Configure static MAC entries, static multicast MAC entries, filter address entires.

3. Clear dynamic address table

Command	Explanation
Admin Mode	
clear mac-address-table dynamic [address <mac-addr>] [vlan <vlan-id>] [interface [ethernet | portchannel] <interface-name>]	Clear the dynamic address table.

18.3 Typical Configuration Examples

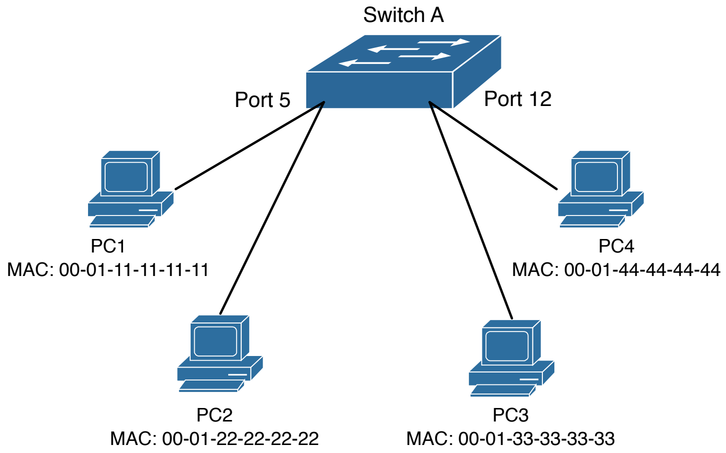


Figure 18.2: MAC Table typical configuration example

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 1/7 and port 1/9, 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 1/7 and port 1/9, respectively.

```
Switch(config)#mac-address-table static address 00-01-22-22-22-22
                        vlan 1 interface ethernet 1/7
Switch(config)#mac-address-table static address 00-01-33-33-33-33
                        vlan 1 interface ethernet 1/9
```

18.4 MAC Table Troubleshooting

Using the show mac-address-table command, a port is found to be failed to learn the MAC of a device connected to it. Possible reasons:

- The connected cable is broken.
- Spanning Tree is enabled and the port is in 'discarding' status; or the device is just connected to the port and Spanning Tree is still under calculation, wait until the Spanning Tree calculation finishes, and the port will learn the MAC address.
- If not the problems mentioned above, please check for the switch portand contact technical support for solution.

18.5 MAC Address Function Extension

18.5.1 MAC Address Binding

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.

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
4. mac-notification trap configuration

1. Enable MAC address binding function for the ports

Command	Explanation
Port Mode	
switchport port-security no switchport port-security	Enable MAC address binding function for the port and lock the port. When a port is locked, the MAC address learning function for the port will be disabled: the 'no switchport port-security' command disables the MAC address binding function for the port, and restores the MAC address learning function for the port.

2. Lock the MAC addresses for a port

Command	Explanation
Port Mode	
switchport port-security lock no switchport port-security lock	Lock the port, then MAC addresses learned will be disabled. The 'no switchport port-security lock' command restores the function.
switchport port-security convert	Convert dynamic secure MAC addresses learned by the port to static secure MAC addresses.
switchport port-security timeout <value> no switchport port-security timeout	Enable port locking timer function; the 'no switchport port-security timeout' restores the default setting.
switchport port-security mac-address <mac-address> no switchport port-security mac-address <mac-address>	Add static secure MAC address; the 'no switchport 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	
switchport port-security maximum <value> no switchport port-security maximum <value>	Set the maximum number of secure MAC addresses for a port; the 'no switchport port-security maximum' command restores the default value.
switchport port-security violation { protect | shutdown } [recovery <30-3600>] no switchport port-security violation	Set the violation mode for the port; the 'no switchport port-security violation' command restores the default setting.

4. **mac-notification trap configuration**

Command	Explanation
Global Mode	
mac-address-table synchronizing enable no mac-address-table synchronizing enable	Enable the monitor function for MAC, if a MAC is added or deleted, the system will report this monitored event; the no command will cancel this function.
mac-address-table periodic-monitor-time <5-86400>	Set the MAC monitor interval to count the added and deleted MAC in time, and send out them with trap message.
mac-address-table trap enable no mac-address-table trap enable	Enable or disable mac notification trap passthrough.

Binding MAC Address Binding Troubleshooting

Enabling MAC address binding for ports may fail in some occasions. Here are some possible causes and solutions:

- If MAC address binding cannot be enabled for a port, make sure the port is not enabling 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.

18.6 MAC Notification Configuration

18.6.1 Introduction to MAC Notification

MAC Notification function depends on the notification. Add or remove the MAC address, namely, when the device is added or removed, it will notify administrator about the changing by the trap function of snmp.

18.6.2 MAC Notification Configuration

Mac notification configuration task list:

1. Configure the global snmp MAC notification
2. Configure the global MAC notification
3. Configure the interval for sending MAC notification
4. Configure the size of history table
5. Configure the trap type of MAC notification supported by the port
6. Show the configuration and the data of MAC notification
7. Clear the statistics of MAC notification trap

1. Configure the global snmp MAC notification

Command	Explanation
Global mode	
snmp-server enable traps mac-notification no snmp-server enable traps mac-notification	Configure or cancel the global snmp MAC notification.

2. Configure the global MAC notification

Command	Explanation
Global mode	
mac-address-table notification no mac-address-table notification	Configure or cancel the global MAC notification.

3. Configure the interval for sending MAC notification

Command	Explanation
Global mode	
mac-address-table notification interval <0-86400> no mac-address-table notification interval	Configure the interval for sending the MAC address notification, the no command restores the default interval.

4. Configure the size of history table

Command	Explanation
Global mode	
mac-address-table notification history-size <0-500> no mac-address-table notification history-size	Configure the history table size, the no command restores the default value.

5. Configure the trap type of MAC notification supported by the port

Command	Explanation
Port mode	
mac-notification { added | both | removed } no mac-notification	Configure or cancel the trap type of MAC notification supported by the port.

6. Show the configuration and the data of MAC notification

Command	Explanation
Admin mode	
show mac-notification summary	Show the configuration and the data of MAC notification.

7. Clear the statistics of MAC notification trap

Command	Explanation
Admin mode	
clear mac-notification statistics	Clear the statistics of MAC notification trap.

18.6.3 MAC Notification Example

IP address of network management station (NMS) is 1.1.1.5, IP address of Agent is 1.1.1.9. NMS will receive Trap message from Agent. (Note: NMS may set the authentication to the community character string of trap, suppose the community character string as usertrap) Configuration procedure in the following:

```
Switch(config)#snmp-server enable
Switch(config)#snmp-server enable traps mac-notification
Switch(config)#mac-address-table notification
Switch(config)#mac-address-table notification interval 5
Switch(config)#mac-address-table notification history-size 100
Switch(Config-If-Ethernet1/4)#mac-notification both
```

18.6.4 MAC Notification Troubleshooting

Check whether trap message is sent successfully by show command and debug command of snmp.

Part IV

MSTP Configuration

Chapter 19

MSTP Configuration

19.1 Introduction to MSTP

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.

19.1.1 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:

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

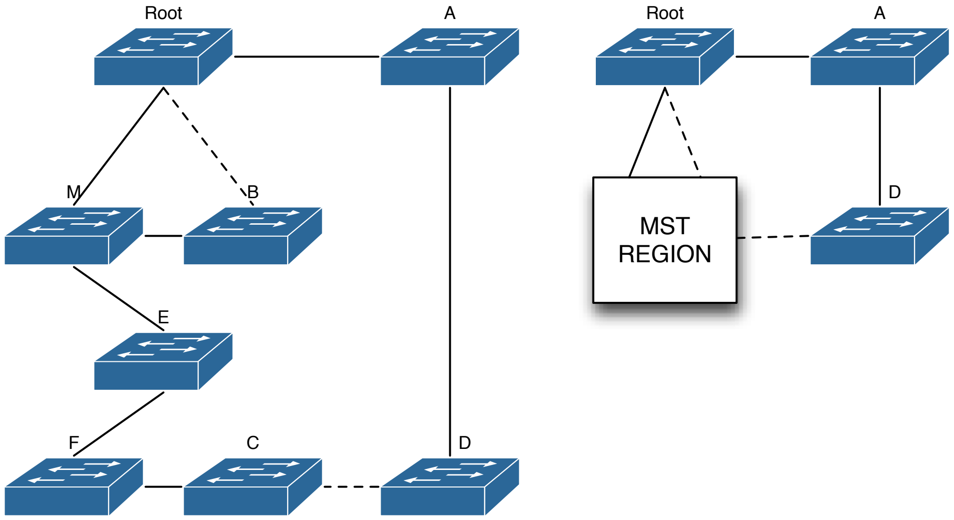


Figure 19.1: Example of CIST and MST Region

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.

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.

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.

19.1.2 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.

19.1.3 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.

19.2 MSTP Configuration Task List

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 spanning-tree attribute of port
8. Configure the snooping attribute of authentication key
9. 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 | rstp } 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 of the switch.
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> port-priority <port-priority> no spanning-tree mst <instance-id> port-priority	Set port priority for specified instance.
spanning-tree mst <instance-id> rootguard no spanning-tree mst <instance-id> root-guard	Configure currently port whether running root-guard in specified instance, configure the root-guard port can't turn to root port.
spanning-tree rootguard no spanning-tree rootguard	Configure currently port whether running root-guard in instance 0, configure the rootguard port can't turn to root port.
spanning-tree [mst <instance-id>] loop-guard no spanning-tree [mst <instance-id>] loop-guard	Enable loopguard function on specified instance, the no command disables this function.

3. Configure MSTP region parameters

Command	Explanation
Global Mode	
spanning-tree mst configuration no spanning-tree mst configuration	Enter MSTP region mode. The no command restores the default setting.
MSTP region mode	
show	Display the information of the current running system.
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.
no	Cancel one command or set initial value.

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 [bpdufilter | bpduguard] [recovery <30-3600>] no spanning-tree portfast	Set and cancel the port to be an boundary port. bpdufilter receives the BPDU discarding; bpduguard receives the BPDU will disable port; no parameter receives the BPDU, the port becomes a non-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 spanning-tree attribute of port

Command	Explanation
Port Mode	
spanning-tree cost no spanning-tree cost	Set the port path cost.

spanning-tree port-priority no spanning-tree port-priority	Set the port priority.
spanning-tree rootguard no spanning-tree rootguard	Set the port is root port.
Global Mode	
spanning-tree transmit-hold-count <tx-hold-count-value> no spanning-tree transmit-hold-count	Set the max transmit-hold-count of port.
spanning-tree cost-format { dot1d | dot1t }	Set port cost format with dot1d or dot1t.

8. 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. The no command restores to use the generated string.

9. Configure the FLUSH mode once topology changes

Command	Explanation
Global Mode	
spanning-tree tcflush { enable | disable | 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. The no command restores to default setting, enable flush once the topology changes.
Port Mode	
spanning-tree tcflush { enable | disable | protect } no spanning-tree tcflush	Configure the port flush mode. The no command restores to use the global configured flush mode.

19.3 MSTP Example

The following is a typical MSTP application example:

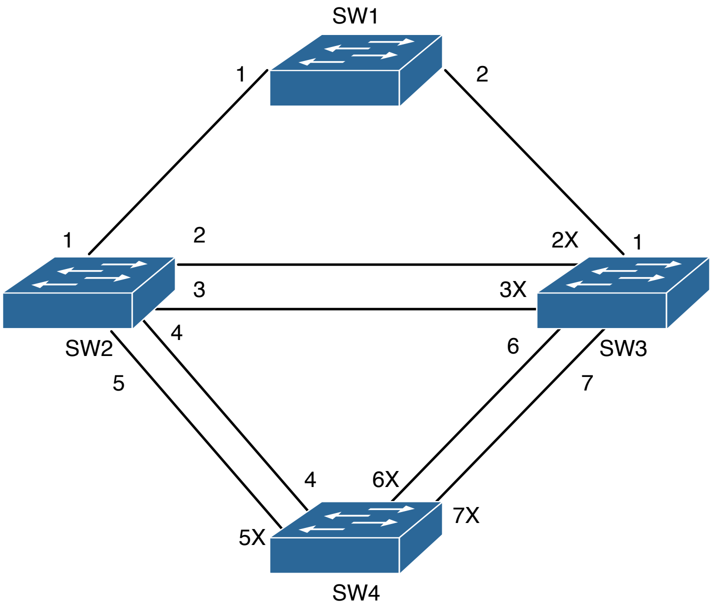


Figure 19.2: Typical MSTP Application Scenario

The connections among the switches are shown in the above figure. All the switches run in the MSTP mode by default, their bridge priority, port priority and port route cost are all in the default values (equal). The default configuration for switches is listed below:

Bridge Name		SW1	SW2	SW3	SW4
Bridge MAC		...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 Switch2, Switch3 and Switch4.
- Set ports 1-7 as trunk ports in Switch2 Switch3 and Switch4.

Step 2: Set Switch2, Switch3 and Switch4 in the same MSTP:

- Set Switch2, Switch3 and Switch4 to have the same region name as mstp.
- Map VLAN 20 and VLAN 30 in Switch2, Switch3 and Switch4 to Instance 3; Map VLAN 40 and VLAN 50 in Switch2, Switch3 and Switch4 to Instance 4.

Step 3: Set Switch3 as the root bridge of Instance 3; Set Switch4 as the root bridge of Instance 4

- Set the bridge priority of Instance 3 in Switch3 as 0.
- Set the bridge priority of Instance 4 in Switch4 as 0.

The detailed configuration is listed below:
Switch2:

```
Switch2(config)#vlan 20
Switch2(Config-Vlan20)#exit
Switch2(config)#vlan 30
Switch2(Config-Vlan30)#exit
Switch2(config)#vlan 40
Switch2(Config-Vlan40)#exit
Switch2(config)#vlan 50
Switch2(Config-Vlan50)#exit
Switch2(config)#spanning-tree mst configuration
Switch2(Config-Mstp-Region)#name mstp
Switch2(Config-Mstp-Region)#instance 3 vlan 20;30
Switch2(Config-Mstp-Region)#instance 4 vlan 40;50
Switch2(Config-Mstp-Region)#exit
Switch2(config)#interface e1/0/1-7
Switch2(Config-Port-Range)#switchport mode trunk
Switch2(Config-Port-Range)#exit
Switch2(config)#spanning-tree
```

Switch3:

```
Switch3(config)#vlan 20
Switch3(Config-Vlan20)#exit
Switch3(config)#vlan 30
Switch3(Config-Vlan30)#exit
Switch3(config)#vlan 40
Switch3(Config-Vlan40)#exit
```

```
Switch3(config)#vlan 50
Switch3(Config-Vlan50)#exit
Switch3(config)#spanning-tree mst configuration
Switch3(Config-Mstp-Region)#name mstp
Switch3(Config-Mstp-Region)#instance 3 vlan 20;30
Switch3(Config-Mstp-Region)#instance 4 vlan 40;50
Switch3(Config-Mstp-Region)#exit
Switch3(config)#interface e1/0/1-7
Switch3(Config-Port-Range)#switchport mode trunk
Switch3(Config-Port-Range)#exit
Switch3(config)#spanning-tree
Switch3(config)#spanning-tree mst 3 priority 0
```

Switch4:

```
Switch4(config)#vlan 20
Switch4(Config-Vlan20)#exit
Switch4(config)#vlan 30
Switch4(Config-Vlan30)#exit
Switch4(config)#vlan 40
Switch4(Config-Vlan40)#exit
Switch4(config)#vlan 50
Switch4(Config-Vlan50)#exit
Switch4(config)#spanning-tree mst configuration
Switch4(Config-Mstp-Region)#name mstp
Switch4(Config-Mstp-Region)#instance 3 vlan 20;30
Switch4(Config-Mstp-Region)#instance 4 vlan 40;50
Switch4(Config-Mstp-Region)#exit
Switch4(config)#interface e1/0/1-7
Switch4(Config-Port-Range)#switchport mode trunk
Switch4(Config-Port-Range)#exit
Switch4(config)#spanning-tree
Switch4(config)#spanning-tree mst 4 priority 0
```

After the above configuration, Switch1 is the root bridge of the instance 0 of the entire network. In the MSTP region which Switch2, Switch3 and Switch4 belong to, Switch2 is the region root of the instance 0, Switch3 is the region root of the instance 3 and Switch4 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 Switch2 is the master port of the instance 3 and the instance 4.

The MSTP calculation generates 3 topologies: the instance 0, the instance 3 and the instance 4 (marked with blue lines). The ports with the mark 'X' are in the status of discarding. The other ports are the status of forwarding. Because the instance 3 and the instance 4 are only valid in the MSTP region, the following figure only shows the topology of the MSTP region.

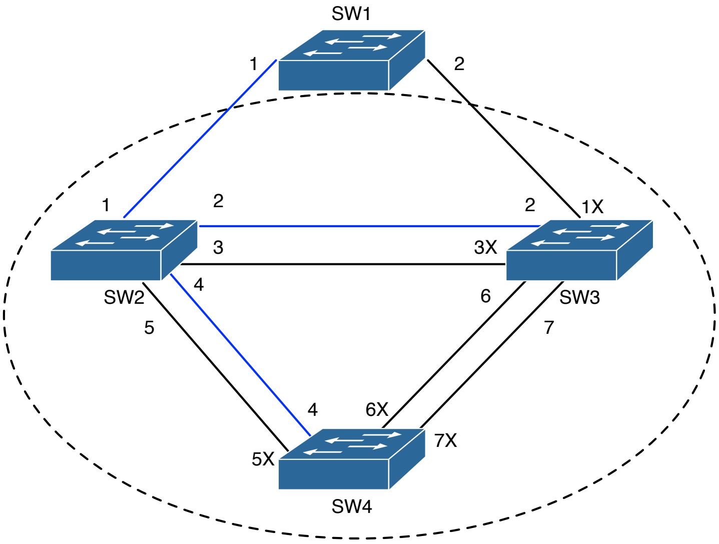


Figure 19.3: The Topology Of the Instance 0 after the MSTP Calculation

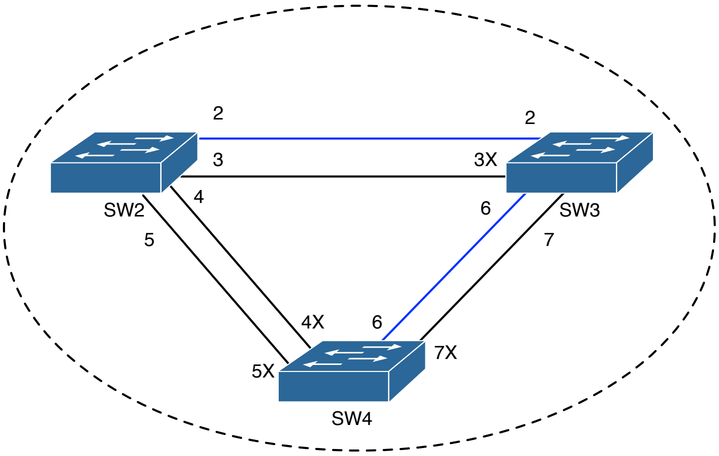


Figure 19.4: The Topology Of the Instance 3 after the MSTP Calculation

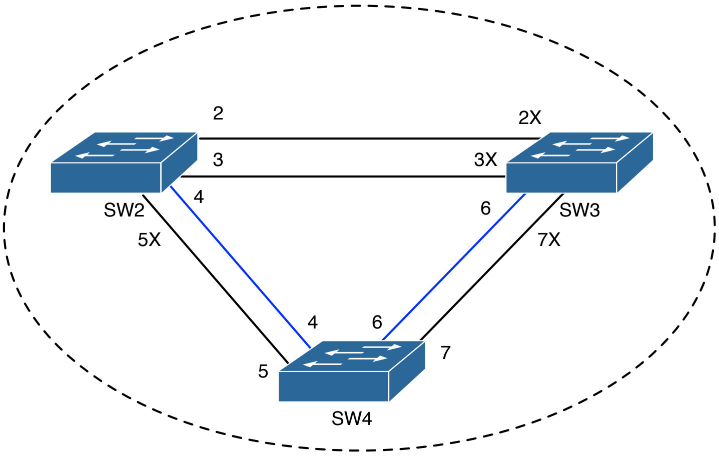


Figure 19.5: The Topology Of the Instance 4 after the MSTP Calculation

19.4 MSTP Troubleshooting

- In order to run the MSTP on the switch port, the MSTP has to be enabled globally. If the MSTP is not enabled globally, it can't be enabled on the port.
- The MSTP parameters co work with each other, so the parameters should meet the following conditions. Otherwise, the MSTP may work incorrectly.

  2 x (Bridge_Forward_Delay - 1.0 seconds) >= Bridge_Max_Age

  Bridge_Max_Age >= 2 x (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.

Part V

QoS and Flow-based Redirection Configuration

Chapter 20

QoS Configuration

20.1 Introduction to QoS

QoS (Quality of Service) is a set of capabilities that allow you to create differentiated services for network traffic, thereby providing better service for selected network traffic. QoS is a guarantee for service quality of consistent and predictable data transfer service to fulfill program requirements. QoS cannot generate extra bandwidth but provides more effective bandwidth management according to the application requirement and network management policy.

20.1.1 QoS Terms

QoS: Quality of Service, provides a guarantee for service quality of consistent and predictable data transfer service to fulfill program requirements. QoS cannot generate new bandwidth but provides more effective bandwidth management according to the application requirement and network management.

QoS Domain: QoS Domain supports QoS devices to form a net-topology that provides Quality of Service, so this topology is defined as QoS Domain.

CoS: Class of Service, the classification information carried by Layer 2 802.1Q frames, taking 3 bits of the Tag field in frame header, is called user priority level in the range of 0 to 7.

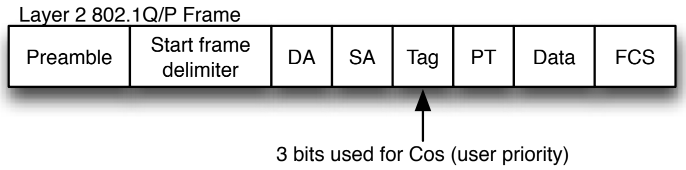


Figure 20.1: CoS priority

ToS: Type of Service, a one-byte field carried in Layer 3 IPv4 packet header to symbolize the service type of IP packets. Among ToS field can be IP Precedence value or DSCP value.

IP Precedence: IP priority. Classification information carried in Layer 3 IP packet header, occupying 3 bits, in the range of 0 to 7.

DSCP: Differentiated Services Code Point, classification information carried in Layer 3 IP packet header, occupying 6 bits, in the range of 0 to 63, and is downward compatible with IP Precedence.

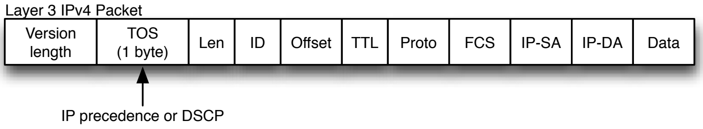


Figure 20.2: ToS priority

MPLS TC(EXP):

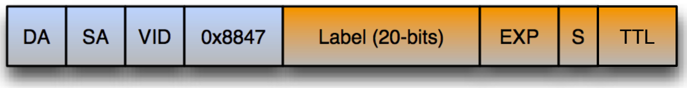


Figure 20.3: MPLS TC

A field of the MPLS packets means the service class, there are 3 bits, the ranging from 0 to 7.

Internal Priority: The internal priority setting of the switch chip, it's valid range relates with the chip, it's shortening is Int-Prio or IntP.

Drop Precedence: When processing the packets, firstly drop the packets with the bigger drop precedence, the ranging is 0-2 in three color algorithm, the ranging is 0-1 in dual color algorithm. It's shortening is Drop-Prec or DP.

Classification: The entry action of QoS, classifying packet traffic according to the classification information carried in the packet and ACLs.

Policing: Ingress action of QoS that lays down the policing policy and manages the classified packets.

Remark: Ingress action of QoS, perform allowing, degrading or discarding operations to packets according to the policing policies.

Scheduling: QoS egress action. Configure the weight for eight egress queues WRR (Weighted Round Robin).

In-Profile: Traffic within the QoS policing policy range (bandwidth or burst value) is called In-Profile.

Out-of-Profile: Traffic out the QoS policing policy range (bandwidth or burst value) is called Out-of-Profile.

20.1.2 QoS Implementation

To implement the switch software QoS, a general, mature reference model should be given. QoS can not create new bandwidth, but can maximize the adjustment and configuration for the current bandwidth resource. Fully implemented QoS can achieve complete management over the network traffic. The following is as accurate as possible a description of QoS.

The data transfer specifications of IP cover only addresses and services of source and destination, and ensure correct packet transmission using OSI layer 4 or above protocols such as TCP. However, rather than provide a mechanism for providing and protecting packet transmission bandwidth, IP provide bandwidth service by the best effort. This is acceptable for services like Mail and FTP, but for increasing multimedia business data and e-business data transmission, this best effort method cannot satisfy the bandwidth and low-lag requirement.

Based on differentiated service, QoS specifies a priority for each packet at the ingress. The classification information is carried in Layer 3 IP packet header or Layer 2 802.1Q frame header. QoS provides same service to packets of the same priority, while offers different operations for packets of different priority. QoS-enabled switch or router can provide different bandwidth according to the packet classification information, and can remark on the classification information according to the policing policies configured, and may discard some low priority packets in case of bandwidth shortage.

If devices of each hop in a network support differentiated service, an end-to-end QoS solution can be created. QoS configuration is flexible, the complexity or simplicity depends on the network topology and devices and analysis to incoming/outgoing traffic.

20.1.3 Basic QoS Model

The basic QoS consists of four parts: Classification, Policing, Remark and Scheduling, where classification, policing and remark are sequential ingress actions, and Queuing and Scheduling are QoS egress actions.

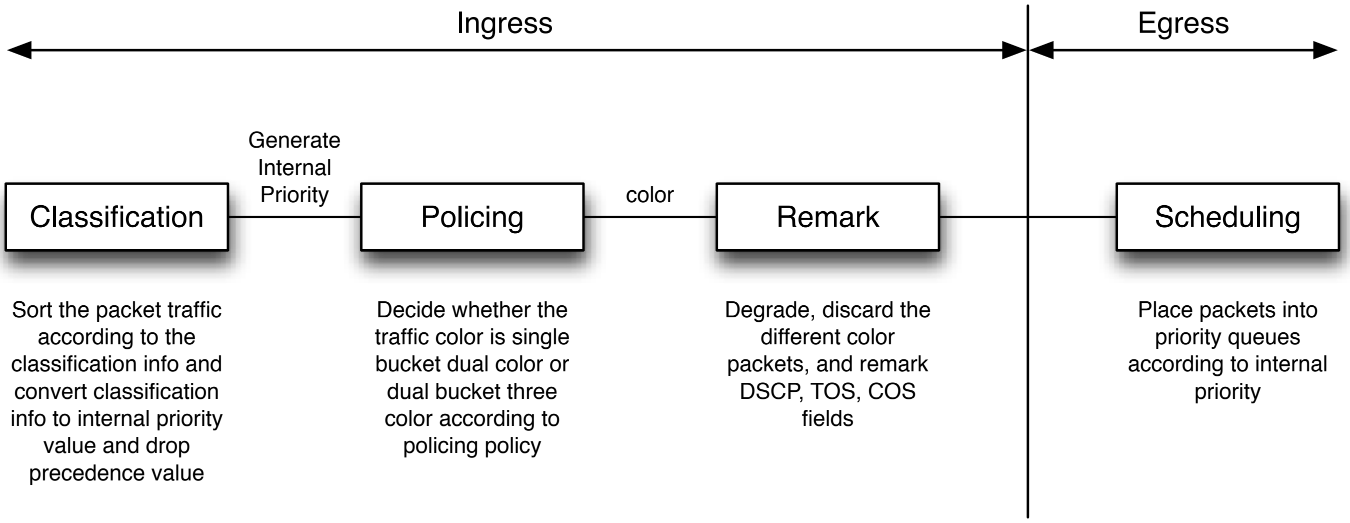

Ingress
Egress
Classification
Generate Internal Priority
Policing
color
Remark
Scheduling
Sort the packet traffic according to the classification info and convert classification info to internal priority value and drop precedence value
Decide whether the traffic color is single bucket dual color or dual bucket three color according to policing policy
Degrade, discard the different color packets, and remark DSCP, TOS, COS fields
Place packets into priority queues according to internal priority

Figure 20.4: Basic QoS Model

Classification: Classify traffic according to packet classification information and generate internal priority and drop precedence based the classification information. For different packet types and switch configurations, classification is performed differently; the flowchart below explains this in detail.

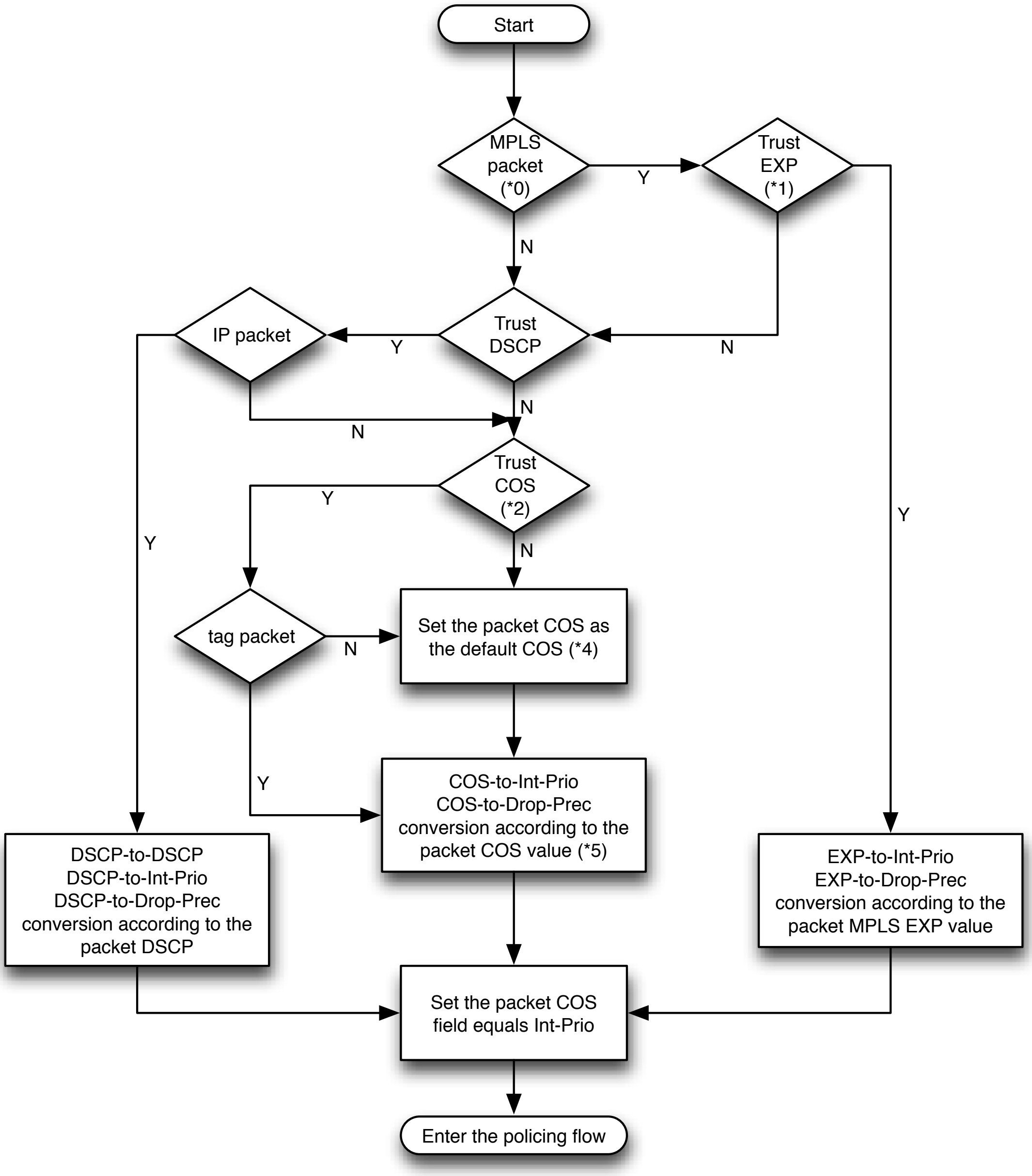


Figure 20.5: Classification process

Policing and remark: Each packet in classified ingress traffic is assigned an internal priority value and a drop precedence value, and can be policed and remarked.

Policing can be performed based on the flow to configure different policies that allocate bandwidth to classified traffic, the assigned bandwidth policy may be dual bucket dual color or dual bucket three color. The traffic, will be assigned with different color, can be discarded or passed, for the passed packets, add the remarking action. Remarking uses a new DSCP value of lower priority to replace the original higher level DSCP value in the packet. The following flowchart describes the operations.

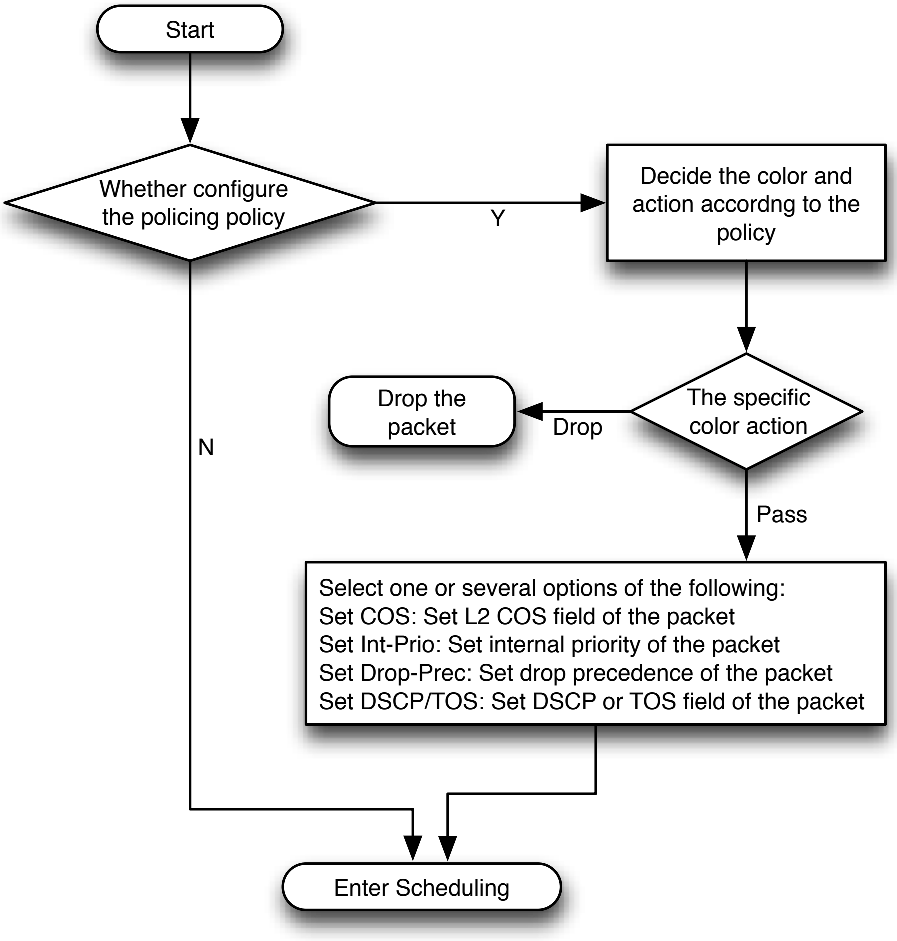

Start
Whether configure the policing policy
Y
N
Decide the color and action accordng to the policy
The specific color action
Drop
Drop the packet
Pass
Select one or several options of the following:
Set COS: Set L2 COS field of the packet
Set Int-Prio: Set internal priority of the packet
Set Drop-Prec: Set drop precedence of the packet
Set DSCP/TOS: Set DSCP or TOS field of the packet
Enter Scheduling

Figure 20.6: Policing and Remarking process

Queuing and scheduling: There are the internal priority and the drop precedence for the egress packets, the queuing operation assigns the packets to different priority queues according to the internal priority, while the scheduling operation perform the packet forwarding according to the priority queue weight and the drop precedence. The following flowchart describes the operations during queuing and scheduling.

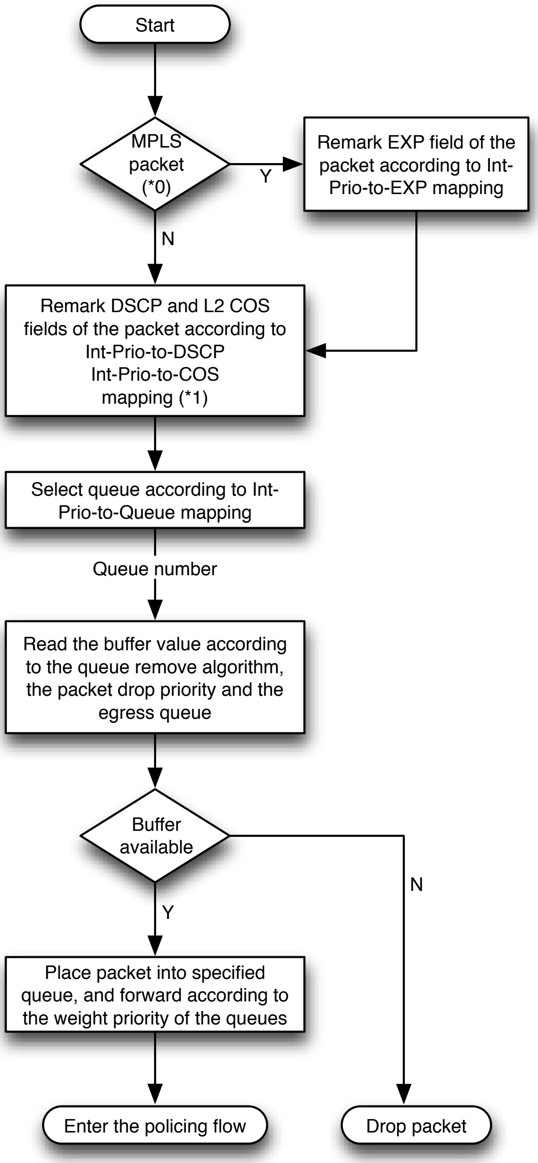

Start
MPLS packet (*0)
Y
Remark EXP field of the packet according to Int-Prio-to-EXP mapping
N
Remark DSCP and L2 COS fields of the packet according to Int-Prio-to-DSCP Int-Prio-to-COS mapping (*1)
Select queue according to Int-Prio-to-Queue mapping
Queue number
Read the buffer value according to the queue remove algorithm, the packet drop priority and the egress queue
Buffer available
N
Y
Place packet into specified queue, and forward according to the weight priority of the queues
Enter the policing flow
Drop packet

Figure 20.7: Queuing and Scheduling process

20.2 QoS Configuration Task List

1. Configure class map

   Set up a classification rule according to ACL, CoS, VLAN ID, IPv4 Precedent, DSCP, IPV6 FL to classify the data stream. Different classes of data streams will be processed with different policies.

2. Configure a policy map

   After data steam classification, a policy map can be created to associate with the class map created earlier and enter class mode. Then different policies (such as bandwidth limit, priority degrading assigning new DSCP value) can be applied to different data streams. You can also define a policy set that can be use in a policy map by several classes.

3. Apply QoS to the ports or the VLAN interfaces

   Configure the trust mode for ports or bind policies to ports. A policy will only take effect on a port when it is bound to that port.

   The policy may be bound to the specific VLAN.

   It is not recommended to synchronously use policy map on VLAN and its port.

4. Configure queue management algorithm

   Configure queue management algorithm, such as sp, wrr, wdrr, and so on.

   Configure QoS mapping

   Configure the mapping from CoS to DP, DSCP to DSCP, IntP or DP, IntP to DSCP.

1. Configure class map.

Command	Explanation
Global Mode	
class-map <class-map-name> no class-map <class-map-name>	Create a class map and enter class map mode; the 'no class-map <class-map-name>' command deletes the specified class map.

match { access-group <acl-index-or-name> | ip dscp <dscp-list>| ip precedence <ip-precedence-list>| ipv6 access-group <acl-index-or-name> | ipv6 dscp <dscp-list> | ipv6 flowlabel <flowlabel-list> | vlan <vlan-list> | cos <cos-list> | exp <exp-list> | vlan range <vlan-list> }
no match { access-group | ip dscp | ip precedence | ipv6 access-group | ipv6 dscp | ipv6 flowlabel | vlan | cos | exp | vlan range }
	Set matching criterion (classify data stream by ACL, CoS, VLAN ID, IPv4 Precedent, IPv6 FL or DSCP, etc) for the class map; the no command deletes specified matching criterion.

2. Configure a policy map

Command	Explanation
Global Mode	
policy-map <policy-map-name> no policy-map <policy-map-name>	Create a policy map and enter policy map mode; the no command deletes the specified policy map.
class <class-map-name> [insert-before <class-map-name>] no class <class-map-name>	After a policy map is created, it can be associated to a class. Different policy or new DSCP value can be applied to different data streams in class mode; the no command deletes the specified class.

set { ip dscp <new-dscp> | ip precedence <new-precedence> | internal priority <new-inp> | drop precedence <new-dp> | cos <new-cos> }
no set { ip dscp | ip precedence | internal priority | drop precedence | cos }
	Assign a new DSCP, CoS, IP Precedence value for the classified traffic; the no command cancels the newly assigned value.

Single bucket mode: policy <bits_per_second> <normal_burst_bytes> ({ conform-action ACTION | exceed-action ACTION }) **Dual bucket mode:** policy <bits_per_second> <normal_burst_bytes> [pir <peak_rate_bps>] | <maximum_burst_bytes> [{ conform-action ACTION | exceed-action ACTION | violate-action ACTION }] **ACTION definition:** drop | transmit | set-dscp-transmit <dscp_value> | set-prec-transmit <ip_precedence_value> | set-cos-transmit <cos_value> | set-internal-priority <inp_value> | set-Drop-Precedence <dp_value> no policy	Configure a policy for the classified flow. The non-aggregation policy command supports three colors. Analyze the working mode of the token bucket, whether it is singe rate single bucket, single rate dual bucket, dual rate dual bucket, set corresponding action to different color packets. The no command will delete the mode configuration. Single bucket mode is supported by the specific switch.
policy aggregate <aggregate-policy-name> no policy aggregate <aggregate-policy-name>	Apply a policy to classified traffic; the no command deletes the specified policy set.
accounting no accounting	Set statistic function for the classified traffic. After enable this function under the policy class map mode, add statistic function to the traffic of the policy class map. In single bucket mode, the messages can only red or green when passing policy. In the print information, in-profile means green and out-profile means red. In dual bucket mode, there are three colors of the packets. In the print information, in-profile means green and out-profile means red and yellow.

3. Apply QoS to port or VLAN interface

Policy class map configuration mode	
drop no drop transmit no transmit	Drop or transmit data package that match the class, the no command cancels the assigned action.

3. Apply QoS to port or VLAN interface

Command	Explanation
Interface Configuration Mode	
mls qos trust { cos | dscp } no mls qos trust { cos | dscp }	Configure port trust; the no command disables the current trust status of the port.
mls qos cos {<default-cos>} no mls qos cos	Configure the default CoS value of the port; the no command restores the default setting.
service-policy input <policy-map-name> no service-policy input {<policy-map-name>}	Apply a policy map to the specified port; the no command deletes the specified policy map applied to the port or deletes all the policy maps applied on the ingress direction of the port. Egress policy map is not supported yet.
Global Mode	
service-policy input <policy-map-name> vlan <vlan-list> no service-policy input {<policy-map-name>} vlan <vlan-list>	Apply a policy map to the specified VLAN interface; the no command deletes the specified policy map applied to the VLAN interface or deletes all the policy maps applied in the ingress direction of the vlan interface.

4. Configure queue management algorithm and weight

Command	Explanation
Port Configuration Mode	
mls qos queue algorithm { sp | wrr | wdrr } no mls qos queue algorithm	Set queue management algorithm, the default queue management algorithm is wrr.
mls qos queue wrr weight <weight0..weight7> no mls qos queue wrr weight	Set queue weight based a port, the default queue weight is 1 2 3 4 5 6 7 8.
mls qos queue wdrr weight <weight0..weight7> no mls qos queue wdrr weight	Set queue weight based a port, the default queue weight is 10 20 40 80 160 320 640 1280.
mls qos queue <queue-id> bandwidth <minimum-bandwidth> <maximum-bandwidth> no mls qos queue <queue-id> bandwidth	Set bandwidth guarantee based a port.

5. Configure QoS mapping

Command	Explanation
Global Mode	
mls qos map (cos-dp <dp1..dp8> | dscp-dscp <in-dscp list> to <out-dscp> | dscp-intp <in-dscp list> to <intp> | dscp-dp <in-dscp list> to <dp>) no mls qos map (cos-dp | dscp-dscp | dscp-intp | dscp-dp) mls qos map intp-dscp <dscp1..dscp8> no mls qos map intp-dscp	Set the priority mapping for QoS, the no command restores the default mapping value.

6. Clear accounting data of the specific ports or VLANs

Command	Explanation
Admin Mode	
clear mls qos statistics [interface <interface-name> | vlan <vlan-id>]	Clear accounting data of the specified ports or VLAN Policy Map. If there are no parameters, clear accounting data of all policy map.

7. Show configuration of QoS

Command	Explanation
Admin Mode	
show mls qos maps [cos-dp | dscp-dscp | dscp-intp | dscp-dp | intp-dscp]	Display the configuration of QoS mapping.
show class-map [<class-map-name>]	Display the classified map information of QoS.
show policy-map [<policy-map-name>]	Display the policy map information of QoS.
show mls qos { interface [<interface-id>] [policy | queuing] | vlan <vlan-id> }	Displays QoS configuration information on a port.

20.3 QoS Example

Example 1:

Enable QoS function, change the queue out weight of port ethernet 1/0/1 to 1:1:2:2:4:4:8:8, set the port in trust CoS mode without changing DSCP value, and set the default CoS value of the port to 5. The configuration steps are listed below:

```
Switch#config
Switch(config)#interface ethernet 1/0/1
Switch(Config-If-Ethernet1/0/1)#mls qos queue weight 1 1 2 2 4 4 8 8
Switch(Config-If-Ethernet1/0/1)#mls qos cos 5
```

Configuration result:

When QoS enabled in Global Mode, the egress queue bandwidth proportion of port ethernet1/0/1 is 1:1:2:2:4:4:8:8. When packets have CoS value coming in through port ethernet1/0/1, it will be map to the queue out according to the CoS value, CoS value 0 to 7 correspond to queue out 1, 2, 3, 4, 5, 6, 7, 8 respectively. If the incoming packet has no CoS value, it is default to 5 and will be put in queue6. All passing packets would not have their DSCP values changed.

