OLT Management Configuration Manual

INDEX

1. ACCESSING SWITCH

This chapter is the basic knowledge for system management, including:

- Command line interface
- Command syntax comprehension
- Syntax help
- History command
- Symbols in command
- Parameter in command
- User management
- Ways for switch management

1.1. Command Line Interface

System provides a series of configuration command and command line interface. User can configure and manage switch by command line. Command line interface has the features as following:

- Local configuration by Console interface
- Local or remote configuration by TelNet
- Configure command classification protection to guarantee unauthorized user illegal accessing.
- Input "?"at any moment to obtain help information
- Provide such network test command as ping to diagnose network fault
- Provide FTP, TFTP, Xmodem to download and upload files
- Keywords partial matching searching is adopted by command line convertor for user to input non-conflicting key words, such as: interface command can only input "interf"

1.1.1. Command Line Configuration Mode

System command line adopts classification protection to prevent illegal accessing of unauthorized user. Each command mode is for different configuration with the connection and distinction. For example, after successful accessing, user of all level can enter common user mode which can only see the system operation information; administrator can input "enable" to enter privileged mode; input "configure terminal" to enter global configuration mode from privileged mode which can enter related configuration mode according to inputting different configuration command. For example:

Command line provides command mode as following:

- User mode
- Privileged mode
- Global configuration mode
- Interface configuration mode
- VLAN configuration mode
- AAA configuration mode

- RADIUS configuration mode
- Domain configuration mode
- VLAN interface configuration mode
- superVLAN interface configuration mode
- RIP configuration mode
- OSPF configuration mode
- PIM configuration mode
- GN.Link configuration mode

The function and details of each command mode are as following:

Table 1.1 Command Line Configuration Mode

Command line mode	**Function**	**Prompt character**	**Command for entering**	**Command for exiting**
User mode	See switch operation information	OLT>	Connect with switch after inputting user name and password	**exit** disconnect with switch
Privileged mode	See switch operation information and manage system	OLT#	Input **enable** in user mode	**exit** return to user mode **quit** disconnect with switch
Global configuration mode	Configure global parameter	OLT(config)#	Input **configure terminal** in privileged mode	**exit**、**end** return to privileged mode **quit** disconnect with switch
Interface configuration mode	Configure interface parameter	OLT(config- if-ethernet-0/1)#	Input “interface Ethernet 0/1” in global configuration mode, interface configuration can enter other interface mode and VLAN configuration mode without inputting “exit”.	**end** return to privileged mode **exit** return to global configuration mode **quit** disconnect with switch
VLAN configuration mode	Configure VLAN parameter	OLT(config- if-VLAN)#	Input “**VLAN 2”** in global configuration mode, VLAN configuration mode can enter other VLAN mode and interface configuration mode without inputting “exit”.	
AAA configuration mode	Create domain	OLT(config-aaa)#	Input “aaa” in global configuration mode	
RADIUS configuration	Configure RADIUS server parameter	OLT(config-aaa-radius-	Input “radius host default” in AAA configuration mode	**end** return to privileged mode

mode		default)#		
Domain configuration mode	Configure domain parameter	OLT(config-aaa-domain-test.com)#	Input “domain test.com” in AAA configuration mode	**exit** return to AAA configuration mode **quit** disconnect with switch
VLAN Interface mode	Configure VLAN L3 interface	OLT(config- if-VLANInterface- 2)#	Input “interface VLAN-interface 2”in global configuration mode	**end** return to privileged mode **exit** return to global configuration mode **quit** disconnect with switch
SuperVLAN Interface mode	Configure SuperVLAN L3 interface	OLT(config- if-superVLANInterface-1)#	Input “interface superVLAN- interface 1” in global configuration mode	**end** return to privileged mode **exit** return to global configuration mode **quit** disconnect with switch
RIP configuration mode	Configure RIP parameter	OLT(config-router-rip)#	Input “route rip” in global configuration mode	**end** return to privileged mode **exit** return to global configuration mode **quit** disconnect with switch
OSPF configuration mode	Configure OSPF parameter	OLT(config-router-ospf#	Input “route ospf” in global configuration mode	**end** return to privileged mode **exit** return to global configuration mode **quit** disconnect with switch

1.1.2 Command Syntax Comprehension

This chapter describes the steps needed for command configuration. Please read this section and related detail information of command line interface in the following sections carefully.