Example 2:

In port ethernet1/0/2, set the bandwidth for packets from segment 192.168.1.0 to 10 Mb/s, with a burst value of 4 MB, all packets exceed this bandwidth setting will be dropped.

The configuration steps are listed below:

```
Switch#config
Switch(config)#access-list 1 permit 192.168.1.0 0.0.0.255
Switch(config)#class-map c1
Switch(Config-ClassMap-c1)#match access-group 1
Switch(Config-ClassMap-c1)#exit
Switch(config)#policy-map p1
Switch(Config-PolicyMap-p1)#class c1
Switch(Config-PolicyMap-p1-Class-c1)#policy 10000 4000 exceed-action drop
Switch(Config-PolicyMap-p1-Class-c1)#exit
Switch(Config-PolicyMap-p1)#exit
Switch(config)#interface ethernet 1/0/2
Switch(Config-If-Ethernet1/0/2)#service-policy input p1
```

Configuration result:

An ACL name 1 is set to matching segment 192.168.1.0. Enable QoS globally, create a class map named c1, matching ACL1 in class map; create another policy map named p1 and refer to c1 in p1, set appropriate policies to limit bandwidth and burst value. Apply this policy map on port ethernet1/0/2. After the above settings done, bandwidth for packets from segment 192.168.1.0 through port ethernet 1/0/2 is set to 10 Mb/s, with a burst value of 4 MB, all packets exceed this bandwidth setting in that segment will be dropped.

Example 3:

As shown in the figure, inside the block is a QoS domain, Switch1 classifies different traffics and assigns different IP precedences. For example, set CoS precedence for packets from segment 192.168.1.0 to 5 on port ethernet1/0/1. The port connecting to switch2 is a trunk port. In Switch2, set port ethernet 1/0/1 that connecting to swtich1 to trust cos. Thus inside the QoS domain, packets of different priorities will go to different queues and get different bandwidth.

The configuration steps are listed below:

QoS configuration in Switch1:

```
Switch#config
Switch(config)#access-list 1 permit 192.168.1.0 0.0.0.255
Switch(config)#class-map c1
Switch(Config-ClassMap-c1)#match access-group 1
Switch(Config-ClassMap-c1)#exit
Switch(config)#policy-map p1
Switch(Config-PolicyMap-p1)#class c1
Switch(Config-PolicyMap-p1-Class-c1)#set ip precedence 5
```

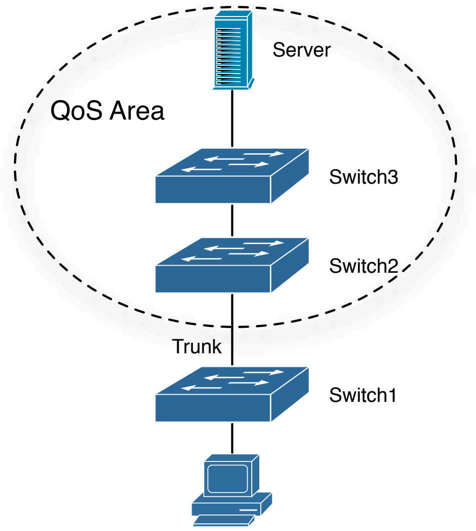


Figure 20.8: Typical QoS topology

```
Switch(Config-PolicyMap-p1-Class-c1)#exit
Switch(Config-PolicyMap-p1)#exit
Switch(config)#interface ethernet 1/0/1
Switch(Config-If-Ethernet1/0/1)#service-policy input p1
```

QoS configuration in Switch2:

```
Switch#config
Switch(config)#interface ethernet 1/0/1
Switch(Config-If-Ethernet1/0/1)#mls qos trust cos
```

20.4 QoS Troubleshooting

- trust cos and exp can be used with other trust or Policy Map.
- trust dscp can be used with other trust or Policy Map. This configuration takes effect to IPv4 and IPv6 packets.
- trust exp, trust dscp and trust cos may be configured at the same time, the priority is: EXP>DSCP>COS.
- If the dynamic VLAN (mac vlan/voice vlan/ip subnet vlan/protocol vlan) is configured, then the packet COS value equals COS value of the dynamic VLAN.
- Policy map can only be bound to ingress direction, egress is not supported yet.
- At present, it is not recommended to synchronously use policy map on VLAN and VLAN's port.

Chapter 21

Flow-based Redirection

21.1 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. Special 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.

21.2 Flow-based Redirection Configuration Task Sequence

- Flow-based redirection configuration
- 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; the '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.

21.3 Flow-based Redirection Examples

Example:

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 port6.

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 1/0/1
Switch(Config-If-Ethernet1/0/1)# access-group 1 redirect to interface ethernet 1/0/6
```

21.4 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, nomenclature standard IP ACL, nomenclature extensive IP ACL, digital standard IPv6 ACL, and nomenclature standard IPv6 ACL;
- Parameters of Timerange and Portrange can not be set in ACL, the type of ACL should be Permit.
- The redirection port must be 1000Mb port in the flow-based redirection function.

Part VI

L3 Forward and ARP Configuration

Chapter 22

Layer 3 Management Configuration

Switch only support Layer 2 forwarding, but can configure a Layer 3 management port for the communication of all kinds of management protocols based on IP protocol.

22.1 Layer 3 Management Interface

22.1.1 Introduction to Layer 3 Management Interface

Only one layer 3 management interface can be created on switch. The Layer 3 interface is not a physical interface but a virtual interface. Layer 3 interface is built on VLANs. The Layer 3 interface can contain one or more 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. The switch can use the IP addresses set in the layer 3 interfaces to communicate with the other devices via IP.

22.1.2 Layer 3 Management Interface Configuration Task List

1. Create Layer 3 management interface
2. Configure VLAN interface description
3. Open or close the VLAN interface

1. Create Layer 3 management interface

Command	Explanation
Global Mode	
interface vlan <vlan-id> no interface vlan <vlan-id>	Creates a management VLAN interface; the no command deletes the VLAN interface created in the switch.

2. Configure VLAN interface description

Command	Explanation
VLAN Interface Mode	
description <text> no description	Configure the description information of VLAN interface. The no command will cancel the description information of VLAN interface.

22.2 IP Configuration

22.2.1 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 Exterior Gateway Protocols (EGP for short). For example, IPv6 Routing Protocol such as RIPng, OSPFv3, IS-ISv6 and MBGP4+, etc.

Multicast addresses increased and the support for multicast has enhanced. By dealing with IPv4 broadcast functions such as Router Discovery and Router Query, IPv6 multicast has completely replaced IPv4 broadcast in the sense of function. Multicast not only saves network bandwidth, but enhances network efficiency as well.

22.2.2 IP Configuration

Layer 3 interface can be configured as IPv4 interface, IPv6 interface.

IPv4 Address Configuration

IPv4 address configuration task list:

1. Configure the IPv4 address of three-layer interface
2. Configure the default gateway

1. Configure the IPv4 address of three-layer interface

Command	Explanation
VLAN Interface Configuration 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.

2. Configure the default gateway

Command	Explanation
Global Mode	
ip default-gateway <A.B.C.D> no ip default-gateway <A.B.C.D>	Configure the default gateway of the route. The no command cancels the configuration.

IPv6 Address Configuration

The configuration Task List of IPv6 is as follows:

1. IPv6 basic configuration
   (a) Configure interface IPv6 address
   (b) Configure default gateway
2. IPv6 Neighbor Discovery Configuration
   (a) Configure DAD neighbor solicitation message number
   (b) Configure send neighbor solicitation message interval
   (c) Configure static IPv6 neighbor entries
   (d) Delete all entries in IPv6 neighbor table

1. IPv6 Basic Configuration
(a) Configure interface IPv6 address

Command	Explanation
Interface Configuration Mode	
ipv6 address <ipv6-address/prefix-length> [eui-64] no ipv6 address <ipv6-address/prefix-length>	Configure IPv6 address, including aggregatable global unicast addresses, site-local addresses and link-local addresses. The **no ipv6 address <ipv6-address/prefix-length>** command cancels IPv6 address.

(b) Set default gateway

Command	Explanation
Global Mode	
ipv6 default-gateway <X:X::X:X> no ipv6 default-gateway <X:X::X:X>	Configure IPv6 default gateway of the router. The no command cancels the configuration.

2. IPv6 Neighbor Discovery Configuration
(a) Configure DAD Neighbor solicitation Message number

Command	Explanation
Interface Configuration Mode	
ipv6 nd dad attempts <value> no ipv6 nd dad attempts	Set the neighbor query message number sent in sequence when the interface makes duplicate address detection. The no command resumes default value (1).

(b) Configure Send Neighbor solicitation Message Interval

Command	Explanation
Interface Configuration Mode	
ipv6 nd ns-interval <seconds> no ipv6 nd ns-interval	Set the interval of the interface to send neighbor query message. The NO command resumes default value (1 second).

(c) Configure static IPv6 neighbor Entries

Command	Explanation
Interface Configuration Mode	
ipv6 neighbor <ipv6-address> <hardware-address> interface <interface-type interface-name>	Set static neighbor table entries, including neighbor IPv6 address, MAC address and two-layer port.
no ipv6 neighbor <ipv6-address>	Delete neighbor table entries.

(d) Delete all entries in IPv6 neighbor table

Command	Explanation
Admin Mode	
clear ipv6 neighbors	Clear all static neighbor table entries.

22.2.3 IPv6 Troubleshooting

- If the connected PC has not obtained IPv6 address, you should check the RA announcement switch (the default is turned off)

22.3 Static Route

22.3.1 Introduction to Static Route

As mentioned earlier, the static route is the manually specified path to a network or a host. Static route is simple and consistent, and can prevent illegal route modification, and is convenient for load balance and route backup. However, it also has its own defects. Static route, as its name indicates, is static, it won’t modify the route automatically on network failure, and manual configuration is required on such occasions, therefore it is not suitable for mid and large-scale networks.

Static route is mainly used in the following two conditions: 1) in stable networks to reduce load of route selection and routing data streams. For example, static route can be used in route to STUB network. 2) For route backup, configure static route in the backup line, with a lower priority than the main line.

Static route and dynamic route can coexist; layer3 switch will choose the route with the highest priority according to the priority of routing protocols. At the same time, static route can be introduced (redistribute) in dynamic route, and change the priority of the static route introduced as required.

22.3.2 Introduction to Default Route

Default route is a kind of static route, which is used only when no matching route is found. In the route table, default route in is indicated by a destination address of 0.0.0.0 and a network mask of 0.0.0.0, too. If the route table does not have the destination of a packet and has no default route configured, the packet will be discarded, and an ICMP packet will be sent to the source address indicate the destination address or network is unreachable.

22.3.3 Static Route Configuration Task List

1. Static route configuration

1. Static route configuration

Command	Explanation
Global mode	
ip route {<ip-prefix> <mask> | <ip-prefix>/<prefix-length>} {<gateway-address> | <gateway-interface>} [<distance>] no ip route {<ip-prefix> <mask> | <ip-prefix>/<prefix-length>} [<gateway-address> | <gateway-interface>] [<distance>]	Set static routing; the **no ip route {<ip-prefix> <mask> | <ip-prefix>/<prefix-length>} [<gateway-address> | <gateway-interface>] [<distance>]** command deletes a static route entry

22.3.4 Static Route Configuration Examples

The figure shown below is a simple network consisting of three layer3 switches, the network mask for all switches and PC is 255.255.255.0. PC-A and PC-C are connected via the static route set in SwtichA and SwitchC; PC-A and PC-B are connected via the static route set in SwtichC to SwitchB; PC-B and PC-C is connected via the default route set in SwitchB.

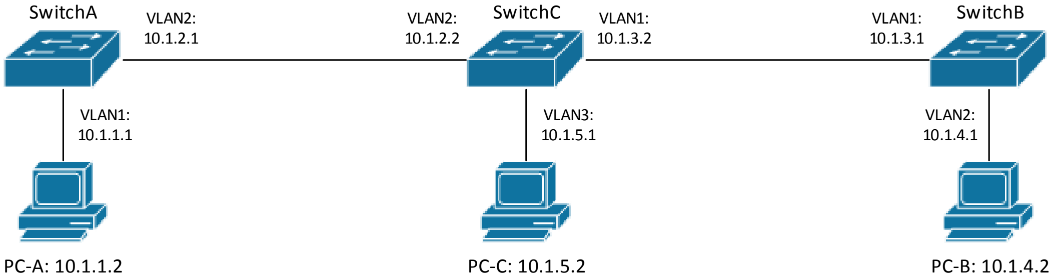


Figure 22.1: Static Route Configurations

Configuration steps:

Configuration of layer3 SwitchA

```
Switch#config
Switch(config)#ip route 10.1.5.0 255.255.255.0 10.1.2.2
```

Configuration of layer3 SwitchC

```
Switch#config
#Next hop use the partner IP address
Switch(config)#ip route 10.1.1.0 255.255.255.0 10.1.2.1
#Next hop use the partner IP address
Switch(config)#ip route 10.1.4.0 255.255.255.0 10.1.3.1
```

Configuration of layer3 SwitchB

```
Switch#config
Switch(config)#ip route 0.0.0.0 0.0.0.0 10.1.3.2
```

In this way, ping connectivity can be established between PC-A and PC-C, and PC-B and PC-C.

22.4 ARP

22.4.1 Introduction to ARP

ARP (Address Resolution Protocol) is mainly used to resolve IP address to Ethernet MAC address. Switch supports both dynamic ARP and static ARP configuration.

22.4.2 ARP Configuration Task List

ARP Configuration Task List:

1. Configure static ARP

1. Configure static ARP

Command	Explanation
VLAN Interface Mode	
arp <ip_address> <mac_address> { interface [ethernet] <portName> } no arp <ip_address>	Configures a static ARP entry; the no command deletes a ARP entry of the specified IP address.

22.4.3 ARP Troubleshooting

If ping from the switch to directly connected network devices fails, the following can be used to check the possible cause and create a solution.

- Check whether the corresponding ARP has been learned by the switch.
- If ARP has not been learned, then enabled ARP debugging information and view the sending/receiving condition of ARP packets.
- Defective cable is a common cause of ARP problems and may disable ARP learning.

Chapter 23

ARP Scanning Prevention Function Configuration

23.1 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. 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.

23.2 ARP Scanning Prevention Configuration Task Sequence

1. Enable the ARP Scanning Prevention function.
2. Configure the threshold of the port-based and IP-based ARP Scanning Prevention
3. Configure trusted ports

4. Configure trusted IP
5. Configure automatic recovery time
6. Display relative information of debug information and ARP scanning

1. Enable the ARP Scanning Prevention function.

Command	Explanation
Global configuration mode	
anti-arpscan enable no anti-arpscan enable	Enable or disable the ARP Scanning Prevention function globally.

2. Configure the threshold of the port-based and IP-based ARP Scanning Prevention

Command	Explanation
Global configuration mode	
anti-arpscan port-based threshold <threshold-value> no anti-arpscan port-based threshold	Set the threshold of the port-based ARP Scanning Prevention.
anti-arpscan ip-based threshold <threshold-value> no anti-arpscan ip-based threshold	Set the threshold of the IP-based ARP Scanning Prevention.

3. Configure trusted ports

Command	Explanation
Port configuration mode	
anti-arpscan trust <port | supertrust-port> no anti-arpscan trust <port | supertrust-port>	Set the trust attributes of the ports.

4. Configure trusted IP

Command	Explanation
Global configuration mode	
anti-arpscan trust ip <ip-address> [<netmask>] no anti-arpscan trust ip <ip-address> [<netmask>]	Set the trust attributes of IP.

5. Configure automatic recovery time

Command	Explanation
Global configuration mode	
anti-arpscan recovery enable no anti-arpscan recovery enable	Enable or disable the automatic recovery function.
anti-arpscan recovery time <seconds> no anti-arpscan recovery time	Set automatic recovery time.

6. Display relative information of debug information and ARP scanning

Command	Explanation
Global configuration mode	
anti-arpscan log enable no anti-arpscan log enable	Enable or disable the log function of ARP scanning prevention.
anti-arpscan trap enable no anti-arpscan trap enable	Enable or disable the SNMP Trap function of ARP scanning prevention.
show anti-arpscan [trust <ip | port | supertrust-port> | prohibited <ip | port>]	Display the state of operation and configuration of ARP scanning prevention.
Admin Mode	
debug anti-arpscan <port | ip> no debug anti-arpscan <port | ip>	Enable or disable the debug switch of ARP scanning prevention.

23.3 ARP Scanning Prevention Typical Examples

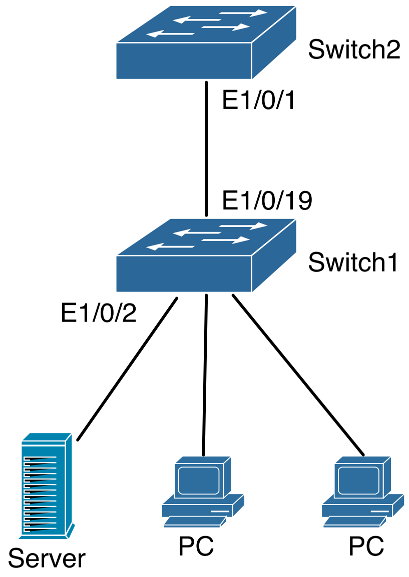


Figure 23.1: ARP scanning prevention typical configuration example

In the network topology above, port E1/0/1 of SWITCH B is connected to port E1/0/19 of SWITCH A, the port E1/0/2 of SWITCH A is connected to file server (IP address is 192.168.1.100/24), and all the other ports of SWITCH A are connected to common PC. The following configuration can prevent ARP scanning effectively without affecting the normal operation of the system.

SWITCH A configuration task sequence:

```
SwitchA(config)#anti-arpscan enable
SwitchA(config)#anti-arpscan recovery time 3600
SwitchA(config)#anti-arpscan trust ip 192.168.1.100 255.255.255.0
SwitchA(config)#interface ethernet1/0/2
SwitchA(Config-If-Ethernet1/0/2)#anti-arpscan trust port
SwitchA(Config-If-Ethernet1/0/2)#exit
SwitchA(config)#interface ethernet1/0/19
SwitchA(Config-If-Ethernet1/0/19)#anti-arpscan trust supertrust-port
SwitchA(Config-If-Ethernet1/0/19)#exit
```

SWITCH B configuration task sequence:

```
SwitchB(config)#anti-arpscan enable
SwitchB(config)#interface ethernet1/0/1
SwitchB(Config-If-Ethernet1/0/1)#anti-arpscan trust port
SwitchB(Config-If-Ethernet1/0/1)#exit
```

23.4 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.

Chapter 24

Prevent ARP Spoofing Configuration

24.1 Overview

24.1.1 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 f8-f0-82-FD-1D-2B. What the whole mapping process is that a host computer send broadcast data packet involving IP address information of destination host computer, ARP request, and then the destination host computer send a data packet involving its IP address and Mac address to the host, so two host computers can exchange data by MAC address.

24.1.2 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.

24.1.3 How to prevent void ARP Spoofing

There are many sniff, monitor and attack behaviors based on ARP protocol in networks, and most of attack behaviors are based on ARP spoofing, so it is very important to prevent ARP spoofing. ARP spoofing accesses normal network environment by counterfeiting legal IP address firstly, and sends a great deal of counterfeited ARP application packets to switches, after switches learn these packets, they will cover previously corrected IP, mapping of MAC address, and then some corrected IP, MAC address mapping are modified to correspondence relationship configured by attack packets so that the switch makes mistake on transfer packets, and takes an effect on the whole network. Or the switches are made used of by vicious attackers, and they intercept and capture packets transferred by switches or attack other switches, host computers or network equipment.

What the essential method on preventing attack and spoofing switches based on ARP in networks is to disable switch automatic update function; the cheater can't modify corrected MAC address in order to avoid wrong packets transfer and can't obtain other information. At one time, it doesn't interrupt the automatic learning function of ARP. Thus it prevents ARP spoofing and attack to a great extent.

24.2 Prevent ARP Spoofing configuration

The steps of preventing ARP spoofing configuration as below:

1. Disable ARP automatic update function
2. Disable ARP automatic learning function
3. Changing dynamic ARP to static ARP

1. Disable ARP automatic update function

Command	Explanation
Global Mode and Port Mode	
ip arp-security updateprotect no ip arp-security updateprotect	Disable and enable ARP automatic update function.

2. Disable ARP automatic learning function

Command	Explanation
Global mode and Interface Mode	
ip arp-security learnprotect no ip arp-security learnprotect	Disable and enable ARP automatic learning function.

3. Function on changing dynamic ARP to static ARP

Command	Explanation
Global Mode and Port Mode	
ip arp-security convert	Change dynamic ARP to static ARP.

24.3 Prevent ARP Spoofing Example

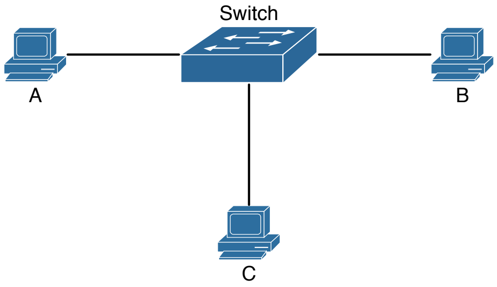


Figure 24.1: Prevent ARP spoofing configuration example

Equipment Explanation

Equipment	Configuration	Quality
switch	IP:192.168.2.4; mac: 00-00-00-00-00-04	1
A	IP:192.168.2.1; mac: 00-00-00-00-00-01	1
B	IP:192.168.1.2; mac: 00-00-00-00-00-02	1
C	IP:192.168.2.3; mac: 00-00-00-00-00-03	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 packet to switch, format is: 192.168.2.3, 00-00-00-00-00-01, 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 00-00-00-00-00-01 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)#interface vlan 1
Switch(Config-If-Vlan1)#arp 192.168.2.1 00-00-00-00-00-01 interface eth 1/0/2
Switch(Config-If-Vlan1)#interface vlan 2
Switch(Config-If-Vlan2)#arp 192.168.1.2 00-00-00-00-00-02 interface eth 1/0/2
Switch(Config-If-Vlan2#interface vlan 3
Switch(Config-If-Vlan3)#arp 192.168.2.3 00-00-00-00-00-03 interface eth 1/0/2
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 packet, and protect use data from sniffing.

```
Switch#config
Switch(config)#ip arp-security updateprotect
```

Chapter 25

ARP Guard Configuration

25.1 Introduction to ARP Guard

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.

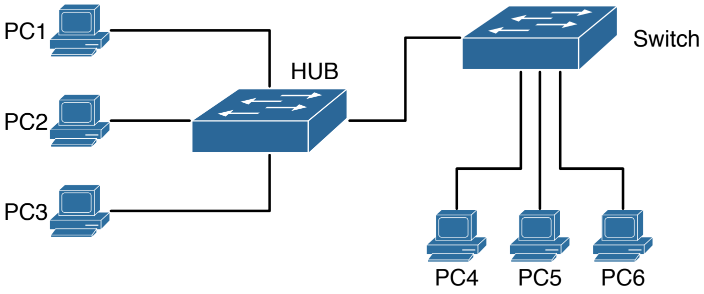


Figure 25.1: ARP Guard schematic diagram

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.

25.2 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

Chapter 26

Gratuitous ARP Configuration

26.1 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 the switch is as below: The Layer 3 interfaces of the switch can be configured to advertise gratuitous ARP packets period 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 requests. This will reduce the frequency the host's 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.

26.2 Gratuitous ARP Configuration Task List

1. Enable gratuitous ARP and configure the interval to send gratuitous ARP request

2. Display configurations about gratuitous ARP

1. Enable gratuitous ARP and configure the interval to send gratuitous ARP request.

Command	Explanation
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. The no command cancels the gratuitous ARP.

2. Display configurations about gratuitous ARP

Command	Explanation
Admin Mode and Configuration Mode	
show ip gratuitous-arp [interface vlan <1-4094>]	To display configurations about gratuitous ARP.

26.3 Gratuitous ARP Configuration Example

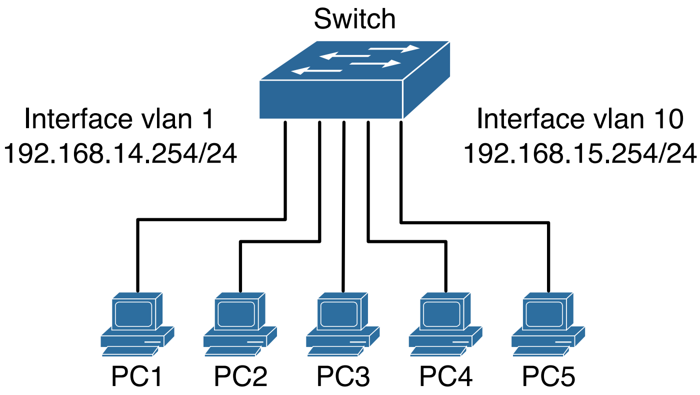


Figure 26.1: Gratuitous ARP Configuration Example

For the network topology shown in the figure above, interface VLAN10 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. Configure two interfaces to use gratuitous ARP at one time.

```
Switch(config)#ip gratuitous-arp 300
```

2. 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
```

26.4 Gratuitous ARP Troubleshooting

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.

Part VII

DHCP Configuration

Chapter 27

DHCP Configuration

27.1 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:

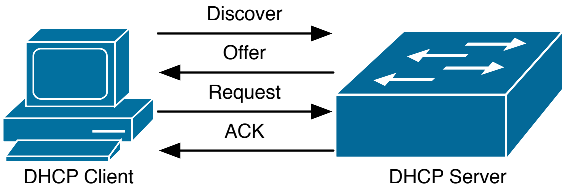


Figure 27.1: DHCP protocol interaction

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.

Switch can act as both a DHCP server and a DHCP relay. DHCP server supports not only dynamic IP address assignment, but also manual IP address binding (i.e. specify a specific IP address to a specified MAC address or specified device ID over a long period. The differences and relations between dynamic IP address allocation and manual IP address binding are:

1. IP address obtained dynamically can be different every time; manually bound IP address will be the same all the time.
2. The lease period of IP address obtained dynamically is the same as the lease period of the address pool, and is limited; the lease of manually bound IP address is theoretically endless.
3. Dynamically allocated address cannot be bound manually.
4. Dynamic DHCP address pool can inherit the network configuration parameters of the dynamic DHCP address pool of the related segment.

27.2 DHCP Server Configuration

DHCP Sever Configuration Task List:

1. Enable/Disable DHCP service
2. Configure DHCP Address pool
   (a) Create/Delete DHCP Address pool
   (b) Configure DHCP address pool parameters
   (c) Configure manual DHCP address pool parameters
3. Enable logging for address conflicts

1. Enable/Disable DHCP service

Command	Explanation
Global Mode	
service dhcp no service dhcp	Enable DHCP server. The no command disables DHCP server.
Port Mode	
ip dhcp disbale no ip dhcp disable	The port disables DHCP services, the no command enables DHCP services.

2. Configure DHCP Address pool

(a) Create/Delete DHCP Address pool

Command	Explanation
Global Mode	
ip dhcp pool <name> no ip dhcp pool <name>	Configure DHCP Address pool. The no operation cancels the DHCP Address pool.

(b) 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. The no operation of this command cancels the allocation address pool.
default-router [<address1> [<address2> [...<address8>]]] no default-router	Configure default gateway for DHCP clients. The no operation cancels the default gateway.
dns-server [<address1> [<address2> [...<address8>]]] no dns-server	Configure DNS server for DHCP clients. The no command deletes DNS server configuration.
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> [...<address8>]]] no netbios-name-server	Configure the address for WINS server. The no operation cancels the address for server.
netbios-node-type { b-node | h-node | m-node | p-node | <type-number> } no netbios-node-type	Configure node type for DHCP clients. The no operation cancels the node type for DHCP clients.
bootfile <filename> no bootfile	Configure the file to be imported for DHCP clients on boot up. The no command cancels this operation.
next-server [<address1> [<address2> [...<address8>]]] no next-server [<address1> [<address2> [...<address8>]]]	Configure the address of the server hosting file for importing. The no command deletes the address of the server hosting file for importing.
option <code> { ascii <string> | hex <hex> | ipaddress <ipaddress> } no option <code>	Configure the network parameter specified by the option code. The no command deletes the network parameter specified by the option code.
lease { days [hours][minutes] | infinite } no lease	Configure the lease period allocated to addresses in the address pool. The no command deletes the lease period allocated to addresses in the address pool.
max-lease-time { [<days>] [<hours>] [<minutes>] | infinite } no max-lease-time	Set the maximum lease time for the addresses in the address pool; the no command restores the default setting.

Global Mode	
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.

(c) Configure manual DHCP address pool parameters

Command	Explanation
DHCP Address Pool Mode	
hardware-address <hardware-address> [{ Ethernet | IEEE802 | <type-number> }] no hardware-address	Specify/delete the hardware address when assigning address manually.
host <address> [<mask> | <prefix-length>] no host	Specify/delete the IP address to be assigned to the specified client when binding address manually.
client-identifier <unique-identifier> no client-identifier	Specify/delete the unique ID of the user when binding address manually.

3. Enable logging for address conflicts

Command	Explanation
Global Mode	
ip dhcp conflict logging no ip dhcp conflict logging	Enable/disable 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.

27.3 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.

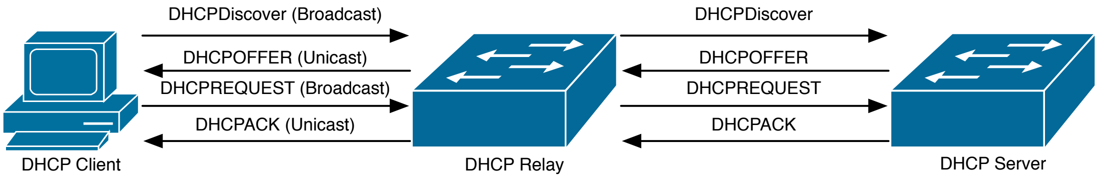


Figure 27.2: DHCP relay

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.

DHCP Relay Configuration Task List:

1. Enable DHCP relay.

2. Configure DHCP relay to forward DHCP broadcast packet.

3. Configure share-vlan

1. Enable DHCP relay.

Command	Explanation
Global Mode	
service dhcp no service dhcp	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 bootps no ip forward-protocol udp bootps	The UDP port 67 is used for DHCP broadcast packet forwarding.
Interface Configuration Mode	
ip helper-address <ipaddress> no ip helper-address <ipaddress>	Set the destination IP address for DHCP relay forwarding; the 'no ip helper-address <ipaddress>' command cancels the setting.

3. Configure share-vlan

When the user want to use layer 2 device as DHCP relay, there is the number limitation that create layer 3 interface on layer 2 device, but using the layer 3 interface of share-vlan (it may include many sub-vlan, however a sub-vlan only correspond to a share-vlan) can implement DHCP relay forwarding, and the relay device needs to enable option82 function at the same time.

Command	Explanation
Global Mode	
ip dhcp relay share-vlan <vlanid> sub-vlan <vlanlist> no dhcp relay share-vlan	Create or delete share-vlan and it's sub-vlan.

27.4 DHCP Configuration Examples

Scenario 1:

Too save configuration efforts of network administrators and users, a company is using switch as a DHCP server. The Admin VLAN IP address is 10.16.1.2/16. The local area network for the company is divided into network A and B according to the office locations. The network configurations for location A and B are shown below.

Pool A (network 10.16.1.0)		**Pool B (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	WWW server	10.16.1.209
WINS node type	H-node		
Lease	3 days	Lease	1day

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 10.16.1.201
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 10.16.2.201
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)#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:

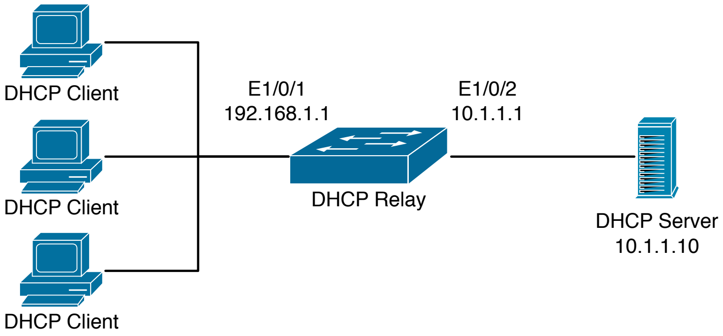


Figure 27.3: DHCP Relay Configuration

As shown in the above figure, route switch is configured as a DHCP relay. The DHCP server address is 10.1.1.10, 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 1/0/2
Switch(Config-Erthernet1/0/2)#switchport access vlan 2
Switch(Config-Erthernet1/0/2)#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 bootps
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.

Scenario 3:

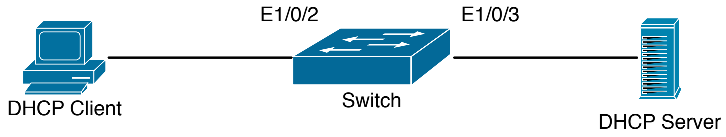


Figure 27.4: DHCP configuration example

As shown in the above figure, PC1 is DHCP client, obtain the address through DHCP. Switch1 is a layer 2 access device, it enables DHCP Relay and option82 functions, Ethernet1/0/2 is a access port, belongs to vlan3, Ethernet1/0/3 is a trunk port, connects to DHCP Server, DHCP Server address is 192.168.40.199. Switch1 creates vlan1 and interface vlan1, configure IP address of interface vlan1 as 192.168.40.50, configure the address of DHCP Relay forwarding as 192.168.40.199, configure vlan3 as a sub-vlan of vlan1. The configuration is as follows:

```
switch(config)#vlan 1
switch(config)#vlan 3
switch(config)#interface ethernet 1/0/2
Switch(Config-If-Ethernet1/0/2)#switchport access vlan 3
switch(config)#interface ethernet 1/0/3
Switch(Config-If-Ethernet1/0/2)#switchport mode trunk
switch(config)#service dhcp
switch(config)#ip forward-protocol udp bootps
switch(config)#ip dhcp relay information option
switch(config)#ip dhcp relay share-vlan 1 sub-vlan 3
switch(config-if-vlan1)#ip address 192.168.40.50 255.255.255.0
switch(config-if-vlan1)#ip helper-address 192.168.40.199
```

27.5 DHCP Troubleshooting

If the DHCP clients cannot obtain IP addresses and other network parameters, the following procedures can be followed when DHCP client hardware and cables have been verified ok.

- Verify the DHCP server is running, start the related DHCP server if not running.
- 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 switch cannot assign IP address for different segments, see solution 2 for details.)
- In DHCP service, pools for dynamic IP allocation and manual binding are conflicting, i.e., if command 'network-address' and 'host' are run for a pool, only one of them will take effect; furthermore, in manual binding, only one IP-MAC binding can be configured in one pool. If multiple bindings are required, multiple manual pools can be created and IP-MAC bindings set for each pool. New configuration in the same pool overwrites the previous configuration.

Chapter 28

DHCPv6 Configuration

28.1 Introduction to DHCPv6

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 entities 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.

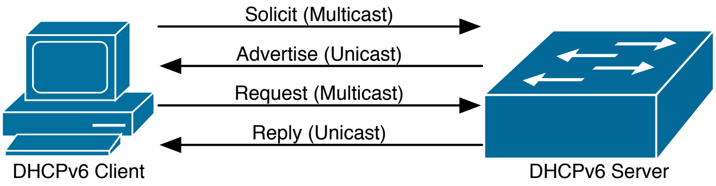


Figure 28.1: DHCPv6 negotiation

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, will 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 a REQUEST message to request the address which is advertised in the ADVERTISE message.

4. The selected DHCPv6 server then confirms the client about the IPv6 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 DHCPv6 client, it will encapsulate the request in a Relay-forward packet and deliver it to the next DHCPv6 relay or the DHCPv6 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 delivers it 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 address prefix manually. The protocol negotiation between the client and the prefix delegation client is quite similar to that when getting a DHCPv6 address. Then the CPE router divides the allocated prefix - whose length should be less than 64 characters, into 64 subnets. The divided address prefix will be advertised through routing advertisement messages (RA) to the host directly connected to the client.

28.2 DHCPv6 Server Configuration

DHCPv6 server configuration task list as below:

1. To enable/disable DHCPv6 service

2. To configure DHCPv6 address pool

    (a) To achieve/delete DHCPv6 address pool

    (b) To configure parameter of DHCPv6 address pool

3. To enable DHCPv6 server function on port

1. To enable/disable DHCPv6 service

Command	Explanation
Global Mode	
service dhcpv6 no service dhcpv6	To enable DHCPv6 service.

2. To configure DHCPv6 address pool
(a) To achieve/delete DHCPv6 address pool

Command	Explanation
Global Mode	
ipv6 dhcp pool <poolname> no ipv6 dhcp pool <poolname>	To configure DHCPv6 address pool.

(b)To configure parameter of DHCPv6 address pool

Command	Explanation
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	Explanation
Interface Configuration Mode	
ipv6 dhcp server <poolname> [preference <value>] [rapid-commit] [allow-hint] no ipv6 dhcp server <poolname>	To enable DHCPv6 server function on specified port, and binding the used DHCPv6 address pool.

28.3 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	Explanation
Global Mode	
service dhcpv6 no service dhcpv6	To enable DHCPv6 service.

2. To configure DHCPv6 relay delegation on port

Command	Explanation
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.

28.4 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
   (a) To achieve/delete DHCPv6 address pool
   (b) To configure prefix delegation pool used by DHCPv6 address pool
   (c) To configure static prefix delegation binding
   (d) To configure other parameters of DHCPv6 address pool
4. To enable DHCPv6 prefix delegation server function on port

1. To enable/delete DHCPv6 service

Command	Explanation
Global Mode	
service dhcpv6 no service dhcpv6	To enable DHCPv6 service.

2. To configure prefix delegation pool

Command	Explanation
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

(a) To achieve/delete DHCPv6 address pool

Command	Explanation
Global Mode	
ipv6 dhcp pool <poolname> no ipv6 dhcp pool <poolname>	To configure DHCPv6 address pool.

(b) To configure prefix delegation pool used by DHCPv6 address pool

Command	Explanation
DHCPv6 address pool Configuration Mode	
prefix-delegation pool <pool-name> [lifetime <valid-time> <preferred-time>] no prefix-delegation pool <pool-name>	To specify prefix delegation pool used by DHCPv6 address pool, and assign usable prefix to client.

(c) To configure static prefix delegation binding

Command	Explanation
DHCPv6 address pool Configuration Mode	
prefix-delegation <ipv6-prefix/prefix-length> <client-DUID> [iaid <iaid>] [lifetime <valid-time> <preferred-time>] no prefix-delegation <ipv6-prefix/prefix-length> <client-DUID> [iaid <iaid>]	To specify IPv6 prefix and any prefix required static binding by client.

(d) To configure other parameter of DHCPv6 address pool

Command	Explanation
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	Explanation
Interface Configuration Mode	
ipv6 dhcp server <poolname> [preference <value>] [rapid-commit] [allow-hint] no ipv6 dhcp server <poolname>	To enable DHCPv6 server function on specified port, and binding used DHCPv6 address pool.

28.5 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	Explanation
Global Mode	
service dhcpv6 no service dhcpv6	To enable DHCPv6 service.

2. To enable DHCPv6 prefix delegation client function on port

Command	Explanation
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.

28.6 DHCPv6 Configuration Examples

Example 1:

When deploying IPv6 networking, the switch can be configured as DHCPv6 server in order to manage the allocation of IPv6 addresses. Both the state and the stateless DHCPv6 are supported.

Topology:

The access layer use Switch1 switch to connect users of dormitory buildings and it is configured as DHCPv6 relay delegation; Switch3 is configured as DHCPv6 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.

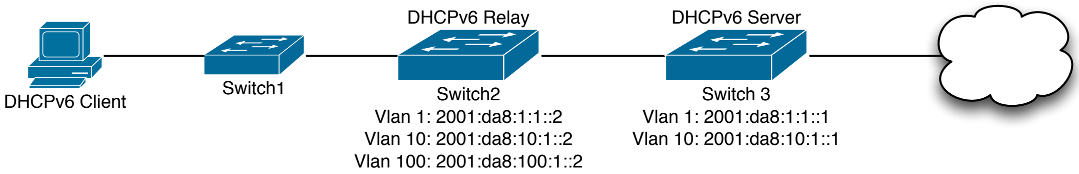


Figure 28.2: DHCPv6 Configuration Example

Usage guide:

Switch3 configuration:

```
Switch3(config)#service dhcpv6
Switch3(config)#ipv6 dhcp pool EDP
Switch3(dhcpv6-EDP-config)#network-address 2001:da8:100:1::1 2001:da8:100:1::100
Switch3(dhcpv6-EDP-config)#excluded-address 2001:da8:100:1::1
Switch3(dhcpv6-EDP-config)#dns-server 2001:da8::20
Switch3(dhcpv6-EDP-config)#dns-server 2001:da8::21
Switch3(dhcpv6-EDP-config)#domain-name dhcpv6.com
Switch3(dhcpv6-EDP-config)#lifetime 1000 600
Switch3(dhcpv6-EDP-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 EDP preference 80
Switch3(Config-if-Vlan10)#exit
```

Switch2 configuration:

```
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)#exit
```

Switch1 configuration:

```
Switch1(config)#service dhcpv6
Switch1(config)#interface vlan 1
Switch1(Config-if-Vlan1)#ipv6 address 2001:da8:100:1::2/64
Switch1(Config-if-Vlan1)#ipv6 dhcp relay destination 2001:da8:10:1::1
```

28.7 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 three 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 29

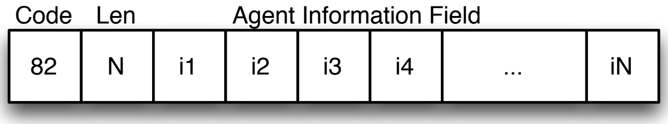
DHCP option 82 Configuration

29.1 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.

29.1.1 DHCP option 82 Message Structure

A DHCP message can have several option segments; option 82 is one of them. It has to be placed after other options but before option 255. The following is its format:



Code: represents the sequence number of the relay agent information option, the option 82 is called so because RFC3046 is defined as 82.

Len: the number of bytes in Agent Information Field, not including the two bytes in Code segment and Len segment.

Option 82 can have several sub-options, and need at least one sub-option. RFC3046 defines the following two sub-options, whose formats are showed as follows:

SubOpt: 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.

SubOpt	Len	Sub-option Value					
1	N	s1	s2	s3	s4	...	sN

SubOpt	Len	Sub-option Value					
2	N	i1	i2	i3	i4	...	iN

Len: the number of bytes in Sub-option Value, not including the two bytes in SubOpt segment and Len segment.

29.1.2 DHCP option 82 Working Mechanism

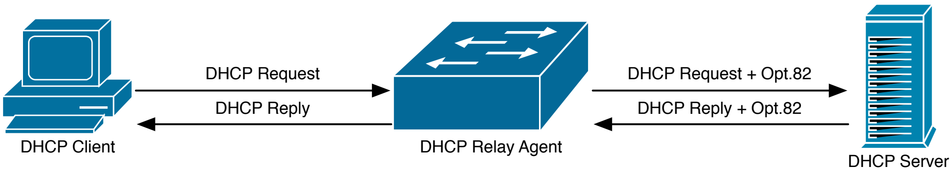


Figure 29.1: DHCP option 82 flow chart

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.

29.2 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. Configure DHCP option 82 default format of Relay Agent
5. Configure delimiter
6. Configure creation method of option82
7. Diagnose and maintain DHCP option 82

1. Enabling the DHCP option 82 of the Relay Agent.

Command	Explanation
Global 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+Ethernet1/0/12', <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.

Global Mode	
ip dhcp relay information option remote-id { standard | <remote-id> } no ip dhcp relay information option remote-id	Set the suboption2 (remote ID option) content of option 82 added by DHCP request packets (They are received by the interface). The no command sets the additive suboption2 (remote ID option) format of option 82 as standard.

3. Enable the DHCP option 82 of server

Command	Explanation
Global 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. Configure DHCP option 82 default format of Relay Agent

Command	Explanation
Global Mode	
ip dhcp relay information option subscriber-id format { hex | acsii | vs-hp }	Set subscriber-id format of Relay Agent option82.
ip dhcp relay information option remote-id format { default | vs-hp }	Set remote-id format of Relay Agent option82.

5. Configure delimiter

Command	Explanation
Global Mode	
ip dhcp relay information option delimiter [colon | dot | slash | space] no ip dhcp relay information option delimiter	Set the delimiter of each parameter for suboption of option82 in global mode, no command restores the delimiter as slash.

6. Configure creation method of option82

Command	Explanation
Global Mode	
ip dhcp relay information option self-defined remote-id { hostname | mac | string WORD } no ip dhcp relay information option self-defined remote-id	Set creation method for option82, users can define the parameters of remote-id suboption by themselves.

ip dhcp relay information option self-defined remote-id format [ascii | hex]	Set self-defined format of remote-id for relay option82.
ip dhcp relay information option self-defined subscriber-id { vlan | port | id (switch-id (mac | hostname) | remote-mac) | string WORD } no ip dhcp relay information option self-defined subscriber-id	Set creation method for option82, users can define the parameters of circute-id suboption by themselves.
ip dhcp relay information option self-defined subscriber-id format [ascii | hex]	Set self-defined format of circuit-id for relay option82.

7. 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.

29.3 DHCP option 82 Application Examples

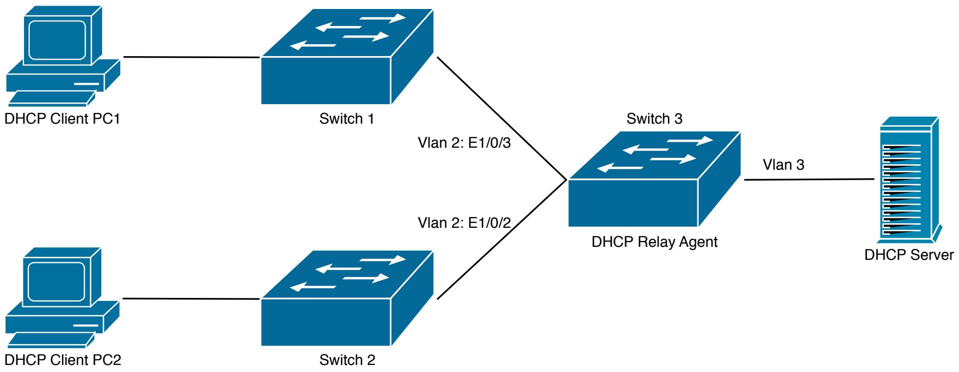


Figure 29.2: A DHCP option 82 typical application example

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 f8:f0:82:02:33:01):

```
Switch3(Config)#service dhcp
Switch3(Config)#ip dhcp relay information option
Switch3(Config)#ip forward-protocol udp bootps
Switch3(Config)#interface vlan 3
Switch3(Config-if-vlan3)#ip address 192.168.10.222 255.255.255.0
Switch3(Config)#interface vlan 2
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.conf is

```
ddns-update-style interim;
ignore client-updates;

class "Switch3Vlan2Class1" {
  match if option agent.circuit-id = "Vlan2+Ethernet1/0/2"
       and option agent.remote-id=f8:f0:82:02:33:01;
}

class "Switch3Vlan2Class2" {
  match if option agent.circuit-id = "Vlan2+Ethernet1/0/3"
       and option agent.remote-id=f8:f0:82:02:33:01;
}

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.

29.4 DHCP option 82 Troubleshooting

- 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 30

DHCPv6 option37, 38

30.1 Introduction to DHCPv6 option37, 38

DHCPv6 (Dynamic Host Configuration Protocol for IPv6) is designed for IPv6 address scheme and is used for assigning IPv6 prefixes, IPv6 addresses and other configuration parameters to hosts.

When DHCPv6 client wants to request address and configure parameter of DHCPv6 server from different link, it needs to communicate with server through DHCPv6 relay agent. DHCPv6 message received by relay agent node is reencapsulated to be relay-forward packets and they are forwarded to the server which sends the relay-reply packets to DHCPv6 relay agent node in different link, after that, relay agent node restores DHCPv6 message to DHCPv6 client to finish communication between client and server.

There are some problems when using DHCPv6 relay agent, for example: How to assign IP address in the fixed range to the specifiec users? How to avoid illegal DHCPv6 client to forge IP address exhaust attack triggered by MAC address fields of DHCPv6 packets? How to avoid illegal DHCPv6 client to trigger deny service attack through using MAC address of other legal clients? Therefore, IETF set rfc4649 and rfc4580, i.e. DHCPv6 option 37 and option 38 to solve these problems.

DHCPv6 option 37 and option 38 is similar to DHCP option 82. When DHCPv6 client sends request packets to DHCPv6 server though DHCPv6 relay agent, if DHCPv6 relay agent supports option 37 and option 38, they will be added to request packets. For the respond packets of server, option 37 and option 38 are meaningless and are peeled from the respond packets. Therefore, the application of option 37 and option 38 is transparent for client.

DHCPv6 server can authenticate identity of DHCPv6 client and DHCPv6 relay device by option 37 and option 38, assign and manage client address neatly through configuring the assign policy, prevent DHCPv6 attack availably according to the inclusive client information, such as forging MAC address fields of DHCPv6 packets to trigger IP address exhaust attack. Since server can identify multiple request packets from the same access port, it can assign the address number through policy limit to avoid address exhaust. However, rfc4649 and rfc4580 do not set how to use opton 37 and option 38 for DHCPv6 server, users can use it neatly according to their own demand.

30.2 DHCPv6 option37, 38 Configuration Task List

1. Dhcpv6 snooping option basic functions configuration
2. Dhcpv6 relay option basic functions configuration
3. Dhcpv6 server option basic functions configuration

1.DHCPv6 snooping option basic functions configuration

Command	Explanation
Global mode	
ipv6 dhcp snooping remote-id option no ipv6 dhcp snooping remote-id option	This command enables DHCPv6 SNOOPING to support option 37 option, no command disables it.
ipv6 dhcp snooping subscriber-id option no ipv6 dhcp snooping subscriber-id option	This command enables DHCPv6 SNOOPING to support option 38 option, no command disables it.
ipv6 dhcp snooping remote-id policy { drop | keep | replace } no ipv6 dhcp snooping remote-id policy	This command is used to configure the reforward policy of the system when receiving DHCPv6 packets with option 37, which can be: drop, the system simply discards it with option 37; keep, the system keeps option 37 unchanged and forwards the packet to the server; replace, the system replaces option 37 of current packet with its own before forwarding it to the server. no command configures the reforward policy of DHCPv6 packets with option 37 as replace.
ipv6 dhcp snooping subscriber-id policy { drop | keep | replace } no ipv6 dhcp snooping subscriber-id policy	This command is used to configure the reforward policy of the system when receiving DHCPv6 packets with option 38, which can be: drop, the system simply discards it with option 38; keep, the system keeps option 38 unchanged and forwards the packet to the server; replace, the system replaces option 38 of current packet with its own before forwarding it to the server. no command configures the reforward policy of DHCPv6 packets with option 38 as replace.
ipv6 dhcp snooping subscriber-id select (sp | sv | pv | spv) delimiter WORD (delimiter WORD |) no ipv6 dhcp snooping subscriber-id select delimiter	Configures user configuration options to generate subscriber-id, no command restores to its original default configuration, i.e. enterprise number together with vlan MAC.

ipv6 dhcp snooping subscriber-id select (sp | sv | pv | spv) delimiter WORD (delimiter WORD |) no ipv6 dhcp snooping subscriber-id select delimiter	Configures user configuration options to generate subscriber-id. The no command restores to its original default configuration, i.e. vlan name together with port name.
Port mode	
ipv6 dhcp snooping remote-id <remote-id> no ipv6 dhcp snooping remote-id	This command is used to set the form of adding option 37 in received DHCPv6 request packets, of which <remote-id> is the content of remote-id in user-defined option 37 and it is a string with a length of less than 128. The no operation restores remote-id in option 37 to enterprise-number together with vlan MAC address.
ipv6 dhcp snooping subscriber-id <subscriber-id> no ipv6 dhcp snooping subscriber-id	This command is used to set the form of adding option 38 in received DHCPv6 request packets, of which <subscriber-id> is the content of subscriber-id in user-defined option 38 and it is a string with a length of less than 128. The no operation restores subscriber-id in option 38 to vlan name together with port name such as "Vlan2+Ethernet1/0/2".

2. **DHCPv6 relay option basic functions configuration**

Command	Explanation
Global mode	
ipv6 dhcp relay remote-id option no ipv6 dhcp relay remote-id option	This command enables the switch relay to support option 37 and the no form of this command disables it.
ipv6 dhcp relay subscriber-id option no ipv6 dhcp relay subscriber-id option	This command enables the switch relay to support the option 38, the no form of this command disables it.
ipv6 dhcp relay remote-id delimiter WORD no ipv6 dhcp relay remote-id delimiter	Configures user configuration options to generate remote-id. The no command restores to its original default configuration, i.e. enterprise number together with vlan MAC.
ipv6 dhcp relay subscriber-id select (sp | sv | pv | spv) delimiter WORD (delimiter WORD |) no ipv6 dhcp relay subscriber-id select delimiter	Configures user configuration options to generate subscriber-id. The no command restores to its original default configuration, i.e. vlan name together with port name.
Layer3 Interface configuration mode	
ipv6 dhcp relay remote-id <remote-id> no ipv6 dhcp relay remote-id	This command is used to set the form of adding option 37 in received DHCPv6 request packets, of which <remote-id> is the content of remote-id in user-defined option 37 and it is a string with a length of less than 128. The no operation restores remote-id in option 37 to enterprise-number together with vlan MAC address.

ipv6 dhcp relay subscriber-id <subscriber-id> no ipv6 dhcp relay subscriber-id	This command is used to set the form of adding option 38 in received DHCPv6 request packets, of which <subscriber-id> is the content of subscriber-id in user-defined option 38 and it is a string with a length of less than 128. The no operation restores subscriber-id in option 38 to vlan name together with port name such as "Vlan2+Ethernet1/0/2".

3. **Dhcpv6 server option basic functions configuration**

Command	Explanation
Global mode	
ipv6 dhcp server remote-id option no ipv6 dhcp server remote-id option	This command enables DHCPv6 server to support the identification of option 37, the no form of this command disables it.
ipv6 dhcp server subscriber-id option no ipv6 dhcp server subscriber-id option	This command enables DHCPv6 server to support the identification of option 38, the no form of this command disables it.
ipv6 dhcp use class no ipv6 dhcp use class	This command enables DHCPv6 server to support the using of DHCPv6 class during address assignment, the no form of this command disables it without removing the relative DHCPv6 class information that has been configured.
ipv6 dhcp class <class-name> no ipv6 dhcp class <class-name>	This command defines a DHCPv6 class and enters DHCPv6 class mode, the no form of this command removes this DHCPv6 class.
Interface configuration mode	
ipv6 dhcp server select relay-forw no ipv6 dhcp server select relay-forw	This command enables the DHCPv6 server to support selections when multiple option 37 or option 38 options exist and the option 37 and option 38 of relay-forw in the innermost layer are selected. The no operation of it restores the default configuration, i.e. selecting option 37 and option 38 of the original packets.
IPv6 DHCP Class configuration mode	

{ remote-id [*] <remote-id> [*] | subscriber-id [*] <subscriber-id> [*] }
no { remote-id [*] <remote-id> [*] | subscriber-id [*] <subscriber-id> [*] }
	This command configures option 37 and option 38 that match the class in ipv6 dhcp class configuration mode.

DHCPv6 address pool configuration mode	
class <class-name> no class <class-name>	This command associates class to address pool in DHCPv6 address pool configuration mode and enters class configuration mode in address pool. Use no command to remove the link.

address range <start-ip> <end-ip> no address range <start-ip> <end-ip>	This command is used to set address range for a DHCPv6 class in DHCPv6 address pool configuration mode, the no command is used to remove the addreass range. The prefix/plen form is not supported.

30.3 DHCPv6 option37, 38 Examples

30.3.1 DHCPv6 Snooping option37, 38 Example

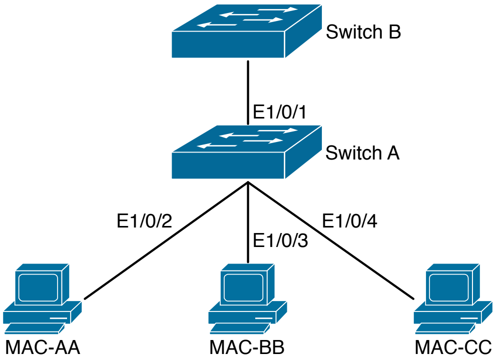


Figure 30.1: DHCPv6 Snooping option schematic

As is shown in the figure above, Mac-AA, Mac-BB and Mac-CC are normal users, connected to untrusted interface 1/0/2, 1/0/3 and 1/0/4 respectively, and they get IP 2010:2, 2010:3 and 2010:4 through DHCPv6 Client; DHCPv6 Server is connected to the trusted interface 1/0/1. Configure three address assignment policies (CLASS), of which CLASS1 matches option 38, CLASS2 matches option 37 and CLASS3 matches option 37 and option 38. In the address pool EDP, the requests matched with CLASS1, CLASS2 and CLASS3 will be assigned an address ranging from 2001:da8:100:1::2 to 2001:da8:100:1::30, from 2001:da8:100:1::31 to 2001:da8:100:1::60 and from 2001:da8:100:1::61 to 2001:da8:100:1::100 respectively; DHCPv6 snooping function is enabled and option 37 and option 38 are configured in Switch A.

Switch A configuration:

```
SwitchA(config)#ipv6 dhcp snooping remote-id option
SwitchA(config)#ipv6 dhcp snooping subscriber-id option
SwitchA(config)#int e 1/0/1
SwitchA(config-if-ethernet1/0/1)#ipv6 dhcp snooping trust
SwitchA(config-if-ethernet1/0/1)#exit
SwitchA(config)#interface vlan 1
SwitchA(config-if-vlan1)#ipv6 address 2001:da8:100:1::1
SwitchA(config-if-vlan1)#exit
SwitchA(config)#interface ethernet 1/0/1-4
SwitchA(config-if-port-range)#switchport access vlan 1
SwitchA(config-if-port-range)#exit
SwitchA(config)#
```

Switch B configuration:

```
SwitchB(config)#service dhcpv6
SwitchB(config)#ipv6 dhcp server remote-id option
SwitchB(config)#ipv6 dhcp server subscriber-id option
SwitchB(config)#ipv6 dhcp pool EDP
SwitchB(dhcpv6-edp-config)#network-address 2001:da8:100:1::2 2001:da8:100:1::1000
SwitchB(dhcpv6-edp-config)#dns-server 2001::1
SwitchB(dhcpv6-edp-config)#domain-name dhcpv6.com
SwitchB(dhcpv6-edp-config)#excluded-address 2001:da8:100:1::2
SwitchB(dhcpv6-edp-config)#exit
SwitchB(config)#
SwitchB(config)#ipv6 dhcp class CLASS1
SwitchB(dhcpv6-class-class1-config)#remote-id f8-f0-82-00-00-01 subscriber-id
                                      vlan1+Ethernet1/0/1
SwitchB(dhcpv6-class-class1-config)#exit
SwitchB(config)#ipv6 dhcp class CLASS2
SwitchB(dhcpv6-class-class2-config)#remote-id f8-f0-82-00-00-01 subscriber-id
                                      vlan1+Ethernet1/0/2
SwitchB(dhcpv6-class-class2-config)#exit
SwitchB(config)#ipv6 dhcp class CLASS3
SwitchB(dhcpv6-class-class3-config)#remote-id f8-f0-82-00-00-01 subscriber-id
                                      vlan1+Ethernet1/0/3
SwitchB(dhcpv6-class-class3-config)#exit
SwitchB(config)#ipv6 dhcp pool EDP
SwitchB(dhcpv6-edp-config)#class CLASS1
SwitchB(dhcpv6-pool-edp-class-class1-config)#address range 2001:da8:100:1::3
                                               2001:da8:100:1::30
SwitchB(dhcpv6-pool-edp-class-class1-config)#exit
SwitchB(dhcpv6-edp-config)#class CLASS2
SwitchB(dhcpv6-pool-edp-class-class2-config)#address range 2001:da8:100:1::31
                                               2001:da8:100:1::60
SwitchB(dhcpv6-edp-config)#class CLASS3
SwitchB(dhcpv6-pool-edp-class-class3-config)#address range 2001:da8:100:1::61
                                               2001:da8:100:1::100
SwitchB(dhcpv6-pool-edp-class-class3-config)#exit
SwitchB(dhcpv6-edp-config)#exit
SwitchB(config)#interface vlan 1
SwitchB(config-if-vlan1)#ipv6 address 2001:da8:100:1::2/64
SwitchB(config-if-vlan1)#ipv6 dhcp server EDP
SwitchB(config-if-vlan1)#exit
SwitchB(config)#
```

30.3.2 DHCPv6 Relay option37, 38 Example

Example 1:

When deploying IPv6 campus network, DHCPv6 server function of routing device can be used for IPv6 address allocation if special server is used for uniform allocation and management for IPv6 address. DHCPv6 server supports both stateful and stateless DHCPv6.

Network topology:

In access layer, layer2 access device Switch1 connects users in dormitory; in first-level aggregation layer, aggregation device Switch2 is used as DHCPv6 relay agent; in second-level aggregation layer, aggregation device Switch3 is used as DHCPv6 server and connects with backbone network or devices in higher aggregation layer; in user side, PCs are generally loaded with Windows Vista system, thus having DHCPv6 client.

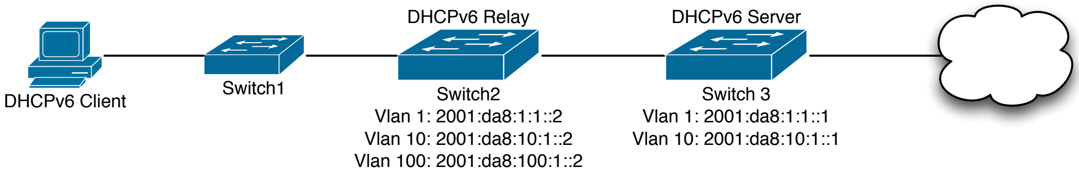


Figure 30.2: DHCPv6 relay option schematic

Switch2 configuration:

```
S2(config)#service dhcpv6
S2(config)#ipv6 dhcp relay remote-id option
S2(config)#ipv6 dhcp relay subscriber-id option
S2(config)#vlan 10
S2(config-vlan10)#int vlan 10
S2(config-if-vlan10)#ipv6 address 2001:da8:1:::2/64
S2(config-if-vlan10)#ipv6 dhcp relay destination 2001:da8:10:1::1
S2(config-if-vlan10)#exit
```

30.4 DHCPv6 option37, 38 Troubleshooting

- Request packets sent by DHCPv6 client are multicast packets received by the device within its VLAN, if DHCPv6 server wants to receive the packets from client, DHCPv6 client and DHCPv6 server must be in the same VLAN, otherwise it needs to use DHCPv6 relay.
- Snooping option37,38 can process one of the following operations for DHCPv6 request packets with option37,38: replace the original option37,38 with its own; discard the packets with option37,38; do not execute adding, discarding or forwarding operation. Therefore, please check policy configuration of snooping option37,38 on second device when obtaining the false address or no address is obtained according to option37,38.
- DHCPv6 server obtains option37,38 of the packets from client by default, if no, it will obtain option37,38 of the packet sent by relay.
- DHCPv6 server only checks whether the first DHCPv6 relay adds option37,38 that means only option37,38 of the innermost relay-forw is valid in relay packets.

Chapter 31

DHCP Snooping Configuration

31.1 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 DCHP 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.

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 Black hole).

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 user based 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 authentication 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.

31.2 DHCP Snooping Configuration Task Sequence

1. Enable DHCP Snooping
2. Enable DHCP Snooping binding function
3. Enable DHCP Snooping binding ARP function
4. Enable DHCP Snooping option82 function
5. Set the private packet version
6. Set DES encrypted key for private packets
7. Set helper server address
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
15. Configure DHCP Snooping option 82 attributes

1. Enable DHCP Snooping

Command	Explanation
Global mode	
ip dhcp snooping enable no ip dhcp snooping enable	Enable or disable the DHCP snooping function.

2. Enable DHCP Snooping binding

Command	Explanation
Global mode	
ip dhcp snooping binding enable no ip dhcp snooping binding enable	Enable or disable the DHCP snooping binding function.

3. Enable DHCP Snooping binding ARP function

Command	Explanation
Global mode	
ip dhcp snooping binding arp no ip dhcp snooping binding arp	Enable or disable the dhcp snooping binding ARP function.

4. Enable DHCP Snooping option82 function

Command	Explanation
Global mode	
ip dhcp snooping information enable no ip dhcp snooping information enable	Enable/disable DHCP Snooping option 82 function.

5. Set the private packet version

Command	Explanation
Global mode	
ip user private packet version two no ip user private packet version two	To configure/delete the private packet version.

6. Set DES encrypted key for private packets

Command	Explanation
Global mode	
enable trustview key 0/7 <password> no enable trustview key	To configure/delete DES encrypted key for private packets.

7. Set helper server address

Command	Explanation
Global mode	
ip user helper-address A.B.C.D [port <udpport>] source <ipAddr> (secondary|) no ip user helper-address (secondary|)	Set or delete helper server address.

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
Global mode	
ip dhcp snooping binding user <mac> address <ipAddr> 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
Global 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 update debug ip dhcp snooping binding	Please refer to the chapter on system troubleshooting.

15. Configure DHCP Snooping option 82 attributes

Command	Explanation
Global mode	
ip dhcp snooping information option subscriber-id format { hex | acsii | vs-hp }	This command is used to set subscriber-id format of DHCP snooping option82.
ip dhcp snooping information option remote-id { standard | <remote-id> } no ip dhcp snooping information option remote-id	Set the suboption2 (remote ID option) content of option 82 added by DHCP request packets (they are received by the port). The no command sets the additive suboption2 (remote ID option) format of option 82 as standard.
ip dhcp snooping information option delimiter [colon | dot | slash | space] no ip dhcp snooping information option delimiter	Set the delimiter of each parameter for suboption of option82 in global mode, no command restores the delimiter as slash.
ip dhcp snooping information option self-defined remote-id { hostname | mac | string WORD } no ip dhcp snooping information option self-defined remote-id	Set creation method for option82, users can define the parameters of remote-id suboption by themselves.
ip dhcp snooping information option self-defined remote-id format [ascii | hex]	Set self-defined format of remote-id for snooping option82.
ip dhcp snooping information option self-defined subscriber-id { vlan | port | id (switch-id (mac | hostname) | remote-mac) | string WORD } no ip dhcp snooping information option type self-defined subscriber-id	Set creation method for option82, users can define the parameters of circute-id suboption by themselves.
ip dhcp snooping information option self-defined subscriber-id format [ascii | hex]	Set self-defined format of circuit-id for snooping option82.
Port mode	
ip dhcp snooping information option subscriber-id { standard | <circuit-id> } no ip dhcp snooping information option subscriber-id	Set the suboption1 (circuit ID option) content of option 82 added by DHCP request packets (they are received by the port). The no command sets the additive suboption1 (circuit ID option) format of option 82 as standard.
Globe mode	
ip dhcp snooping information option allow-untrusted (replace|) no ip dhcp snooping information option allow-untrusted (replace|)	This command is used to set that allow untrusted ports of DHCP snooping to receive DHCP packets with option82 option. When the 'replace' is setting, the potion82 option is allowed to replace. When disabling this command, all untrusted ports will drop DHCP packets with option82 option.

31.3 DHCP Snooping Typical Application

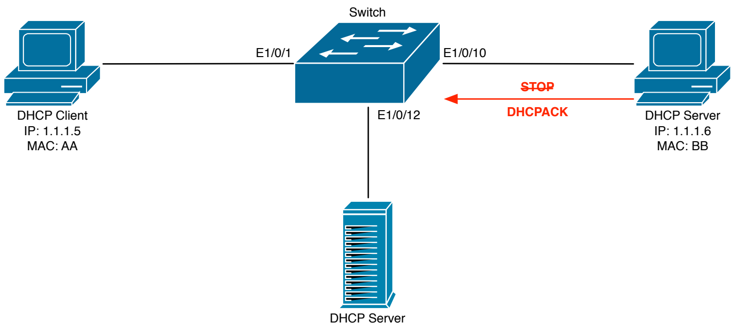


Figure 31.1: Sketch Map of TRUNK

As showed in the above chart, Mac-AA device is the normal user, connected to the non-trusted port 1/0/1 of the switch. It operates via DHCP Client, IP 1.1.1.5; DHCP Server and GateWay are connected to the trusted ports 1/0/11 and 1/0/12 of the switch; the malicious user Mac-BB is connected to the non-trusted port 1/0/10, 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(config)#ip dhcp snooping enable
switch(config)#interface ethernet 1/0/11
switch(Config-Ethernet1/0/11)#ip dhcp snooping trust
switch(Config-Ethernet1/0/11)#exit
switch(config)#interface ethernet 1/0/12
switch(Config-Ethernet1/0/12)#ip dhcp snooping trust
switch(Config-Ethernet1/0/12)#exit
switch(config)#interface ethernet 1/0/1-10
switch(Config-Port-Range)#ip dhcp snooping action shutdown
```

31.4 DHCP Snooping Troubleshooting Help

31.4.1 Monitor and Debug Information

The 'debug ip dhcp snooping' command can be used to monitor the debug information.

31.4.2 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.

Part VIII

Multicast Protocol

Chapter 32

IPv4 Multicast Protocol

32.1 IPv4 Multicast Protocol Overview

This chapter will give an introduction to the configuration of IPv4 Multicast Protocol.

32.1.1 Introduction to Multicast

Various transmission modes can be adopted when the destination of packet (including data, sound and video) transmission is the minority users in the network. One way is to use Unicast mode, i.e. to set up a separate data transmission path for each user; or, to use Broadcast mode, which is to send messages to all users in the network, and they will receive the Broadcast messages no matter they need or not. For example, if there are 200 users in a network who want to receive the same packet, then the traditional solution is to send this packet for 200 times separately via Unicast to guarantee the users who need the data can get all data wanted, or send the data in the entire domain via Broadcast. Transferring the data in the whole range of network .The users who need these data can get directly from the network. Both modes waste a great deal of valuable bandwidth resource, and furthermore, Broadcast mode goes against the security and secrecy.

The emergence of IP Multicast technology solved this problem in time. The Multicast source only sends out the message once, Multicast Routing Protocol sets up tree-routing for Multicast data packet, and then the transferred packet just starts to be duplicated and distributed in the bifurcate crossing as far as possible. Thus the packet can be sent to every user who needs it accurately and effectively.

It should be noticed that it is not necessary for Multicast source to join in Multicast group. It sends data to some Multicast groups, but it is not necessarily a receiver of the group itself. There can be more than one source sending packets to a Multicast group simultaneously. There may exist routers in the network which do not support Multicast, but a Multicast router can encapsulate the Multicast packets into Unicast IP packets with tunnel mode to send them to the Multicast router next to it, which will take off the Unicast IP header and continue the Multicast transmission process, thus a big alteration of network structure is avoided. The primary advantages of Multicast are:

1. Enhance efficiency: reduce network traffic, lighten the load of server and CPU
2. Optimize performance: reduce redundant traffic
3. Distributed application: Enable Multipoint Application

32.1.2 Multicast Address

The destination address of Multicast message uses class D IP address with range from 224.0.0.0 to 239.255.255.255. D class address can not appear in the source IP address field of an IP message. In the process of Unicast data transmission, the transmission path of a data packet is from source address routing to destination address, and the transmission is performed with hop-by-hop principle. However, in IP Multicast environment, the destination addresses is a group instead of a single one, they form a group address. All message receivers will join in a group, and once they do, the data flowing to the group address will be sent to the receivers immediately and all members in the group will receive the data packets. The members in a Multicast group are dynamic, the hosts can join and leave the Multicast group at any time.

Multicast group can be permanent or temporary. Some of the Multicast group addresses are assigned officially; they are called Permanent Multicast Group. Permanent Multicast Group keeps its IP address fixed but its member structure can vary within. The member amount of Permanent Multicast Group can be arbitrary, even zero. The IP Multicast addresses which are not kept for use by Permanent Multicast Group can be utilized by temporary Multicast groups.

224.0.0.0 - 224.0.0.255 are reserved Multicast addresses (Permanent Group Address), address 224.0.0.0 is reserved but not assigned, and other addresses are used by Routing Protocol; 224.0.1.0 - 238.255.255.255 are Multicast addresses available to users (Temporary Group Address) and are valid in the entire domain of the network; 239.0.0.0 - 239.255.255.255 are local management Multicast addresses, which are valid only in specific local domain. Frequently used reserved multicast address list is as follows:

```
Benchmark address (reserved)
224.0.0.1 Address of all hosts
224.0.0.2 Address of all Multicast Routers
224.0.0.3 Unassigned
224.0.0.4 DVMRP Router
224.0.0.5 OSPF Router
224.0.0.6 OSPF DR
224.0.0.7 ST Router
224.0.0.8 ST host
224.0.0.9 RIP-2 Router
224.0.0.10 IGRP Router
224.0.0.11 Active Agent
224.0.0.12 DHCP Server/Relay Agent
224.0.0.13 All PIM Routers
224.0.0.14 RSVP Encapsulation
224.0.0.15 All CBT Routers
224.0.0.16 Specified SBM
224.0.0.17 All SBMS
224.0.0.18 VRRP
224.0.0.22 IGMP
```

When Ethernet transmits Unicast IP messages, the destination MAC address it uses is the receiver's MAC address. But in transmitting Multicast packets, the transmission destination is not a specific receiver any more, but a group with uncertain members, thus Multicast MAC address is used. Multicast MAC address is corresponding to Multicast IP address. It is prescribed in

IANA (Internet Assigned Number Authority) that the higher 25 bits in Multicast MAC address is 0x01005e, and the lower 23bits in MAC address is the lower 23bits in Multicast IP address.

Since only 23bits out of the lower 28bits in IP Multicast address are mapped into MAC address, therefore there are 32 IP Multicast addresses which are mapped into the same MAC address.

32.1.3 IP Multicast Packet Transmission

In Multicast mode, the source host sends packets to the host group indicated by the Multicast group address in the destination address field of IP data packet. Unlike Unicast mode, Multicast data packet must be forwarded to a number of external interfaces to be sent to all receiver sites in Multicast mode, thus Multicast transmission procedure is more complicated than Unicast transmission procedure.

In order to guarantee that all Multicast packets get to the router via the shortest path, the receipt interface of the Multicast packet must be checked in some certain way based on Unicast router table; this checking mechanism is the basis for most Multicast Routing Protocol to forward in Multicast mode --- RPF (Reverse Path Forwarding) check. Multicast router makes use of the impressed packet source address to query Unicast Router Table or independent Multicast Router Table to determine if the packet ingress interface is on the shortest path from receipt site to source address. If shortest path Tree is used, then the source address is the address of source host which sends Multicast Data Packets; if Shared Tree is used, then the source address is the address of the root of the Shared-Tree. When Multicast data packet gets to the router, if RPF check passes, then the data packet is forwarded according to Multicast forward item, and the data packet will be discarded else wise.

32.1.4 IP Multicast Application

IP Multicast technology has effectively solved the problem of sending in single point and receiving in multipoint. It has achieved the effective data transmission from a point to multiple points, saved a great deal of network bandwidth and reduced network load. Making use of the Multicast property of network, some new value-added operations can be supplied conveniently. In Information Service areas such as online living broadcast, network TV, remote education, remote medicine, real time video/audio meeting, the following applications may be supplied:

1. Application of Multimedia and Streaming Media
2. Data repository, finance application (stock) etc
3. Any data distribution application of 'one point to multiple points'

In the situation of more and more multimedia operations in IP network, Multicast has tremendous market potential and Multicast operation will be generalized and popularized.

32.2 DCSCM

32.2.1 Introduction to DCSCM

DCSCM (Destination control and source control multicast) technology mainly includes three aspects, i.e. Multicast Packet Source Controllable, Multicast User Controllable and Service-Oriented

Priority Strategy Multicast.

The Multicast Packet Source Controllable technology of Security Controllable Multicast technology is mainly processed in the following manners:

1. On the edge switch, if source under-control multicast is configured, then only multicast data from specified group of specified source can pass.
2. For RP switch in the core of PIM-SM, for REGISTER information out of specified source and specified group, REGISTER_STOP is transmitted directly and table entry is not allowed to set up. (This task is implemented in PIM-SM model).

The implement of Multicast User Controllable technology of Security Controllable Multicast technology is based on the control over IGMP report message sent out by the user, thus the model being controlled is IGMP snooping and IGMP model, of which the control logic includes the following three, i.e. to take control based on VLAN+MAC address transmitting packets, to take control based on IP address of transmitting packets and to take control based on the port where messages enter, in which IGMP snooping can use the above three methods to take control simultaneously, while since IGMP model is located at layer 3, it only takes control over the IP address transmitting packets.

The Service-Oriented Priority Strategy Multicast of Security Controllable technology adopts the following mode: for multicast data in limit range, set the priority specified by the user at the join-in end so that data can be sent in a higher priority on TRUNK port, consequently guarantee the transmission is processed in user-specified priority in the entire network.

32.2.2 DCSCM Configuration Task List

1. Source Control Configuration
2. Destination Control Configuration
3. Multicast Strategy Configuration

1. Source Control Configuration

Source Control Configuration has three parts, of which the first is to enable source control. The command of source control is as follows:

Command	Explanation
Global Configuration Mode	
[no] ip multicast source-control (Required)	Enable source control globally, the 'no ip multicast source-control' command disables source control globally. It is noticeable that, after enabling source control globally, all multicast packets are discarded by default. All source control configuration can not be processed until that it is enabled globally, while source control can not be disabled until all configured rules are disabled.

The next is to configure the rule of source control. It is configured in the same manner as for ACL, and uses ACL number of 5000-5099, every rule number can be used to configure 10 rules. It is noticeable that these rules are ordered, the front one is the one which is configured the earliest.

Once the configured rules are matched, the following rules won't take effect, so rules of globally allow must be put at the end. The commands are as follows:

Command	Explanation
Global Configuration Mode	
[no] access-list <5000-5099> { deny | permit } ip { { <source> <source-wildcard> } | { host-source <source-host-ip> } | any-source } { { <destination> <destination-wildcard> } | { host-destination <destination-host-ip> } | any-destination }	The rule used to configure source control. This rule does not take effect until it is applied to specified port. Using the NO form of it can delete specified rule.

The last is to configure the configured rule to specified port.

Note: If the rules being configured will occupy the table entries of hardware, configuring too many rules will result in configuration failure caused by bottom table entries being full, so we suggest user to use the simplest rules if possible. The configuration rules are as follows:

Command	Explanation
Port Configuration Mode	
[no] ip multicast source-control access-group <5000-5099>	Used to configure the rules source control uses to port, the NO form cancels the configuration.

2. Destination Control Configuration

Like source control configuration, destination control configuration also has three steps.

First, enable destination control globally. Since destination control need to prevent unauthorized user from receiving multicast data, the switch won't broadcast the multicast data it received after configuring global destination control. Therefore, It should be avoided to connect two or more other Layer 3 switches in the same VLAN on a switch on which destination control is enabled. The configuration commands are as follows:

Command	Explanation
Global Configuration Mode	
[no] multicast destination-control (required)	Globally enable IPv4 and IPv6destination control. The no operation of this command will globally disable destination control. All of the other configuration can only take effect after globally enabled. The next is configuring destination control rules, which are similar.

Next is to configure destination control rule. It is similar to source control, except to use ACL No. of 6000-7999.

Command	Explanation
Global Configuration Mode	
[no] access-list <6000-7999> { deny | permit } ip { { <source> <source-wildcard> } | { host-source <source-host-ip> { range<2-65535> | } } | any-source } { { <destination> <destination-wildcard> } | { host-destination <destination-host-ip> { range<2-255> | } } | any-destination }	The rule used to configure destination control. This rule does not take effect until it is applied to source IP or VLAN-MAC and port. Using the NO form of it can delete specified rule.

The last is to configure the rule to specified source IP, source VLAN MAC or specified port. It is noticeable that, due to the above situations, these rules can only be used globally in enabling IGMP-SNOOPING. And if IGMP-SNOOPING is not enabled, then only source IP rule can be used under IGMP Protocol. The configuration commands are as follows:

Command	Explanation
Port Configuration Mode	
[no] ip multicast destination-control access-group <6000-7999>	Used to configure the rules destination control uses to port, the NO form cancels the configuration.
Global Configuration Mode	
[no] ip multicast destination-control <1-4094> <macaddr> access-group <6000-7999>	Used to configure the rules destination control uses to specify VLAN-MAC, the NO form cancels the configuration.
[no] ip multicast destination-control <IPADDRESS/M> access-group <6000-7999>	Used to configure the rules destination control uses to specified IP address/net mask, the NO form cancels the configuration.

3. Multicast Strategy Configuration

Multicast Strategy uses the manner of specifying priority for specified multicast data to achieve and guarantee the effects the specific user requires. It is noticeable that multicast data can not get a special care all along unless the data are transmitted at TRUNK port. The configuration is very simple, it has only one command, i.e. to set priority for the specified multicast. The commands are as follows:

Command	Explanation
Global Configuration Mode	
[no] ip multicast policy <IPADDRESS/M> <IPADDRESS/M> cos <priority>	Configure multicast strategy, specify priority for sources and groups in specific range, and the range is <0-7>.

32.2.3 DCSCM Configuration Examples

1. Source Control

In order to prevent an Edge Switch from putting out multicast data ad asbitsium, we configure Edge Switch so that only the switch at port Ethernet1/0/5 is allowed to transmit multicast, and the data group must be 225.1.2.3. Also, switch connected up to port Ethernet1/0/10 can transmit multicast data without any limit, and we can make the following configuration.

```
Switch(config)#access-list 5000 permit ip any host 225.1.2.3
Switch(config)#access-list 5001 permit ip any any
Switch(config)#ip multicast source-control
Switch(config)#interface ethernet1/0/5
Switch(Config-If-Ethernet1/0/5)#ip multicast source-control access-group 5000
Switch(config)#interface ethernet1/0/10
Switch(Config-If-Ethernet1/0/10)#ip multicast source-control access-group 5001
```

2. Destination Control

We want to limit users with address in 10.0.0.0/8 network segment from entering the group of 238.0.0.0/8, so we can make the following configuration:

Firstly enable IGMP snooping in the VLAN it is located (Here it is assumed to be in VLAN2)

```
Switch(config)#ip igmp snooping
Switch(config)#ip igmp snooping vlan 2
```

After that, configure relative destination control access-list, and configure specified IP address to use that access-list.

```
Switch(config)#access-list 6000 deny ip any 238.0.0.0 0.255.255.255
Switch(config)#access-list 6000 permit ip any any
Switch(config)#multicast destination-control
Switch(config)#ip multicast destination-control 10.0.0.0/8 access-group 6000
```

In this way, users of this network segment can only join groups other than 238.0.0.0/8.

3. Multicast strategy

Server 210.1.1.1 is distributing important multicast data on group 239.1.2.3, we can configure on its join-in switch as follows:

```
Switch(config)#ip multicast policy 210.1.1.1/32 239.1.2.3/32 cos 4
```

In this way, the multicast stream will have a priority of value 4 (Usually this is pretty higher, the higher possible one is protocol data; if higher priority is set, when there is too many multicast data, it might cause abnormal behavior of the switch protocol) when it gets to other switches through this switch.

32.2.4 DCSCM Troubleshooting

The effect of DCSCM module itself is similar to ACL, and the problems occurred are usually related to improper configuration. Please read the descriptions above carefully. If you still can not determine the cause of the problem, please send your configurations and the effects you expect to the after-sale service staff of our company.

32.3 IGMP Snooping

32.3.1 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 an 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 an 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.

Switch provides IGMP Snooping and is able to send a query from the switch so that the user can use switch in IP multicast.

32.3.2 IGMP Snooping Configuration Task List

1. Enable IGMP Snooping
2. Configure IGMP Snooping

1. Enable IGMP Snooping

Command	Explanation
Global Configuration Mode	
ip igmp snooping no ip igmp snooping	Enables IGMP Snooping. The no operation disables IGMP Snooping function.

2. Configure IGMP Snooping

Command	Explanation
Global Configuration Mode	
ip igmp snooping vlan <vlan-id> no ip igmp snooping vlan <vlan-id>	Enables IGMP Snooping for specified VLAN. The no operation disables IGMP Snooping for specified VLAN.
ip igmp snooping proxy no ip igmp snooping proxy	Enable IGMP Snooping proxy function, the no command disables the function.
ip igmp snooping vlan <vlan-id> limit { group <g_limit> | source <s_limit> } no ip igmp snooping vlan <vlan-id> limit	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.
ip igmp snooping vlan <1-4094> interface (ethernet | port-channel |) IFNAME limit { group <1-65535> | source <1-65535> } strategy (replace | drop) no ip igmp snooping vlan <1-4094> interface (ethernet | port-channel |) IFNAME limit group source strategy	Configure the number of groups which are allowed joining and the maximum of the source in each group under the IGMP Snooping port. Configure the strategy when it is up to the upper limit, including 'replace' and 'drop'. No command configures as 'no limitation'.
ip igmp snooping vlan <vlan-id> l2-general-querier no ip igmp snooping vlan <vlan-id> l2-general-querier	Set this vlan to layer 2 general querier. It is recommended to configure a layer 2 general querier on a segment. The 'no ip igmp snooping vlan <vlan-id> l2-general-querier' command cancels this configuration.
ip igmp snooping vlan <vlan-id> l2-general-querier-version <version>	Configure the version number of a general query from a layer 2 general querier.

ip igmp snooping vlan <vlan-id> l2-general-querier-source <source>	Configure the source address of a general query from a layer 2 general querier.
ip igmp snooping vlan <vlan-id> mrouter-port interface <interface-name> no ip igmp snooping vlan <vlan-id> mrouter-port interface <interface-name>	Configure static mrouter port of vlan. The no form of the command cancels this configuration.
ip igmp snooping vlan <vlan-id> mrouter-port learnpim no ip igmp snooping vlan <vlan-id> mrouter-port learnpim	Enable the function that the specified VLAN learns mrouter-port (according to pim packets), the no command will disable the function.
ip igmp snooping vlan <vlan-id> mrpt <value> no ip igmp snooping vlan <vlan-id> mrpt	Configure this survive time of mrouter port. The 'no ip igmp snooping vlan <vlan-id> mrpt' command restores the default value.
ip igmp snooping vlan <vlan-id> query-interval <value> no ip igmp snooping vlan <vlan-id> query-interval	Configure this query interval. The 'no ip igmp snooping vlan <vlan-id> query-interval' command restores the default value.
ip igmp snooping vlan <vlan-id> immediately-leave no ip igmp snooping vlan <vlan-id> immediately-leave	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.
ip igmp snooping vlan <vlan-id> query-mrsp <value> no ip igmp snooping vlan <vlan-id> query-mrsp	Configure the maximum query response period. The 'no ip igmp snooping vlan <vlan-id> query-mrsp' command restores to the default value.
ip igmp snooping vlan <vlan-id> query-robustness <value> no ip igmp snooping vlan <vlan-id> query-robustness	Configure the query robustness. The 'no ip igmp snooping vlan <vlan-id> query-robustness' command restores to the default value.
ip igmp snooping vlan <vlan-id> suppression-query-time <value> no ip igmp snooping vlan <vlan-id> suppression-query-time	Configure the suppression query time. The 'no ip igmp snooping vlan <vlan-id> suppression-query-time' command restores to the default value.
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>	Configure static-group on specified port of the VLAN. The no form of the command cancels this configuration.
ip igmp snooping vlan <vlan-id> report source-address <A.B.C.D> no ip igmp snooping vlan <vlan-id> report source-address	Configure forwarding IGMP packet source address, The no operation cancels the packet source address.

ip igmp snooping vlan <vlan-id> specific-query-mrsp <value> no ip igmp snooping vlan <vlan-id> specific-query-mrsp	Configure the maximum query response time of the specific group or source, the no command restores the default value.

32.3.3 IGMP Snooping Examples

Scenario 1: IGMP Snooping function

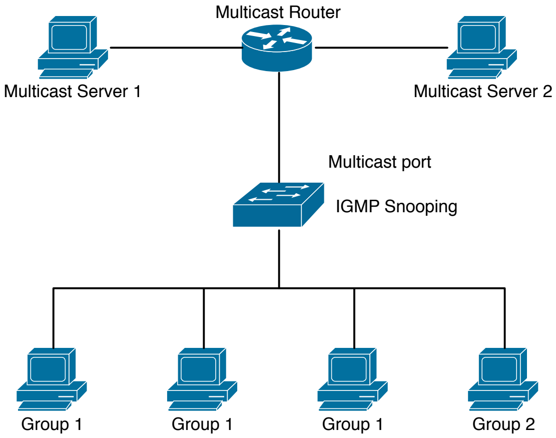


Figure 32.1: Enabling IGMP Snooping function

Example: As shown in the above figure, a VLAN 100 is configured in the switch and includes ports 1, 2, 6, 10 and 12. Four hosts are connected to port 2, 6, 10 and 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)#ip igmp snooping
Switch(config)#ip igmp snooping vlan 100
Switch(config)#ip igmp snooping vlan 100 mrouter interface ethernet 1/0/1
```

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

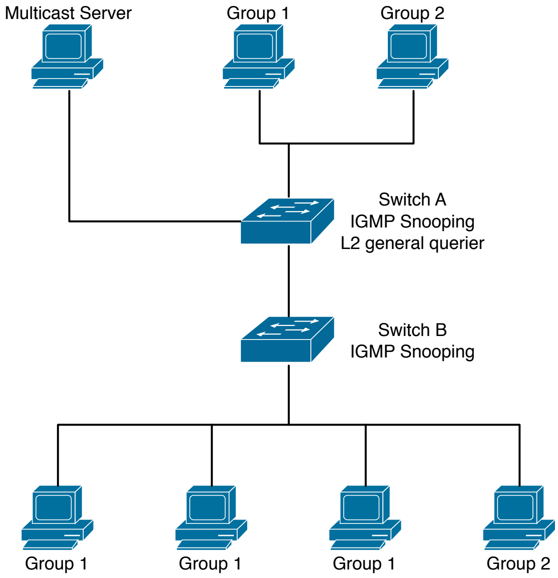


Figure 32.2: The switches as IGMP Queries

The configuration of Switch2 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, 10 and 12. Port 1 connects to the multicast server, and port 2 connects to Switch2. 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)#ip igmp snooping
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 1/0/1
```

Multicast Configuration

The same as scenario 1

IGMP Snooping listening result:

Similar to scenario 1

Scenario 3: To run in cooperation with layer 3 multicast protocols.

SWITCH which is used in Scenario 1 is replaced with ROUTER with specific configurations remains the same. And multicast and IGMP snooping configurations are the same with what it is in Scenario 1. To configure PIM-SM on ROUTER, and enable PIM-SM on vlan 100 (use the same PIM mode with the connected multicast router)

Configurations are listed as below:

```
switch(config)#ip pim multicast-routing
switch(config)#interface vlan 100
switch(config-if-vlan100)#ip pim sparse-mode
```

IGMP snooping does not distribute entries when layer 3 multicast protocol is enabled. It only does the following tasks.

- Remove the layer 2 multicast entries.
- Provide query functions to the layer 3 with vlan, S, and G as the parameters.
- When layer 3 IGMP is disabled, re-enable distributing layer 2 multicast entries.

By looking up the layer 3 IPMC entries, it can be found that ports can be indicated by the layer 3 multicast entries. This ensures the IGMP snooping can work in cooperation with the layer 3 multicast protocols.

32.3.4 IGMP Snooping Troubleshooting

On IGMP Snooping function configuration and usage, IGMP Snooping might not run properly because of physical connection or configuration mistakes. So the users should note that:

- Make sure correct physical connection
- Activate IGMP Snooping on whole configuration mode (use ip igmp snooping)
- Configure IGMP Snooping at VLAN on whole configuration mode (use ip igmp snooping vlan <vlan-id>)
- Make sure one VLAN is configured as L2 common checker in same mask, or make sure configured static mrouter
- Use show ip igmp snooping vlan <vid> command check IGMP Snooping information

Chapter 33

IPv6 Multicast Protocol

33.1 IPv6 DCSCM

33.2 MLD Snooping

33.2.1 Introduction to MLD Snooping

MLD, the Multicast Listener Discovery Protocol, is used to realize multicasting in the IPv6. MLD is used by the network equipments such as routers which supports multicast for multicast listener discovery, also used by listeners looking forward to join certain multicast group informing the router to receive data packets from certain multicast address, all of which are done through MLD message exchange. First the router send an MLD Multicast listener Query message through a multicast address which can address all the listeners (namely ff02::1). Once there is a listener who wishes to join the multicast address, it will send a MLD Multicast listener Report back through the multicast address.

MLD Snooping is namely the MLD listening. The switch restricts the multicast traffic from flooding through MLD Snooping, and forward the multicast traffic to ports associated to multicast devices only. The switch listens to the MLD messages between multicast routers and listeners, and maintains the multicast group forwarding list based on the listening result. The switches forwards multicast packets according to the multicast forwarding list

The switch realizes the MLD Snooping function while supporting MLD v2. This way, the user can acquire IPv6 multicast with the switch.

33.2.2 MLD Snooping Configuration Task

1. Enable the MLD Snooping function

2. Configure the MLD Snooping

1. Enable the MLD Snooping function

Command	Explanation
Global Mode	
ipv6 mld snooping no ipv6 mld snooping	Enable global MLD Snooping, the 'no ipv6 mld snooping' command disables the global MLD snooping.

2. Configure MLD Snooping

Command	Explanation
Global Mode	
ipv6 mld snooping vlan <vlan-id> no ipv6 mld snooping vlan <vlan-id>	Enable MLD Snooping on specific VLAN. The 'no' form of this command disables MLD Snooping on specific VLAN.
ipv6 mld snooping vlan <vlan-id> limit { group <g_limit> | source <s_limit> } no ipv6 mld snooping vlan <vlan-id> limit	Configure the number of the groups in which the MLD Snooping can join, and the maximum number of sources in each group. The 'no' form of this command restores to the default.
ipv6 mld snooping vlan <vlan-id> l2-general-querier no ipv6 mld snooping vlan <vlan-id> l2-general-querier	Set the VLAN level 2 general querier, which is recommended on each segment. The 'no' form of this command cancels the level 2 general querier configuration.
ipv6 mld snooping vlan <vlan-id> mrouter-port interface <interface-name> no ipv6 mld snooping vlan <vlan-id> mrouter-port interface <interface-name>	Configure the static mrouter port in specific vlan. The 'no' form of this command cancels the mrouter port configuration.
ipv6 mld snooping vlan <vlan-id> mrouter-port learnpim6 no ipv6 mld snooping vlan <vlan-id> mrouter-port learnpim6	Enable the function that the specified VLAN learns mrouter-port (according to pimv6 packets), the no command will disable the function.
ipv6 mld snooping vlan <vlan-id> mrpt <value> no ipv6 mld snooping vlan <vlan-id> mrpt	Configure the keep-alive time of the mrouter port. The 'no' form of this command restores to the default.
ipv6 mld snooping vlan <vlan-id> query-interval <value> no ipv6 mld snooping vlan <vlan-id> query-interval	Configure the query interval. The 'no' form of this command restores to the default.
ipv6 mld snooping vlan <vlan-id> immediate-leave no ipv6 mld snooping vlan <vlan-id> immediate-leave	Configure immediate leave multicast group function for the MLD Snooping of specific VLAN. The 'no' form of this command cancels the immediate leave configuration.
ipv6 mld snooping vlan <vlan-id> query-mrsp <value> no ipv6 mld snooping vlan <vlan-id> query-mrsp	Configure the query maximum response period. The 'no' form of this command restores to the default.
ipv6 mld snooping vlan <vlan-id> query-robustness <value> no ipv6 mld snooping vlan <vlan-id> query-robustness	Configure the query robustness, the 'no' form of this command restores to the default.
ipv6 mld snooping vlan <vlan-id> suppression-query-time <value> no ipv6 mld snooping vlan <vlan-id> suppression-query-time	Configure the suppression query time. The 'no' form of this command restores to the default.

ipv6 mld snooping vlan <vlan-id> static-group <X:X::X:X> [source <X:X::X:X>] interface [ethernet | port-channel] <IFNAME> no ipv6 mld snooping vlan <vlan-id> static-group <X:X::X:X> [source <X:X::X:X>] interface [ethernet | port-channel] <IFNAME>	Configure static-group on specified port of the VLAN. The no form of the command cancels this configuration.

33.2.3 MLD Snooping Examples

Scenario 1: MLD Snooping Function

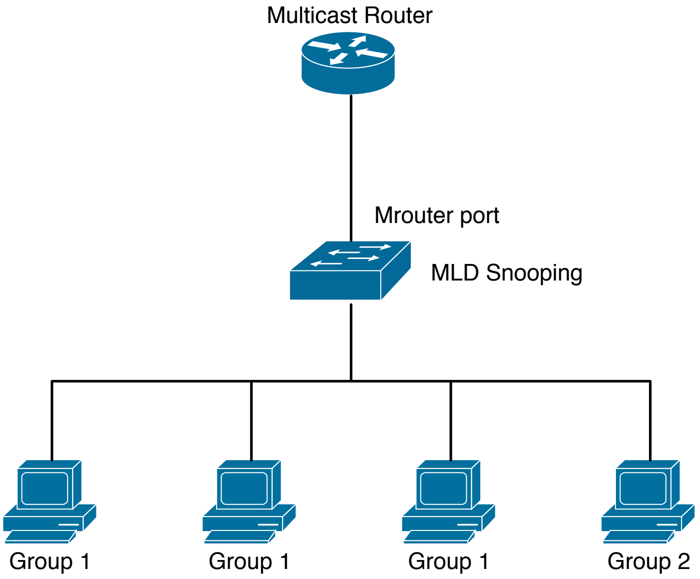


Figure 33.1: Open the switch MLD Snooping Function figure

As shown above, the vlan 100 configured on the switch consists of ports 1, 2, 6, 10 and 12. Four hosts are respectively connected to 2, 6, 10 and 12 while the multicast router on port 1. Suppose we need MLD Snooping on VLAN 100, however by default, the global MLD Snooping as well as the MLD Snooping on each VLAN are, therefore first we have to enable the global MLD Snooping at the same time enable the MLD Snooping on VLAN 100, furthermore we need to set the port 1 of VLAN 100 as a mrouter port.

Configuration procedure is as follows.