The logging in identity verification of the system console of this switch is used to verify the identity of the operating user. It permits and refuses the logging in by matching recognizing user name and password.

Step 1: Following are showed when entering command line interface,

Username(1-32 chars):

Please input user name, press Enter button, and then the prompt is as following:
Password (1-16 chars)：

Input password. If it is correct, enter the user mode with the following prompt:

OLT>

In switch system, there are 2 different privileges. One is administrator, and the other is common user. Common user only can see the configuration information of switch without right to modify it but administrator can manage and configure the switch by specified command.

Logging in as administrator can enter privileged mode from user mode.

OLT>enable

Step 2: Input command

Skip to step 3, if the command needs input the parameter. Continue this step if the command need input the parameter.

If the command needs a parameter, please input it. When inputting a parameter, keyword is needed.

The parameter of the command is specified which is the number or character string or IP address in a certain range. Input "?" when you are uncomprehending, and input the correct keyword according to the prompt. Keyword is what is to be operated in command.

If more than one parameter are needed, please input keywords and each parameter in turn according to the prompt until "<enter>"is showed in prompt to press enter button.

Step 3: Press enter button after inputting complete command.

For example:

！User need not input parameter

OLT#quit

"quit" is a command without parameter. The name of the command is quit. Press enter button after inputting it to execute this command.

！User need input parameter

OLT(config)#VLAN 3

"VLAN 3"is a command with parameter and keyword, VLAN of which is command keyword and 3 of which is parameter.

1.1.3 Syntax Help

There is built-in syntax help in command line interface. If you are not sure about the syntax of some command, obtain all command and its simple description of the current mode by inputting "?" or help command; list all keywords beginning with the current character string by inputting "?" closely after the command character string; input "?" after space, if "?" is in the same location of the keyword, all keywords and its simple description will be listed, if "?"is in the same location of parameter, all the parameter description will be listed, and you can continue to input command according to the prompt until the prompt command is "＜enter＞" to press enter button to execute command.

For example:

1． Directly input "?"in privileged mode

OLT#?

```
System mode commands:
cls  clear screen
help description of the interactive help
ping ping command
quit disconnect from switch and quit
……
```

2． Input “?” closely after keyword

```
OLT(config)#interf?
interface
```

3． Input “?”after command character string and space

```
OLT(config)#spanning-tree ? forward-
time config switch delaytime hello-
time   config switch hellotime
max-age      config switch max agingtime
priority     config switch priority
<enter>      The command end.
```

4． Parameter range and form

```
OLT(config)#spanning-tree forward-time ?
INTEGER<4-30> switch delaytime: <4-30>(second)
```

5. Command line end prompt

```
OLT(config)#spanning-tree ?
<enter> The command end.
```

1.1.4 History command

Command line interface will save history command inputted by user automatically so that user can invoke history command saved by command line interface and re-execute it. At most 100 history commands can be saved by command line interface for each user. Input “Ctrl+P” to access last command, and “Ctrl+N” for next command.

1.1.5 Symbols in command

There are all kinds of symbols in command syntax which is not a part of command but used to describe how to input this command. Table 1-2 makes a brief description of these symbols.

Table 1.2 Description of symbols

Symbols	Description
Vertical bars |	Vertical bars (|) means coordinate, together using with braces ({ }) and square brackets ([ ]).
Square brackets [ ]	Square brackets ([ ]) mean optional elements. For example： **show VLAN** [*VLAN-id*]
Braces { }	Braces ({ }) group required choices, and vertical bars (|) separate the alternative elements. Braces and vertical bars within square brackets ([{ | }]) mean a required choice within an optional element.

1.1.6 Command Parameter Categories

There are 5 categories command parameter as following:

- scale

Two numerical value linked by hyphen in angle brackets (< >) means this parameter is some number in the range of those two numbers.

For example: INTEGER<1-10> means user can input any integer between 1 and 10 (include 1 and 10), such as 8 is a valid number.

- IP address

The prompt which is in the form of A.B.C.D. means the parameter is an IP address. A valid IP address is needed to input.

For example: 192.168.0.100 is a valid IP address.

- MAC address

The prompt which is in the form of H:H:H:H:H:H means the parameter is a MAC address. A valid MAC address is needed to input. If a multicast MAC address is needed, there will be related prompt.

For example: 01:02:03:04:05:06 is a valid MAC address.

- Interface list

The prompt of interface list is STRING<3-4>. Interface parameter interface-num is in the form of interface-type + interface-number. Interface-type is Ethernet and interface-number is slot-num/port-num, in which slot-num is in the range of 0 to 2, and port-num is in the range of 1 to 24. Seriate interfaces with the same type can be linked by to keyword, but the port number to the right of the to keyword must be larger than the one to the left of the keyword, and this argument only can be repeated for up to 3 times. The special declaration of interface parameter interface list will be displayed in the command.

For example: show spanning-tree interface ethernet 0/1 ethernet 0/3 to ethernet 0/5 means displaying spanning-tree information of interface ethernet 0/1 ethernet 0/3 to ethernet 0/5

- Character string

The prompt which is in the form of STRING<3-4> means the parameter is a character string which is in the form of 1 to 19 characters. “?”can be inputted to display the concrete command description.

1.2. User management

There are 2 privileges for user:

- ADMIN administrator
- NORMAL normal user

Normal user can only enter user mode not privileged mode after logging in, so that he can only see system information but not to configure it. Administrator has the right to enter all modes, and query and configure all parameters.

1.2.1 System default user name

There is a system default built-in user name called admin, and the initial password is 123456. It is suggested modifying password when logging in switch for the first time to avoid leaking it. This user name cannot be deleted and the privilege cannot be modified either. It also possesses the right to manage other users. Please remember your modified password.

1.2.2 Add user

Log in with the identity of system administrator admin to enter privileged mode, then global configuration mode by using username command. Input user name, user’s privilege, password to add new user according to system prompt or by using the following command.

username username [privilege level] { password encryption-type password }

username：User name of new users and existed users ranges from 1 to 32 printable characters excluding such wildcards as '/'、':'、'*'、'?'、'\\'、'<'、'>'、'|'、'"' etc.

privilege：Privilege of new user ranges from 0 to 15. 0 to 1 means user while 2 to 15 means administrator.

encryption-type: the value of it is 0 or 7. 0 means non-encryption and 7 means encryption (It is not supported now).

password：Log in password for new user and modified password of the existed user ranges from 1 to 16 characters or numbers.

If the privilege doesn’t configure, the default privilege is ordinary user. At most 8 users are supported.

Caution: User name supports case insensitivity while password doesn’t support case sensitivity. Example：

！ Add a new administrator “nic”， configure privilege to be 3，and password to be 1234

```
OLT(config)#username nic privilege 3 password 0 1234
```

1.2.3 Modify password

In global configuration mode, system administrator admin can use the following command to modify password of his or other user. Other user can only modify his own password.

username change-password

For example：

！Modify the password of user “nic” to be 123456

```
OLT(config)#username  change-password
please input you login password : ******
please input username :nic
Please input user new password :******
Please input user comfirm password :******
change user nic password success.
```

1.2.4 Modify privilege

In global configuration mode, only administrator admin can use following command to modify the privilege of other user.

username username [privilege level] { password encryption-type password }

username：User name of new users and existed users ranges from 1 to 32 printable characters excluding such wildcards as '/'、':'、'*'、'?'、'\\'、'<'、'>'、'|'、'"' etc.

privilege：Privilege of new user or the modified privilege of existed user ranges from 0 to 15. 0 to 1 means user while 2 to 15 means administrator. Caution: the privilege of administrator cannot be modified.

encryption-type: the value of it is 0 or 7. 0 means non-encryption and 7 means encryption (It is not supported now).

password：Log in password for new user and modified password of the existed user ranges from 1 to 16 characters or numbers.

If inputting nothing to modify the privilege of existed user, the privilege doesn’t modify.

Caution: User name supports case insensitivity while password doesn’t support case sensitivity.

For example:

！Modify the privilege of administrator “nic” to be 1，and password to be 1234

```
OLT(config)#username nic privilege 1 password 0 1234
```

1.2.5 Remove user name

System administrator admin can use following command to remove user name in global configuration mode

```
no username username
```

Username is the user name to be deleted.

For example：

```
！Remove user nic
OLT(config)#no username nic
```

1.2.6 View system user information

View user list, and input show username command or show usename [username] command in any configuration mode to display information of all users.

For example：

```
！Display information of user nic
OLT(config)#show username nic
```

1.3. Remote authentication of administrator

After authentication, user’s default privilege is normal user. Only when there is Service-Type field in authentication accepting packet the value of which is Administrative, user’s privilege is administrator.