```
Switch(config)#ipv6 mld snooping
Switch(config)#ipv6 mld snooping vlan 100
Switch(config)#ipv6 mld snooping vlan 100 mrouter-port interface ethernet 1/0/1
```

Multicast configuration:

Assume there are two multicast servers: the Multicast Server 1 and the Multicast Server 2, amongst program 1 and 2 are supplied on the Multicast Server 1 while program 3 on the Multicast server 2, using group addresses respectively the Group 1, Group 2 and Group 3. Concurrently multicast application is operating on the four hosts. Two hosts connected to port 2, 6 are playing program 1 while the host connected to port 10 playing program 2, and the one to port 12 playing program 3.

MLD Snooping interception results:

The multicast table on vlan 100 shows: port 1, 2, 6 are in (Multicasting Server 1, Group1), port1, 10 are in (Multicasting Server 1, Group2), and port1, 121, 12 are in (Multicasting Server 2, Group3)

All the four hosts successfully receive programs they are interested in. port2, 6 receives no traffic from program2 and 3; port10 receives no traffic from program 1 and 3, and port12 receives no traffic from program1 and 2.

Scenario 2: MLD L2-general-querier

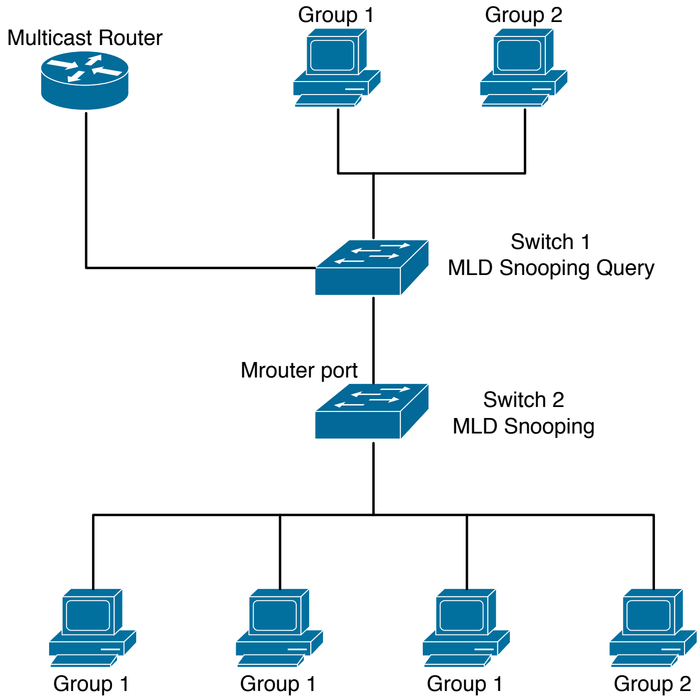


Figure 33.2: Switch as MLD Querier Function figure

Configuration of switch B is the same as the switches in case 1, and here the switch 1 replaces the Multicast Router in case 1. Assume the vlan 60 configured on it contains port 1, 2, 10 and 12, amongst port 1 is connected to multicast server, port 2 to switch2. To send Query periodically, global MLD Snooping has to be enabled while executing the mld snooping vlan 60 l2-general-querier, setting the vlan 60 to a Level 2 General Querier.

Configuration procedure is as follows:

```
SwitchA(config)#ipv6 mld snooping
SwitchA(config)#ipv6 mld snooping vlan 60
SwitchA(config)#ipv6 mld snooping vlan 60 l2-general-querier

SwitchB(config)#ipv6 mld snooping
SwitchB(config)#ipv6 mld snooping vlan 100
SwitchB(config)#ipv6 mld snooping vlan 100 mrouter interface ethernet 1/0/1
```

Multicast configuration:
Same as scenario 1
MLD Snooping interception results:
Same as scenario 1

33.2.4 MLD Snooping Troubleshooting

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

- Ensure the physical connection is correct
- Ensure the MLD Snooping is enabled under global mode (using ipv6 mld snooping)
- Ensure the MLD Snooping is configured on the vlan under global mode (using ipv6 mld snooping vlan <vlan-id>)
- Ensure there is a vlan configured as a L2 general querier, or there is a static mrouter configured in a segment,
- Use command to check if the MLD snooping information is correct

Chapter 34

Multicast VLAN

34.1 Introductions to Multicast VLAN

Based on current multicast order method, when orders from users in different VLAN, each VLAN will copy a multicast traffic in this VLAN, which is a great waste of the bandwidth. By configuration of the multicast VLAN, we add the switch port to the multicast VLAN, with the IGMP Snooping/MLD Snooping functions enabled, users from different VLAN will share the same multicast VLAN. The multicast traffic only exists within a multicast VLAN, so the bandwidth is saved. As the multicast VLAN is absolutely separated from the user VLAN, security and bandwidth concerns can be met at the same time, after the multicast VLAN is configured, the multicast traffic will be continuously sent to the users.

34.2 Multicast VLAN Configuration Task List

1. Enable the multicast VLAN function
2. Configure the IGMP Snooping

1. Enable the multicast VLAN function

Command	Explanation
VLAN configuration mode	
multicast-vlan no multicast-vlan	Configure a VLAN and enable the multicast VLAN on it. The 'no multicast-vlan' command disables the multicast function on the VLAN.
multicast-vlan association <vlan-list> no multicast-vlan association <vlan-list>	Associate a multicast VLAN with several VLANs. The no form of this command deletes the related VLANs associated with the multicast VLAN.
multicast-vlan association interface (ethernet | port-channel |) IFNAME no multicast-vlan association interface (ethernet | port-channel |) IFNAME	Associate the specified port with the multicast VLAN, so the associated ports are able to receive the multicast flow. The no command cancels the association between the ports and the multicast VLAN.

2. Configure the IGMP Snooping

Command	Explanation
Global Mode	
ip igmp snooping vlan <vlan-id> no ip igmp snooping vlan <vlan-id>	Enable the IGMP Snooping function on the multicast VLAN. The no form of this command disables the IGMP Snooping on the multicast VLAN.
ip igmp snooping no ip igmp snooping	Enable the IGMP Snooping function. The no form of this command disables the IGMP snooping function.

34.3 Multicast VLAN Examples

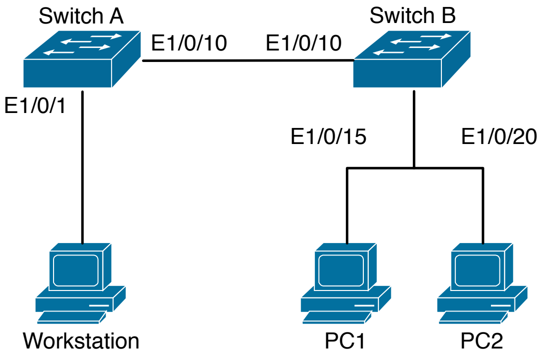


Figure 34.1: Function configuration of the Multicast VLAN

As shown in the figure, WORKSTATION (multicast server) is connected to the layer 3 switch switchA through port 1/0/1 which belongs to the VLAN10 of the switch. The layer 3 switch switchA is connected with layer 2 switches through the port1/0/10, which configured as trunk port. On the switchB the VLAN100 is configured set to contain port1/0/15, and VLAN101 to contain port1/0/20. PC1 and PC2 are respectively connected to port 1/0/15 and 1/0/20. The switchB is connected with the switchA through port1/0/10, which configured as trunk port. VLAN 20 is a multicast VLAN. By configuring multicast vlan, the PC1 and PC2 will receives the multicast data from the multicast VLAN.

Following configuration is based on the IP address of the switch has been configured and all the equipment are connected correctly.

Configuration procedure

```
SwitchA#config
SwitchA(config)#vlan 10
SwitchA(config-vlan10)#switchport access ethernet 1/0/1
SwitchA(config-vlan10)exit
SwitchA(config)#interface vlan 10
Switch(Config-if-Vlan10)#ip pim dense-mode
Switch(Config-if-Vlan10)#exit
SwitchA(config)#vlan 20
SwitchA(config-vlan20)#exit
SwitchA(config)#interface vlan 20
SwitchA(Config-if-Vlan20)#ip pim dense-mode
SwitchA(Config-if-Vlan20)#exit
SwitchA(config)#ip pim multicast
SwitchA(config)# interface ethernet1/0/10
SwitchA(Config-If-Ethernet1/0/10)switchport mode trunk
```

```
SwitchB#config
SwitchB(config)#vlan 20
SwitchB(config)#vlan 100
SwitchB(config)#vlan 101
SwitchB(config)#interface ethernet 1/0/20
SwitchB(config-If-Ethernet)#switchport access vlan 101
SwitchB(config-If-Ethernet)exit
SwitchB(config)#interface ethernet 1/0/15
SwitchB(config-If-Ethernet)#switchport access vlan 100
SwitchB(config-If-Ethernet)exit
SwitchB(config)#interface ethernet 1/0/10
SwitchB(Config-If-Ethernet1/0/10)#switchport mode trunk
SwitchB(Config-If-Ethernet1/0/10)#exit
SwitchB(config)#vlan 20
SwitchB(config-vlan20)#multicast-vlan
SwitchB(config-vlan20)#multicast-vlan association 100,101
SwitchB(config-vlan20)#exit
SwitchB(config)#ip igmp snooping
SwitchB(config)#ip igmp snooping vlan 20
```

Part IX

Security Function Configuration

Chapter 35

ACL Configuration

35.1 Introduction to ACL

ACL (Access Control List) is an IP packet filtering mechanism employed in switches, providing network traffic control by granting or denying access the switches, effectively safeguarding the security of networks. The user can lay down a set of rules according to some information specific to packets, each rule describes the action for a packet with certain information matched: 'permit' or 'deny'. The user can apply such rules to the incoming direction of switch ports, so that data streams in the incoming direction of specified ports must comply with the ACL rules assigned.

35.1.1 Access-list

Access-list is a sequential collection of conditions that corresponds to a specific rule. Each rule consist of filter information and the action when the rule is matched. Information included in a rule is the effective combination of conditions such as source IP, destination IP, IP protocol number and TCP port, UDP port. Access-lists can be categorized by the following criteria:

- **Filter information based criterion:** IP access-list (layer 3 or higher information), MAC access-list (layer 2 information), and MAC-IP access-list (layer 2 or layer 3 or higher).
- **Configuration complexity based criterion:** standard and extended, the extended mode allows more specific filtering of information.
- **Nomenclature based criterion:** numbered and named.

Description of an ACL should cover the above three aspects.

35.1.2 Access-group

When a set of access-lists are created, they can be applied to traffic of incoming direction on all ports. Access-group is the description to the binding of an access-list to the incoming direction on a specific port. When an access-group is created, all packets from in the incoming direction through the port will be compared to the access-list rule to decide whether to permit or deny access.

The current firmware only supports ingress ACL configuration.

35.1.3 Access-list Action and Global Default Action

There are two access-list actions and default actions: 'permit' or 'deny'. The following rules apply:

- An access-list can consist of several rules. Filtering of packets compares packet conditions to the rules, from the first rule to the first matched rule; the rest of the rules will not be processed. Global default action applies only to IP packets in the incoming direction on the ports.
- Global default action applies only when packet flirter is enabled on a port and no ACL is bound to that port, or no binding ACL matches.

35.2 ACL Configuration Task List

ACL Configuration Task Sequence:

1. Configuring access-list
    (a) Configuring a numbered standard IP access-list
    (b) Configuring a numbered extended IP access-list
    (c) Configuring a standard IP access-list based on nomenclature
        i. Create a standard IP access-list based on nomenclature
        ii. Specify multiple 'permit' or 'deny' rule entries
        iii. Exit ACL Configuration Mode
    (d) Configuring an extended IP access-list based on nomenclature
        i. Create an extensive IP access-list based on nomenclature
        ii. Specify multiple 'permit' or 'deny' rule entries
        iii. Exit ACL Configuration Mode
    (e) Configuring a numbered standard MAC access-list
    (f) Configuring a numbered extended MAC access-list
    (g) Configuring a extended MAC access-list based on nomenclature
        i. Create a extensive MAC access-list based on nomenclature
        ii. Specify multiple 'permit' or 'deny' rule entries
        iii. Exit ACL Configuration Mode
    (h) Configuring a numbered extended MAC-IP access-list
    (i) Configuring a extended MAC-IP access-list based on nomenclature
        i. Create a extensive MAC-IP access-list based on nomenclature
        ii. Specify multiple 'permit' or 'deny' rule entries
        iii. Exit MAC-IP Configuration Mode
    (j) Configuring a numbered standard IPv6 access-list
    (k) Configuring a numbered extended IPv6 access-list

(l) Configuring a standard IPv6 access-list based on nomenclature
   i. Create a standard IPv6 access-list based on nomenclature
   ii. Specify multiple permit or deny rule entries
   iii. Exit ACL Configuration Mode

(m) Configuring an extended IPv6 access-list based on nomenclature.
   i. Create an extensive IPv6 access-list based on nomenclature
   ii. Specify multiple permit or deny rule entries
   iii. Exit ACL Configuration Mode

2. Configuring the packet filtering function
   (a) Enable global packet filtering function
   (b) Configure default action
3. Configuring time range function
   (a) Create the name of the time range
   (b) Configure periodic time range
   (c) Configure absolute time range
4. Bind access-list to an incoming direction of the specified port
5. Clear the filtering information of the specified port

1. Configuring access-list
(a) Configuring a numbered standard IP access-list

Command	Explanation
Global Mode	
access-list <num> { deny | permit } { { <sIpAddr> <sMask> } | any-source | { host-source <sIpAddr> } } no access-list <num>	Creates a numbered standard IP access-list, if the access-list already exists, then a rule will add to the current access-list; the 'no access-list <num>' command deletes a numbered standard IP access-list.

(b) Configuring a numbered extensive IP access-list

Command	Explanation
Global Mode	
access-list <num> { deny | permit } icmp { { <sIpAddr> <sMask> } | any-source | { host-source <sIpAddr> } } { { <dIpAddr> <dMask> } | any-destination | { host-destination <dIpAddr> } } [<icmp-type> [<icmp-code>]] [precedence <prec>] [tos <tos>][time-range<time-range-name>]	Creates a numbered ICMP extended IP access rule; if the numbered extended access-list of specified number does not exist, then an access-list will be created using this number.

access-list <num> { deny | permit } igmp { { <sIpAddr> <sMask> } | any-source | { host-source <sIpAddr> } } { { <dIpAddr> <dMask> } | any-destination | { host-destination <dIpAddr> } } [<igmp-type>] [precedence <prec>] [tos <tos>][time-range<time-range-name>]	Creates a numbered IGMP extended IP access rule; if the numbered extended access-list of specified number does not exist, then an access-list will be created using this number.
access-list <num> { deny | permit } tcp { { <sIpAddr> <sMask> } | any-source | { host-source <sIpAddr> } } [s-port { <sPort> | range <sPortMin> <sPortMax> }] { { <dIpAddr> <dMask> } | any-destination | { host-destination <dIpAddr> } } [d-port { <dPort> | range <dPortMin> <dPortMax> }] [ack+fin+psh+rst+urg+syn] [precedence <prec>] [tos <tos>][time-range<time-range-name>]	Creates a numbered TCP extended IP access rule; if the numbered extended access-list of specified number does not exist, then an access-list will be created using this number.
access-list <num> { deny | permit } udp { { <sIpAddr> <sMask> } | any-source | { host-source <sIpAddr> } } [s-port { <sPort> | range <sPortMin> <sPortMax> }] { { <dIpAddr> <dMask> } | any-destination | { host-destination <dIpAddr> } } [d-port { <dPort> | range <dPortMin> <dPortMax> }] [precedence <prec>] [tos <tos>][time-range<time-range-name>]	Creates a numbered UDP extended IP access rule; if the numbered extended access-list of specified number does not exist, then an access-list will be created using this number.
access-list <num> { deny | permit } { eigrp | gre | igrp | ipinip | ip | ospf | <protocol-num> } { { <sIpAddr> <sMask> } | any-source | { host-source <sIpAddr> } } { { <dIpAddr> <dMask> } | any-destination | { host-destination <dIpAddr> } } [precedence <prec>] [tos <tos>][time-range<time-range-name>]	Creates a numbered IP extended IP access rule for other specific IP protocol or all IP protocols; if the numbered extended access-list of specified number does not exist, then an access-list will be created using this number.
no access-list <num>	Deletes a numbered extensive IP access-list.

(c) Configuring a standard IP access-list basing on nomenclature

i. Create a name-based standard IP access-list

Command	Explanation
Global Mode	
ip access-list standard <name> no ip access-list standard <name>	Creates a standard IP access-list based on nomenclature; the 'no ip access-list standard <name>' command deletes the name-based standard IP access-list.

ii. Specify multiple 'permit' or 'deny' rules

Command	Explanation
Standard IP ACL Mode	
[no] { deny | permit } { { <sIpAddr> <sMask> } | any-source | { host-source <sIpAddr> } }	Creates a standard name-based IP access rule; the 'no' form command deletes the name-based standard IP access rule.

iii. Exit name-based standard IP ACL configuration mode

Command	Explanation
Standard IP ACL Mode	
exit	Exits name-based standard IP ACL configuration mode.

(d) Configuring an name-based extended IP access-list
i. Create an extended IP access-list basing on nomenclature

Command	Explanation
Global Mode	
ip access-list extended <name> no ip access-list extended <name>	Creates an extended IP access-list basing on nomenclature; the 'no ip access-list extended <name> ' command deletes the name-based extended IP access-list.

ii. Specify multiple 'permit' or 'deny' rules

Command	Explanation
Extended IP ACL Mode	
[no] { deny | permit } icmp { { <sIpAddr> <sMask> } | any-source | { host-source <sIpAddr> } } { { <dIpAddr> <dMask> } | any-destination | { host-destination <dIpAddr> } } [<icmp-type> [<icmp-code>]] [precedence <prec>] [tos <tos>][time-range<time-range-name>]	Creates an extended name-based ICMP IP access rule; the no form command deletes this name-based extended IP access rule.
1 [no] { deny | permit } igmp { { <sIpAddr> <sMask> } | any-source | { host-source <sIpAddr> } } { { <dIpAddr> <dMask> } | any-destination | { host-destination <dIpAddr> } } [<igmp-type>] [precedence <prec>] [tos <tos>][time-range<time-range-name>]	Creates an extended name-based IGMP IP access rule; the no form command deletes this name-based extended IP access rule.

[no] { deny | permit } tcp { { <sIpAddr> <sMask> } | any-source | { host-source <sIpAddr> } } [s-port { <sPort> | range <sPortMin> <sPortMax> }] { { <dIpAddr> <dMask> } | any-destination | { host-destination <dIpAddr> } } [d-port { <dPort> | range <dPortMin> <dPortMax> }] [ack+fin+psh+rst+urg+syn] [precedence <prec>] [tos <tos>][time-range<time-range-name>]	Creates an extended name-based TCP IP access rule; the no form command deletes this name-based extended IP access rule.
[no] { deny | permit } udp { { <sIpAddr> <sMask> } | any-source | { host-source <sIpAddr> } } [s-port { <sPort> | range <sPortMin> <sPortMax> }] { { <dIpAddr> <dMask> } | any-destination | { host-destination <dIpAddr> } } [d-port { <dPort> | range <dPortMin> <dPortMax> }] [precedence <prec>] [tos <tos>][time-range<time-range-name>]	Creates an extended name-based UDP IP access rule; the no form command deletes this name-based extended IP access rule.
[no] { deny | permit } { eigrp | gre | igrp | ipinip | ip | ospf | <protocol-num> } { { <sIpAddr> <sMask> } | any-source | { host-source <sIpAddr> } } { { <dIpAddr> <dMask> } | any-destination | { host-destination <dIpAddr> } } [precedence <prec>] [tos <tos>][time-range<time-range-name>]	Creates an extended name-based IP access rule for other IP protocols; the no form command deletes this name-based extended IP access rule.

iii. Exit extended IP ACL configuration mode

Command	Explanation
Extended IP ACL Mode	
exit	Exits extended name-based IP ACL configuration mode.

(e) Configuring a numbered standard MAC access-list

Command	Explanation
Global Mode	
access-list<num> { deny | permit } { any-source-mac | { host-source-mac<host_smac> } | { <smac><smac-mask> } } no access-list <num>	Creates a numbered standard MAC access-list, if the access-list already exists, then a rule will add to the current access-list; the 'no access-list <num>' command deletes a numbered standard MAC access-list.

(f) Creates a numbered MAC extended access-list

Command	Explanation
Global Mode	
access-list<num> { deny | permit } { any-source-mac | { host-source-mac<host_smac> } | { <smac><smac-mask> } } { any-destination-mac | { host-destination-mac<host_dmac> } | { <dmac><dmac-mask> } } [{ untagged-eth2 | tagged-eth2 | untagged-802-3 | tagged-802-3 } [<offset1> <length1> <value1> [<offset2> <length2> <value2> [<offset3> <length3> <value3> [<offset4> <length4> <value4>]]]]] no access-list <num>	Creates a numbered MAC extended access-list, if the access-list already exists, then a rule will add to the current access-list; the 'no access-list <num>' command deletes a numbered MAC extended access-list.

(g) Configuring a extended MAC access-list based on nomenclature

i. Create an extensive MAC access-list based on nomenclature

Command	Explanation
Global Mode	
mac-access-list extended <name> no mac-access-list extended <name>	Creates an extended name-based MAC access rule for other IP protocols; the no form command deletes this name-based extended MAC access rule.

ii. Specify multiple 'permit' or 'deny' rule entries

Command	Explanation
Extended name-based MAC access rule Mode	
[no] { deny | permit } { any-source-mac | { host-source-mac <host_smac> } | { <smac><smac-mask> } } { any-destination-mac | { host-destination-mac <host_dmac> } | { <dmac> <dmac-mask> } } [cos <cos-val> [<cos-bitmask>] [vlanId <vid-value> [<vid-mask>][ethertype<protocol>[<protocol-mask>]]]] [no] { deny | permit } { any-source-mac | { host-source-mac<host_smac> } | { <smac><smac-mask> } } { any-destination-mac | { host-destination-mac<host_dmac> } | { <dmac><dmac-mask> } } [ethertype <protocol> [<protocol-mask>]] [no] { deny | permit } { any-source-mac | { host-source-mac<host_smac> } | { <smac><smac-mask> } } { any-destination-mac | { host-destination-mac<host_dmac> } | { <dmac><dmac-mask> } } [vlanid <vid-value> [<vid-mask>][ethertype <protocol> [<protocol-mask>]]]	Creates an extended name-based MAC access rule matching MAC frame; the no form command deletes this name-based extended MAC access rule.

[no] { deny | permit } { any-source-mac | { host-source-mac<host_smac> } | { <smac><smac-mask> } } { any-destination-mac | { host-destination-mac<host_dmac> } | { <dmac><dmac-mask> } } [untagged-eth2 [ethertype <protocol> [protocol-mask]]]	Creates an extended name-based MAC access rule matching untagged ethernet 2 frame; the no form command deletes this name-based extended MAC access rule.
[no] { deny | permit } { any-source-mac | { host-source-mac<host_smac> } | { <smac><smac-mask> } } { any-destination-mac | { host-destination-mac <host_dmac> } | { <dmac><dmac-mask> } } [untagged-802-3]	Creates an name-based extended MAC access rule matching 802.3 frame; the no form command deletes this name-based extended MAC access rule.
[no] { deny | permit } { any-source-mac | { host-source-mac<host_smac> } | { <smac><smac-mask> } } { any-destination-mac | { host-destination-mac<host_dmac> } | { <dmac><dmac-mask> } } [tagged-eth2 [cos <cos-val> [<cos-bitmask>]] [vlanId <vid-value> [<vid-mask>]] [ethertype<protocol> [<protocol-mask>]]]	Creates an name-based extended MAC access rule matching tagged ethernet 2 frame; the no form command deletes this name-based extended MAC access rule.
[no] { deny | permit } { any-source-mac | { host-source-mac <host_smac> } | { <smac><smac-mask> } } { any-destination-mac | { host-destination-mac<host_dmac> } | { <dmac><dmac-mask> } } [tagged-802-3 [cos <cos-val> [<cos-bitmask>]] [vlanId <vid-value> [<vid-mask>]]]	Creates an name-based extended MAC access rule matching tagged 802.3 frame; the no form command deletes this name-based extended MAC access rule.

iii. Exit ACL Configuration Mode

Command	Explanation
Extended name-based MAC access configure Mode	
exit	Quit the extended name-based MAC access configure mode.

(h) Configuring a numbered extended MAC-IP access-list

Command	Explanation
Global Mode	
access-list<num> { deny | permit } { any-source-mac | { host-source-mac <host_smac> } | { <smac> <smac-mask> } } { any-destination-mac | { host-destination-mac <host_dmac> } | { <dmac><dmac-mask> } } icmp { { <source> <source-wildcard> } | any-source | { host-source <source-host-ip> } } { { <destination> <destination-wildcard> } | any-destination | { host-destination <destination-host-ip> } } [<icmp-type> [<icmp-code>]] [precedence <precedence>] [tos <tos>] [time-range <time-range-name>]	Creates a numbered mac-icmp extended mac-ip access rule; if the numbered extended access-list of specified number does not exist, then an access-list will be created using this number.

access-list<num> { deny | permit } { any-source-mac | { host-source-mac<host_smac> } | { <smac><smac-mask> } } { any-destination-mac | { host-destination-mac <host_dmac> } | { <dmac><dmac-mask> } } igmp { { <source><source-wildcard> } | any-source | { host-source<source-host-ip> } } { { <destination><destination-wildcard> } | any-destination | { host-destination<destination-host-ip> } } [<igmp-type>] [precedence <precedence>] [tos <tos>][time-range<time-range-name>]	Creates a numbered mac-igmp extended mac-ip access rule; if the numbered extended access-list of specified number does not exist, then an access-list will be created using this number.
access-list<num> { deny | permit } { any-source-mac | { host-source-mac<host_smac> } | { <smac><smac-mask> } } { any-destination-mac | { host-destination-mac <host_dmac> } | { <dmac><dmac-mask> } } tcp { { <source><source-wildcard> } | any-source | { host-source<source-host-ip> } } [s-port { <port1> | range <sPortMin> <sPortMax> }] { { <destination><destination-wildcard> } | any-destination | { host-destination <destination-host-ip> } } [d-port { <port3> | range <dPortMin> <dPortMax> }] [ack+fin+psh+rst+urg+syn] [precedence <precedence>] [tos <tos>][time-range<time-range-name>]	Creates a numbered mac-ip extended mac-tcp access rule; if the numbered extended access-list of specified number does not exist, then an access-list will be created using this number.
access-list<num> { deny | permit } { any-source-mac | { host-source-mac<host_smac> } | { <smac><smac-mask> } } { any-destination-mac | { host-destination-mac <host_dmac> } | { <dmac><dmac-mask> } } udp { { <source><source-wildcard> } | any-source | { host-source<source-host-ip> } } [s-port { <port1> | range <sPortMin> <sPortMax> }] { { <destination><destination-wildcard> } | any-destination | { host-destination<destination-host-ip> } } [d-port { <port3> | range <dPortMin> <dPortMax> }] [precedence <precedence>] [tos <tos>][time-range<time-range-name>]	Creates a numbered mac-udp extended mac-ip access rule; if the numbered extended access-list of specified number does not exist, then an access-list will be created using this number.
access-list<num> { deny | permit } { any-source-mac | { host-source-mac<host_smac> } | { <smac><smac-mask> } } { any-destination-mac | { host-destination-mac <host_dmac> } | { <dmac><dmac-mask> } } { eigrp | gre | igrp | ip | ipinip | ospf | { <protocol-num> } } { { <source><source-wildcard> } | any-source | { host-source<source-host-ip> } } { { <destination><destination-wildcard> } | any-destination | { host-destination<destination-host-ip> } } [precedence <precedence>] [tos <tos>][time-range<time-range-name>]	Creates a numbered extended mac-ip access rule for other specific mac-ip protocol or all mac-ip protocols; if the numbered extended access-list of specified number does not exist, then an access-list will be created using this number.
no access-list <num>	Deletes this numbered extended MAC-IP access rule.

(i) Configuring a extended MAC-IP access-list based on nomenclature

i. Create an extensive MAC-IP access-list based on nomenclature

Command	Explanation
Global Mode	
mac-ip-access-list extended <name> no mac-ip-access-list extended <name>	Creates an extended name-based MAC-IP access rule; the no form command deletes this name-based extended MAC-IP access rule.

ii. Specify multiple 'permit' or 'deny' rule entries

Command	Explanation
Extended name-based MAC-IP access Mode	
[no] { deny | permit } { any-source-mac | { host-source-mac <host_smac> } | { <smac><smac-mask> } } { any-destination-mac | { host-destination-mac <host_dmac> } | { <dmac><dmac-mask> } } icmp { { <source><source-wildcard> } | any-source | { host-source<source-host-ip> } } { { <destination><destination-wildcard> } | any-destination | { host-destination <destination-host-ip> } } [<icmp-type> [<icmp-code>]] [precedence <precedence>][tos<tos>][time-range<time-range-name>]	Creates an extended name-based MAC-ICMP access rule; the no form command deletes this name-based extended MAC-ICMP access rule.
[no] { deny | permit } { any-source-mac | { host-source-mac <host_smac> } | { <smac><smac-mask> } } { any-destination-mac | { host-destination-mac <host_dmac> } | { <dmac><dmac-mask> } } igmp { { <source><source-wildcard> } | any-source | { host-source<source-host-ip> } } { { <destination><destination-wildcard> } | any-destination | { host-destination <destination-host-ip> } } [<igmp-type>] [precedence <precedence>] [tos <tos>][time-range<time-range-name>]	Creates an extended name-based MAC-IGMP access rule; the no form command deletes this name-based extended MAC-IGMP access rule.
[no] { deny | permit } { any-source-mac | { host-source-mac<host_smac> } | { <smac><smac-mask> } } { any-destination-mac | { host-destination-mac <host_dmac> } | { <dmac><dmac-mask> } } tcp { { <source><source-wildcard> } | any-source | { host-source<source-host-ip> } } [s-port { <port1> | range <sPortMin> <sPortMax> }] { { <destination><destination-wildcard> } | any-destination | { host-destination <destination-host-ip> } } [d-port { <port3> | range <dPortMin> <dPortMax> }] [ack+fin+psh+rst+urg+syn] [precedence<precedence>][tos<tos>][time-range<time-range-name>]	Creates an extended name-based MAC-TCP access rule; the no form command deletes this name-based extended MAC-TCP access rule.

[no] { deny | permit } { any-source-mac | { host-source-mac<host_smac> } | { <smac><smac-mask> } } { any-destination-mac | { host-destination-mac <host_dmac> } | { <dmac><dmac-mask> } } udp { { <source><source-wildcard> } | any-source | { host-source<source-host-ip> } } [s-port { <port1> | range <sPortMin> <sPortMax> }] { { <destination><destination-wildcard> } | any-destination | { host-destination <destination-host-ip> } } [d-port { <port3> | range <dPortMin> <dPortMax> }] [precedence <precedence>] [tos <tos>][time-range<time-range-name>]	Creates an extended name-based MAC-UDP access rule; the no form command deletes this name-based extended MAC-UDP access rule.
[no] { deny | permit } { any-source-mac | { host-source-mac<host_smac> } | { <smac><smac-mask> } } { any-destination-mac | { host-destination-mac <host_dmac> } | { <dmac><dmac-mask> } } { eigrp | gre | igrp | ip | ipinip | ospf | { <protocol-num> } } { { <source><source-wildcard> } | any-source | { host-source<source-host-ip> } } { { <destination><destination-wildcard> } | any-destination | { host-destination<destination-host-ip> } } [precedence<precedence>][tos<tos>][time-range<time-range-name>]	Creates an extended name-based access rule for the other IP protocol; the no form command deletes this name-based extended access rule.

iii. Exit MAC-IP Configuration Mode

Command	Explanation
Extended name-based MAC-IP access Mode	
exit	Quit extended name-based MAC-IP access mode.

(j) Configuring a numbered standard IPv6 access-list

Command	Explanation
Global Mode	
ipv6 access-list <num> { deny | permit } { { <sIPv6Addr> <sPrefixlen> } | any-source | { host-source <sIpv6Addr> } } no ipv6 access-list <num>	Creates a numbered standard IPv6 access-list, if the access-list already exists, then a rule will add to the current access-list; the 'no access-list <num>' command deletes a numbered standard IPv6 access-list.

(k) Configuring a numbered extensive IPv6 access-list

Command	Explanation
Global Mode	
ipv6 access-list <num-ext> { deny | permit } icmp { { <sIPv6Prefix/sPrefixlen> } | any-source | { host-source <sIPv6Addr> } } { <dIPv6Prefix/dPrefixlen> | any-destination | { host-destination <dIPv6Addr> } } [<icmp-type> [<icmp-code>]] [dscp <dscp>] [flow-label <fl>][time-range<time-range-name>] ipv6 access-list <num-ext> { deny | permit } tcp { { <sIPv6Prefix/<sPrefixlen> } | any-source | { host-source <sIPv6Addr> } } [s-port { <sPort> | range <sPortMin> <sPortMax> }] { { < dIPv6Prefix/<dPrefixlen> } | any-destination | { host-destination <dIPv6Addr> } } [dPort { <dPort> | range <dPortMin> <dPortMax> }] [syn | ack | urg | rst | fin | psh] [dscp <dscp>] [flow-label <flowlabel>][time-range<time-range-name>] ipv6 access-list <num-ext> { deny | permit } udp { { <sIPv6Prefix/<sPrefixlen> } | any-source | { host-source <sIPv6Addr> } } [s-port { <sPort> | range <sPortMin> <sPortMax> }] { { <dIPv6Prefix/<dPrefixlen> } | any-destination | { host-destination <dIPv6Addr> } } [dPort { <dPort> | range <dPortMin> <dPortMax> }] [dscp <dscp>] [flow-label <flowlabel>][time-range<time-range-name>] ipv6 access-list <num-ext> { deny | permit } <next-header> { <sIPv6Prefix/sPrefixlen> | any-source | { host-source <sIPv6Addr> } } { <dIPv6Prefix/dPrefixlen> | any-destination | { host-destination <dIPv6Addr> } } [dscp <dscp>] [flow-label <fl>][time-range<time-range-name>] no ipv6 access-list <num>	Creates a numbered extended IPv6 access-list, if the access-list already exists, then a rule will add to the current access-list; the no command deletes a numbered standard IPv6 access-list.

(l) Configuring a standard IPv6 access-list based on nomenclature

i. Create a standard IPv6 access-list based on nomenclature

Command	Explanation
Global Mode	
ipv6 access-list standard <name> no ipv6 access-list standard <name>	Creates a standard IP access-list based on nomenclature; the no command delete the name-based standard IPv6 access-list.

ii. Specify multiple permit or deny rules

Command	Explanation
Standard IPv6 ACL Mode	
[no] { deny | permit } { { <sIPv6Prefix/sPrefixlen> } | any-source | { host-source <sIPv6Addr> } }	Creates a standard name-based IPv6 access rule; the no form command deletes the name-based standard IPv6 access rule.

iii. Exit name-based standard IP ACL configuration mode

Command	Explanation
Standard IPv6 ACL Mode	
exit	Exits name-based standard IPv6 ACL configuration mode.

(m) Configuring an name-based extended IPv6 access-list

i. Create an extended IPv6 access-list basing on nomenclature

Command	Explanation
Global Mode	
ipv6 access-list extended <name> no ipv6 access-list extended <name>	Creates an extended IPv6 access-list basing on nomenclature; the no command deletes the name-based extended IPv6 access-list.

ii. Specify multiple permit or deny rules

Command	Explanation
Extended IPv6 ACL Mode	
[no] { deny | permit } icmp { { <sIPv6Prefix/sPrefixlen> } | any-source | { host-source <sIPv6Addr> } } { <dIPv6Prefix/dPrefixlen> | any-destination | { host-destination <dIPv6Addr> } } [<icmp-type> [<icmp-code>]] [dscp <dscp>] [flow-label <flowlabel>] [time-range <time-range-name>]	Creates an extended name-based ICMP IPv6 access rule; the no form command deletes this name-based extended IPv6 access rule.
[no] { deny | permit } tcp { <sIPv6Prefix/sPrefixlen> | any-source | { host-source <sIPv6Addr> } } [s-port { <sPort> | range <sPortMin> <sPortMax> }] { <dIPv6Prefix/dPrefixlen> | any-destination | { host-destination <dIPv6Addr> } } [d-port { <dPort> | range <dPortMin> <dPortMax> }] [syn | ack | urg | rst | fin | psh] [dscp <dscp>] [flow-label <fl>] [time-range<time-range-name>]	Creates an extended name-based TCP IPv6 access rule; the no form command deletes this name-based extended IPv6 access rule.
[no] { deny | permit } udp { <sIPv6Prefix/sPrefixlen> | any-source | { host-source <sIPv6Addr> } } [s-port { <sPort> | range <sPortMin> <sPortMax> }] { <dIPv6Prefix/dPrefixlen> | any-destination | { host-destination <dIPv6Addr> } } [d-port { <dPort> | range <dPortMin> <dPortMax> }] [dscp <dscp>] [flow-label <fl>] [time-range<time-range-name>]	Creates an extended name-based UDP IPv6 access rule; the no form command deletes this name-based extended IPv6 access rule.

[no] { deny | permit } <proto> { <sIPv6Prefix/sPrefixlen> | any-source | { host-source <sIPv6Addr> } } { <dIPv6Prefix/dPrefixlen> | any-destination | { host-destination <dIPv6Addr> } } [dscp <dscp>] [flow-label <flowlabel>] [time-range <time-range-name>]	Creates an extended name-based IPv6 access rule for other IPv6 protocols; the no form command deletes this name-based extended IPv6 access rule.
[no] { deny | permit } { <sIPv6Prefix/sPrefixlen> | any-source | { host-source <sIPv6Addr> } } { <dIPv6Prefix/dPrefixlen> | any-destination | { host-destination <dIPv6Addr> } } [dscp <dscp>] [flow-label <flowlabel>] [time-range <time-range-name>]	Creates an extended name-based IPv6 access rule; the no form command deletes this name-based extended IPv6 access rule.

iii. Exit extended IPv6 ACL configuration mode

Command	Explanation
Extended IPv6 ACL Mode	
exit	Exits extended name-based IPv6 ACL configuration mode.

2. Configuring packet filtering function

(a) Enable global packet filtering function

Command	Explanation
Global Mode	
firewall enable	Enables global packet filtering function.
firewall disable	Disables global packet filtering function.

(b) Configure default action

Command	Explanation
Global Mode	
firewall default { permit | deny [ipv4 | ipv6 | all] }	Sets default action to firewall.

3. Configuring time range function

(a) Create the name of the time range

Command	Explanation
Global Mode	
time-range <time_range_name>	Create a time range named time_range_name.
no time-range <time_range_name>	Stop the time range function named time_range_name.

(b) Configure periodic time range

Command	Explanation
Time range Mode	
absolute-periodic { Monday | Tuesday | Wednesday | Thursday | Friday | Saturday | Sunday } <start_time> to { Monday | Tuesday | Wednesday | Thursday | Friday | Saturday | Sunday } <end_time> periodic { { Monday + Tuesday + Wednesday + Thursday + Friday + Saturday + Sunday } | daily | weekdays | weekend } <start_time> to <end_time>	Configure the time range for the request of the week, and every week will run by the time range.
[no] absolute-periodic { Monday | Tuesday | Wednesday | Thursday | Friday | Saturday | Sunday } <start_time> to { Monday | Tuesday | Wednesday | Thursday | Friday | Saturday | Sunday } <end_time> [no] periodic { { Monday + Tuesday + Wednesday + Thursday + Friday + Saturday + Sunday } | daily | weekdays | weekend } <start_time> to <end_time>	Stop the function of the time range in the week.

(c) Configure absolute time range

Command	Explanation
Global Mode	
absolute start <start_time> <start_data> [end <end_time> <end_data>]	Configure absolute time range.
[no] absolute start <start_time> <start_data> [end <end_time> <end_data>]	Stop the function of the time range.

4. Bind access-list to a specific direction of the specified port.

Command	Explanation
Physical Port Mode/VLAN Interface Mode	
{ ip | ipv6 | mac | mac-ip } access-group <acl-name> { in } [traffic-statistic] no { ip | ipv6 | mac | mac-ip } access-group <acl-name> { in }	**Physical interface mode:** Applies an access-list to the specified direction on the port; the no command deletes the access-list bound to the port. **VLAN interface mode:** Applies an access-list to the specified direction on the port of VLAN; the no command deletes the access-list bound to the port of VLAN.

5. Clear the filtering information of the specified port

Command	Explanation
Admin Mode	
clear access-group statistic [ethernet <interface-name>]	Clear the filtering information of the specified port.

35.3 ACL Example

Scenario 1:

The user has the following configuration requirement: port 10 of the switch connects to 10.0.0.0/24 segment, ftp is not desired for the user.

Configuration description:

1. Create a proper ACL
2. Configuring packet filtering function
3. Bind the ACL to the port

The configuration steps are listed below:

```
Switch(config)#access-list 110 deny tcp 10.0.0.0 0.0.0.255 any-destination d-port 21
Switch(config)#firewall enable
Switch(config)#firewall default permit
Switch(config)#interface ethernet 1/0/10
Switch(Config-If-Ethernet1/0/10)#ip access-group 110 in
Switch(Config-If-Ethernet1/0/10)#exit
Switch(config)#exit
```

Configuration result:

```
Switch#show firewall
Firewall status: enable.
Firewall Default Rule: Permit.
Switch#show access-lists
access-list 110(used 1 time(s)) 1 rule(s)
access-list 110 deny tcp 10.0.0.0 0.0.0.255 any-destination d-port 21

Switch#show access-group interface ethernet 1/0/10
interface name:Ethernet1/0/10
the ingress acl use in firewall is 110, traffic-statistics Disable.
```

Scenario 2:

The configuration requirement is stated as below: The switch should drop all the 802.3 datagram with 00-12-11-23-xx-xx as the source MAC address coming from interface 10.

Configuration description:

1. Create the corresponding MAC ACL.
2. Configure datagram filtering.
3. Bind the ACL to the related interface.

The configuration steps are listed as below.