⚠ Caution：Admin user only supports local database authentication

1.3.1 Start RADIUS remote authentication

Use following command in global configuration mode:

```
muser { local | { radius radiusname { pap | chap } [ local ] } }
```

It can be configured to authenticate only by RADIUS remote authentication or by local database authentication after no response of RADIUS server caused by failing connection.

1.3.2 Display authentication configuration

Use following command to display authentication configuration.

```
show muser
```

1.4. Ways of managing switch

System provides following ways of management：

- By hyper terminal accessing command-line interface（CLI）
- By telnet managing system
- By SNMP managing software management system

- By Web browser，such as Internet Explorer managing system

1.4.1 Manage switch by hyper terminal

Use hyper terminal (or simulation terminal software) connect to Console to access system command line interface (CLI) by hyper terminal.

Configuration: Open “file” -> “attribute” menu, popping up a window. Enter configuration to restore it to default value, and click “setting” and then choose “auto-detect” in the pulldown list of “terminal simulation” and click *ok+. After the successful connection and seeing logging in interface of operation system in terminal, configure switch by command line interface. The steps are as following:

Step 1: Connect switch Console with computer serial port;

Step 2: After the switch power on and system successful booting, logging in prompt can be seen:

```
Username(1-32 chars):
```

Step 3: Input correct user name, press enter button, then input corresponding password. If it is the first time to logging in switch, use default user name admin and its password 123456 to log in and operate as system administrator. If your own user name and password exist, log in with your own user name and password;

Step 4: After successfully logging in, following information is displayed:

```
OLT>
```

Step 5: As administrator, after entering privileged mode, use copy running-config startup-config command to save configuration.

```
OLT#copy running-config startup-config
```

When following information is displayed:

```
Startup config in flash will be updated, are you sure(y/n)? [n]y
Building, please wait...
```

It means system is saving configuration. Please wait, then the prompt is:

```
Build successfully.
```

It means current configuration is saved successfully.

Following information is displayed when system booting:

```
Ready to load startup-config, press ENTER to run or CTRL+C to cancel:
```

Press enter button to make saved configuration be effective, and press CTRL+C to restore system default configuration.

Step 6: Administrator can use stop connection when overtime, while normal user can use this function in user mode. Input timeout command to configure the overtime of user’s logging in to be 20 minutes. And use no timeout command to configure overtime to be non-over timing.

Step 7: Input following command after finishing operation to switch:

```
OLT#quit
```

It is used to exit user interface.

1.4.2 Manage switch by telnet

Step 1: Establish configuration environment by connecting computer by network to switch interface;

Step 2: Run Telnet program in computer;

Step 3: After switch is power on, input switch IP address to connect to switch, and input configured logging in password according to the prompt, then the command line prompt is displayed （such as OLT>）. It will be disconnected after 1 minute when there is not any input before successfully logging in or wrong inputting of user name and password for 5 times. If there is such prompt as “Sorry，session limit reached.”, please connect later (At most 2 telnet users are allowed to log in at the same time.);

Step 4: Use related command to configure switch system parameter or view switch operation. If you want to enter privileged mode, user must possess the privilege of administrator. If you need any help, please input “?”at any moment. For concrete command, please refer to following chapters.

Step 5: If you want to exit telnet, use quit or exit command to exit in user mode, and quit command to exit in other mode. Administrator can use stop username command in privileged mode to exit logging in.

2. PORT CONFIGURATION

2.1. Port configuration introduction

System can provide 24 10/100Base-T Ethernet interfaces, 2 100Base-TX Ethernet interfaces and a Console interface. Ethernet interface can work in half duplex and full duplex mode, and can negotiate other working mode and speed rate with other network devices to option the best working mode and speed rate automatically to predigest system configuration and management.

2.2. Port Configuration

2.2.1 Port related configuration

Configuring parameter of port should enter port configuration mode first. For fast and easy configuration, system provides interface to configure a group of ports and input command once can configure all the ports in the group. This group dynamically existed and user can specify the member in it.all the command used in interface configuration mode can be used here. For a configuration command, it will alarm the failured port and will not stop the following configuration.