```
Switch(config)#access-list 1100 deny 00-12-11-23-00-00 00-00-00-00-ff-ff
                      any-destination-mac untagged-802-3
Switch(config)#access-list 1100 deny 00-12-11-23-00-00 00-00-00-00-ff-ff
                      any tagged-802
Switch(config)#firewall enable
Switch(config)#firewall default permit
Switch(config)#interface ethernet1/0/10
Switch(Config-If-Ethernet1/0/10)#mac access-group 1100 in
Switch(Config-If-Ethernet1/0/10)#exit
Switch(config)#exit
```

Configuration result:

```
Switch#show firewall
  Firewall Status: Enable.
  Firewall Default Rule: Permit.

Switch #show access-lists
access-list 1100(used 1 time(s))
  access-list 1100 deny 00-12-11-23-00-00 00-00-00-00-ff-ff
any-destination-mac
  untagged-802-3
    access-list 1100 deny 00-12-11-23-00-00 00-00-00-00-ff-ff
any-destination-mac
Switch #show access-group interface ethernet 1/0/10
interface name:Ethernet1/0/10
   MAC Ingress access-list used is 1100,traffic-statistics Disable.
```

Scenario 3:

The configuration requirement is stated as below: The MAC address range of the network connected to the interface 10 of the switch is 00-12-11-23-xx-xx, and IP network is 10.0.0.0/24. FTP should be disabled and ping requests from outside network should be disabled.

Configuration description:

1. Create the corresponding access list.
2. Configure datagram filtering.
3. Bind the ACL to the related interface.

The configuration steps are listed as below.

```
Switch(config)#access-list 3110 deny 00-12-11-23-00-00 00-00-00-00-ff-ff
                        any-destination-mac tcp 10.0.0.0 0.0.0.255
                        any-destination d-port 21
Switch(config)#access-list 3110 deny any-source-mac 00-12-11-23-00-00 00-00-00-00-ff-ff
                        icmp any-source 10.0.0.0 0.0.0.255

Switch(config)#firewall enable
Switch(config)#firewall default permit
Switch(config)#interface ethernet 1/0/10
Switch(Config-If-Ethernet1/0/10)#mac-ip access-group 3110 in
Switch(Config-Ethernet1/0/10)#exit
Switch(config)#exit
```

Configuration result:

```
Switch#show firewall
  Firewall Status: Enable.
  Firewall Default Rule: Permit.

Switch#show access-lists
   access-list 3110(used 1 time(s))
access-list 3110 deny 00-12-11-23-00-00 00-00-00-00-ff-ff
   any-destination-mac
tcp 10.0.0.0 0.0.0.255 any-destination d-port 21
      access-list 3110 deny any-source-mac 00-12-11-23-00-00 00-00-00-00-ff-ff
                            icmp any-source 10.0.0.0 0.0.0.255

Switch #show access-group interface ethernet 1/0/10
interface name:Ethernet1/0/10
   MAC-IP Ingress access-list used is 3110, traffic-statistics Disable.
```

Scenario 4:

The configuration requirement is stated as below: IPv6 protocol runs on the interface 600 of the switch. And the IPv6 network address is 2003:1:1:1::0/64. Users in the 2003:1:1:1:66::0/80 subnet should be disabled from accessing the outside network.

Configuration description:

1. Create the corresponding access list.
2. Configure datagram filting.
3. Bind the ACL to the related interface.

The configuration steps are listed as below.

```
Switch(config)#ipv6 access-list 600 permit 2003:1:1:1:66::0/80 any-destination
Switch(config)#ipv6 access-list 600 deny 2003:1:1:1::0/64 any-destination

Switch(config)#firewall enable
Switch(config)#firewall default permit
Switch(config)#interface ethernet 1/0/10
Switch(Config-If-Ethernet1/0/10)#ipv6 access-group 600 in
Switch(Config-If-Ethernet1/0/10)#exit
Switch(config)#exit
```

Configuration result:

```
Switch#show firewall
  Firewall Status: Enable.
  Firewall Default Rule: Permit.

Switch#show ipv6 access-lists
Ipv6 access-list 600(used 1 time(s))
  ipv6 access-list 600 deny 2003:1:1:1::0/64 any-source
  ipv6 access-list 600 permit 2003:1:1:1:66::0/80 any-source

Switch #show access-group interface ethernet 1/0/10
interface name:Ethernet1/0/10
  IPv6 Ingress access-list used is 600, traffic-statistics Disable.
```

Scenario 5:

The configuration requirement is stated as below: The interface 1, 2, 5, 7 belongs to vlan100, Hosts with 192.168.0.1 as its IP address should be disabled from accessing the listed interfaces.

Configuration description:

1. Create the corresponding access list.
2. Configure datagram filtering.
3. Bind the ACL to the related interface.

The configuration steps are listed as below.

```
Switch (config)#firewall enable
Switch (config)#vlan 100
Switch (Config-Vlan100)#switchport interface ethernet 1/0/1;2;5;7
Switch (Config-Vlan100)#exit
Switch (config)#access-list 1 deny host-source 192.168.0.1
Switch (config)#interface ethernet1/0/1;2;5;7
Switch (config-if-port-range)#ip access-group 1 in
Switch (Config-if-Vlan100)#exit
```

Configuration result:

```
Switch (config)#show access-group interface vlan 100
Interface VLAN 100:
Ethernet1/0/1:   IP Ingress access-list used is 1, traffic-statistics Disable.
Ethernet1/0/2:   IP Ingress access-list used is 1, traffic-statistics Disable.
Ethernet1/0/5:   IP Ingress access-list used is 1, traffic-statistics Disable.
Ethernet1/0/7:   IP Ingress access-list used is 1, traffic-statistics Disable.
```

35.4 ACL Troubleshooting

- Checking for entries in the ACL is done in a top-down order and ends whenever an entry is matched.

- Default rule will be used only if no ACL is bound to the incoming direction of the port, or no ACL entry is matched.Each ingress port can bind one MAC-IP ACL, one IP ACL, one MAC ACL, one IPv6 standard ACL (via the physical interface mode or Vlan interface mode).
- When binding four ACL and packet matching several ACL at the same time, the priority relations are as follows in a top-down order. If the priority is same, then the priority of configuration at first is higher.
  - Ingress IPv6 ACL
  - Ingress MAC-IP ACL
  - Ingress IP ACL
  - Ingress MAC ACL
- The number of ACLs that can be successfully bound depends on the content of the ACL bound and the hardware resource limit. Users will be prompted if an ACL cannot be bound due to hardware resource limitation.
- If an access-list contains same filtering information but conflicting action rules, binding to the port will fail with an error message. For instance, configuring 'permit tcp any any-destination' and 'deny tcp any any-destination' at the same time is not permitted.
- Viruses such as 'worm.blaster' can be blocked by configuring ACL to block specific ICMP packets or specific TCP or UDP port packet.
- If the physical mode of an interface is TRUNK, ACL can only be configured through physical interface mode.
- ACL configured in the physical mode can only be disabled in the physical mode. Those configured in the VLAN interface configuration mode can only be disabled in the VLAN interface mode.
- When a physical interface is added into or removed from a VLAN (with the trunk interfaces as exceptions), ACL configured in the corresponding VLAN will be bound or unbound respectively. If ACL configured in the target VLAN, which is configured in VLAN interface mode, conflicts with existing ACL configuration on the interface, which is configured in physical interface mode, the configuration will fail to effect.
- When no physical interfaces are configured in the VLAN, the ACL configuration of the VLAN will be removed. And it can not recover if new interfaces are added to the VLAN.
- When the interface mode is changed from access mode to trunk mode, the ACL configured in VLAN interface mode which is bound to physical interface will be removed. And when the interface mode is changed from trunk mode to access mode, ACL configured in VLAN1 interface mode will be bound to the physical interface. If binding fails, the changing will fail either.
- When removing a VLAN configuration, if there are any ACLs bound to the VLAN, the ACL will be removed from all the physical interfaces belonging to the VLAN, and it will be bound to VLAN 1 ACL(if ACL is configured in VLAN1). If VLAN 1 ACL binding fails, the VLAN removal operation will fail.

Chapter 36

Self-defined ACL Configuration

36.1 Introduction to Self-defined ACL

ACL (Access Control Lists) is a packet filtering mechanism implemented by switch, providing network access control by granting or denying access the switches, effectively safeguarding the security of networks. The user can set a set of rules according to some information specific to packets, each rule describes the action for a packet with certain information matched: “permit” or “deny”. The user can apply such rules to the incoming direction of switch ports, so that data streams of specified ports must comply with the ACL rules assigned..

Self-defined ACL means that users can configure several self-defined windows as the matching field when users configure ACL. Self-defined windows do not specify which field definitely, but specify the offset in a packet and ignore the meaning of field. It matches the data at offset position which begins to fix the byte length according to the value and mask configuration.

36.1.1 Standard Self-defined ACL Template

Standard self-defined ACL can configure 11 windows and each of them can specify a start offset position: L2 end of tag / start of L3 header / start of L4 header. Each window can specify offset, its value from 0 to 31, unit is 2Bytes, namely, 0 means 0Bytes offset and 1 means 2Bytes offset. Besides, offset is according to the start offset position.

A standard self-defined ACL template should be configured for the offset configuration of every window before configuring the standard self-defined ACL list. This template is global and takes effect to all standard self-defined ACL list. Standard self-defined ACL template can configure the start offset position and offset for 11 windows at most. The window which is not configured is not available, that means it cannot transmit configuration successfully if the standard self-defined ACL use this window. When a window in the template is configured, it cannot be modified if the standard self-defined ACL rule is configured with this window. But the standard self-defined ACL rule is not configured, the window can be reconfigured, modified or deleted.

36.1.2 Extended Self-defined ACL Template

Extended self-defined ACL template can configure 2 swindows and 8 lwindows. Every swindow can specify a start offset position: Start of L2 header / L2 end of tag / start of L3 header / start of L4 header; every lwindow can specify a start offset position: L2 end of tag / start of L3 header /

start of L4 header. Every swindow can specify the offset□from 0 to 31,unit is 2Bytes, namely, 0 means 0Bytes offset and 1 means 2Bytes offset; Every lwindow can specify the offset: from 0 to 15, unit is 4Bytes, namely, 0 means 0Bytes offset and 1 means 4Bytes offset. Offset is according to the start offset position.

Extended self-defined ACL template should be configured for the offset configuration of every swindow and lwindow before configuring the extended self-defined ACL list. This template is global and takes effect to all extended self-defined ACL list. Extended self-defined ACL template can configure the start offset position and offset for 2 swindows and 8 lwindows at most. Swindow and lwindow which are not configured are not available, that means it cannot configured successfully if the extended self-defined ACL use this swindow or lwindow. When a swindow or lwindow in the template is configured, it cannot be modified if the extended self-defined ACL rule is configured with this swindow or lwindow. But the extended self-defined ACL rule is not configured, the swindow or lwindow can be reconfigured, modified or deleted.

36.1.3 Standard Self-defined ACL

Standard self-defined ACL can configure multi-ACL lists and each of them can configure multi-rules. One rule can configure value and mask for 11 windows at most. The length of every window is 2Bytes; the name range of standard self-defined ACL list is <1200-1299>.

36.1.4 Extended Self-defined ACL

Extended self-defined ACL can configure multi-ACL lists and each of them can configure multi-rules. One rule can configure value and mask for 2 swindows and 8 lwindows at most. The length of every swindow is 2Bytes; the length of every lwindow is 4Bytes. The name range of extended self-defined ACL list is <1300-1399>.

36.1.5 Self-defined ACL Configuration Transmitting

Standard self-defined ACL and extended self-defined ACL both can be configured to in direction of vlan and port. If there is a rule which matches vlan id in self-defined ACL and this ACL is configured to a vlan, the matching condition for the message is subject to vlan configuration.

36.1.6 Special Explanation

Because of the limit of the chip, standard self-defined ACL function cannot be configured with am, ARP Scanning Prevention or dot1x at the same time. Besides, extended self-defined ACL function cannot be configured with ipv6 ACL, savi, ip/ipv6 dcscm, ipv6 flow redirect or qos(match ipv6 acl) at the same time.

36.2 Self-defined ACL Configuration

Task list of self-defined ACL configuration:

1. Configure user-defined ACL template

   (a) Configure standard user-defined ACL template
   (b) Configure extended user-defined ACL template

2. Configure user-defined ACL
   (a) Configure standard user-defined ACL
   (b) Configure extended user-defined ACL

3. Bind user-defined ACL to specified port

4. Bind user-defined ACL to specified VLAN

1. Configure user-defined ACL template
(a) Configure standard user-defined ACL template

Command	Explanation
Global Mode	
userdefined-access-list standard offset [window1 {l2endoftag | l3start | l4start} <offset>] [window2 {l2endoftag | l3start | l4start} <offset>] [window3 {l2endoftag | l3start | l4start} <offset>] [window4 {l2endoftag | l3start | l4start} <offset>] [window5 {l2endoftag | l3start | l4start} <offset>] [window6 {l2endoftag | l3start | l4start} <offset>] [window7 {l2endoftag | l3start | l4start} <offset>] [window8 {l2endoftag | l3start | l4start} <offset>] [window9 {l2endoftag | l3start | l4start} <offset>] [window10 {l2endoftag | l3start | l4start} <offset>] [window11 {l2endoftag | l3start | l4start} <offset>] no userdefined-access-list standard offset [window1] [window2] [window3] [window4] [window5] [window6] [window7] [window8] [window9] [window10] [window11]	Create a standard self-defined ACL template. If the template exists, the corresponding window of the template can be modified; the no command deletes the window of the standard self-defined ACL template. If the window is not specified, the standard self-defined ACL template will be deleted.

(b) Configure extended user-defined ACL template

Command	Explanation
Global Mode	
userdefined-access-list extended offset [swindow1 {l2start | l2endoftag | l3start | l4start} <sOffset>] [swindow2 {l2start | l2endoftag | l3start | l4start} <sOffset>] [lwindow1 {l2endoftag | l3start | l4start} <lOffset>] [lwindow2 {l2endoftag | l3start | l4start} <lOffset>] [lwindow3 {l2endoftag | l3start | l4start} <lOffset>] [lwindow4 {l2endoftag | l3start | l4start} <lOffset>] [lwindow5 {l2endoftag | l3start | l4start} <lOffset>] [lwindow6 {l2endoftag | l3start | l4start} <lOffset>] [lwindow7 {l2endoftag | l3start | l4start} <lOffset>] [lwindow8 {l2endoftag | l3start | l4start} <lOffset>] no userdefined-access-list extended offset [swindow1] [swindow2] [lwindow1] [lwindow2] [lwindow3] [lwindow4] [lwindow5] [lwindow6] [lwindow7] [lwindow8]	Create a extended self-defined ACL template. If the template exists, the corresponding swindow or lwindow of the template can be modified; the no command deletes the swindow or lwindow of the extended self-defined ACL template. If the swindow or lwindow is not specified, the extended self-defined ACL template will be deleted.

2. Configure user-defined ACL

(a) Configure standard user-defined ACL

Command	Explanation
Global Mode	
userdefined-access-list standard <num> {deny | permit} {any-source-mac | { host-source-mac <host_smac>} | {<smac> <smac-mask>}} {any-destination-mac | {host-destination-mac <host_dmac>} | {<dmac> <dmac-mask>}} {untagged-eth2 | tagged-eth2 [cos <value> [<mask>]] [vlanId <value> [<mask>]] | untagged-802-3 | tagged-802-3 [cos <value> [<mask>]] [vlanId <value> [<mask>]]} [window1 <value> <mask>] [window2 <value> <mask>] [window3 <value> <mask>] [window4 <value> <mask>] [window5 <value> <mask>] [window6 <value> <mask>] [window7 <value> <mask>] [window8 <value> <mask>] [window9 <value> <mask>] [window10 <value> <mask>] [window11 <value> <mask>] no userdefined-access-list <num>	Create a numbered standard self-defined ACL. If the standard self-defined ACL exists, then a rule will be added to the ACL. The no command deletes a numbered standard self-defined ACL.

(b) Configure extended user-defined ACL

Command	Explanation
Global Mode	
userdefined-access-list extended <num> {deny | permit} {untagged-eth2 | tagged-eth2 [cos <value> [<mask>]] [vlanId <value> [<mask>]] | untagged-802-3 | tagged-802-3 [cos <value> [<mask>]] [vlanId <value> [<mask>]]} [swindow1 <value> <mask>] [swindow2 <value> <mask>] [lwindow1 <value> <mask>] [lwindow2 <value> <mask>] [lwindow3 <value> <mask>] [lwindow4 <value> <mask>] [lwindow5 <value> <mask>] [lwindow6 <value> <mask>] [lwindow7 <value> <mask>] [lwindow8 <value> <mask>] no userdefined-access-list <num>	Create a numbered extended self-defined ACL. If the extended self-defined ACL exists, then a rule will be added to the ACL. The no command deletes a numbered extended self-defined ACL.

3. Bind user-defined ACL to specified port

Command	Explanation
Physical Port Mode	
[no] userdefined access-group <name> {in} [traffic-statistic]	Apply userdefined-access-list to one direction of the port. Decide whether the statistical counter should be added to the ACL according to the options. The no command deletes the configuration bound to the port.

4. Bind user-defined ACL to specified VLAN

Command	Explanation
Global Mode	
[no] vacl userdefined access-group <name> {in} vlan <vlanId> [traffic-statistic]	Apply userdefined-access-list to one direction of the specified VLAN, decide whether the statistical counter should be added to the ACL according to the options. The no command deletes the configuration bound to the specified VLAN.

36.3 Self-defined ACL Example

Scenario 1:

The user has the following configuration requirement: port 10 of the switch connects to 10.0.0.0/24 segment; ftp is not desired for the user.

Configuration description:

1. Create a self-defined ACL template according to condition
2. Create a corresponding self-defined ACL
3. Bind the self-defined ACL to the port

The configuration steps are listed below:

```
Switch(config)#userdefined-access-list extended offset swindow1
                l3start 4 swindow2 l4start 1 lwindow1 l3start 3
Switch(config)#userdefined-access-list extended 1300 deny untagged-eth2
                swindow1 0006 00FF swindow2 0015 FFFF lwindow1 0A000000 FFFFFF00
Switch(config)#firewall enable
Switch(config)#interface ethernet1/10
Switch(config-if-ethernet1/10)#userdefined access-group 1300 in
Switch(config-if-ethernet1/10)#exit
Switch(config)#exit
Configuration result:
Switch#show access-lists
userdefined-access-list extended 1300(used 1 time(s)) 1 rule(s)
rule ID 1: deny untagged-eth2 swindow1 6 ff swindow2 15 ffff lwindow1 a000000 ffffff00
Switch#show access-group interface ethernet 1/10
interface name:Ethernet1/10
   Userdefined Ingress access-list used is 1300,traffic-statistics Disable.
```

Scenario 2:

The configuration requirement is stated as below: The switch should drop all the 802.3 datagram with 00-12-11-23-xx-xx as the source MAC address and 10.1.1.0/24 segment as the source IP coming from VLAN 10.

Configuration description:

1. Create a self-defined ACL template according to condition
2. Create a corresponding self-defined ACL
3. Bind the self-defined ACL to the port

The configuration steps are listed below:

```
Switch(config)#userdefined-access-list standard offset window1 l3start 6
                        window2 l3start 7
Switch(config)#userdefined-access-list standard 1200 deny 00-12-11-23-00-00
                        00-00-00-00-ff-ff any-destination-mac untagged-802-3
                        window1 0A01 FFFF window2 0100 FF00
Switch(config)#userdefined-access-list standard 1200 deny 00-12-11-23-00-00
                        00-00-00-00-ff-ff any-destination-mac tagged-802-3
                        window1 0A01 FFFF window2 0100 FF00
Switch(config)#firewall enable
Switch(config)#vacl userdefined access-group 1200 in vlan 10
Switch(config)#exit
Configuration result:
Switch #show access-lists
userdefined-access-list standard 1200(used 1 time(s)) 2 rule(s)
   rule ID 1: deny 00-12-11-23-00-00 00-00-00-00-ff-ff any-destination-mac
            untagged-802-3 window1 a01 ffff window2 100 ff00
   rule ID 2: deny 00-12-11-23-00-00 00-00-00-00-ff-ff any-destination-mac
            tagged-802-3 window1 a01 ffff window2 100 ff00
Switch #show vacl vlan 10
VLAN 10:
Userdefined Ingress access-list used is 1200, traffic-statistics Disable.
```

Chapter 37

802.1x Configuration

37.1 Introduction to 802.1x

The 802.1x protocol originates from 802.11 protocol, the wireless LAN protocol of IEEE, which is designed to provide a solution to doing authentication when users access a wireless LAN. The LAN defined in IEEE 802 LAN protocol does not provide access authentication, which means as long as the users can access a LAN controlling device (such as a LAN Switch), they will be able to get all the devices or resources in the LAN. There was no looming danger in the environment of LAN in those primary enterprise networks.

However, along with the boom of applications like mobile office and service operating networks, the service providers should control and configure the access from user. The prevailing application of WLAN and LAN access in telecommunication networks, in particular, make it necessary to control ports in order to implement the user-level access control. And as a result, IEEE LAN/WAN committee defined a standard, which is 802.1x, to do Port-Based Network Access Control. This standard has been widely used in wireless LAN and ethernet.

'Port-Based Network Access Control' means to authenticate and control the user devices on the level of ports of LAN access devices. Only when the user devices connected to the ports pass the authentication, can they access the resources in the LAN, otherwise, the resources in the LAN won't be available.

37.1.1 The Authentication Structure of 802.1x

The system using 802.1x has a typical Client/Server structure, which contains three entities (as illustrated in the next figure): Supplicant system, Authenticator system, and Authentication server system.

- The supplicant system is an entity on one end of the LAN segment, should be authenticated by the access controlling unit on the other end of the link. A Supplicant system usually is a user terminal device. Users start 802.1x authentication by starting supplicant system software. A supplicant system should support EAPOL (Extensible Authentication Protocol over LAN).

- The authenticator system is another entity on one end of the LAN segment to authenticate the supplicant systems connected. An authenticator system usually is a network device supporting 802,1x protocol, providing ports to access the LAN for supplicant systems. The ports provided can either be physical or logical.

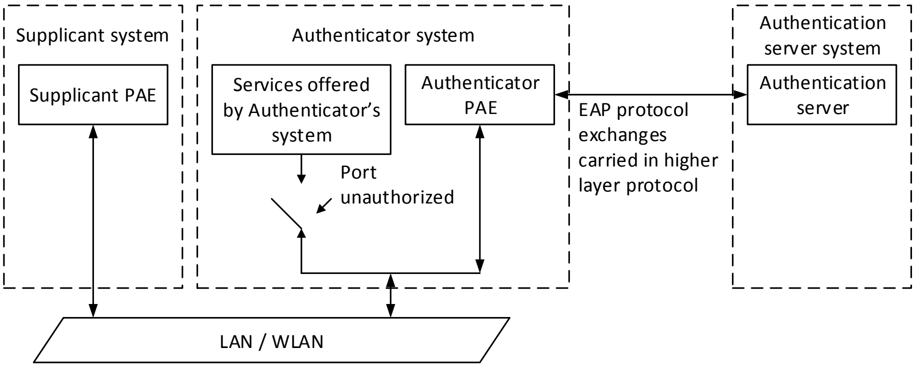

Supplicant system
Supplicant PAE
Authenticator system
Services offered by Authenticator's system
Authenticator PAE
Port unauthorized
EAP protocol exchanges carried in higher layer protocol
Authentication server system
Authentication server
LAN / WLAN

Figure 37.1: The Authentication Structure of 802.1x

- The authentication server system is an entity to provide authentication service for authenticator systems. The authentication server system is used to authenticate and authorize users, as well as does fee-counting, and usually is a RADIUS (Remote Authentication Dial-In User Service) server, which can store the relative user information, including username, password and other parameters such as the VLAN and ports which the user belongs to.

The three entities above concerns the following basic concepts: PAE of the port, the controlled ports and the controlled direction.

1. PAE

PAE (Port Access Entity) is the entity to implement the operation of algorithms and protocols.

- The PAE of the supplicant system is supposed to respond the authentication request from the authenticator systems and submit user's authentication information to the authenticator system. It can also send authentication request and off-line request to authenticator.

- The PAE of the authenticator system authenticates the supplicant systems needing to access the LAN via the authentication server system, and deal with the authenticated/unauthenticated state of the controlled port according to the result of the authentication. The authenticated state means the user is allowed to access the network resources, the unauthenticated state means only the EAPOL messages are allowed to be received and sent while the user is forbidden to access network resources.

2. Controlled/uncontrolled ports

The authenticator system provides ports to access the LAN for the supplicant systems. These ports can be divided into two kinds of logical ports: controlled ports and uncontrolled ports.

- The uncontrolled port is always in bi-directionally connected status, and mainly used to transmit EAPOL protocol frames, to guarantee that the supplicant systems can always send or receive authentication messages.

- The controlled port is in connected status authenticated to transmit service messages. When unauthenticated, no message from supplicant systems is allowed to be received.

- The controlled and uncontrolled ports are two parts of one port, which means each frame reaching this port is visible on both the controlled and uncontrolled ports.

3. Controlled direction

In unauthenticated status, controlled ports can be set as unidirectional controlled or bi-directionally controlled.

- When the port is bi-directionally controlled, the sending and receiving of all frames is forbidden.
- When the port is unidirectional controlled, no frames can be received from the supplicant systems while sending frames to the supplicant systems is allowed.

Notes: At present, this kind of switch only supports unidirectional control.

37.1.2 The Work Mechanism of 802.1x

IEEE 802.1x authentication system uses EAP (Extensible Authentication Protocol) to implement exchange of authentication information between the supplicant system, authenticator system and authentication server system.

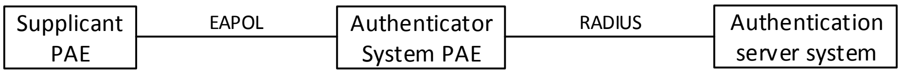


Figure 37.2: the Work Mechanism of 802.1x

- EAP messages adopt EAPOL encapsulation format between the PAE of the supplicant system and the PAE of the authenticator system in the environment of LAN.
- Between the PAE of the authenticator system and the RADIUS server, there are two methods to exchange information: one method is that EAP messages adopt EAPOR (EAP over RADIUS) encapsulation format in RADIUS protocol; the other is that EAP messages terminate with the PAE of the authenticator system, and adopt the messages containing RAP (Password Authentication Protocol) or CHAP (Challenge Handshake Authentication Protocol) attributes to do the authentication interaction with the RADIUS server.
- When the user pass the authentication, the authentication server system will send the relative information of the user to authenticator system, the PAE of the authenticator system will decide the authenticated/unauthenticated status of the controlled port according to the authentication result of the RADIUS server.

37.1.3 The Encapsulation of EAPOL Messages

1. The Format of EAPOL Data Packets

EAPOL is a kind of message encapsulation format defined in 802.1x protocol, and is mainly used to transmit EAP messages between the supplicant system and the authenticator system in order to allow the transmission of EAP messages through the LAN. In IEEE 802/Ethernet LAN environment, the format of EAPOL packet is illustrated in the next figure. The beginning of the EAPOL packet is the Type/Length domain in MAC frames.

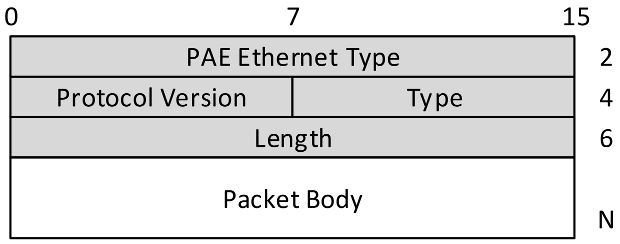


Figure 37.3: the Format of EAPOL Data Packet

PAE Ethernet Type: Represents the type of the protocol whose value is 0x888E.

Protocol Version: Represents the version of the protocol supported by the sender of EAPOL data packets.

Type: represents the type of the EAPOL data packets, including:

- EAP-Packet (whose value is 0x00): the authentication information frame, used to carry EAP messages. This kind of frame can pass through the authenticator system to transmit EAP messages between the supplicant system and the authentication server system.
- EAPOL-Start (whose value is 0x01): the frame to start authentication.
- EAPOL-Logoff (whose value is 0x02): the frame requesting to quit.
- EAPOL-Key (whose value is 0x03): the key information frame.
- EAPOL-Encapsulated-ASF-Alert (whose value is 0x04): used to support the Alerting messages of ASF (Alert Standard Forum). This kind of frame is used to encapsulate the relative information of network management such as all kinds of alerting information, terminated by terminal devices.

Length: represents the length of the data, that is, the length of the 'Packet Body', in byte. There will be no following data domain when its value is 0.

Packet Body: represents the content of the data, which will be in different formats according to different types.

2. The Format of EAP Data Packets

When the value of Type domain in EAPOL packet is EAP-Packet, the Packet Body is in EAP format (illustrated in the next figure).

Code: specifies the type of the EAP packet. There are four of them in total: Request (1), Response (2), Success (3), Failure (4).

- There is no Data domain in the packets of which the type is Success or Failure, and the value of the Length domains in such packets is 4.
- The format of Data domains in the packets of which the type is Request and Response is illustrated in the next figure. Type is the authentication type of EAP, the content of Type data depends on the type. For example, when the value of the type is 1, it means Identity, and is used to query the identity of the other side. When the type is 4, it means MD5-Challenge, like PPP CHAP protocol, contains query messages.

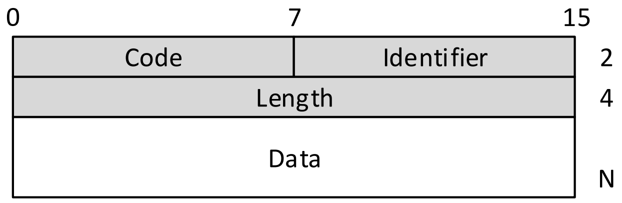


Figure 37.4: the Format of EAP Data Packets

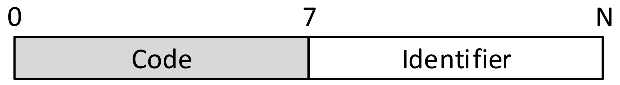


Figure 37.5: the Format of Data Domain in Request and Response Packets

Identifier: to assist matching the Request and Response messages.

Length: the length of the EAP packet, covering the domains of Code, Identifier, Length and Data, in byte.

Data: the content of the EAP packet, depending on the Code type.

37.1.4 The Encapsulation of EAP Attributes

RADIUS adds two attribute to support EAP authentication: EAP-Message and Message-Authenticator. Please refer to the Introduction of RADIUS protocol in 'AAA-RADIUS-HWTACACS operation' to check the format of RADIUS messages.

1. EAP-Message

As illustrated in the next figure, this attribute is used to encapsulate EAP packet, the type code is 79, String domain should be no longer than 253 bytes. If the data length in an EAP packet is larger than 253 bytes, the packet can be divided into fragments, which then will be encapsulated in several EAP-Messages attributes in their original order.

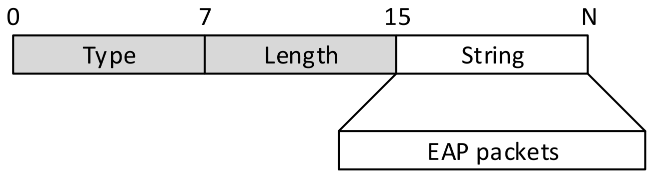


Figure 37.6: the Encapsulation of EAP-Message Attribute

2. Message-Authenticator

As illustrated in the next figure, this attribute is used in the process of using authentication methods like EAP and CHAP to prevent the access request packets from being eavesdropped.

Message-Authenticator should be included in the packets containing the EAP-Message attribute, or the packet will be dropped as an invalid one.

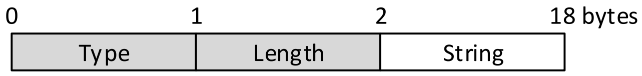


Figure 37.7: Message-Authenticator Attribute

37.1.5 The Authentication Methods of 802.1x

The authentication can either be started by supplicant system initiatively or by devices. When the device detects unauthenticated users to access the network, it will send supplicant system EAP-Request/Identity messages to start authentication. On the other hand, the supplicant system can send EAPOL-Start message to the device via supplicant software.

802.1x systems supports EAP relay method and EAP termination method to implement authentication with the remote RADIUS server. The following is the description of the process of these two authentication methods, both started by the supplicant system.

EAP Relay Mode

EAP relay is specified in IEEE 802.1x standard to carry EAP in other high-level protocols, such as EAP over RADIUS, making sure that extended authentication protocol messages can reach the authentication server through complicated networks. In general, EAP relay requires the RADIUS server to support EAP attributes: EAP-Message and Message-Authenticator.

EAP is a widely-used authentication frame to transmit the actual authentication protocol rather than a special authentication mechanism. EAP provides some common function and allows the authentication mechanisms expected in the negotiation, which are called EAP Method. The advantage of EAP lies in that EAP mechanism working as a base needs no adjustment when a new authentication protocol appears. The following figure illustrates the protocol stack of EAP authentication method.

By now, there are more than 50 EAP authentication methods has been developed, the differences among which are those in the authentication mechanism and the management of keys. The 4 most common EAP authentication methods are listed as follows:

- EAP-MD5
- EAP-TLS (Transport Layer Security)
- EAP-TTLS (Tunneled Transport Layer Security)
- PEAP (Protected Extensible Authentication Protocol)

They will be described in detail in the following part.

Attention:

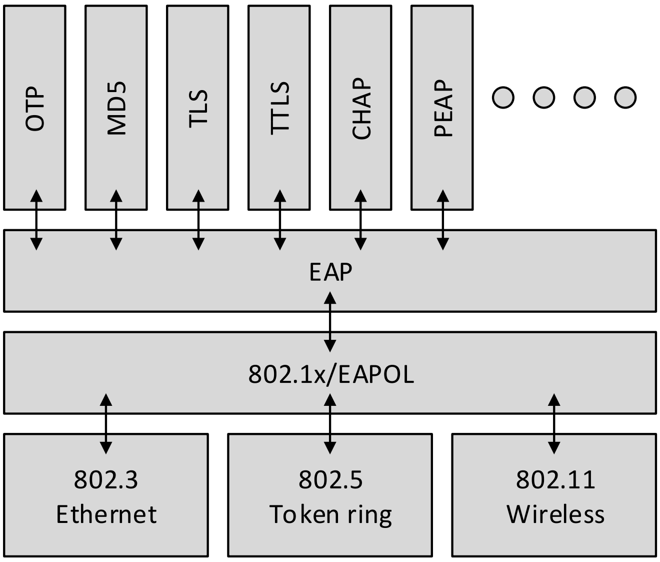


Figure 37.8: the Protocol Stack of EAP Authentication Method

- The switch, as the access controlling unit of Pass-through, will not check the content of a particular EAP method, so can support all the EAP methods above and all the EAP authentication methods that may be extended in the future.

- In EAP relay, if any authentication method in EAP-MD5, EAP-TLS, EAP-TTLS and PEAP is adopted, the authentication methods of the supplicant system and the RADIUS server should be the same.

1. EAP-MD5 Authentication Method

EAP-MD5 is an IETF open standard which providing the least security, since MD5 Hash function is vulnerable to dictionary attacks.

The following figure illustrated the basic operation flow of the EAP-MD5 authentication method.

2. EAP-TLS Authentication Method

EAP-TLS is brought up by Microsoft based on EAP and TLS protocols. It uses PKI to protect the id authentication between the supplicant system and the RADIUS server and the dynamically generated session keys, requiring both the supplicant system and the Radius authentication server to possess digital certificate to implement bidirectional authentication. It is the earliest EAP authentication method used in wireless LAN. Since every user should have a digital certificate, this method is rarely used practically considering the difficult maintenance. However it is still one of the safest EAP standards, and enjoys prevailing supports from the vendors of wireless LAN hardware and software.

The following figure illustrates the basic operation flow of the EAP-TLS authentication method.

3. EAP-TTLS Authentication Method

EAP-TTLS is a product of the cooperation of Funk Software and Certicom. It can provide an authentication as strong as that provided by EAP-TLS, but without requiring users to have their own digital certificate. The only request is that the Radius server should have a digital certificate. The authentication of users' identity is implemented with passwords transmitted in a safely

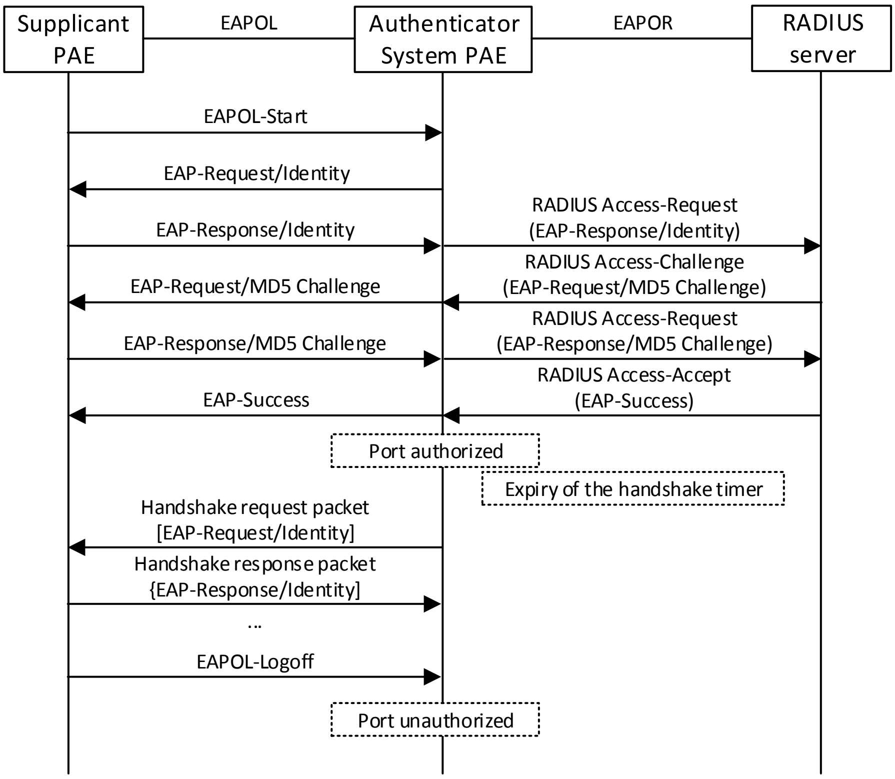

Supplicant PAE
EAPOL
Authenticator System PAE
EAPOR
RADIUS server
EAPOL-Start
EAP-Request/Identity
EAP-Response/Identity
RADIUS Access-Request (EAP-Response/Identity)
EAP-Request/MD5 Challenge
RADIUS Access-Challenge (EAP-Request/MD5 Challenge)
EAP-Response/MD5 Challenge
RADIUS Access-Request (EAP-Response/MD5 Challenge)
EAP-Success
RADIUS Access-Accept (EAP-Success)
Port authorized
Expiry of the handshake timer
Handshake request packet [EAP-Request/Identity]
Handshake response packet {EAP-Response/Identity]
...
EAPOL-Logoff
Port unauthorized

Figure 37.9: the Authentication Flow of 802.1x EAP-MD5

encrypted tunnel established via the certificate of the authentication server. Any kind of authentication request including EAP, PAP and MS-CHAPV2 can be transmitted within TTLS tunnels.

4. PEAP Authentication Method

EAP-PEAP is brought up by Cisco, Microsoft and RAS Security as a recommended open standard. It has long been utilized in products and provides very good security. Its design of protocol and security is similar to that of EAP-TTLS, using a server's PKI certificate to establish a safe TLS tunnel in order to protect user authentication.

The following figure illustrates the basic operation flow of PEAP authentication method.

EAP Termination Mode

In this mode, EAP messages will be terminated in the access control unit and mapped into RADIUS messages, which is used to implement the authentication, authorization and fee-counting. The basic operation flow is illustrated in the next figure.

In EAP termination mode, the access control unit and the RADIUS server can use PAP or CHAP authentication method. The following figure will demonstrate the basic operation flow using CHAP authentication method.

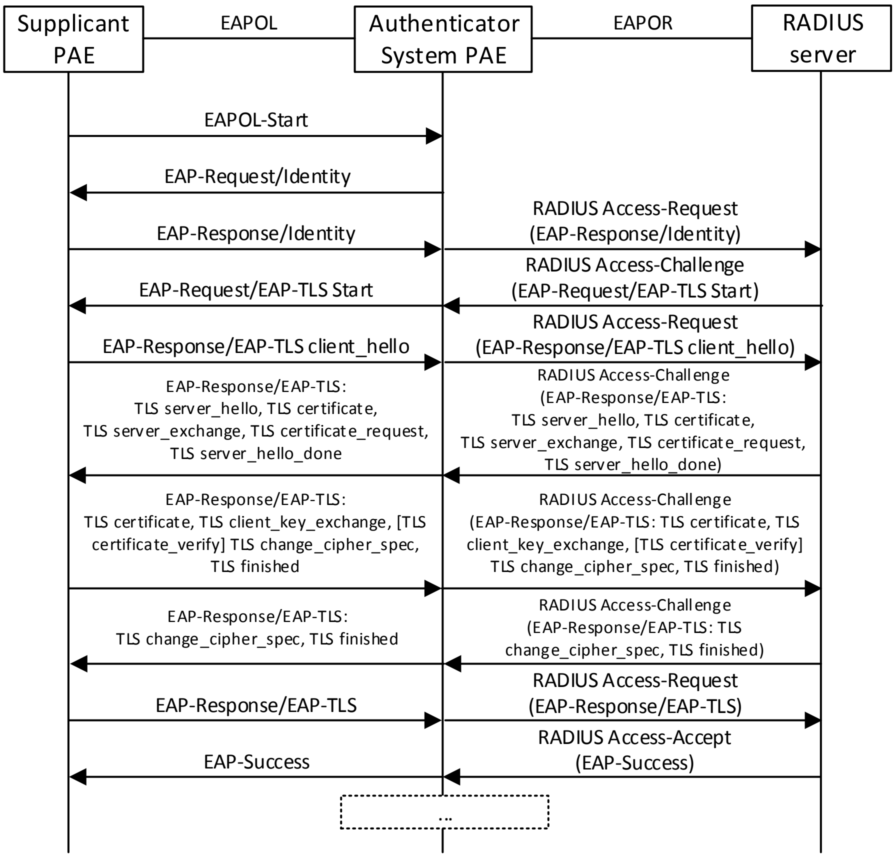

Supplicant PAE
EAPOL
Authenticator System PAE
EAPOR
RADIUS server
EAPOL-Start
EAP-Request/Identity
EAP-Response/Identity
RADIUS Access-Request (EAP-Response/Identity)
EAP-Request/EAP-TLS Start
RADIUS Access-Challenge (EAP-Request/EAP-TLS Start)
EAP-Response/EAP-TLS client_hello
RADIUS Access-Request (EAP-Response/EAP-TLS client_hello)
EAP-Response/EAP-TLS: TLS server_hello, TLS certificate, TLS server_exchange, TLS certificate_request, TLS server_hello_done
RADIUS Access-Challenge (EAP-Response/EAP-TLS: TLS server_hello, TLS certificate, TLS server_exchange, TLS certificate_request, TLS server_hello_done)
EAP-Response/EAP-TLS: TLS certificate, TLS client_key_exchange, [TLS certificate_verify] TLS change_cipher_spec, TLS finished
RADIUS Access-Challenge (EAP-Response/EAP-TLS: TLS certificate, TLS client_key_exchange, [TLS certificate_verify] TLS change_cipher_spec, TLS finished)
EAP-Response/EAP-TLS: TLS change_cipher_spec, TLS finished
RADIUS Access-Challenge (EAP-Response/EAP-TLS: TLS change_cipher_spec, TLS finished)
EAP-Response/EAP-TLS
RADIUS Access-Request (EAP-Response/EAP-TLS)
EAP-Success
RADIUS Access-Accept (EAP-Success)
...

Figure 37.10: the Authentication Flow of 802.1x EAP-TLS

37.1.6 The Extension and Optimization of 802.1x

Besides supporting the port-based access authentication method specified by the protocol, devices also extend and optimize it when implementing the EAP relay mode and EAP termination mode of 802.1x.

- Supports some applications in the case of which one physical port can have more than one users
- There are three access control methods (the methods to authenticate users): port-based, MAC-based and user-based (IP address+ MAC address+ port).
  - When the port-based method is used, as long as the first user of this port passes the authentication, all the other users can access the network resources without being authenticated. However, once the first user is offline, the network won't be available to all the other users.
  - When the MAC-based method is used, all the users accessing a port should be authenticated separately, only those pass the authentication can access the network, while the others can not. When one user becomes offline, the other users will not be affected.
  - When the user-based (IP address+ MAC address+ port) method is used, all users can access limited resources before being authenticated. There are two kinds of control in

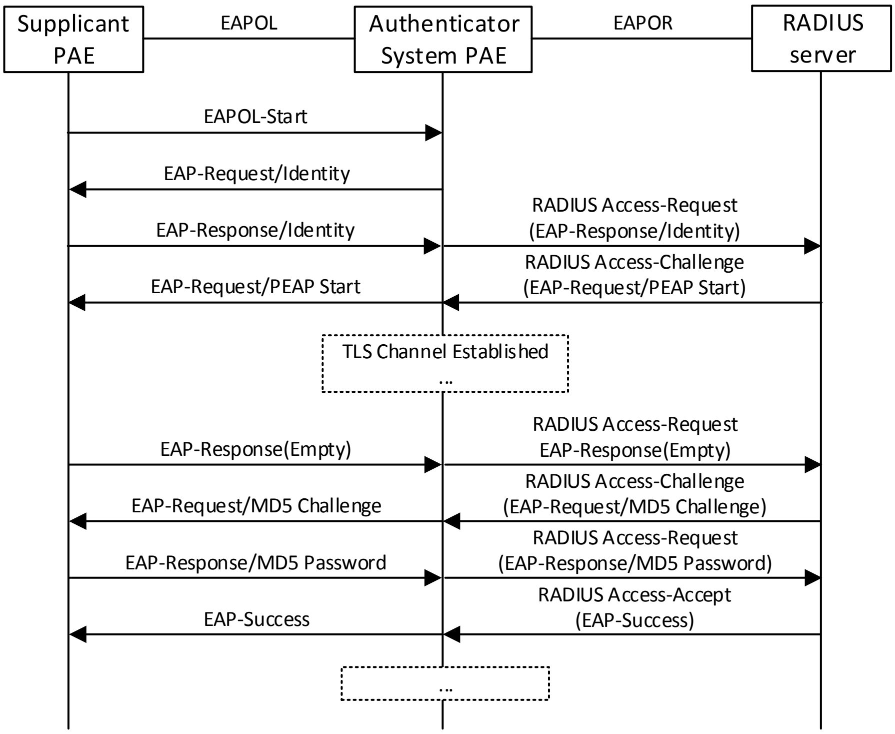

Supplicant PAE
EAPOL
Authenticator System PAE
EAPOR
RADIUS server
EAPOL-Start
EAP-Request/Identity
EAP-Response/Identity
RADIUS Access-Request (EAP-Response/Identity)
EAP-Request/PEAP Start
RADIUS Access-Challenge (EAP-Request/PEAP Start)
TLS Channel Established
...
EAP-Response(Empty)
RADIUS Access-Request EAP-Response(Empty)
EAP-Request/MD5 Challenge
RADIUS Access-Challenge (EAP-Request/MD5 Challenge)
EAP-Response/MD5 Password
RADIUS Access-Request (EAP-Response/MD5 Password)
EAP-Success
RADIUS Access-Accept (EAP-Success)
...

Figure 37.11: the Authentication Flow of 802.1x PEAP

this method: standard control and advanced control. The user-based standard control will not restrict the access to limited resources, which means all users of this port can access limited resources before being authenticated. The user-based advanced control will restrict the access to limited resources, only some particular users of the port can access limited resources before being authenticated. Once those users pass the authentication, they can access all resources.

Attention: when using private supplicant systems, user-based advanced control is recommended to effectively prevent ARP cheat.

For the maximum number of the authenticated users, the maximum number of IPv4 users supported by user-based is 400, the maximum number of IPv6 users supported by user-based is 800. mac-based relates to ratelimit value of switch, it can supports 4000 authenticated users, but it is recommended that the number of the authenticated users should not exceed 2000.

37.1.7 The Features of VLAN Allocation

1. Auto VLAN

Auto VLAN feature enables RADIUS server to change the VLAN to which the access port belongs, based on the user information and the user access device information. When an 802.1x user passes authentication on the server, the RADIUS server will send the authorization information to the device, if the RADIUS server has enabled the VLAN-assigning function, then the following attributes should be included in the Access-Accept messages:

- Tunnel-Type = VLAN (13)

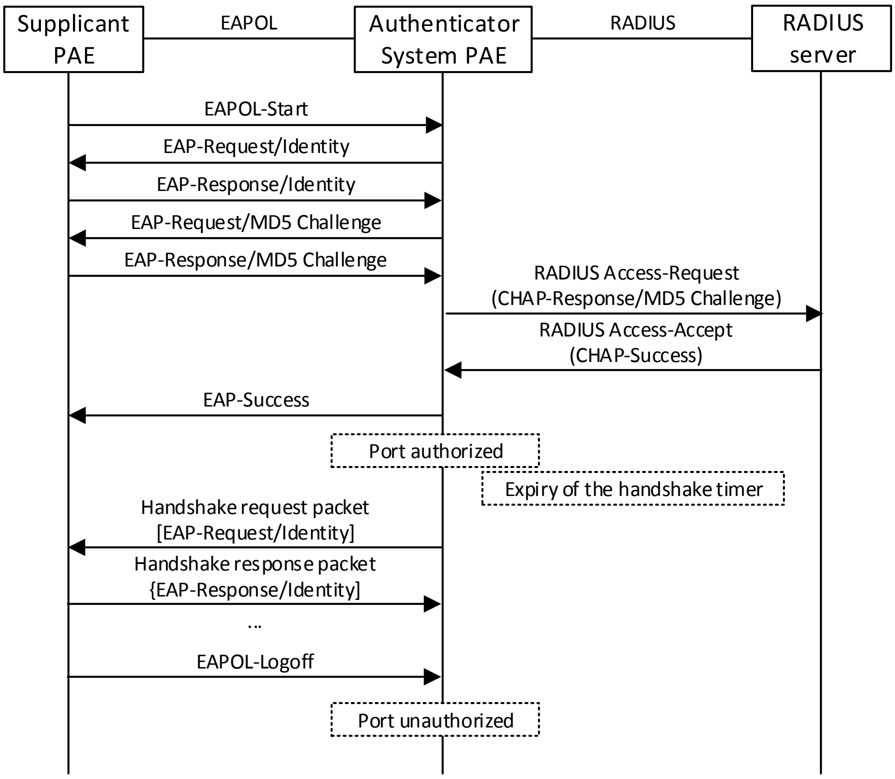

Supplicant PAE
EAPOL
Authenticator System PAE
RADIUS
RADIUS server
EAPOL-Start
EAP-Request/Identity
EAP-Response/Identity
EAP-Request/MD5 Challenge
EAP-Response/MD5 Challenge
RADIUS Access-Request (CHAP-Response/MD5 Challenge)
RADIUS Access-Accept (CHAP-Success)
EAP-Success
Port authorized
Expiry of the handshake timer
Handshake request packet [EAP-Request/Identity]
Handshake response packet {EAP-Response/Identity]
...
EAPOL-Logoff
Port unauthorized

Figure 37.12: the Authentication Flow of 802.1x EAP Termination Mode

- Tunnel-Medium-Type = 802 (6)
- Tunnel-Private-Group-ID = VLANID

The VLANID here means the VID of VLAN, ranging from 1 to 4094. For example, Tunnel-Private-Group-ID = 30 means VLAN 30.

When the switch receives the assigned Auto VLAN information, the current Access port will leave the VLAN set by the user and join Auto VLAN.

Auto VLAN won't change or affect the port's configuration. But the priority of Auto VLAN is higher than that of the user-set VLAN, that is Auto VLAN is the one takes effect when the authentication is finished, while the user-set VLAN do not work until the user become offline.

Notes: At present, Auto VLAN can only be used in the port-based access control mode, and on the ports whose link type is Access.

2. Guest VLAN

Guest VLAN feature is used to allow the unauthenticated user to access some specified resources.

The user authentication port belongs to a default VLAN (Guest VLAN) before passing the 802.1x authentication, with the right to access the resources within this VLAN without authentication. But the resources in other networks are beyond reach. Once authenticated, the port will leave Guest VLAN, and the user can access the resources of other networks.

In Guest VLAN, users can get 802.1x supplicant system software, update supplicant system or update some other applications (such as anti-virus software, the patches of operating system).

The access device will add the port into Guest VLAN if there is no supplicant getting authenticated successfully in a certain stretch of time because of lacking exclusive authentication supplicant system or the version of the supplicant system being too low.

Once the 802.1x feature is enabled and the Guest VLAN is configured properly, a port will be added into Guest VLAN, just like Auto VLAN, if there is no response message from the supplicant system after the device sends more authentication-triggering messages than the upper limit (EAP-Request/Identity) from the port.

- The authentication server assigns an Auto VLAN, and then the port leaves Guest VLAN and joins the assigned Auto VLAN. When the user becomes offline, the port will be allocated to the specified Guest VLAN again.
- The authentication server assigns an Auto VLAN, and then the port leaves Guest VLAN and joins the specified VLAN. When the user becomes offline, the port will be allocated to the specified Guest VLAN again.

37.2 802.1x Configuration Task List

802.1x Configuration Task List:

1. Enable IEEE 802.1x function
2. Access management unit property configuration
    (a) Configure port authentication status
    (b) Configure access management method for the port: MAC-based or port-based
    (c) Configure expanded 802.1x function
    (d) Configure the max user number
3. User access devices related property configuration (optional)

1. Enable 802.1x function

Command	Explanation
Global Mode	
dot1x enable no dot1x enable	Enables the 802.1x function in the switch and ports; the no command disables the 802.1x function.
dot1x privateclient enable no dot1x privateclient enable	Enables the switch force client software using private 802.1x authentication packet format. The no command will disable this function.
dot1x user free-resource <prefix> <mask> no dot1x user free-resource	Sets free access network resource for unauthorized dot1x user. The no command close the resource.
dot1x unicast enable no dot1x unicast enable	Enable the 802.1x unicast passthrough function of switch; the no operation of this command will disable this function.

2. **Access management unit property configuration**

(a) Configure port authentication status

Command	Explanation
Port Mode	
dot1x port-control { auto | force-authorized | force-unauthorized } no dot1x port-control	Sets the 802.1x authentication mode; the no command restores the default setting.

(b) Configure port access management method

Command	Explanation
Port Mode	
dot1x port-method { macbased | portbased | user-based { standard | advanced } } no dot1x port-method	Sets the port access management method; the no command restores MAC-based access management.
dot1x max-user macbased <number> no dot1x max-user macbased	Sets the maximum number of access users for the specified port; the no command restores the default setting of allowing 1 user.
dot1x max-user userbased <number> no dot1x max-user userbased	Set the upper limit of the number of users allowed accessing the specified port, only used when the access control mode of the port is userbased; the no command is used to reset the limit to 10 by default.
dot1x guest-vlan <vlanID> no dot1x guest-vlan	Set the guest vlan of the specified port; the no command is used to delete the guest vlan.
dot1x portbased mode single-mode no dot1x portbased mode single-mode	Set the single-mode based on portbase authentication mode; the no command disables this function.

(c) Configure expanded 802.1x function

Command	Explanation
Global Mode	
dot1x macfilter enable no dot1x macfilter enable	Enables the 802.1x address filter function in the switch; the no command disables the 802.1x address filter function.
dot1x macbased port-down-flush no dot1x macbased port-down-flush	Enables this command, when the dot1x certification according to mac is down, delete the user who passed the certification of the port; The no command does not make the down operation.
dot1x accept-mac <mac-address> [interface <interface-name>] no dot1x accept-mac <mac-address> [interface <interface-name>]	Adds 802.1x address filter table entry, the no command deletes 802.1x filter address table entries.

dot1x eapor enable no dot1x eapor enable	Enables the EAP relay authentication function in the switch; the no command sets EAP local end authentication.

(d) Configure the max user number

Command	Explanation
Global Configuration Mode	
user-control limit <count>	Configure the max controlled/trusted user number supported by the switch; Without implementing this command, the default number would be 128.

3. Supplicant related property configuration

Command	Explanation
Global Mode	
dot1x max-req <count> no dot1x max-req	Sets the number of EAP request/MD5 frame to be sent before the switch re-initials authentication on no supplicant response, the no command restores the default setting.
dot1x re-authentication no dot1x re-authentication	Enables periodical supplicant authentication; the no command disables this function.
dot1x timeout quiet-period <seconds> no dot1x timeout quiet-period	Sets time to keep silent on port authentication failure; the no command restores the default value.
dot1x timeout re-authperiod <seconds> no dot1x timeout re-authperiod	Sets the supplicant re-authentication interval; the no command restores the default setting.
dot1x timeout tx-period <seconds> no dot1x timeout tx-period	Sets the interval for the supplicant to retransmit EAP request/identity frame; the no command restores the default setting.
dot1x re-authenticate [interface <interface-name>]	Enables IEEE 802.1x re-authentication (no wait timeout requires) for all ports or a specified port.

37.3 802.1x Application Example

37.3.1 Examples of Guest Vlan Applications

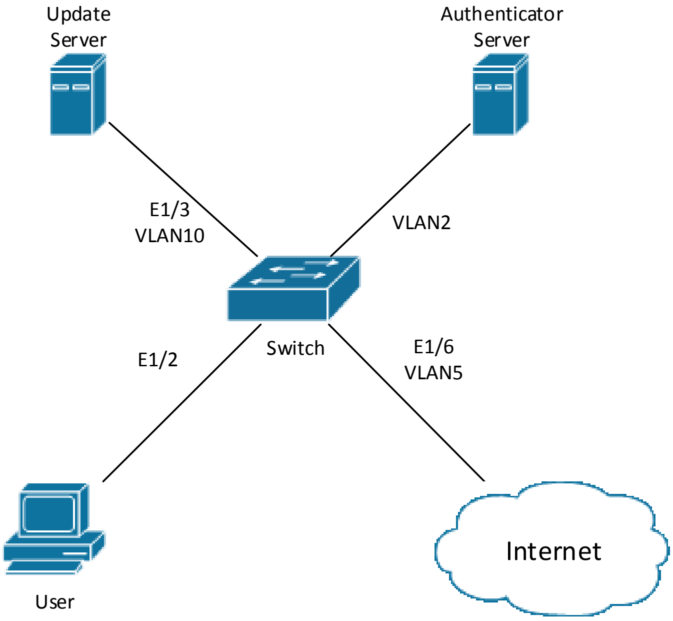


Figure 37.13: The Network Topology of Guest VLAN

Notes: in the figures in this session, E2 means Ethernet 1/0/2, E3 means Ethernet 1/0/3 and E6 means Ethernet 1/0/6.

As showed in the next figure, a switch accesses the network using 802.1x authentication, with a RADIUS server as its authentication server. Ethernet1/0/2, the port through which the user accesses the switch belongs to VLAN100; the authentication server is in VLAN2; Update Server, being in VLAN10, is for the user to download and update supplicant system software; Ethernet1/0/6, the port used by the switch to access the Internet is in VLAN5.

As illustrated in the up figure, on the switch port Ethernet1/0/2, the 802.1x feature is enabled, and the VLAN10 is set as the port's Guest VLAN. Before the user gets authenticated or when the user fails to do so, port Ethernet1/0/2 is added into VLAN10, allowing the user to access the Update Server.

As illustrated in the up figure, when the users become online after a successful authentication, the authentication server will assign VLAN5, which makes the user and Ethernet1/0/6 both in VLAN5, allowing the user to access the Internet.

The following are configuration steps:

```
# Configure RADIUS server.
Switch(config)#radius-server authentication host 10.1.1.3
Switch(config)#radius-server accounting host 10.1.1.3
Switch(config)#radius-server key test
Switch(config)#aaa enable
Switch(config)#aaa-accounting enable
```

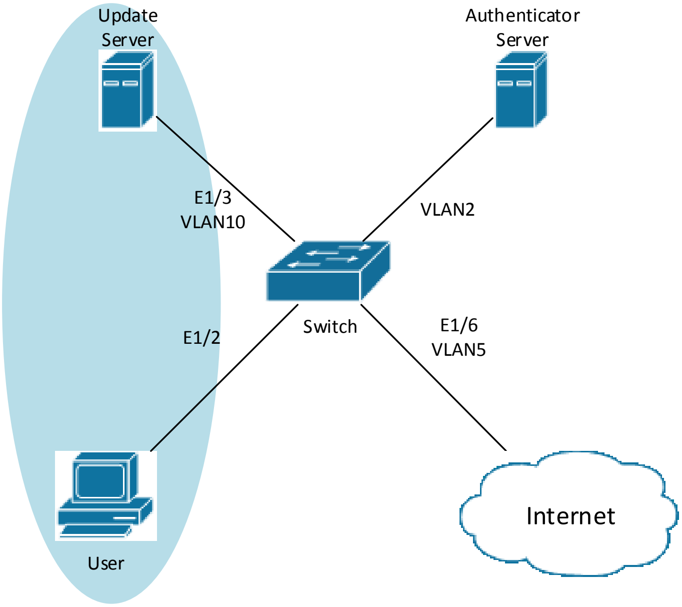


Figure 37.14: User Joining Guest VLAN

```
# Create VLAN100.
Switch(config)#vlan 100

# Enable the global 802.1x function
Switch(config)#dot1x enable

# Enable the 802.1x function on port Ethernet1/0/2
Switch(config)#interface ethernet1/0/2
Switch(Config-If-Ethernet1/0/2)#dot1x enable

# Set the link type of the port as access mode.
Switch(Config-If-Ethernet1/0/2)#switch-port mode access

# Set the access control mode on the port as portbased.
Switch(Config-If-Ethernet1/0/2)#dot1x port-method portbased

# Set the access control mode on the port as auto.
Switch(Config-If-Ethernet1/0/2)#dot1x port-control auto

# Set the port's Guest VLAN as 100.
Switch(Config-If-Ethernet1/0/2)#dot1x guest-vlan 100
Switch(Config-If-Ethernet1/0/2)#exit
```

Using the command of show running-config or show interface ethernet1/0/2, users can check the configuration of Guest VLAN. When there is no online user, no failed user authentication or no user gets offline successfully, and more authentication-triggering messages (EAP-Request/Identity)

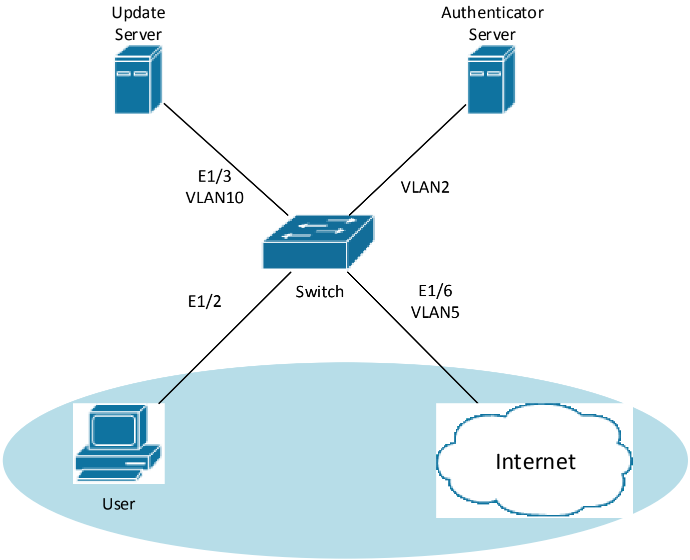


Figure 37.15: User Being Online, VLAN Being Offline

are sent than the upper limit defined, users can check whether the Guest VLAN configured on the port takes effect with the command show vlan id 100.

37.3.2 Examples of IPv4 Radius Applications

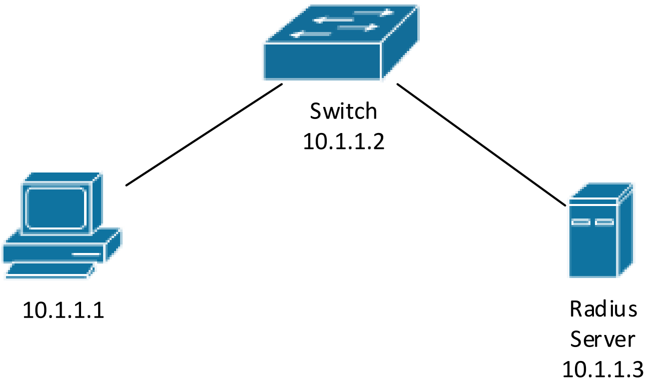


Figure 37.16: IEEE 802.1x Configuration Example Topology

The PC is connecting to port 1/0/2 of the switch; IEEE 802.1x authentication is enabled on port1/0/2; the access mode is the default MAC-based authentication. The switch IP address is 10.1.1.2. Any port other than port 1/0/2 is used to connect to RADIUS authentication server, which has an IP address of 10.1.1.3, and use the default port 1812 for authentication and port 1813 for accounting. IEEE 802.1x authentication client software is installed on the PC and is used in IEEE 802.1x authentication.

The configuration procedures are listed below:

```
Switch(config)#interface vlan 1
Switch(Config-if-vlan1)#ip address 10.1.1.2 255.255.255.0
Switch(Config-if-vlan1)#exit
Switch(config)#radius-server authentication host 10.1.1.3
Switch(config)#radius-server accounting host 10.1.1.3
Switch(config)#radius-server key test
Switch(config)#aaa enable
Switch(config)#aaa-accounting enable
Switch(config)#dot1x enable
Switch(config)#interface ethernet 1/0/2
Switch(Config-Ethernet1/0/2)#dot1x enable
Switch(Config-Ethernet1/0/2)#dot1x port-control auto
Switch(Config-Ethernet1/0/2)#exit
```

37.3.3 Examples of IPv6 Radius Application

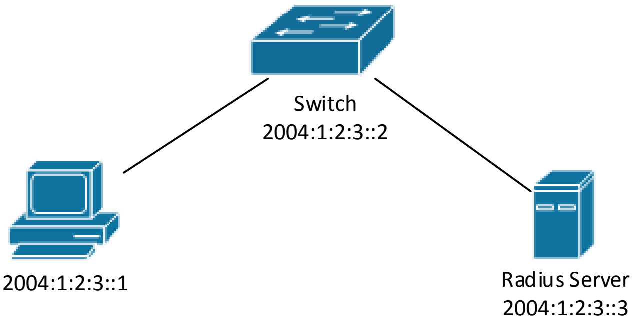


Figure 37.17: IPv6 Radius

Connect the computer to the interface 1/0/2 of the switch, and enable IEEE802.1x on interface1/0/2. Use MAC based authentication. Configure the IP address of the switch as 2004:1:2:3::2, and connect the switch with any interface except interface 1/0/2 to the RADIUS authentication server. Configure the IP address of the RADIUS server to be 2004:1:2:3::3. Use the default ports 1812 and 1813 for authentication and accounting respectively. Install the IEEE802.1x authentication client software on the computer, and use the client for IEEE802.1x authentication.

The detailed configurations are listed 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
Switch(config)#dot1x enable
Switch(config)#interface ethernet 1/0/2
Switch(Config-If-Ethernet1/0/2)#dot1x enable
Switch(Config-If-Ethernet1/0/2)#dot1x port-control auto
Switch(Config-If-Ethernet1/0/2)#exit
```

37.4 802.1x Troubleshooting

It is possible that 802.1x be configured on ports and 802.1x authentication be set to auto, t switch can't be to authenticated state after the user runs 802.1x supplicant software. Here are some possible causes and solutions:

- If 802.1x cannot be enabled for a port, make sure the port is not executing MAC binding, or configured as a port aggregation. To enable the 802.1x authentication, the above functions must be disabled.
- If the switch is configured properly but still cannot pass through authentication, connectivity between the switch and RADIUS server, the switch and 802.1x client should be verified, and the port and VLAN configuration for the switch should be checked, too.
- Check the event log in the RADIUS server for possible causes. In the event log, not only unsuccessful logins are recorded, but prompts for the causes of unsuccessful login. If the event log indicates wrong authenticator password, radius-server key parameter shall be modified; if the event log indicates no such authenticator, the authenticator needs to be added to the RADIUS server; if the event log indicates no such login user, the user login ID and password may be wrong and should be verified and input again.

Chapter 38

The Number Limitation Function of MAC and IP in Port, VLAN Configuration

38.1 Introduction to the Number Limitation Function of MAC and IP in Port, VLAN

MAC address list is used to identify the mapping relationship between the destination MAC addresses and the ports of switch. There are two kinds of MAC addresses in the list: static MAC address and dynamic MAC address. The static MAC address is set by users, having the highest priority (will not be overwritten by dynamic MAC address), and will always be effective; dynamic MAC address is learnt by the switch through transmitting data frames, and will only be effective in a specific time range. When the switch receives a data framed waiting to be transmitted, it will study the source MAC address of the data frame, build a mapping relationship with the receiving port, and then look up the MAC address list for the destination MAC address. If any matching list entry is found, the switch will transmit the data frame via the corresponding port, or, the switch will broadcast the data frame over the VLAN it belongs to. If the dynamically learnt MAC address matches no transmitted data in a long time, the switch will delete it from the MAC address list.

Usually the switch supports both the static configuration and dynamic study of MAC address, which means each port can have more than one static set MAC addresses and dynamically learnt MAC addresses, and thus can implement the transmission of data traffic between port and known MAC addresses. When a MAC address becomes out of date, it will be dealt with broadcast. No number limitation is put on MAC address of the ports of our current switches; every port can have several MAC addressed either by configuration or study, until the hardware list entries are exhausted. To avoid too many MAC addresses of a port, we should limit the number of MAC addresses a port can have.

For each INTERFACE VLAN, there is no number limitation of IP; the upper limit of the number of IP is the upper limit of the number of user on an interface, which is, at the same time, the upper limit of ARP and ND list entry. There is no relative configuration command can be used to control the sent number of these list entries. To enhance the security and the controllability of our products, we need to control the number of MAC address on each port and the number of ARP, ND on each INTERFACE VLAN. The number of static or dynamic MAC address on a port should not exceed the configuration. The number of user on each VLAN should not exceed the configuration, either.

Limiting the number of MAC and ARP list entry can avoid DOS attack to a certain extent. When malicious users frequently do MAC or ARP cheating, it will be easy for them to fill the MAC and ARP list entries of the switch, causing successful DOS attacks.

To summer up, it is very meaningful to develop the number limitation function of MAC and IP in port, VLAN. Switch can control the number of MAC address of ports and the number ARP, ND list entry of ports and VLAN through configuration commands.

Limiting the number of dynamic MAC and IP of ports:

1. Limiting the number of dynamic MAC. If the number of dynamically learnt MAC address by the switch is already larger than or equal with the max number of dynamic MAC address, then shutdown the MAC study function on this port, otherwise, the port can continue its study.
2. Limiting the number of dynamic IP. If the number of dynamically learnt ARP and ND by the switch is already larger than or equal with the max number of dynamic ARP and ND, then shutdown the ARP and ND study function of this port, otherwise, the port can continue its study.

Limiting the number of MAC, ARP and ND of interfaces:

1. Limiting the number of dynamic MAC. If the number of dynamically learnt MAC address by the VLAN of the switch is already larger than or equal with the max number of dynamic MAC address, then shutdown the MAC study function of all the ports in this VLAN, otherwise, all the ports in this VLAN can continue their study (except special ports).
2. Limiting the number of dynamic IP. If the number of dynamically learnt ARP and ND by the switch is already larger than or equal with the max number of dynamic ARP and ND, then the VLAN will not study any new ARP or ND, otherwise, the study can be continued.

38.2 The Number Limitation Function of MAC and IP in Port, VLAN Configuration Task Sequence

1. Enable the number limitation function of MAC and IP on ports
2. Enable the number limitation function of MAC and IP in VLAN
3. Configure the timeout value of querying dynamic MAC
4. Configure the violation mode of ports
5. Display and debug the relative information of number limitation of MAC and IP on ports

1. Enable the number limitation function of MAC and IP on ports

Command	Explanation
Port configuration mode	
switchport mac-address dynamic maximum <value> no switchport mac-address dynamic maximum	Enable and disable the number limitation function of MAC on the ports.

switchport arp dynamic maximum <value> no switchport arp dynamic maximum	Enable and disable the number limitation function of ARP on the ports.
switchport nd dynamic maximum <value> no switchport nd dynamic maximum	Enable and disable the number limitation function of ND on the ports.

2. Enable the number limitation function of MAC and IP in VLAN

Command	Explanation
VLAN configuration mode	
vlan mac-address dynamic maximum <value> no vlan mac-address dynamic maximum	Enable and disable the number limitation function of MAC in the VLAN.
Interface configuration mode	
ip arp dynamic maximum <value> no ip arp dynamic maximum	Enable and disable the number limitation function of ARP in the VLAN.
ipv6 nd dynamic maximum <value> no ipv6 nd dynamic maximum	Enable and disable the number limitation function of NEIGHBOR in the VLAN.

3. Configure the timeout value of querying dynamic MAC

Command	Explanation
Global configuration mode	
mac-address query timeout <seconds>	Configure the timeout value of querying dynamic MAC.

4. Configure the violation mode of ports

Command	Explanation
Port mode	
switchport mac-address violation { protect | shutdown } [recovery <5-3600>] no switchport mac-address violation	Set the violation mode of the port, the no command restores the violation mode to protect.

5. Display and debug the relative information of number limitation of MAC and IP on ports

Command	Explanation
Admin mode	
show mac-address dynamic count { vlan <vlan-id> | interface ethernet <portName> }	Display the number of dynamic MAC in corresponding ports and VLAN.
show arp-dynamic count { vlan <vlan-id> | interface ethernet <portName> }	Display the number of dynamic ARP in corresponding ports and VLAN.

show nd-dynamic count { vlan <vlan-id> | interface ethernet <portName> }	Display the number of dynamic NEIGHBOUR in corresponding ports and VLAN.
debug switchport mac count no debug switchport mac count	All kinds of debug information when limiting the number of MAC on ports.
debug switchport arp count no debug switchport arp count	All kinds of debug information when limiting the number of ARP on ports.
debug switchport nd count no debug switchport nd count	All kinds of debug information when limiting the number of NEIGHBOUR on ports.
debug vlan mac count no debug vlan mac count	All kinds of debug information when limiting the number of MAC in VLAN.
debug ip arp count no debug ip arp count	All kinds of debug information when limiting the number of ARP in VLAN.
debug ipv6 nd count no debug ipv6 nd count	All kinds of debug information when limiting the number of MAC in VLAN.

38.3 The Number Limitation Function of MAC and IP in Port, VLAN Typical Examples

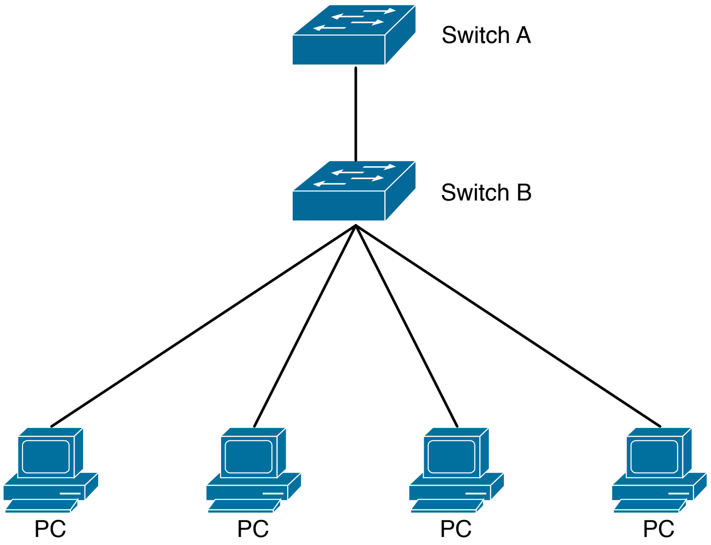


Figure 38.1: The Number Limitation of MAC and IP in Port, VLAN Typical Configuration Example

In the network topology above, SWITCH B connects to many PC users, before enabling the number limitation function of MAC and IP in Port, VLAN, if the system hardware has no other limitation, SWTICH A and SWTICH B can get the MAC, ARP, ND list entries of all the PC, so limiting the MAC, ARP list entry can avoid DOS attack to a certain extent. When malicious users frequently do MAC, ARP cheating, it will be easy for them to fill the MAC, ARP list entries of the switch, causing successful DOS attacks. Limiting the MAC, ARP, ND list entry can prevent DOS attack.

On port 1/0/1 of SWITCH A, set the max number can be learnt of dynamic MAC address as 20, dynamic ARP address as 20, NEIGHBOR list entry as 10. In VLAN 1, set the max number of dynamic MAC address as 30, of dynamic ARP address as 30, NEIGHBOR list entry as 20.

SWITCH A configuration task sequence:

```
Switch(config)#interface ethernet 1/0/1
Switch(Config-If-Ethernet1/0/1)#switchport mac-address dynamic maximum 20
Switch(Config-If-Ethernet1/0/1)#switchport arp dynamic maximum 20
Switch(Config-If-Ethernet1/0/1)#switchport nd dynamic maximum 10
Switch(Config-if-Vlan1)#vlan mac-address dynamic maximum 30
```

38.4 The Number Limitation Function of MAC and IP in Port, VLAN Troubleshooting Help

The number limitation function of MAC and IP in Port, VLAN is disabled by default, if users need to limit the number of user accessing the network, they can enable it. If the number limitation function of MAC address can not be configured, please check whether Spanning-tree, dot1x, TRUNK is running on the switch and whether the port is configured as a MAC-binding port. The number limitation function of MAC address is mutually exclusive to these configurations, so if the users need to enable the number limitation function of MAC address on the port, they should check these functions mentioned above on this port are disabled.

If all the configurations are normal, after enabling the number limitation function of MAC and IP in Port, VLAN, users can use debug commands to debug every limitation, check the details of number limitations and judge whether the number limitation function is correct. If there is any problem, please sent result to technical service center.

Chapter 39

Operational Configuration of AM Function

39.1 Introduction to AM Function

AM (Access Management) means that when a switch receives an IP or ARP message, it will compare the information extracted from the message (such as source IP address or source MAC-IP address) with the configured hardware address pool. If there is an entry in the address pool matching the information (source IP address or source MAC-IP address), the message will be forwarded, otherwise, dumped. The reason why source-IP-based AM should be supplemented by source-MAC-IP-based AM is that IP address of a host might change. Only with a bound IP, can users change the IP of the host into forwarding IP, and hence enable the messages from the host to be forwarded by the switch. Given the fact that MAC-IP can be exclusively bound with a host, it is necessary to make MAC-IP bound with a host for the purpose of preventing users from maliciously modifying host IP to forward the messages from their hosts via the switch.

With the interface-bound attribute of AM, network mangers can bind the IP (MAC-IP) address of a legal user to a specified interface. After that, only the messages sending by users with specified IP (MAC-IP) addresses can be forwarded via the interface, and thus strengthen the monitoring of the network security.

39.2 AM Function Configuration Task List

1. Enable AM function
2. Enable AM function on an interface
3. Configure the forwarding IP
4. Configure the forwarding MAC-IP
5. Delete all of the configured IP or MAC-IP or both
6. Display relative configuration information of AM

1. Enable AM function

Command	Explanation
Global Mode	
am enable no am enable	Globally enable or disable AM function.

2. Enable AM function on an interface

Command	Explanation
Port Mode	
am port no am port	Enable/disable AM function on the port. When the AM function is enabled on the port, no IP or ARP message will be forwarded by default.

3. Configure the forwarding IP

Command	Explanation
Port Mode	
am ip-pool <ip-address> <num> no am ip-pool <ip-address> <num>	Configure the forwarding IP of the port.

4. Configure the forwarding MAC-IP

Command	Explanation
Port Mode	
am mac-ip-pool <mac-address> <ip-address> no am mac-ip-pool <mac-address> <ip-address>	Configure the forwarding MAC-IP of the port.

5. Delete all of the configured IP or MAC-IP or both

Command	Explanation
Global Mode	
no am all [ip-pool | mac-ip-pool]	Delete MAC-IP address pool or IP address pool or both pools configured by all users.

6. Display relative configuration information of AM

Command	Explanation
Global Configuration Mode	
show am [interface <interface-name>]	Display the AM configuration information of one port or all ports.

39.3 AM Function Example

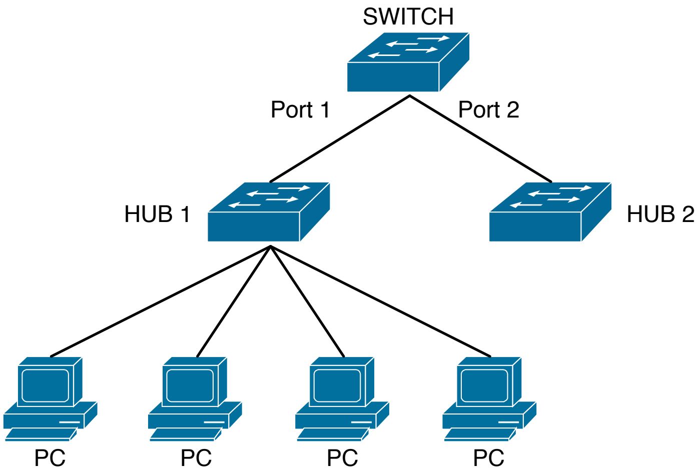


Figure 39.1: a typical configuration example of AM function

In the topology above, 30 PCs, after converged by HUB1, connect with interface1 on the switch. The IP addresses of these 30 PCs range from 100.10.10.1 to 100.10.10.30. Considering security, the system manager will only take user with an IP address within that range as legal ones. And the switch will only forward data packets from legal users while dumping packets from other users.

According to the requirements mentioned above, the switch can be configured as follows:

```
Switch(config)#am enable
Switch(config)#interface ethernet1/0/1
Switch(Config-If-Ethernet 1/0/1)#am port
Switch(Config-If-Ethernet 1/0/1)#am ip-pool 10.10.10.1 10
```

39.4 AM Function Troubleshooting

AM function is disabled by default, and after it is enabled, relative configuration of AM can be made.

Users can view the current AM configuration with 'show am' command, such as whether the AM is enabled or not, and AM information on each interface, they can also use 'show am [interface <interface-name>]' command to check the AM configuration information on a specific interface.

If any operational error happens, the system will display detailed corresponding prompt.

Chapter 40

Security Feature Configuration

40.1 Introduction to Security Feature

Before introducing the security features, we here first introduce the DoS. The DoS is short for Denial of Service, which is a simple but effective destructive attack on the internet. The server under DoS attack will drop normal user data packet due to non-stop processing the attacker's data packet, leading to the denial of the service and worse can lead to leak of sensitive data of the server.

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

40.2 Security Feature Configuration

40.2.1 Prevent IP Spoofing Function Configuration Task Sequence

1. Enable the IP spoofing function.

Command	Explanation
Global mode	
[no] dosattack-check srcip-equal-dstip enable	Enable/disable the function of checking if the IP source address is the same as the destination address.

40.2.2 Prevent TCP Unauthorized Label Attack Function Configuration Task Sequence

1. Enable the anti TCP unauthorized label attack function

Command	Explanation
Global mode	
[no] dosattack-check tcp-flags enable	Enable/disable checking TCP label function.

40.2.3 Anti Port Cheat Function Configuration Task Sequence

1. Enable the anti port cheat function

Command	Explanation
Global mode	
[no] dosattack-check srcport-equal-dstport enable	Enable/disable the prevent-port-cheat function.

40.2.4 Prevent TCP Fragment Attack Function Configuration Task Sequence

1. Enable the prevent TCP fragment attack function

2. Configure the minimum permitted TCP head length of the packet

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

Note: This function is not supported by switch.

40.2.5 Prevent ICMP Fragment Attack Function Configuration Task Sequence

1. Enable the prevent ICMP fragment attack function

2. Configure the max permitted ICMPv4 net load length

Command	Explanation
Global mode	
[no] dosattack-check icmp-attacking enable	Enable/disable the prevent ICMP fragment attack function.
dosattack-check icmpv4-size <size>	Configure the max permitted ICMPv4 net load length. This command has not effect when used separately, the user have to enable the dosattack-check icmp-attacking enable.

40.3 Security Feature Example

Scenario:

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

Configuration procedure:

```
Switch(config)# dosattack-check srcip-equal-dstip enable
Switch(config)# dosattack-check srcport-equal-dstport enable
Switch(config)# dosattack-check icmp-attacking enable
Switch(config)# dosattack-check icmpV4-size 100
```

Chapter 41

TACACS+ Configuration

41.1 Introduction to TACACS+

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+.

41.2 TACACS+ Configuration Task List

1. Configure the TACACS+ authentication key
2. Configure the TACACS+ server
3. Configure the TACACS+ authentication timeout time
4. Configure the IP address of the RADIUS NAS

1. Configure the TACACS+ authentication key

Command	Explanation
Global Mode	
tacacs-server key { 0 | 7 } <string> no tacacs-server key	Configure the TACACS+ server key; the 'no tacacs-server key' command deletes the key.

2. **Configure TACACS+ server**

Command	Explanation
Global Mode	
tacacs-server authentication host <ip-address> [port <port-number>] [timeout <seconds>] [key { 0 | 7 } <string>] [primary] no tacacs-server authentication host <ip-address>	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	
tacacs-server timeout <seconds> no tacacs-server timeout	Configure the authentication timeout for the TACACS+ server, the 'no tacacs-server timeout' command restores the default configuration.

4. **Configure the IP address of the TACACS+ NAS**

Command	Explanation
Global Mode	
tacacs-server nas-ipv4 <ip-address> no tacacs-server nas-ipv4	To configure the source IP address for the TACACS+ packets for the switch.

41.3 TACACS+ Scenarios Typical Examples

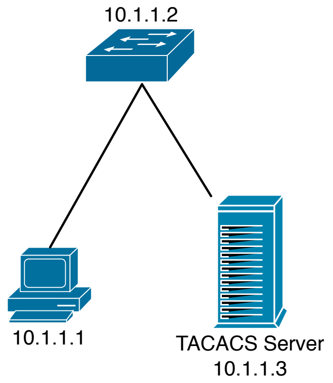


Figure 41.1: TACACS Configuration

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, set telnet log on authentication of the switch as tacacs local, via using TACACS+ authentication server to achieve telnet user authentication.

```
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 line vty login tacacs
```

41.4 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.

Chapter 42

RADIUS Configuration

42.1 Introduction to RADIUS

42.1.1 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 communicates with the RADIUS client through RADIUS protocol. The RADIUS protocol is the most common used protocol in the AAA framework.

42.1.2 Message structure for RADIUS

The RADIUS protocol uses UDP to deliver protocol packets. The packet format is shown as below.

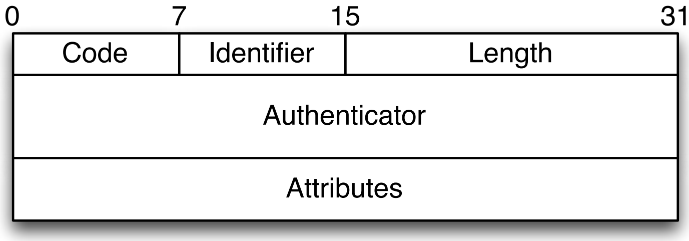


Figure 42.1: Message structure for RADIUS

Code field(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.

42.2 RADIUS Configuration Task List

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	
radius-server key { 0 | 7 } <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 { <ipv4-address> | <ipv6-address> } [port <port-number>] [key { 0 | 7 } <string>] [primary] [access-mode { dot1x | telnet }] no radius-server authentication host { <ipv4-address> | <ipv6-address> }	Specifies the IPv4/IPv6 address and the port number, whether be primary server for RADIUS accounting server; the no command deletes the RADIUS accounting server.

radius-server accounting host { <ipv4-address> | <ipv6-address> } [port <port-number>] [key { 0 | 7 } <string>] [primary] no radius-server accounting host { <ipv4-address> | <ipv6-address> }	Specifies the IPv4/IPv6 address and the port number, whether be primary server for RADIUS accounting server; the no command deletes the RADIUS accounting server.

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 restores 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.

42.3 RADIUS Typical Examples

42.3.1 IPv4 Radius Example

A computer connects to a switch, of which the IP address is 10.1.1.2 and connected with a RADIUS authentication server without Ethernet1/0/2; 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
```

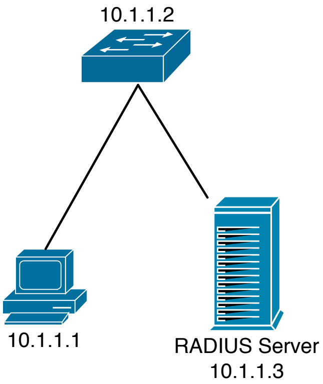


Figure 42.2: The Topology of IEEE802.1x configuration

```
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
```

42.3.2 IPv6 Radius Example

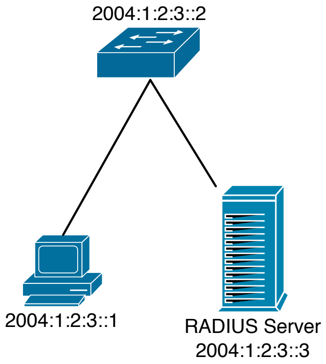


Figure 42.3: The Topology of IPv6 Radius configuration

A computer connects to a switch, of which the IP address is 2004:1:2:3::2 and connected with a RADIUS authentication server without Ethernet1/0/2; 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
```

42.4 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

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

Chapter 43

SSL Configuration

43.1 Introduction to SSL

As the computer networking technology spreads, the security of the network has been taking more and more important impact on the availability and the usability of the networking application. The network security has become one of the greatest barriers of modern networking applications.

To protect sensitive data transferred through Web, Netscape introduced the Secure Socket Layer - SSL protocol, for its Web browser. Up till now, SSL 2.0 and 3.0 has been released. SSL 2.0 is obsolete because of security problems, and it is not supported on the switches of Network. The SSL protocol uses the public-key encryption, and has become the industry standard for secure communication on internet for Web browsing. The Web browser integrates HTTP and SSL to realize secure communication.

SSL is a safety protocol to protect private data transmission on the Internet. SSL protocols are designed for secure transmission between the client and the server, and authentication both at the server sides and optional client. SSL protocols must build on reliable transport layer (such as TCP). SSL protocols are independent for application layer. Some protocols such as HTTP, FTP, TELNET and so on, can build on SSL protocols transparently. The SSL protocol negotiates for the encryption algorithm, the encryption key and the server authentication before data is transmitted. Ever since the negotiation is done, all the data being transferred will be encrypted.

Via above introduction, the security channel is provided by SSL protocols have below three characteristics:

- Privacy. First they encrypt the suite through negotiation, then all the messages be encrypted.
- Affirmation. Though the client authentication of the conversational is optional, but the server is always authenticated.
- Reliability. The message integrality inspect is included in the sending message (use MAC).

43.1.1 Basic Element of SSL

The basic strategy of SSL provides a safety channel for random application data forwarding between two communication programs. In theory, SSL connect is similar with encrypt TCP connect. The position of SSL protocol is under application layer and on the TCP. If the mechanism of the data forwarding in the lower layer is reliable, the data read-in the network will be forwarded to the other program in sequence, lose packet and re-forwarding will not appear. A lot of transmission protocols can provide such kind of service in theory, but in actual application, SSL is almost running on TCP, and not running on UDP and IP directly.

When web function is running on the switch and client visit our web site through the internet browser, we can use SSL function. The communication between client and switch through SSL connect can improve the security.

Firstly, SSL should be enabled on the switch. When the client tries to access the switch through https method, a SSL session will be set up between the switch and the client. When the SSL session has been set up, all the data transmission in the application layer will be encrypted.

SSL handshake is done when the SSL session is being set up. The switch should be able to provide certification keys. Currently the keys provided by the switch are not the formal certification keys issued by official authentic, but the private certification keys generated by SSL software under Linux which may not be recognized by the web browser. With regard to the switch application, it is not necessary to apply for a formal SSL certification key. A private certification key is enough to make the communication safe between the users and the switch. Currently it is not required that the client is able to check the validation of the certification key. The encryption key and the encryption method should be negotiated during the handshake period of the session which will be then used for data encryption.

SSL session handshake process:

1	Client ->	encryption algorithm random key for encryption	-> Server
2	Client <-	The selected encryption algorithm, the certification which is randomly generated	<- Server
3	Client ->	The encrypted master_key	-> Server
4	Client <-	To compute the encryption key	<- Server
5	Client ->	The MAC value of the handshaking messages	-> Server
6	Client <-	The MAC value of the handshaking messages	<- Server

43.2 SSL Configuration Task List

1. Enable/disable SSL function
2. Configure/delete port number by SSL used
3. Configure/delete secure cipher suite by SSL used
4. Maintenance and diagnose for the SSL function

1. Enable/disable SSL function

Command	Explanation
Global Mode	
ip http secure-server no ip http secure-server	Enable/disable SSL function.