Interface configuration list is as following:

- Enter interface configuration mode
- Enable /disable specified interface
- Configure duplex mode and speed rate
- Configure interface privilege
- Configure interface limited speed
- Configure type of receiving frame
- Configure interface type
- Configure default VLAN ID of trunk port
- Add access port to specified VLAN
- Display interface information

2.2.2 Enter interface configuration mode

Enter interface configuration mode before configuration.

Configure as following in global configuration mode:

- Enter interface configuration mode

interface { interface_type interface_num | interface_name }

interface_type：type of interface, for example the type of ethernet interface is ethernet

Interface-num is Ethernet interface number which is in the form of device-num/slot-num/port-num, in which device-num is in the range of 0 to 7, slot-num is in the range of 0 to 2, and port-num is in the range of 1 to 48 interface_name：the abbreviation of interface type(such as Ethernet port can be Ethernet or any character from e) and port number (the same as interface-num), such as Ethernet port 0/8 can be e0/8 or ethernet 0/8.

2.2.3 Enter interface configuration mode

- Enter interface configuration mode

```
interface range interface-list
```

Example：

```
！Enter interface group configuration mode which includes Ethernet 1 to 3
OLT(config)#interface range ethernet 0/1 to e 0/3
```

2.2.4 Enable/disable specified interface

After system booting, all the interfaces are defaulted to be enable, and each interface can be configured according to real situation.

Use following commands to enable/disable an Ethernet port.

```
shutdown
no shutdown
```

Shutdown means disable a port, while no shutdown means enable a port.

For example：

```
！Enable Ethernet interface 1
OLT(config-if-ethernet-0/1)#no shutdown
！Disable Ethernet interface 1
OLT(config-if-ethernet-0/1)#shutdown
```

When interface is shutdown, the physical link is working for diagnosis.

2.2.5 Configure interface duplex mode and speed rate

100 BASE TX supports the speed of 10Mbps and 100Mbps, while 100 BASE FX supports the speed of 100Mbps. 1000 BASE TX supports the speed of 10Mbps, 100Mbps and 1000Mbps, while 1000 BASE FX supports the speed of 1000Mbps. 100 BASE TX and 1000 BASE TX support the duplex mode of half, full duplex and auto-negotiation mode. 100 BASE FX and 1000 Base FX only support the duplex mode of full duplex. By default, 100 Base FX is in the mode of 100M and full duplex, and other interfaces are auto-negotiation. User can configure the working mode by himself. Use speed command to configure the speed and duplex command to configure duplex.

- Command form in interface mode

```
speed { 10 | 10auto | 100 | 100 auto | 1000 | 1000 auto | auto }
no speed
```

duplex { auto | full | half }

no duplex

For example：

！Configure the speed of Ethernet 0/1 to 100Mbps and duplex mode to be full duplex

```
OLT(config-if-ethernet-0/1)#speed 100
OLT(config-if-ethernet-0/1)#duplex full
```

In system, one of the value of speed and duplex is configured to be auto，the other will be auto.

2.2.6 Interface Prioruty Configuration

There are 8 priorities from 0 to 7, and the default interface priority is 0. The larger the priority value is, the higher the priority is. And the packet with the higher priority will be quickly handled. If there are too much packet to be handled in some interface or the packet is urgent to be handled, priority of this interface can be configured to be high-priority.

Use following command in interface configuration mode:

Configure priority of Ethernet 0/5 to be 1

```
OLT(config-if-ethernet-0/5)#priority 1
```

Restore the default priority of Ethernet 0/5

```
OLT(config-if-ethernet-0/5)#no priority
```

2.2.7 Interface description configuration

Use following command to describe interface to distinguish each interface from others. Configure it in interface configuration mode.

description description-list

For example：

！Configure description string “nic” for the Ethernet 0/3

```
OLT(config-if-ethernet-0/3)#description nic
```

！Display description of Ethernet 0/3

```
OLT(config)#show description interface ethernet 0/3
```

2.2.8 Enable/disable VLAN filtration of receiving packet of interface

When enabling VLAN ingress filtration, received 802.1Q packet which doesn’t belong to the VLAN where the interface locates will be dropped. The packet will not be dropped if it is disabled.

Use this command in interface configuration mode.

ingress filtering

no ingress filtering

Example：

！Enable VLAN ingress filtration of e0/5

OLT(config-if-ethernet-0/5)#ingress filtering

！Disable VLAN ingress filtration of e0/5

OLT(config-if-ethernet-0/5)#no ingress filtering

2.2.9 Interface ingress acceptable-frame configuration

Configure ingress acceptable frame mode to be all types or only tagged.