2. Configure/delete port number by SSL used

Command	Explanation
Global Mode	
ip http secure-port <port-number> no ip http secure-port	Configure port number by SSL used, the 'no ip http secure-port' command deletes the port number.

3. Configure/delete secure cipher suite by SSL used

Command	Explanation
Global Mode	
ip http secure-ciphersuite { des-cbc3-sha | rc4-128-sha | des-cbc-sha } no ip http secure-ciphersuite	Configure/delete secure cipher suite by SSL used.

4. Maintenance and diagnose for the SSL function

Command	Explanation
Admin Mode or Configuration Mode	
show ip http secure-server status	Show the configured SSL information.
debug ssl no debug ssl	Open/close the DEBUG for SSL function.

43.3 SSL Typical Example

When the Web function is enabled on the switch, SSL can be configured for users to access the web interface on the switch. If the SSL has been configured, communication between the client and the switch will be encrypted through SSL for safety.

Firstly, SSL should be enabled on the switch. When the client tries to access the switch through https method, a SSL session will be set up between the switch and the client. When the SSL session has been set up, all the data transmission in the application layer will be encrypted.

Configuration on the switch:

```
Switch(config)#ip http secure-server
Switch(config)#ip http secure-port 1025
Switch(config)#ip http secure-ciphersuite rc4-128-sha
```

43.4 SSL Troubleshooting

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

- First good condition of the physical connection;
- Second all interface and link protocols are in the UP state (use 'show interface' command);
- Then, make sure SSL function is enabled (use ip http secure-server command);

- Don't use the default port number if configured port number, pay attention to the port number when input the web wide;
- If SSL is enabled, SSL should be restarted after changes on the port configuration and encryption configuration;
- IE 7.0 or above should be used for use of des-cbc-sha;
- If the SSL problems remain unsolved after above try, please use debug SSL and other debugging command and copy the DEBUG message within 3 minutes, send the recorded message to technical server center of our company.

Chapter 44

IPv6 Security RA Configuration

44.1 Introduction to IPv6 Security RA

In IPv6 networks, the network topology is generally compromised of routers, layer-two switches and IPv6 hosts. Routers usually advertise RA, including link prefix, link MTU and other information, when the IPv6 hosts receive RA, they will create link address, and set the default router as the one sending RA in order to implement IPv6 network communication. If a vicious IPv6 host sends RA to cause that normal IPv6 users set the default router as the vicious IPv6 host user, the vicious user will be able to capture the information of other users, which will threat the network security. Simultaneously, the normal users get incorrect address and will not be able to connect to the network. So, in order to implement the security RA function, configuring on the switch ports to reject vicious RA messages is necessary, thus to prevent forwarding vicious RA to a certain extent and to avoid affecting the normal operation of the network.

44.2 IPv6 Security RA Configuration Task Sequence

1. Globally enable IPv6 security RA
2. Enable IPv6 security RA on a port
3. Display and debug the relative information of IPv6 security RA

1. Globally enable IPv6 security RA

Command	Explanation
Global Configuration Mode	
ipv6 security-ra enable no ipv6 security-ra enable	Globally enable and disable IPv6 security RA.

2. Enable IPv6 security RA on a port

Command	Explanation
Port Configuration Mode	
ipv6 security-ra enable no ipv6 security-ra enable	Enable and disable IPv6 security RA in port configuration mode.

3. Display and debug the relative information of IPv6 security RA

Command	Explanation
Admin Mode	
debug ipv6 security-ra no debug ipv6 security-ra	Enable the debug information of IPv6 security RA module, the no operation of this command will disable the output of debug information of IPv6 security RA.
show ipv6 security-ra [interface <interface-list>]	Display the distrust port and whether globally security RA is enabled.

44.3 IPv6 Security RA Typical Examples

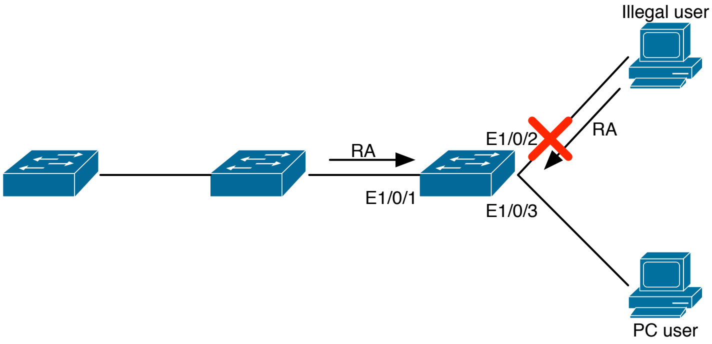


Figure 44.1: IPv6 Security RA sketch map

Instructions: if the illegal user in the graph advertises RA, the normal user will receive the RA, set the default router as the vicious IPv6 host user and change its own address. This will cause the normal user to not be able to connect the network. We want to set security RA on the 1/0/2 port of the switch, so that the RA from the illegal user will not affect the normal user.

Switch configuration task sequence:

```
Switch(config)#ipv6 security-ra enable
Switch(Config-If-Ethernet1/0/2)# ipv6 security-ra enable
```

44.4 IPv6 Security RA Troubleshooting Help

The function of IPv6 security RA is quite simple, if the function does not meet the expectation after configuring IPv6 security RA:

- Check if the switch is correctly configured.
- Check if there are rules conflicting with security RA function configured on the switch, this kind of rules will cause RA messages to be forwarded.

Chapter 45

MAB Configuration

45.1 Introduction to MAB

In actual network existing the device which can not install the authentication client, such as printer, PDA devices, they can not process 802.1x authentication. However, to access the network resources, they need to use MAB authentication to replace 802.1x authentication.

MAB authentication is a network accessing authentication method based on the accessing port and the MAC address of MAB user. The user needn't install any authentication client, after the authentication device receives ARP packets sent by MAB user, it will authenticate the MAC address of the MAB user and there is the corresponding authentication information in the authentication server, the matched packets of the port and the source MAC are allowed to pass when the authentication is successful. MAB user didn't need to input the username and password manually in the process of authentication.

At present, MAB authentication device only supports RADIUS authentication method. There is the selection method for the authentication username and password: use the MAC address of the MAB user as the username and password, or the fixed username and password (all users use the configured username and password to authenticate).

45.2 MAB Configuration Task List

MAB Configuration Task List:

1. Enable MAB function
   (a) Enable global MAB function
   (b) Enable port MAB function
2. Configure MAB authentication username and password
3. Configure MAB parameters
   (a) Configure guest-vlan
   (b) Configure the binding-limit of the port
   (c) Configure the reauthentication time

(d) Configure the offline detection time

(e) Configure other parameters

1. Enable MAB function

Command	Explanation
Global Mode	
mac-authentication-bypass enable no mac-authentication-bypass enable	Enable the global MAB authentication function.
Port Mode	
mac-authentication-bypass enable no mac-authentication-bypass enable	Enable the port MAB authentication function.

2. Configure MAB authentication username and password

Command	Explanation
Global Mode	
mac-authentication-bypass username-format { mac-address | { fixed username WORD password WORD } }	Set the authentication mode of MAB authentication function.

3. Configure MAB parameters

Command	Explanation
Port Mode	
mac-authentication-bypass guest-vlan <1-4094> no mac-authentication-bypass guest-vlan	Set guest vlan of MAB authentication, only Hybrid port uses this command, it is not take effect on access port.
mac-authentication-bypass binding-limit <1-100> no mac-authentication-bypass binding-limit	Set the max MAB binding-limit of the port.
Global Mode	
mac-authentication-bypass timeout reauth-period <1-3600> no mac-authentication-bypass timeout reauth-period	Set the reauthentication interval after the authentication is unsuccessful.
mac-authentication-bypass timeout offline-detect (0 | <60-7200>) no mac-authentication-bypass timeout offline-detect	Set offline detection interval.
mac-authentication-bypass timeout quiet-period <1-60> no mac-authentication-bypass timeout quiet-period	Set quiet-period of MAB authentication.
mac-authentication-bypass timeout stale-period <0-60> no mac-authentication-bypass timeout stale-period	Set the time that delete the binding after the port is down.

mac-authentication-bypass timeout linkup-period <0-30> no mac-authentication-bypass timeout linkup-period	To obtain IP again, set the interval of down/up when MAB binding is changing into VLAN.
mac-authentication-bypass spoofing-garp-check enable no mac-authentication-bypass spoofing-garp-check enable	Enable the spoofing-garp-check function, MAB function will not deal with spoofing-garp any more; the no command disables the function.
authentication mab { radius | none } no authentication mab	Configure the authentication mode and priority of MAC address, the no command restores the default authentication mode.

45.3 MAB Example

The typical example of MAB authentication function:

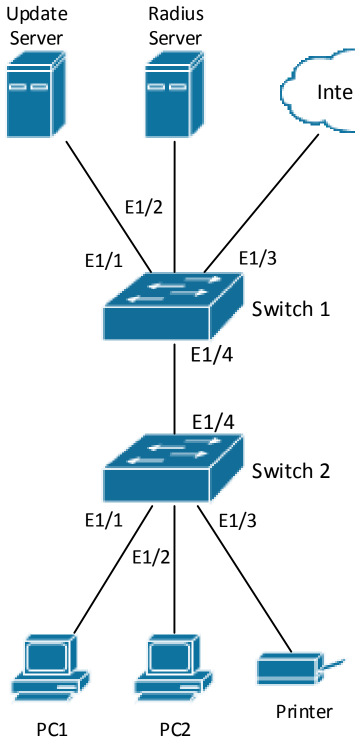


Figure 45.1: MAB application

Switch1 is a layer 2 accessing switch, Switch2 is a layer 3 aggregation switch.

Ethernet 1/1 is an access port of Switch1, connects to PC1, it enables 802.1x port-based function and configures guest vlan as vlan8.

Ethernet 1/2 is a hybrid port, connects to PC2, native vlan of the port is vlan1, and configures guest vlan as vlan8, it joins in vlan1, vlan8 and vlan10 with untag method and enables MAB function.

Ethernet 1/3 is an access port, connects to the printer and enables MAB function.

Ethernet 1/4 is a trunk port, connects to Switch2.

Ethernet 1/4 is a trunk port of Switch2, connects to Switch1.

Ethernet 1/1 is an access port, belongs to vlan8, connects to update server to download and upgrade the client software.

Ethernet 1/2 is an access port, belongs to vlan9, connects to radius server which configure auto vlan as vlan10.

Ethernet 1/3 is an access port, belongs to vlan10, connects to external internet resources.

To implement this application, the configuration is as follows:

Switch1 configuration:

(1) Enable 802.1x and MAB authentication function globally, configure username and password of MAB authentication and radius-server address

```
Switch(config)#dot1x enable
Switch(config)#mac-authentication-bypass enable
Switch(config)#mac-authentication-bypass username-format fixed
                username mabuser password mabpwd
Switch(config)#vlan 8-10
Switch(config)#interface vlan 9
Switch(config-if-vlan9)ip address 192.168.61.9 255.255.255.0
Switch(config-if-vlan9)exit
Switch(config)#radius-server authentication host 192.168.61.10
Switch(config)#radius-server accounting host 192.168.61.10
Switch(config)#radius-server key test
Switch(config)#aaa enable
Switch(config)#aaa-accounting enable
```

(2) Enable the authentication function of each port

```
Switch(config)#interface ethernet 1/1
Switch(config-if-ethernet1/1)#dot1x enable
Switch(config-if-ethernet1/1)#dot1x port-method portbased
Switch(config-if-ethernet1/1)#dot1x guest-vlan 8
Switch(config-if-ethernet1/1)#exit
Switch(config)#interface ethernet 1/2
Switch(config-if-ethernet1/2)#switchport mode hybrid
Switch(config-if-ethernet1/2)#switchport hybrid native vlan 1
Switch(config-if-ethernet1/2)#switchport hybrid allowed vlan 1;8;10 untag
Switch(config-if-ethernet1/2)#mac-authentication-bypass enable
Switch(config-if-ethernet1/2)#mac-authentication-bypass enable guest-vlan 8
Switch(config-if-ethernet1/2)#exit
Switch(config)#interface ethernet 1/3
Switch(config-if-ethernet1/3)#switchport mode access
Switch(config-if-ethernet1/3)#mac-authentication-bypass enable
Switch(config-if-ethernet1/3)#exit
Switch(config)#interface ethernet 1/4
Switch(config-if-ethernet1/4)#switchport mode trunk
```

45.4 MAB Troubleshooting

If there is any problem happens when using MAB function, please check whether the problem is caused by the following reasons:

- Make sure global and port MAB function are enabled;
- Make sure the correct username and password of MAB authentication are used;
- Make sure the radius-server configuration is correct.

Chapter 46

PPPoE Intermediate Agent Configuration

46.1 Introduction to PPPoE Intermediate Agent

46.1.1 Brief Introduction to PPPoE

PPPoE (Point to Point Protocol over Ethernet) is a protocol that apply PPP protocol to Ethernet. PPP protocol is a link layer protocol and supply a communication method of point-to-point, it is usually selected by host dial-up link, for example the link is line dial-up. PPP protocol is applied to Ethernet that means PPPoE protocol makes many hosts of Ethernet to connect a remote access collector through one or multiple bridge devices. If the remote access collector is broadband access server (BAS), it can supply broadband access and accounting functions for these hosts, so PPPoE protocol is used to broadband access authentication of Ethernet usually.

46.1.2 Introduction to PPPoE IA

Along with broadband access technique is rapidly developed, broadband access network is also developing from strength to strength, but security problem gradually becomes the focus, soever the clients or the access device and the network are faced with security problem (especially from the client) in the current access network. Traditional Ethernet user can not be identified, traced and located exactly, however in exoteric and controllable network, identification and location are the basic character and requirement for user, for example, when supplying the application that use user accounts to login, this method supplied by PPPoE Intermediate Agent can availably avoid user accounts embezzled.

There are two stages for PPPoE protocol work: discovery stage and session stage. Discovery stage is used to obtain MAC address of the remote server to establish a point-to-point link and a session ID with the server, and session stage uses this session ID to communicate. PPPoE Intermediate Agent only relates to discovery stage, so we simply introduce discovery stage.

There are four steps for discovery stage:

1. **Client sends PADI packet:** The first step, client uses broadcast address as destination address and broadcast PADI (PPPoE Active Discovery Initiation) packet to discover access collector in layer 2 network. Notice: This message may be sent to many access collector of the network.

2. **Broadband Access Server responds PADO packet:** The second step, server responds

PADO (PPPoE Active Discovery Offer) packet to client according to the received source MAC address of PADI packet, the packet will take sever name and service name.

3. **Client sends PADR packet:** The third step, client selects a server to process the session according to the received PADO packet. It may receives many PADO packets for PADI message of the first step may be sent to many servers (select the server according to whether the service information of PADO packet match with the servce information needed by client). MAC address of the other end used for session will be known after server is selected, and send PADR (PPPoE Active Discovery Request) packet to it to announce server the session requirement.

4. **Server responds PADS packet:** The fourth step, server establishes a session ID according to the received PADR packet, this session ID will be sent to client through PADS (PPPoE Active Discovery Session-confirmation) packet, hereto PPPoE discovery stage is completed, enter session stage.

PADT (PPPoE Active Discovery Terminate) packet is an especial packet of PPPoE, it's Ethernet protocol number (0x8863) is the same as four packets above, so it can be considered a packet of discovery stage. To stop a PPPoE session, PADT may be sent at the discretional time of the session. (It can be sent by client or server)

PPPoE Intermediate Agent supplies a function that identify and locate the user. When passing network access device, PADI and PADR messages sent by client with the access link tag of this device at PPPoE discovery stage, so as to exactly identify and locate the user on server.

If the direct-link access device is LAN switch, the added information include: MAC, Slot ID, Port Index, Vlan ID, and so on. This function is implemented according to Migration to Ethernet-based DSL aggregation.

PPPoE Intermediate Agent Exchange Process

PPPoE Intermediate Agent exchange process is similar to PPPoE exchange process, for the first exchange process, the access link tag is added to PADI and PADR packets. The exchange process is as follows:

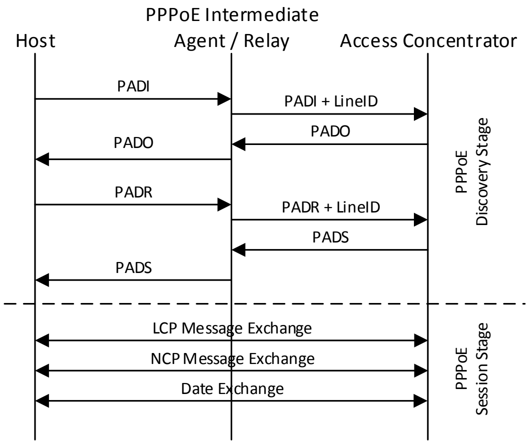


Figure 46.1: PPPoE IA protocol exchange process

PPPoE Packet Format

PPPoE packet format is as follows:

Ethernet II frame

Destination MAC	Source MAC	Type Field	PPPoE Data	CRC Check Sum

PPPoE Data

Version	Type	Code	Session ID	Length Field	TLV 1	...	TLV N

TLV frame

Type	Length	Data

Figure 46.2: PPPoE packet format

Each field meanings in the following:

Type field (2 bytes) of Ethernet II frame: The protocol sets type field value of PPPoE protocol packet as 0x8863 (include 5 kinds of packets in PPPoE discovery stage only), type field value of session stage as 0x8864.

PPPoE version field (4 bits): Specify the current PPPoE protocol version, the current version must be set as 0x1.

PPPoE type field (4 bits): Specify the protocol type, the current version must be set as 0x1.

PPPoE code field (1 byte): Specify the packet type. 0x09 means PADI packet, 0x07 means PADO packet, 0x19 means PADR packet, 0x65 means PADS packet, 0xa7 means PADT packet.

PPPoE session ID field (2 bytes): Specify the session ID.

PPPoE length field (2 bytes): Specify the sum of all TLV length.

TLV type field (2 bytes): A TLV frame means a TAG, type field means TAG type, the table is as follows.

TLV length field (2 bytes): Specify the length of TAG data field.

TLV data field (the length is not specified): Specify the transmitted data of TAG.

Tag Type	Tag Explanation
0x0000	The end of a series tag in PPPoE data field, it is saved for ensuring the version compatibility and is applied by some packets.
0x0101	Service name. Indicate the supplied services by network.
0x0102	Server name. When user receives the PADO response packet of AC, it can obtain the server name from the tag and select the corresponding server.
0x0103	Exclusive tag of the host. It is similar to tag field of PPPoE data packets and is used to match the sending and reveiving end (Because broadcast network may exist many PPPoE data packets synchronously).
0x0104	AC-Cookies. It is used to avoid the vicious DOS attack.
0x0105	The identifier of vendor.
0x0110	Relay session ID. PPPoE data packet can be interrupted to other AC, this field is used to keep other connection.
0x0201	The error of service name. When the requested service name is not accepted by other end, the response packet will take this tag.
0x0202	The error of server name.
0x0203	Common error.

PPPoE Intermediate Agent vendor tag Frame

The following is the format of tag added by PPPoE IA, adding tag is the Uppermost function of PPPoE IA.

<table>
<tr><td colspan="2">0x0105 (Vendor-Specific)</td><td colspan="2">TAG_LENGTH</td></tr>
<tr><td colspan="4">0x00000DE9 (3561 decimal, i.e. “ADSL Forum” IANA entry)</td></tr>
<tr><td>0x01</td><td>length</td><td colspan="2">Agent Circuit ID value...</td></tr>
<tr><td colspan="4">Agent Circuit ID value (con’t) ...</td></tr>
<tr><td>0x02</td><td>length</td><td colspan="2">Agent Circuit ID value...</td></tr>
<tr><td colspan="4">Agent Circuit ID value (con’t) ...</td></tr>
</table>

Figure 46.3: PPPoE IA - vendor tag (4 bytes in each row)

Add TLV tag as 0x0105 for PPPoE IA, TAG_LENGTH is length field of vendor tag; 0x00000DE9 is 'ADSL Forum' IANA entry of the fixed 4 bytes; 0x01 is type field of Agent Circuit ID, length is length field and Agent Circuit ID value field; 0x02 is type field of Agent Remote ID, length is length field and Agent Remote ID value field.

PPPoE IA supplies a default circuit ID value, the default circuit ID (The figure in the following) includes 5 fields, ANI (Access Node Identifier) can be configured by user, it's length is less than 47 bytes. If there is no ANI configured, MAC is accessed by default, occupy 6 bytes and use space symbol to compart, 'eth' occupies 3 bytes and uses space symbol to compart, 'Slot ID' occupies 2 bytes, use '/' to compart and occupy 1 byte, 'Port Index' occupies 3 bytes, use ':' to compart and occupy 1 byte, 'Vlan ID' occupies 4 bytes, all fields use ASCII, user can configure ciucuit ID for each port according to requirement.

ANI (n byte)	Space (1 byte)	Eth (3 byte)	Space (1 byte)	Slot ID (2 byte)	/ (1 byte)	Port Index (3 byte)	: (1 byte)	VLAN ID (4 byte)

Figure 46.4: Agent Circuit ID value

MAC of the access switch is the default remote ID value of PPPoE IA. remote ID value can be configured by user flexibly, the length is less than 63 bytes.

Trust Port of PPPoE Intermediate Agent

Discovery stage sends five kinds of packets, PADI and PADR packets sent by client to server, PADO and PADS packets sent by server to client, PADT packet can be sent by server or client.

In PPPoE IA, for security and reduce traffic, set a port connected server as trust port, set ports connected client as untrust port, trust port can receive all packets, untrust port can receive only PADI, PADR and PADT packets which are sent to server. To ensure client operation is correct, it must set the port connected server as trust port, each access device has a trust port at least.

PPPoE IA vendor tag can not exist in PPPoE packets sent by server to client, so we can strip and forward these vendor tags if they exist in PPPoE packets. Strip function must be configured on trust port, enabling strip function is not take effect on untrust port.

46.2 PPPoE Intermediate Agent Configuration Task List

1. Enable global PPPoE Intermediate Agent
2. Enable port PPPoE Intermediate Agent

Command	Explanation
Global Mode	
pppoe intermediate-agent no pppoe intermediate-agent	Enabel global PPPoE Intermediate Agent function.
pppoe intermediate-agent type tr-101 circuit-id access-node-id <string> no pppoe intermediate-agent type tr-101 circuit-id access-node-id	Configure access node ID field value of circuit ID in added vendor tag.
pppoe intermediate-agent type tr-101 circuit-id identifier-string <string> option { sp | sv | pv | spv } delimiter <WORD> [delimiter <WORD>] no pppoe intermediate-agent type tr-101 circuit-id identifier-string option delimiter	Configure circuit-id in added vendor tag.
pppoe intermediate-agent type self-defined circuit-id { vlan | port | id (switch-id (mac | hostname) | remote-mac) | string WORD } no pppoe intermediate-agent type self-defined circuit-id	Configure the self-defined circuit-id.
pppoe intermediate-agent type self-defined remote-id { mac | vlan-mac | hostname | string WORD } no pppoe intermediate-agent type self-defined remote-id	Configure the self-defined remote-id.
pppoe intermediate-agent delimiter <WORD> no pppoe intermediate-agent delimiter	Configure the delimiter among the fields in circuit-id and remote-id
pppoe intermediate-agent format (circuit-id | remote-id) (hex | ascii) no pppoe intermediate-agent format (circuit-id | remote-id)	Configure the format with hex or ASCII for circuit-id and remote-id.
Port Mode	
pppoe intermediate-agent no pppoe intermediate-agent	Enable PPPoE Intermediate Agent function of port.
pppoe intermediate-agent vendor-tag strip no pppoe intermediate-agent vendor-tag strip	Set vendor tag strip function of port.
pppoe intermediate-agent trust no pppoe intermediate-agent trust	Set a port as trust port.

pppoe intermediate-agent circuit-id <string> no pppoe intermediate-agent circuit-id	Set circuit-id of port.
pppoe intermediate-agent remote-id <string> no pppoe intermediate-agent remote-id	Set remote-id of port.

46.3 PPPoE Intermediate Agent Typical Application

PPPoE Intermediate Agent typical application is as follows:

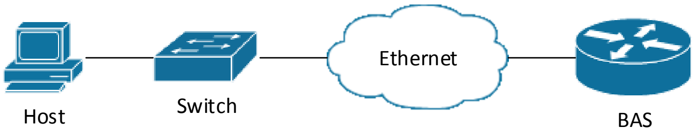


Figure 46.5: PPPoE IA typical application

Both host and BAS server run PPPoE protocol, they are connected by layer 2 ethernet, switch enables PPPoE Intermediate Agent function.

Typical configuration (1) in the following:

Step 1: Switch enables global PPPoE IA function, MAC as 0a0b0c0d0e0f.

```
Switch(config)#pppoe intermediate-agent
```

Step 2: Configure port ethernet1/0/1 which connect server as trust port, and configure vendor tag strip function.

```
Switch(config-if-ethernet1/0/1)#pppoe intermediate-agent trust
Switch(config-if-ethernet1/0/1)#pppoe intermediate-agent vendor-tag strip
```

Step 3: Port ethernet1/0/2 of vlan1 and port ethernet1/0/3 of vlan 1234 enable PPPoE IA function of port.

```
Switch(config-if-ethernet1/0/2)#pppoe intermediate-agent
Switch(config-if-ethernet1/0/3)#pppoe intermediate-agent
```

Step 4: Configure pppoe intermediate-agent access-node-id as abcd.

```
Switch(config)#pppoe intermediate-agent type tr-101 circuit-id access-node-id abcd
```

Step 5: Configure circuit ID as aaaa, remote ID as xyz for port ethernet1/0/3.

```
Switch(config-if-ethernet1/0/3)#pppoe intermediate-agent circuit-id aaaa
Switch(config-if-ethernet1/0/3)#pppoe intermediate-agent remote-id xyz
```

circuit-id value is 'abcd eth 01/002:0001', remote-id value is '0a0b0c0d0e0f' for the added vendor tag of port ethernet1/0/2. circuit-id value is 'aaaa', remote-id value is 'xyz' for the added vendor tag of port ethernet1/0/3.

Typical configuration (2) in the following:

Step 1: Switch enables global PPPoE IA function, MAC as 0a0b0c0d0e0f.

```
Switch(config)#pppoe intermediate-agent
```

Step 2: Configure port ethernet1/0/1 which connect server as trust port, and configure vendor tag strip function.

```
Switch(config-if-ethernet1/0/1)#pppoe intermediate-agent trust
Switch(config-if-ethernet1/0/1)#pppoe intermediate-agent vendor-tag strip
```

Step 3: Port ethernet1/0/2 of vlan1 and port ethernet1/0/3 of vlan 1234 enable PPPoE IA function of port.

```
Switch(config-if-ethernet1/0/2)#pppoe intermediate-agent
Switch(config-if-ethernet1/0/3)#pppoe intermediate-agent
```

Step 4: Configure pppoe intermediate-agent access-node-id as abcd.

```
Switch(config)#pppoe intermediate-agent type tr-101 circuit-id access-node-id abcd
```

Step 5: Configure pppoe intermediate-agent identifier-string as 'efgh', combo mode as spv, delimiter of Slot ID and Port ID as '#', delimiter of Port ID and Vlan ID as '/'.

```
Switch(config)#pppoe intermediate-agent type tr-101 circuit-id identifier-string efgh
                        option spv delimiter # delimiter /
```

Step 6: Configure circuit-id value as bbbb on port ethernet1/0/2.

```
Switch(config-if-ethernet1/0/2)#pppoe intermediate-agent circuit-id bbbb
```

Step 7: Configure remote-id as xyz on ethernet1/0/3.

```
Switch(config-if-ethernet1/0/3)#pppoe intermediate-agent remote-id xyz
```

circuit-id value is 'bbbb', remote-id value is '0a0b0c0d0e0f' for the added vendor tag of port ethernet1/0/2. circuit-id value is 'efgh eth 01#003/1234', remote-id value is 'xyz' for the added vendor tag of port ethernet1/0/3.

46.4 PPPoE Intermediate Agent Troubleshooting

- Only switch enables global PPPoE intermediate agent firstly, this function can be run on port.
- Configure a trust port at least, and this port can connect to server.
- vendor tag strip function must be configured by trust port.
- Circuit-id override priority is: pppoe intermediate-agent circuit-id < pppoe intermediate-agent identifier-string option delimiter < pppoe intermediate-agent access-node-id.

Chapter 47

Web Portal Configuration

47.1 Introduction to Web Portal Authentication

802.1x authentication uses the special client to authenticate, the device uses the special layer 2 switch, the authentication server uses RADIUS server, the format of authentication message uses EAP protocol. Use EAPOL encapsulation technique (encapsulate EAP packets within Ethernet frame) to process the communication between client and authentication proxy switch, but authentication proxy switch and authentication server use EAPOR encapsulation format (runn EAP packets on Radius protocol) to process the communication. The device and RADIUS server use RADIUS protocol to transmit PAP packets or CHAP packets when the device processes to relay.

For implementing identity authentication and network accessing, user should install the special authentication client software, and spring the authentication flow to communicate with Radius server through logging in authentication client. The after 802.1x authentication adds web based authentication mode, the user can download a special Java Applet program by browser or other plug-in to replace 802.1x client.

For the environment which uses 802.1x authentication, installing client or downloading the special Java Applet program become a mortal problem. To satisfy user's actual requirement, the manual describes an application scene based on web portal authentication. Web portal authentication not only implements the basic device authentication without the client but also implement the security detection to the terminal.

47.2 Web Portal Authentication Configuration Task List

1. Enable/disable web portal authentication globally (required)
2. Enable/disable web portal authentication of the port (required)
3. Configure the max web portal binding number allowed by the port (optional)
4. Configure HTTP redirection address of web portal authentication (required)
5. Configure IP source address for communicating between accessing device and portal server (required)
6. Enable dhcp snooping binding web portal function (optional)

7. Delete the binding information of web portal authentication

1. Enable/disable web portal authentication globally

Command	Explanation
Global Mode	
webportal enable no webportal enable	Enable/disable web portal authentication globally.

2. Enable/disable web portal authentication of the port

Command	Explanation
Port mode	
webportal enable no webportal enable	Enable/disable web portal authentication of the port.

3. Configure the max web portal binding number allowed by the port

Command	Explanation
Port mode	
webportal binding-limit <1-256> no webportal binding-limit	Configure the max web portal binding number allowed by the port.

4. Configure HTTP redirection address of web portal authentication

Command	Explanation
Global Mode	
webportal redirect <ip> no webportal redirect	Configure HTTP redirection address of web portal authentication.

5. Configure IP source address for communicating between accessing device and portal server

Command	Explanation
Global Mode	
webportal nas-ip <ip-address> no webportal nas-ip	Configure IP source address for communicating between accessing device and portal server.

6. Enable dhcp snooping binding web portal function

Command	Explanation
Port mode	
ip dhcp snooping binding webportal no ip dhcp snooping binding webportal	Enable dhcp snooping binding web portal function.

7. Delete the binding information of web portal authentication

Command	Explanation
Admin Mode	
clear webportal binding { mac WORD | interface <ethernet IFNAME | IFNAME> | }	Delete the binding information of web portal authentication.

47.3 Web Portal Authentication Typical Example

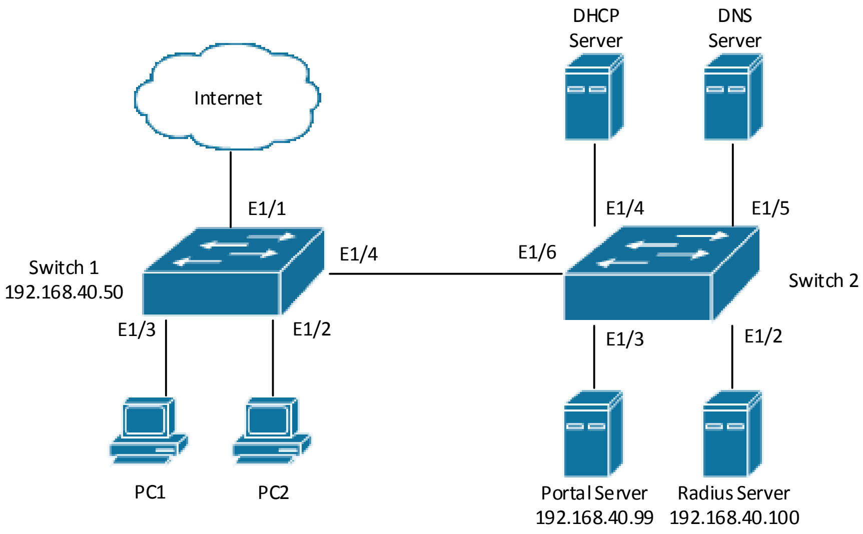


Figure 47.1: Web portal typical application scene

In the above figure, pc1 is end-user, there is http browser in it, but no 802.1x authentication client, pc1 wants to access the network through web portal authentication.

Switch1 is the accessing device, it configures accounting server's address and port as RADIUS server's IP and port, and enable the accounting function. Ethernet 1/0/2 connects to pc1, the port enables web portal authentication, and configure the redirection address and port as portal server's IP and port, so ethernet 1/0/2 forbids all flows except dhcp/dns/arp packets.

Switch2 is the aggregation switch, ethernet1/0/2 connects to radius server, ethernet1/0/3 connects to portal server. The address of radius server is 192.168.40.100, the address of portal server is 192.168.40.99. ethernet1/0/4 connects to DHCP server, ethernet1/0/5 connects to DNS server. ethernet1/0/6 is trunk port and connects to ethernet1/0/4 of switch1.

The configuration of the common web portal authentication is as follows:

```
Switch(config)#interface vlan 1
Switch(config-if-vlan1)#ip address 192.168.40.50 255.255.255.0
Switch(config)#webportal enable
Switch(config)#webportal nas-ip 192.168.40.50
Switch(config)#webportal redirect 192.168.40.99
Switch(config)#interface ethernet 1/0/3
Switch(config-if-ethernet1/0/3)#webportal enable
```

Web portal authentication associates with DHCP snooping binding to use, the configuration is as follows:

```
Switch(config)#ip dhcp snooping enable
Switch(config)#ip dhcp snooping binding enable
Switch(config)#interface ethernet 1/0/2
Switch(config-if-ethernet1/0/2)#webportal enable
Switch(config-if-ethernet1/0/2)#ip dhcp snooping binding webportal
```

47.4 Web Portal Authentication Troubleshooting

When using web portal authentication, the system will show the detailed prompt information if the operation is wrong.

Web portal authentication is disabled by default. After ensure the configuration is correct, use debug command and show command to check the relative information, if you can not determine the cause of the problem, please send the recorded message to technical server center of our company.

Chapter 48

VLAN-ACL Configuration

48.1 Introduction to VLAN-ACL

The user can configure ACL policy to VLAN to implement the accessing control of all ports in VLAN, and VLAN-ACL enables the user to expediently manage the network. The user only needs to configure ACL policy in VLAN, the corresponding ACL action can takes effect on all member ports of VLAN, but it does not need to solely configure on each member port.

When VLAN ACL and Port ACL are configured at the same time, the principle of denying firstly is used. When the packets match VLAN ACL and Port ACL at the same time, as long as one rule is drop, then the final action is drop.

Egress ACL can implement the filtering of the packets on egress and ingress direction, the packets match the specific rules can be allowed or denied. ACL can support IP ACL, MAC ACL, MAC-IP ACL, IPv6 ACL. Ingress direction of VLAN can bind four kinds of ACL at the same time, there are four resources on egress direction of VLAN, IP ACL and MAC ACL engage one resource severally, MAC-IP ACL and IPv6 ACL engage two resources severally, so egress direction of VLAN can not bind four kinds of ACL at the same time. When binding three kinds of ACL at the same time, it should be the types of IP, MAC, MAC-IP or IP, MAC, IPv6. When binding two kinds of ACL at the same time, any combination of ACL type is valid. Each type can only apply one on a VLAN.

48.2 VLAN-ACL Configuration Task List

1. Configure VLAN-ACL of IP type
2. Configure VLAN-ACL of MAC type
3. Configure VLAN-ACL of MAC-IP
4. Configure VLAN-ACL of IPv6 type
5. Show configuration and statistic information of VLAN-ACL
6. Clear statistic information of VLAN-ACL

1. Configure VLAN-ACL of IP type

Command	Explanation
Global mode	
vacl ip access-group { <1-299> | WORD } { in | out } [traffic-statistic] vlan WORD no vacl ip access-group { <1-299> | WORD } { in | out } vlan WORD	Configure or delete IP VLAN-ACL.

2. Configure VLAN-ACL of MAC type

Command	Explanation
Global mode	
vacl mac access-group { <700-1199> | WORD } { in | out } [traffic-statistic] vlan WORD no vacl mac access-group { <700-1199> | WORD } { in | out } vlan WORD	Configure or delete MAC VLAN-ACL.

3. Configure VLAN-ACL of MAC-IP

Command	Explanation
Global mode	
vacl mac-ip access-group { <3100-3299> | WORD } { in | out } [traffic-statistic] vlan WORD no vacl mac-ip access-group { <3100-3299> | WORD } { in | out } vlan WORD	Configure or delete MAC-IP VLAN-ACL.

4. Configure VLAN-ACL of IPv6 type

Command	Explanation
Global mode	
vacl ipv6 access-group { <500-699> | WORD } { in | out } [traffic-statistic] vlan WORD no ipv6 access-group { <500-699> | WORD } { in | out } vlan WORD	Configure or delete IPv6 VLAN-ACL.

5. Show configuration and statistic information of VLAN-ACL

Command	Explanation
Admin mode	
show vacl [in | out] vlan [<vlan-id>]	Show the configuration and the statistic information of VACL.

6. Clear statistic information of VLAN-ACL

Command	Explanation
Admin mode	
clear vacl [in | out] statistic vlan [<vlan-id>]	Clear the statistic information of VACL.

48.3 VLAN-ACL Configuration Example

A company's network configuration is as follows, all departments are divided by different VLANs, technique department is Vlan1, finance department is Vlan2. It is required that technique department can access the outside network at timeout, but finance department are not allowed to access the outside network at any time for the security. Then the following policies are configured:

- Set the policy VACL_A for technique department. At timeout they can access the outside network, the rule as permit, but other times the rule as deny, and the policy is applied to Vlan1.
- Set the policy VACL_B of ACL for finance department. At any time they can not access the outside network, but can access the inside network with no limitation, and apply the policy to Vlan2.

Network environment is shown as below:

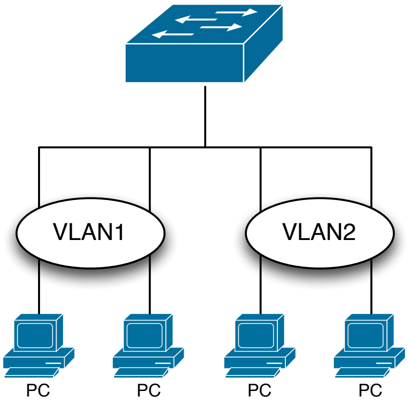


Figure 48.1: VLAN-ACL configuration example

Configuration example:
1) First, configure a timerange, the valid time is the working hours of working day:

```
Switch(config)#time-range t1
Switch(config-time-range-t1)#periodic weekdays 9:00:00 to 12:00:00
Switch(config-time-range-t1)#periodic weekdays 13:00:00 to 18:00:00
```

2) Configure the extended acl_a of IP, at working hours it only allows to access the resource within the internal network (such as 192.168.0.255).

```
Switch(config)# ip access-list extended vacl_a
Switch(config-ip-ext-nacl-vacl_a)#permit ip any-source 192.168.0.0 0.0.0.255
                                          time-range t1
Switch(config-ip-ext-nacl-vacl_a)#deny ip any-source any-destination
                                          time-range t1
```

3) Configure the extended acl_b of IP, at any time it only allows to access resource within the internal network (such as 192.168.1.255).

```
Switch(config)#ip access-list extended vacl_b
Switch(config-ip-ext-nacl-vacl_a)#permit ip any-source 192.168.1.0 0.0.0.255
Switch(config-ip-ext-nacl-vacl_a)#deny ip any-source any-destination
```

4) Apply the configuration to VLAN

```
Switch(config)#vacl ip access-group vacl_a in vlan 1
Switch(config)#vacl ip access-group vacl_b in vlan 2
```

48.4 VLAN-ACL Troubleshooting

- When VLAN ACL and Port ACL are configured at the same time, the principle of denying firstly is used. When the packets match VLAN ACL and Port ACL at the same time, as long as one rule is drop, then the final action is drop.
- Each ACL of different types can only apply one on a VLAN, such as the basic IP ACL, each VLAN can applies one only.

Chapter 49

SAVI Configuration

49.1 Introduction to SAVI

SAVI (Source Address Validation Improvement) is a security authentication method that provides the granularity level of the node source address. It gets the trust node information (such as port, MAC address information), namely, anchor information by monitoring the interaction process of the relative protocol packets (such as ND protocol, DHCPv6 protocol) and using CPS (Control Packet Snooping) mechanism. After that, it binds the anchor information with the node source address and sends the corresponding filter rules, allow the packets which match the filter rules to pass only, so as to reach the aim that check the validity of node source address.

SAVI function includes ND Snooping function, DHCPv6 Snooping function and RA Snooping according to the protocol packet type. ND Snooping function is used to detect ND protocol packet, it sets IPv6 address binding obtained by nodes with the stateless address configuration. DHCPv6 Snooping function is used to detect DHCPv6 protocol packet, it sets IPv6 address binding obtained by nodes with the stateful address configuration. RA Snooping function is used to avoid the lawless node sending the spurious RA packet.

49.2 SAVI Configuration

SAVI configuration task list:

1. Enable or disable SAVI function
2. Enable or disable application scene function for SAVI
3. Configure SAVI binding function
4. Configure the global max-dad-delay for SAVI
5. Configure the global max-dad-prepare-delay for SAVI
6. Configure the global max-slaac-life for SAVI
7. Configure the lifetime period for SAVI bind-protect
8. Enable or disable SAVI prefix check function

9. Configure IPv6 address prefix for a link
10. Configure the filter entry number of IPv6 address
11. Configure the check mode for SAVI conflict binding
12. Enable or disable user authentication
13. Enable or disable DHCPv6 trust of port
14. Enable or disable ND trust of port
15. Configure the binding number

1. Enable or disable SAVI function

Command	Explanation
Global Mode	
savi enable no savi enable	Enable the global SAVI function, no command disables the function.

2. Enable or disable application scene function for SAVI

Command	Explanation
Global Mode	
savi ipv6 { dhcp-only | slaac-only | dhcp-slaac } enable no savi ipv6 { dhcp-only | slaac-only | dhcp-slaac } enable	Enable the application scene function for SAVI, no command disables the function.

3. Configure SAVI binding function

Command	Explanation
Global Mode	
savi ipv6 check source binding ip <ip-address> mac <mac-address> interface <if-name> { type [slaac | dhcp] lifetime <lifetime> | type static } no savi ipv6 check source binding ip <ip-address> interface <if-name>	Configure a static or dynamic binding manually, no command deletes the configured binding. This command may be configured in a global function of savi enable, slaac-only enable, dhcp-only enable or dhcp-slaac enable.

4. Configure the global max-dad-delay for SAVI

Command	Explanation
Global Mode	
savi max-dad-delay <max-dad-delay> no savi max-dad-delay	Configure the max lifetime period of SAVI binding at DETECTION state, no command restores the default value.

5. Configure the global max-dad-prepare-delay for SAVI

Command	Explanation
Global Mode	
savi max-dad-prepare-delay <max-dad-prepare-delay> no savi max-dad-prepare-delay	Configure the max redetection lifetime period for SAVI binding, no command restores the default value.

6. Configure the global max-slaac-life for SAVI

Command	Explanation
Global Mode	
savi max-slaac-life <max-slaac-life> no savi max-slaac-life	Configure the lifetime period of the dynamic slaac binding at BOUND state, no command restores the default value.

7. Configure the lifetime period for SAVI bind-protect

Command	Explanation
Global Mode	
savi timeout bind-protect <protect-time> no savi timeout bind-protect	Configure the bind-protect lifetime period to a port after its state from up to down, no command restores the default value.

8. Enable or disable SAVI prefix check function

Command	Explanation
Global Mode	
ipv6 cps prefix check enable no ipv6 cps prefix check enable	Enable the address prefix check for SAVI, no command disables the function.

9. Configure IPv6 address prefix for a link

Command	Explanation
Global Mode	
ipv6 cps prefix <ip-address> vlan <vid> no ipv6 cps prefix <ip-address>	Configure IPv6 address prefix for a link manually, no command deletes the configured address prefix.

10. Configure the filter entry number of IPv6 address

Command	Explanation
Global Mode	
savi ipv6 mac-binding-limit <limit-num> no savi ipv6 mac-binding-limit	Configure the corresponding dynamic binding number for the same MAC address, no command restores the default value. Note: The binding number only limits the dynamic binding, but does not limit the static binding number.

11. Configure the check mode for SAVI conflict binding

Command	Explanation
Global Mode	
savi check binding <simple | probe> mode no savi check binding mode	Configure the check mode for the conflict binding, no command deletes the check mode.

12. Enable or disable user authentication

Command	Explanation
Port mode	
savi ipv6 check source [ip-address mac-address | ip-address | mac-address] no savi ipv6 check source	Enable the control authentication function for user, no command disables the function.

13. Enable or disable DHCPv6 trust of port

Command	Explanation
Port mode	
ipv6 dhcp snooping trust no ipv6 dhcp snooping trust	Enable DHCPv6 trust port, no command disables the trust function. (port is translated from trust port into untrust port)

14. Enable or disable ND trust of port

Command	Explanation
Port mode	
ipv6 nd snooping trust no ipv6 nd snooping trust	Configure a port as slaac trust and RA trust, no command deletes the port's trust function.

15. Configure the binding number

Command	Explanation
Port mode	
savi ipv6 binding num <limit-num> no savi ipv6 binding num	Configure the binding number of a port, no command restores the default value. Note: The binding number only limits the dynamic binding, but does not limit the static binding number.

49.3 SAVI Typical Application

In actual application, SAVI function is usually applied in access layer switch to check the validity of node source address on direct-link. There are four typical application scenes for SAVI function: DHCP-Only, Slaac-Only, DHCP-Slaac and Static binding. In network environment, users can select the corresponding scene according to the actual requirement; in double stacks network, while SAVI function associates with IPv4 DHCP snooping to use, IPv4 and IPv6 source address authentication is implemented.

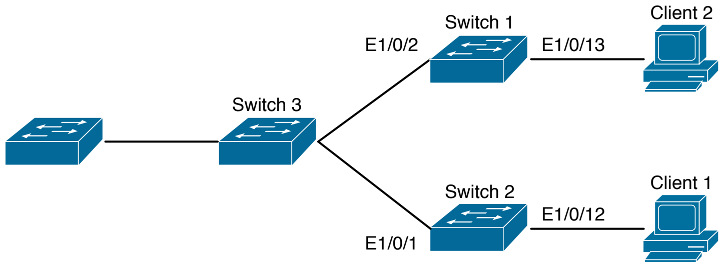


Figure 49.1: Typical network topology application for SAVI function

Client_1 and Client_2 means two different user's PC installed IPv6 protocol, respectively connect with port Ethernet1/0/12 of Switch1 and port Ethernet1/0/13 of Switch2, and enable the source address check function of SAVI. Ethernet1/0/1 and Ethernet1/0/2 are uplink ports of Switch1 and Switch2 respectively, enable DHCP trust and ND trust functions. Aggregation Switch3 enables DHCPv6 server function and route advertisement function.

Configuration steps of SAVI DHCP-SLAAC scene:

```
Switch1(config)#savi enable
Switch1(config)#savi ipv6 dhcp-slaac enable
Switch1(config)#savi check binding probe mode
Switch1(config)#interface ethernet1/0/1
Switch1(config-if-ethernet1/0/1)#ipv6 dhcp snooping trust
Switch1(config-if-ethernet1/0/1)#ipv6 nd snooping trust
Switch1(config-if-ethernet1/0/1)#exit
Switch1(config)#interface ethernet1/0/12-20
Switch1(config-if-port-range)#savi ipv6 check source ip-address mac-address
Switch1(config-if-port-range)#savi ipv6 binding num 4
Switch1(config-if-port-range)#exit
Switch1(config)#exit
```

49.4 SAVI Troubleshooting

After ensure no problem about SAVI client hardware and cable, please check the status which may exist and the propositional solutions in the following:

- If IPv6 packets are filtered incorrectly after enable SAVI function, please ensure the global SAVI function enabled. After that, enable the global function of the corresponding SAVI scene according to the actual application scene and enable the port authentication function.
- If client can not correctly obtain IPv6 address assigned by DHCPv6 server after enable SAVI function, please ensure DHCP port trust is configured by uplink port with DHCPv6 server.

- If node binding can not be set for the new user after enable SAVI function, please check whether the direct-link port configures the max binding number, and whether the binding number reaches to the max number. If the binding number exceeds the max binding limit, it is recommended to configure the bigger binding limit.
- If node binding can not be set for new user after configure the bigger binding limit, please check whether the direct-link port configures the corresponding binding number, and whether the corresponding binding number reaches to the max number in the same MAC address. If the binding number exceeds the max binding limit, it is recommended to configure the bigger binding limit.

Part X

Reliability Configuration

Chapter 50

MRPP Configuration

50.1 Introduction to MRPP

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:

- MRPP specifically uses to Ethernet ring topology
- fast convergence, less than 1 s. ideally it can reach 100-50 ms.

50.1.1 Conception Introduction

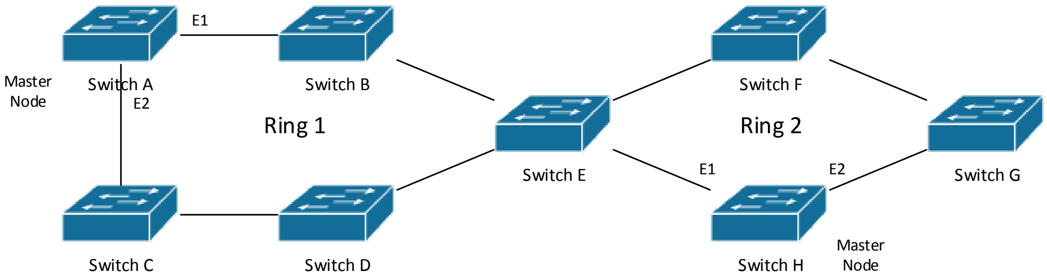


Figure 50.1: MRPP Sketch Map

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 MRPP 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 Fig 50.1, 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 Fig 50.1, Switch A E1 is primary port, E2 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.

50.1.2 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.

50.1.3 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.

50.2 MRPP Configuration Task List

1. Globally enable MRPP
2. Configure MRPP ring
3. Configure the query time of MRPP
4. Configure the compatible mode
5. Display and debug MRPP relevant information

1. Globally enable MRPP

Command	Explanation
Global Mode	
mrpp enable no mrpp enable	Globally enable and disable MRPP.

2. Configure MRPP ring

Command	Explanation
Global Mode	
mrpp ring <ring-id> no mrpp ring <ring-id>	Create MRPP ring. The 'no' command deletes MRPP ring and its configuration.
MRPP ring mode	
control-vlan <vid> 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 < timer> no hello-timer	Configure Hello packet timer sending from primary node of MRPP ring, format 'no' restores default timer value.
fail-timer <timer> 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.
Port mode	
mrpp ring <ring-id> primary-port no mrpp ring <ring-id> primary-port	Specify primary port of MRPP ring.
mrpp ring <ring-id> secondary-port no mrpp ring <ring-id> secondary-port	Specify secondary port of MRPP ring.

3. Configure the query time of MRPP

Command	Explanation
Global Mode	
mrpp poll-time <20-2000>	Configure the query interval of MRPP.

4. Configure the compatible mode

Command	Explanation
Global Mode	
mrpp errp compatible no mrpp errp compatible	Enable the compatible mode for ERRP, the no command disables the compatible mode.
mrpp eaps compatible no mrpp eaps compatible	Enable the compatible mode for EAPS, the no command disables the compatible mode.
errp domain <domain-id> no errp domain <domain-id>	Create ERRP domain, the no command deletes the configured ERRP domain.

5. 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 { <ring-id> }	Display MRPP ring configuration information.
show mrpp statistics { <ring-id> }	Display receiving data packet statistic information of MRPP ring.
clear mrpp statistics { <ring-id> }	Clear receiving data packet statistic information of MRPP ring.

50.3 MRPP Typical Scenario

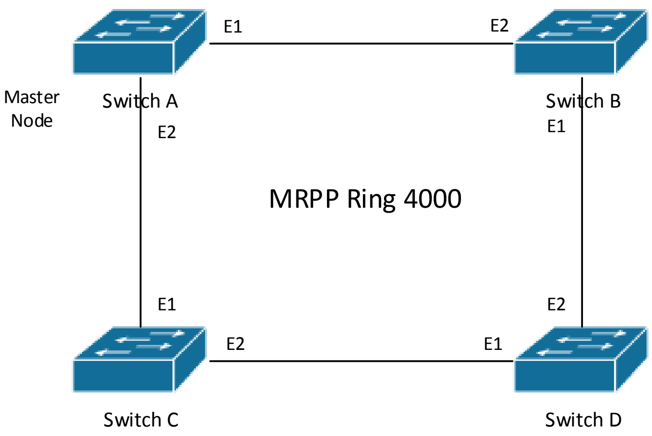


Figure 50.2: MRPP typical configuration scenario

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 4000, thereby constitutes a single MRPP ring.

In above configuration, SWITCH A configuration is primary node of MRPP ring 4000, and configures E1/0/1 to primary port, E1/0/2 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 1/0/1
Switch(config-If-Ethernet1/0/1)#mrpp ring 4000 primary-port
Switch(config-If-Ethernet1/0/1)#interface ethernet 1/0/2
Switch(config-If-Ethernet1/0/2)#mrpp ring 4000 secondary-port
Switch(config-If-Ethernet1/0/2)#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 1/0/1
Switch(config-If-Ethernet1/0/1)#mrpp ring 4000 primary-port
Switch(config-If-Ethernet1/0/1)#interface ethernet 1/0/2
Switch(config-If-Ethernet1/0/2)#mrpp ring 4000 secondary-port
Switch(config-If-Ethernet1/0/2)#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 1/0/1
Switch(config-If-Ethernet1/0/1)#mrpp ring 4000 primary-port
Switch(config-If-Ethernet1/0/1)#interface ethernet 1/0/2
Switch(config-If-Ethernet1/0/2)#mrpp ring 4000 secondary-port
Switch(config-If-Ethernet1/0/2)#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 1/0/1
Switch(config-If-Ethernet1/0/1)#mrpp ring 4000 primary-port
Switch(config-If-Ethernet1/0/1)#interface ethernet 1/0/2
Switch(config-If-Ethernet1/0/2)#mrpp ring 4000 secondary-port
Switch(config-If-Ethernet1/0/2)#exit
Switch(Config)#
```

50.4 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.
- The convergence time of MRPP ring net is relative to the response mode of up/down. If use poll mode, the convergence time as hundreds of milliseconds in simple ring net, if use interrupt mode, the convergence time within 50 milliseconds.
- Generally, the port is configured as poll mode, interrupt mode is only applied to better performance environment, but the security of poll mode is better than interrupt mode, port-scan-mode { interrupt | poll } command can be consulted.
- 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 51

ULPP Configuration

51.1 Introduction to ULPP

Each ULPP group has two uplink ports, they are master port and slave port. The port may be a physical port or a port channel. The member ports of ULPP group have three states: Forwarding, Standby, Down. Normally, only one port at the forwarding state, the other port is blocked at the Standby state. When the master port has the link problem, the master port becomes down state, and the slave port is siwthed to forwarding state.

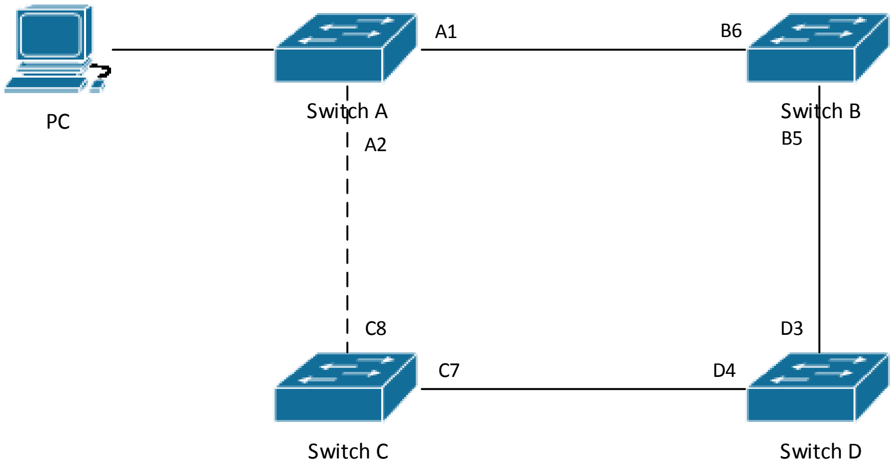


Figure 51.1: the using scene of ULPP

The above figure uses the double-uplink network, this is the typical application scene of ULPP. SwitchA goes up to SwitchD through SwitchB and SwitchC, port A1 and port A2 are the uplink ports. SwitchA configures ULPP, thereinto port A1 is set as the master port, port A2 is set as the slave port. When port A1 at forwarding state has the problem, switch the uplink at once, port A2 turns into forwarding state. After this, when recovering the master port, if the preemption mode is not configured, port A2 keeps the Forwarding state, port A1 turns into the Standby state.

After the preemption mode is enabled, so as to the master port preempts the slave port when it recovered from the problem. For avoiding the frequent uplink switch caused by the abnormity problem, the preemption delay mechanism is imported, and it needs to wait for some times before the master port preempt the slave port. For keeping the continuance of the flows, the master port does not process to preempt by default, but turns into the Standby state.

When configuring ULPP, it needs to specify the VLAN which is protected by this ULPP group through the method of MSTP instances, and ULPP does not provide the protection to other VLANs.

When the uplink switch is happennig, the primary forwarding entries of the device will not be applied to new topology in the network. In the figure, SwitchA configures ULPP, the portA1 as the master port at forwarding state, here the MAC address of PC is learned by Switch D from portD3. After this, portA1 has the problem, the traffic is switched to portA2 to be forwarded. If there is the data sent to PC by SwitchD, still the data will be forwarded from portD3, and will be losed. Therefore, when switching the uplink, the device of configuring ULPP needs to send the flush packets through the port which is switched to Forwarding state, and update MAC address tables and ARP tables of other devices in the network. ULPP respectively uses two kinds of flush packets to update the entries: the updated packets of MAC address and the deleted packets of ARP.

For making use of the bandwidth resource enough, ULPP can implement VLAN load balance through the configuration. As the picture illustrated, SwitchA configures two ULPP groups: portA1 is the master port and portA2 is the slave port in group1, portA2 is the master port and portA1 is the slave port in group2, the VLANs are protected by group1 and group2, they are 1-100 and 101-200. Here both portA1 and portA2 at the forwarding state, the master port and the slave port mutually backup, and respectively forward the packets of the different VLAN ranges. When portA1 has the problem, the traffic of VLAN 1-200 are forwarded by portA2. After this, when portA1 is recovering the normal state, portA2 forwards the data of VLAN 101-200 sequentially, but the data of VLAN 1-100 is switched to portA1 to forward.

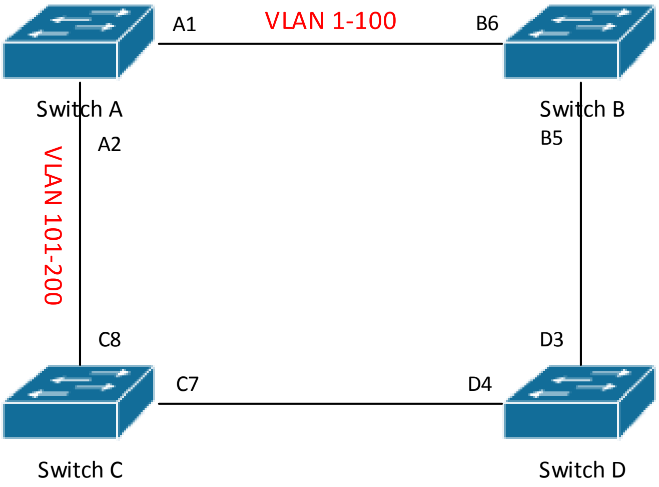


Figure 51.2: VLAN load balance

51.2 ULPP Configuration Task List

1. Create ULPP group globally
2. Configure ULPP group
3. Show and debug the relating information of ULPP

1. Create ULPP group globally

Command	Explanation
Global mode	
ulpp group <integer> no ulpp group <integer>	Configure and delete ULPP group globally.

2. Configure ULPP group

Command	Explanation
ULPP group configuration mode	
preemption mode no preemption mode	Configure the preemption mode of ULPP group. The no operation deletes the preemption mode.
preemption delay <integer> no preemption delay	Configure the preemption delay, the no operation restores the default value 30s.
control vlan <integer> no control vlan	Configure the sending control VLAN, no operation restores the default value 1.
protect vlan-reference-instance <instance-list> no protect vlan-reference-instance <instance-list>	Configure the protection VLANs, the no operation deletes the protection VLANs.
flush enable mac flush disable mac	Enable or disable sending the flush packets which update MAC address.
flush enable arp flush disable arp	Enable or disable sending the flush packets which delete ARP.
flush enable mac-vlan flush disable mac-vlan	Enable or disable sending the flush packets of deleting the dynamic unicast mac according to vlan.
description <string> no description	Configure or delete ULPP group description.
Port mode	
ulpp control vlan <vlan-list> no ulpp control vlan <vlan-list>	Configure the receiving control VLANs, no operation restores the default value 1.
ulpp flush enable mac ulpp flush disable mac	Enable or disable receiving the flush packets which update the MAC address.
ulpp flush enable arp ulpp flush disable arp	Enable or disable receiving the flush packets which delete ARP.
ulpp flush enable mac-vlan ulpp flush disable mac-vlan	Enable or disable receiving the flush packets of mac-vlan type.

ulpp group <integer> master no ulpp group <integer> master	Configure or delete the master port of ULPP group.
ulpp group <integer> slave no ulpp group <integer> slave	Configure or delete the slave port of ULPP group.

3. Show and debug the relating information of ULPP

Command	Explanation
Admin Mode	
show ulpp group [group-id]	Show the configuration information of the configured ULPP group.
show ulpp flush counter interface { ethernet <IF-NAME> | <IFNAME> }	Show the statistic information of the flush packets.
show ulpp flush-receive-port	Show flush type and control VLAN received by the port.
clear ulpp flush counter interface <name>	Clear the statistic information of the flush packets.
debug ulpp flush { send | receive } interface <name> no debug ulpp flush { send | receive } interface <name>	Show the information of the receiving and sending flush packets, the no operation disables the shown information.
debug ulpp flush content interface <name> no debug ulpp flush content interface <name>	Show the contents of the received flush packets, the no operation disables the showing.
debug ulpp error no debug ulpp error	Show the error information of ULPP, the no operation disables the showing.
debug ulpp event no debug ulpp event	Show the event information of ULPP, the no operation disables the showing.

51.3 ULPP Typical Examples

51.3.1 ULPP Typical Example 1

The above topology is the typical application environment of ULPP protocol.

SwitchA has two uplinks, they are SwitchB and SwitchC. When any protocols are not enabled, this topology forms a ring. For avoiding the loopback, SwitchA can configure ULPP protocol, the master port and the slave port of ULPP group. When both master port and slave port are up, the slave port will be set as standby state and will not forward the data packets. When the master port is down, the slave port will be set as forwarding state and switch to the uplink. SwitchB and SwitchC can enable the command that receives the flush packets, it is used to associate with ULPP protocol running of SwitchA to switch the uplink immediately and reduce the switch delay.

When configuring ULPP protocol of SwitchA, first, create a ULPP group and configure the protection VLAN of this group as vlan10, then configure interface Ethernet 1/0/1 as the master port, interface Ethernet 1/0/2 as the slave port, the control VLAN as 10. SwitchB and SwitchC configure the flush packets that receive ULPP.

SwitchA configuration task list:

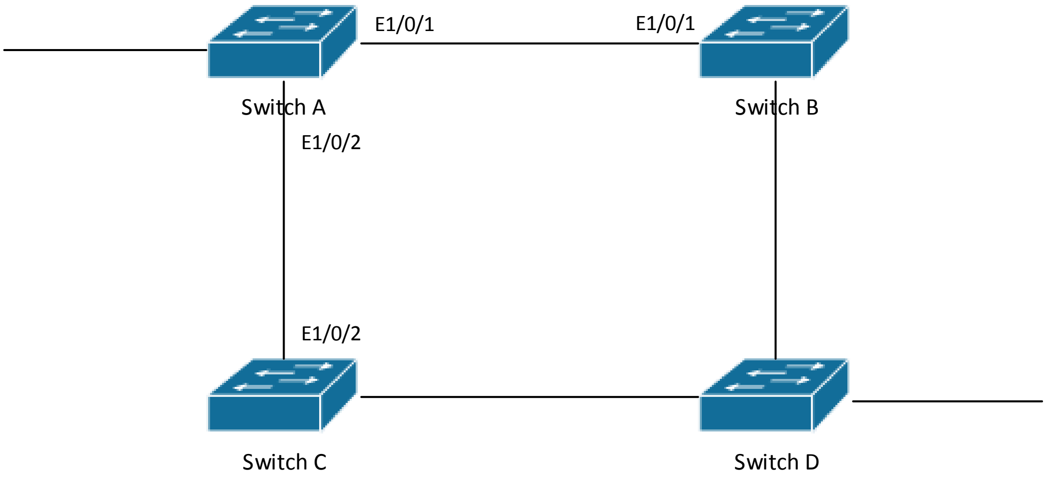


Figure 51.3: ULPP typical example 1

```
Switch(Config)#vlan 10
Switch(Config-vlan10)#switchport interface ethernet 1/0/1; 1/0/2
Switch(Config-vlan10)#exit
Switch(Config)#spanning-tree mst configuration
Switch(Config-Mstp-Region)#instance 1 vlan 10
Switch(Config-Mstp-Region)#exit
Switch(Config)#ulpp group 1
Switch(ulpp-group-1)#protect vlan-reference-instance 1
Switch(ulpp-group-1)#control vlan 10
Switch(ulpp-group-1)#exit
Switch(Config)#interface ethernet 1/0/1
Switch(config-If-Ethernet1/0/1)#ulpp group 1 master
Switch(config-If-Ethernet1/0/1)#exit
Switch(Config)#interface Ethernet 1/0/2
Switch(config-If-Ethernet1/0/2)#ulpp group 1 slave
Switch(config-If-Ethernet1/0/2)#exit
```

SwitchB configuration task list:

```
Switch(Config)#vlan 10
Switch(Config-vlan10)#switchport interface ethernet 1/0/1
Switch(Config-vlan10)#exit
Switch(Config)#interface ethernet 1/0/1
Switch(config-If-Ethernet1/0/1)#ulpp flush enable mac
Switch(config-If-Ethernet1/0/1)#ulpp flush enable arp
Switch(config-If-Ethernet1/0/1)#ulpp control vlan 10
```

SwitchC configuration task list:

```
Switch(Config)#vlan 10
Switch(Config-vlan10)#switchport interface ethernet 1/0/2
Switch(Config-vlan10)#exit
Switch(Config)#interface ethernet 1/0/2
Switch(config-If-Ethernet1/0/2)#ulpp flush enable mac
Switch(config-If-Ethernet1/0/2)#ulpp flush enable arp
Switch(config-If-Ethernet1/0/2)#ulpp control vlan 10
```

51.3.2 ULPP Typical Example 2

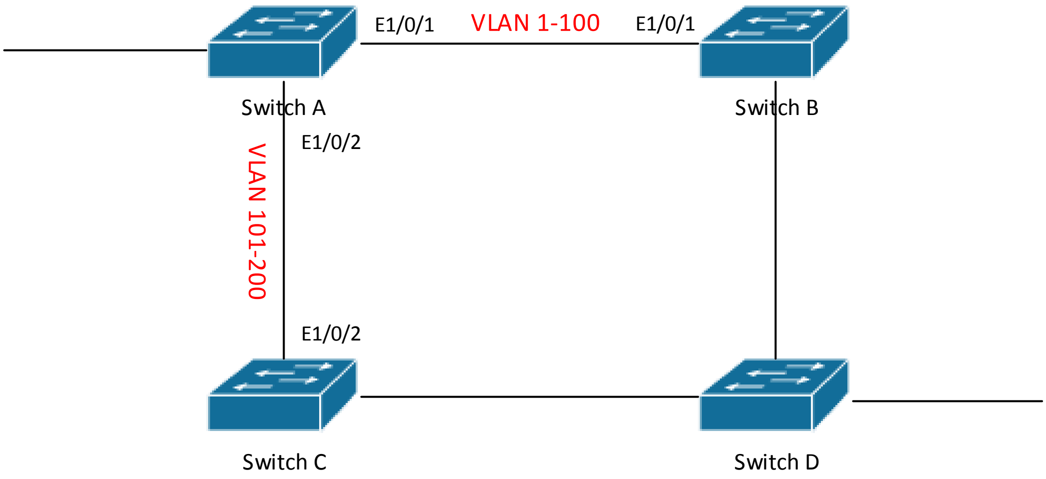


Figure 51.4: ULPP typical example 2

ULPP can implement the VLAN-based load balance. As the picture illustrated, SwitchA configures two ULPP groups: port E1/0/1 is the master port and port 1/0/2 is the slave port in group1, port 1/0/2 is the master port and port 1/0/1 is the slave port in group2. The VLANs protected by group1 are 1-100 and by group2 are 101-200. Here both port E1/0/1 and port E1/0/2 at the forwarding state, the master port and the slave port mutually backup, respectively forward the packets of different VLAN ranges. When port E1/0/1 has the problem, the traffic of VLAN 1-200 are forwarded by port E1/0/2. When port E1/0/1 is recovering the normal state, still port E1/0/2 forwards the data of VLAN 101-200, the data of VLAN 1-100 are switched to port E1/0/1 to forward.

SwitchA configuration task list:

```
Switch(Config)#spanning-tree mst configuration
Switch(Config-Mstp-Region)#instance 1 vlan 1-100
Switch(Config-Mstp-Region)#instance 2 vlan 101-200
Switch(Config-Mstp-Region)#exit
Switch(Config)#ulpp group 1
Switch(ulpp-group-1)#protect vlan-reference-instance 1
Switch(ulpp-group-1)#preemption mode
Switch(ulpp-group-1)#exit
Switch(Config)#ulpp group 2
Switch(ulpp-group-2)#protect vlan-reference-instance 2
Switch(ulpp-group-1)#preemption mode
Switch(ulpp-group-2)#exit
Switch(Config)#interface ethernet 1/0/1
Switch(config-If-Ethernet1/0/1)#switchport mode trunk
Switch(config-If-Ethernet1/0/1)#ulpp group 1 master
Switch(config-If-Ethernet1/0/1)#ulpp group 2 slave
Switch(config-If-Ethernet1/0/1)#exit
Switch(Config)#interface Ethernet 1/0/2
Switch(config-If-Ethernet1/0/2)#switchport mode trunk
Switch(config-If-Ethernet1/0/2)#ulpp group 1 slave
Switch(config-If-Ethernet1/0/2)#ulpp group 2 master
Switch(config-If-Ethernet1/0/2)#exit
```

SwitchB configuration task list:

```
Switch(Config)#interface ethernet 1/0/1
Switch(config-If-Ethernet1/0/1)#switchport mode trunk
Switch(config-If-Ethernet1/0/1)#ulpp flush enable mac
Switch(config-If-Ethernet1/0/1)#ulpp flush enable arp
```

SwitchC configuration task list:

```
Switch(Config)#interface ethernet 1/0/2
Switch(config-If-Ethernet1/0/2)#switchport mode trunk
Switch(config-If-Ethernet1/0/2)#ulpp flush enable mac
Switch(config-If-Ethernet1/0/2)#ulpp flush enable arp
```

51.4 ULPP Troubleshooting

- At present, configuration of more than 2 multi-uplinks is allowed, but it may cause loopback, so is not recommended.
- With the normal configuration, if the broadcast storm happen or the communication along the ring is broken, please enable the debug of ULPP, copy the debug information of 3 minutes and the configuration information, send them to our technical service center.

Chapter 52

ULSM Configuration

52.1 Introduction to ULSM

ULSM (Uplink State Monitor) is used to process the port state synchronization. Each ULSM group is made up of the uplink port and the downlink port, both the uplink port and the downlink port may be multiple. The port may be a physical port or a port channel, but it can not be a member port of a port channel, and each port only belongs to one ULSM group.

The uplink port is the monitored port of ULSM group. When all uplink ports are down or there is no uplink port in ULSM group, ULSM group state is down. ULSM group state is up as long as one uplink port is up.

The downlink port is the controlled port, its state changes along with Up/Down of ULSM group and is always the same with ULSM group state.

ULSM associates with ULPP to enable the downstream device to apperceive the link problem of the upstream device and process correctly. As the picture illustrated, SwitchA configures ULPP, here the traffic is forwarded by port A1. If the link between SwitchB and Switch D has the problem, SwitchA can not apperceive the problem of the upstream link and sequentially forward the traffic from port A1, cause traffic losing.

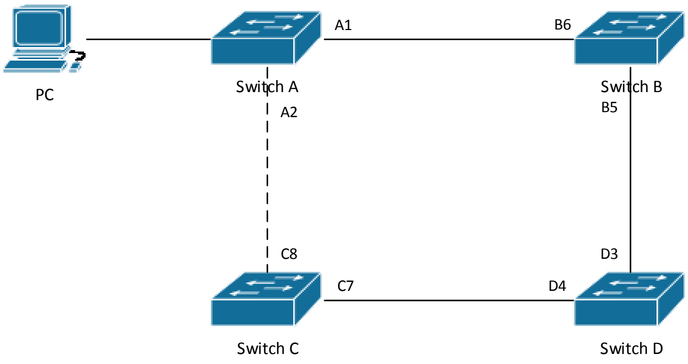


Figure 52.1: ULSM using scene

Configuring ULSM on SwitchB can solve the above problems. The steps are: set port B5 as the uplink port of ULSM group, port B6 as the downlink port. When the link between SwitchB and SwitchD has the problem, both the downlink port B6 and the state of ULSM group are down. It causes Switch A on which ULPP is configured to process uplink switchover and avoid the data dropped.

52.2 ULSM Configuration Task List

1. Create ULSM group globally
2. Configure ULSM group
3. Show and debug the relating information of ULSM

1. Create ULSM group globally

Command	Explanation
Global mode	
ulsm group <group-id> no ulsm group <group-id>	Configure and delete ULSM group globally.

2. Configure ULSM group

Command	Explanation
Port mode	

ulsm group <group-id> { uplink | downlink }
no ulsm group <group-id> { uplink | downlink }
	Configure the uplink/downlink port of ULSM group, the no command deletes the uplink/downlink port.

3. Show and debug the relating information of ULSM

Command	Explanation
Admin mode	
show ulsm group [group-id]	Show the configuration information of ULSM group.
debug ulsm event no debug ulsm event	Show the event information of ULSM, the no operation disables the shown information.

52.3 ULSM Typical Example

The above topology is the typical application environment which is used by ULSM and ULPP protocol.

ULSM is used to process the port state synchronization, its independent running is useless, so it usually associates with ULPP protocol to use. In the topology, SwitchA enables ULPP protocol, it is used to switch the uplink. SwitchB and SwitchC enable ULSM protocol to monitor whether the uplink is down. If it is down, then ULSM will execute the down operation for the downlink port to shutdown it, so ULPP protocol of Swtich A executes the relative operation of the uplink switchover.

SwitchA configuration task list:

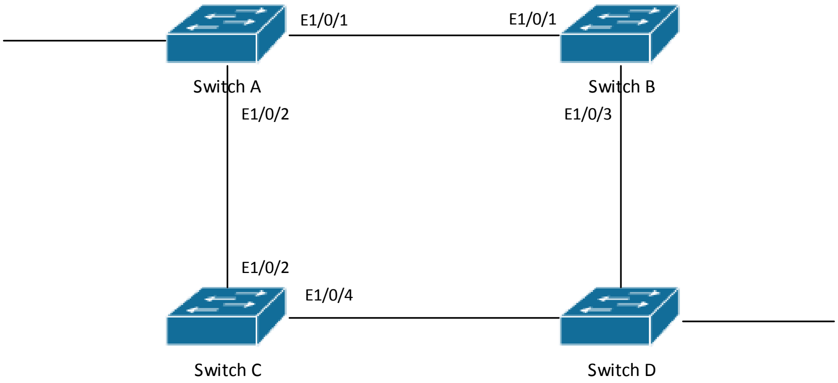


Figure 52.2: ULSM typical example

```
Switch(Config)#spanning-tree mst configuration
Switch(Config-Mstp-Region)#instance 1 vlan 1
Switch(Config-Mstp-Region)#exit
Switch(Config)#ulpp group 1
Switch(ulpp-group-1)#protect vlan-reference-instance 1
Switch(ulpp-group-1)#exit
Switch(Config)#interface ethernet 1/0/1
Switch(config-If-Ethernet1/0/1)# ulpp group 1 master
Switch(config-If-Ethernet1/0/1)#exit
Switch(Config)#interface Ethernet 1/0/2
Switch(config-If-Ethernet1/0/2)# ulpp group 1 slave
Switch(config-If-Ethernet1/0/2)#exit
```

SwitchB configuration task list:

```
Switch(Config)#ulsm group 1
Switch(Config)#interface ethernet 1/0/1
Switch(config-If-Ethernet1/0/1)#ulsm group 1 downlink
Switch(config-If-Ethernet1/0/1)#exit
Switch(Config)#interface ethernet 1/0/3
Switch(config-If-Ethernet1/0/3)#ulsm group 1 uplink
Switch(config-If-Ethernet1/0/3)#exit
```

SwitchC configuration task list:

```
Switch(Config)#ulsm group 1
Switch(Config)#interface ethernet 1/0/2
Switch(config-If-Ethernet1/0/2)#ulsm group 1 downlink
Switch(config-If-Ethernet1/0/2)#exit
Switch(Config)#interface ethernet 1/0/4
Switch(config-If-Ethernet1/0/4)#ulsm group 1 uplink
Switch(config-If-Ethernet1/0/4)#exit
```

52.4 ULSM Troubleshooting

With the normal configuration, if the downlink port does not responds the down event of the uplink port, please enable the debug function of ULSM, copy the debug information of 3 minutes and the configuration information, and send them to our technical service center.

Part XI

Flow Monitor Configuration

Chapter 53

Mirror Configuration

53.1 Introduction to Mirror

Mirror functions include port mirror function, CPU mirror function, flow mirror function.

Port mirror 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 a RMON monitor will be connected at mirror destination port to monitor and manage the network, and diagnose the problems in the network.

CPU mirror function means that the switch exactly copies the data frames received or sent by the CPU to a port.

Flow mirror function means that the switch exactly copies the data frames received or by the specified rule of a port to another port. The flow mirror will take effect only the specified rule is permit.

A chassis switch supports at most 4 mirror destination ports, each boardcard allows a source or destination port of a mirror session. At present, each box switch can set many mirror sessions. There is no limitation on mirror source ports, one port or several ports is allowed. When there are more than one source ports, they can be in the same VLAN or in different VLAN. The source port and destination port can be in different VLAN.

53.2 Mirror Configuration Task List

1. Specify mirror destination port

2. Specify mirror source port (CPU)

3. Specify flow mirror source

1. Specify mirror destination port

Command	Explanation
Global Mode	
monitor session <session> destination interface <interface-number> no monitor session <session> destination interface <interface-number>	Specifies mirror destination port; the no command deletes mirror destination source port.

2. **Specify mirror source port (CPU)**

Command	Explanation
Global Mode	

monitor session <session> source { interface <interface-list> | cpu [slot <slotnum>] } { rx | tx | both }
no monitor session <session> source { interface <interface-list> | cpu [slot <slotnum>] }
	Specifies mirror source port; the no command deletes mirror source port.

3. **Specify flow mirror source**

Command	Explanation
Global Mode	
monitor session <session> source { interface <interface-list> } access-group <num> { rx | tx | both } no monitor session <session> source { interface <interface-list> } access-group <num>	Specifies flow mirror source port and apply rule; the no command deletes flow mirror source port.

53.3 Mirror Examples

1. Example:

The requirement of the configurations is shown as below: to monitor at interface 1 the data frames sent out by interface 9 and received from interface 7, sent and received by CPU, and the data frames received by interface 15 and matched by rule 120(The source IP address is 1.2.3.4 and the destination IP address is 5.6.7.8).

Configuration guidelines:

1. Configure interface 1 to be a mirror destination interface.
2. Configure the interface 7 ingress and interface 9 egress to be mirrored source.
3. Configure the CPU as one of the source.
4. Configure access list 120.
5. Configure access 120 to binding interface 15 ingress.

Configuration procedure is as follows:

```
Switch(config)#monitor session 4 destination interface ethernet 1/0/1
Switch(config)#monitor session 4 source interface ethernet 1/0/7 rx
Switch(config)#monitor session 4 source interface ethernet 1/0/9 tx
Switch(config)#monitor session 4 source cpu
Switch(config)#access-list 120 permit tcp 1.2.3.4 0.0.0.255 5.6.7.8 0.0.0.255
Switch(config)#monitor session 4 source interface ethernet 1/0/15 access-list 120 rx
```

53.4 Device Mirror Troubleshooting

If problems occur on configuring port mirroring, please check the following first for causes:

- Whether the mirror destination port is a member of a TRUNK group or not, if yes, modify the TRUNK group.
- If the throughput of mirror destination port is smaller than the total throughput of mirror source port(s), the destination port will not be able to duplicate all source port traffic; please decrease the number of source ports, duplicate traffic for one direction only or choose a port with greater throughput as the destination port. Mirror destination port can not be pulled into Isolate vlan, or will affect mirror between VLAN.

Chapter 54

sFlow Configuration

54.1 Introduction to sFlow

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 according 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.

54.2 sFlow Configuration Task List

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

8. **Configure the analyzer used by sFlow**

Command	Explanation
Global Mode	
sflow analyzer sflowtrend no sflow analyzer sflowtrend	Configure the analyzer used by sFlow, the **no** command deletes the analyzer.

54.3 sFlow Examples

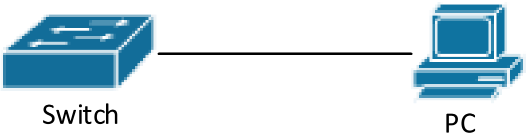


Figure 54.1: sFlow configuration topology

As shown in the figure, sFlow sampling is enabled on the port 1/1 and 1/2 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 SwitchA connected with PC is 192.168.1.100. A loopback interface with the address of 10.1.144.2 is configured on the SwitchA. sFlow configuration is as follows:

Configuration procedure is as follows:

```
Switch#config
Switch(config)#sflow agent-address 10.1.144.2
Switch(config)#sflow destination 192.168.1.200
Switch(config)#sflow priority 1
Switch(config)#interface ethernet1/1
Switch(Config-If-Ethernet1/1)#sflow rate input 10000
Switch(Config-If-Ethernet1/1)#sflow rate output 10000
Switch(Config-If-Ethernet1/1)#sflow counter-interval 20
Switch(Config-If-Ethernet1/1)#exit
Switch(config)#interface ethernet1/2
Switch(Config-If-Ethernet1/2)#sflow rate input 20000
Switch(Config-If-Ethernet1/2)#sflow rate output 20000
Switch(Config-If-Ethernet1/2)#sflow counter-interval 40
```

54.4 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

Part XII

Network Time Management Configuration

Chapter 55

SNTP Configuration

55.1 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 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.

Switch implements SNTPv4 and supports SNTP client unicast as described in RFC2030; SNTP client multicast and unicast are not supported, nor is the SNTP server function.

55.2 Typical Examples of SNTP Configuration

All 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 switch and the two SNTP/NTP servers.

Example: Assume the IP addresses of the SNTP/NTP servers are 10.1.1.1 and 20.1.1.1, respectively, and SNTP/NTP server function (such as NTP master) is enabled, then configurations for any switch should like the following:

```
Switch(config)#sntp server 10.1.1.1
```

Chapter 56

NTP Function Configuration

56.1 Introduction to 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.

56.2 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. To configure the request packet sending interval of ntp client
10. Display information
11. Debug

1. To enable NTP function

Command	Explanation
Global mode	
ntp enable ntp disable	To enable or disable NTP function.

2. To configure NTP server function

Command	Explanation
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	Explanation
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	Explanation
Global mode	
clock timezone WORD { add | subtract } <0-23> [<0-59>] no clock timezone WORD	This command configures timezone in global mode, the no command deletes the configured timezone.

5. To configure NTP access control list

Command	Explanation
Global mode	
[no] ntp access-group server <acl>	To (un)configure NTP server access control list.

6. To configure NTP authentication

Command	Explanation
Global mode	
[no] ntp authenticate	To enable/disable NTP authentication function.
ntp authentication-key <key-id> md5 <value> no ntp authentication-key <key-id>	To configure authentication key for NTP authentication.
[no] ntp trusted-key <key-id>	To (un)configure trusted key.

7. To specified some interface as NTP broadcast/multicast client interface

Command	Explanation
VLAN Configuration Mode	
[no] ntp broadcast client	To (un)configure specified interface to receive NTP broadcast packets.
[no] ntp multicast client	To (un)configure specified interface to receive NTP multicast packets.
[no] ntp ipv6 multicast client	To (un)configure specified interface to receive IPv6 NTP multicast packets.

8. To configure some interface can't receive NTP packets

Command	Explanation
VLAN Configuration Mode	
[no] ntp disable	To enable/disable the NTP function.

9. To configure the request packet sending interval of ntp client

Command	Explanation
Global mode	
[no] ntp syn-interval <1-3600>	(un)Configure the request packet sending interval of ntp client as 1s-3600s. The no command recovers to be the default value of 64s.

10. Display information

Command	Explanation
Admin Mode	
show ntp status	To display the state of time synchronize.
show ntp session [<ip-address> | <ipv6-address>]	To display the information of NTP session.

11. Debug

Command	Explanation
Admin Mode	
[no] debug ntp authentication	To enable/disable debug switch of NTP authentication.
[no] debug ntp packets [send | receive]	To enable/disable debug switch of NTP packet information.
[no] debug ntp adjust	To enable/disable debug switch of time update information.
[no] debug ntp sync	To enable/disable debug switch of time synchronize information.
[no] debug ntp events	To enable/disable debug switch of NTP event information.

56.3 Typical Examples 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 (Switch A and Switch B are the switch or route which support NTP server):

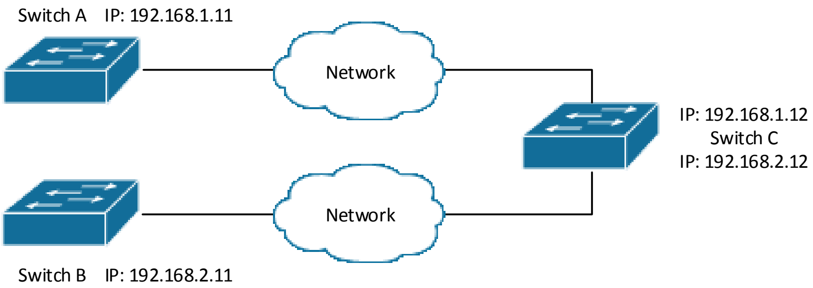


Figure 56.1: Typical NTP Example

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 switches 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
```

56.4 NTP Function Troubleshooting

In configuration procedures, if there is error occurred, the system can give out the debug 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 service center.

Chapter 57

Summer Time Configuration

57.1 Introduction to Summer Time

Summer time is also called daylight saving time, it is a time system for saving energy sources. In summer the time is advanced 1 hour to keep early hours, reduce the lighting, so as to save electrolighting. The rule that adopt summer time is different in each country. At present, almost 110 countries implement summer time.

Compare with the standard time, usually set summer time 1 hour late, for example, when summer time is implementing, 10:00 am of the standard time is considered 11:00 am of summer time.

57.2 Summer Time Configuration Task Sequence

1. Configure absolute or recurrent time range of summer time

Command	Explanation
Global mode	
clock summer-time <word> absolute <HH:MM> <YYYY.MM.DD> <HH:MM> <YYYY.MM.DD> [<offset>] no clock summer-time	Set absolute time range of summer time, start and end summer time is configured with specified year.
clock summer-time <word> recurring <HH:MM> <MM.DD> <HH:MM> <MM.DD> [<offset>] no clock summer-time	Set recurrent time range of summer time, every year the summer time begins from the start time and end at the end time.
clock summer-time <word> recurring <HH:MM> <week> <day> <month> <HH:MM> <week> <day> <month> [<offset>] no clock summer-time	Set recurrent time range of summer time, every year the summer time begins from the start time and end at the end time.

57.3 Examples of Summer Time

Example 1:

The configuration requirement in the following: The summer time from 23:00 on April 1th, 2012 to 00:00 on October 1th, 2012, clock offset as 1 hour, and summer time is named as 2012.

Configuration procedure is as follows:

```
Switch(config)#clock summer-time 2012 absolute 23:00 2012.4.1 00:00 2012.10.1
```

Example 2:

The configuration requirement in the following: The summer time from 23:00 on the first Saturday of April to 00:00 on the last Sunday of October year after year, clock offset as 2 hours, and summer time is named as time_travel.

Configuration procedure is as follows:

```
Switch(config)#clock summer-time time_travel recurring 23:00 first sat apr 00:00
                        last sun oct 120
```

57.4 Summer Time Troubleshooting

If there is any problem happens when using summer time, please check whether the problem is caused by the following reasons:

- Check whether command mode in global mode
- Check whether system clock is correct

Part XIII

Debugging and Diagnosis

Chapter 58

Monitor 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. Switch provides various debug commands including ping, telnet, show and debug, etc. to help the users to check system configuration, operating status and locate problem causes.

58.1 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.

58.2 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.

58.3 Traceroute

Traceroute command is for testing the gateways through which the data packets travel 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.

Traceroute Options and explanations of the parameters of the Traceroute command please refer to traceroute command chapter in the command manual.

58.4 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.

58.5 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.

Command	Explanation
Admin Mode	
show debugging	Display the debugging state.
show flash	Display the files and the sizes saved in the flash.
show history	Display the recent user input history command.
show history all-users [detail]	Show the recent command history of all users. Use clear history all-users command to clear the command history of all users saved by the system, the max history number can be set by history all-users max-length command.
show memory	Display content in specified memory area.
show running-config	Display the switch parameter configuration validating at current operation state.
show running-config current-mode	Show the configuration under the current mode.
show startup-config	Display the switch parameter configuration written in the Flash Memory at current operation state, which is normally the configuration file applied in next time the switch starts up.

show switchport interface [ethernet <IFNAME>]	Display the VLAN port mode and the belonging VLAN number of the switch as well as the Trunk port information.
show tcp show tcp ipv6	Display the TCP connection status established currently on the switch.
show udp show udp ipv6	Display the UDP connection status established currently on the switch.
show telnet login	Display the information of the Telnet client which currently establishes a Telnet connection with the switch.
show tech-support	Display the operation information and the state of each task running on the switch. It is used by the technicians to diagnose whether the switch operates properly.
show version	Display the version of the switch.

58.6 Debug

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

58.7 System log

58.7.1 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.

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.

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.

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.

58.7.2 System Log Configuration

System Log Configuration Task Sequence:

1. Display and clear log buffer zone
2. Configure the log host output channel
3. Enable/disable the log executed-commands
4. Display the log source
5. Display executed-commands state

1. Display and clear log buffer zone

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

2. Configure the log host output channel

Command	Explanation
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.

logging loghost sequence-number no logging loghost sequence-number	Add the loghost sequence-number for the log, the no command does not include the loghost sequence-number.

3. **Enable/disable the log executed-commands**

Command	Explanation
Global Mode	
logging executed-commands { enable | disable }	Enable or disable the logging executed-commands.

4. **Display the log source**

Command	Explanation
Admin and Config Mode	
show logging source mstp	Show the log information source of MSTP module.

5. **Display executed-commands state**

Command	Explanation
Admin Mode	
show logging executed-commands state	Show the state of logging executed-commands.

58.7.3 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
```

Chapter 59

Reload Switch after Specified Time

59.1 Introduce to Reload Switch after Specifid Time

Reload switch after specified 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.

59.2 Reload Switch after Specifid Time Task List

1. Reload switch after specified time

Command	Explanation
Admin Mode	
reload after { [<HH:MM:SS>] [days <days>] }	Reload the switch after a specified time period.
reload cancel	Cancel the specified time period to reload the switch.

Chapter 60

Debugging and Diagnosis for Packets Received and Sent by CPU

60.1 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.

60.2 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 command sets 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 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 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.
Admin Mode	
show cpu-rx protocol [<protocol-type>]	Show the information of the CPU received packets of the protocol type.

debug driver { receive | send } [interface { <interface-name> | all }] [protocol { <protocol-type> | discard | all }] [detail]	Turn on the showing of the CPU receiving or sending packet informations.
no debug driver { receive | send }	Turn off the showing of the CPU receiving or sending packet informations.