Use following command in interface configuration mode to configure or cancel the restriction to ingress acceptable-frame:

ingress acceptable-frame { all | tagged }

no ingress acceptable-frame

For example：

！Configure Ethernet 0/5 only to receive tagged frame

OLT(config-if-ethernet-0/5)#ingress accetable-frame tagged

2.2.10 Enable/disable interface flow-control

If the port is crowded, it needs controlling to avoid congestion and data loss. Use flow-control command to control the flow. Use following command to enable/disable flow-control on current Ethernet port.

flow-control

no flow-control

For example:

！Enable flow control on Ethernet 0/5

OLT(config-if-ethernet-0/5)#flow-control

！Disable flow control on Ethernet 0/5

OLT(config-if-ethernet-0/5)#no flow-control

Use following command in any configuration mode to display interface flow-control:

show flow-control [interface-num]

For example：

！Display flow-control of Ethernet 0/5

OLT(config-if-ethernet-0/5)#show flow-control ethernet 0/5

2.2.11 Configure interface combo type

Use this command to configure interface combo type. E0/1 to e0/ are combo interfaces which can be configured. Combo type can be divided into TX and FX and it is defaulted to be TX. Configure it in inteface configuration mode：

- Configure interface combo type

combo { fiber | copper }

Example：

！Configure e0/1 to be TX

OLT(config-if-ethernet-0/1)#combo copper

2.2.12 Port mode configuration

Use this command to configure port mode. If a port configures to be a trunk port, the VLAN mode changes untagged into tagged, and if a port configures to be an access one, the VLAN mode changes tagged into untagged. Configure it in interface configuration mode:

- Configure port mode

switchport mode { trunk | access }

- Restore default port mode: access port

no switchport mode

For example:

！Configure Ethernet 0/1 to be trunk port

OLT(config-if-ethernet-0/1)#switchport mode trunk

2.2.13 Trunk allowed VLAN configuration

Use switchport trunk allowed VLAN command to add trunk port to specified VLAN. Use no switchport trunk allowed VLAN command to remove trunk port from specified VLAN.

- Add trunk port to specified VLAN

switchport trunk allowed VLAN { VLAN-list | all }

- Remove trunk port from specified VLAN

no switchport trunk allowed VLAN { VLAN-list |

all } For example：

！Add trunk ports Ethernet0/1 to VLAN 3, 4, 70 to 150

OLT(config-if-ethernet-0/1)# switchport trunk allowed VLAN 3,4, 70- 150

2.2.14 The default VLAN-id of trunk port configuration

Use switchport trunk native VLAN command to configure the default VLAN-id (pvid) of trunk port. When receiving untagged packet, it will be transferred to VLAN defaulted VLAN ID. Packet receiving and sending follow IEEE 802.1Q. Configure it in interface configuration:

- Configure default VLAN ID of trunk port

switchport trunk native VLAN VLAN-id

- Restore default VLAN ID of trunk port

no switchport trunk native

Caution: above configuration is effective to trunk port. By default, default VLAN ID is 1. If this port is not in VLAN 1, configuration fails.

2.2.15 Add access interface to specified VLAN

Use switchport access command to add access port to specified VLAN, and the default VLAN-ID is configured to be the specified VLAN. Configure it in interface configuration mode:

- Add current port to specified VLAN, and the default VLAN-ID is configured to be the specified VLAN

switchport access VLAN VLAN-id

- Remove current port from specified VLAN, if the default VLAN-id of the current port is the specified VLAN and this port also belongs to VLAN 1, the default VLAN-id of the current port restores to be 1, or the default VLAN ID will not be changed.

no switchport access VLAN VLAN-id

The precondition to use this command is the current port is access port and the VLAN to be added is not default VLAN 1.

2.2.16 Display interface information

Use show interface [interface-num] to display information of specified interface or all interfaces：

- Interface state (enable/disable)
- Connection
- Working mode (full duplex, half duplex or auto-negotiation)
- Default VLAN ID
- Interface priority
- Port mode (trunk/access port)

If no parameter is input in show interface [interface-num] command, information of all interfaces will be displayed.

Use show statistics dynamic interface to display statistics information and use show utilization interface to display port receiving and sending rate.

2.2.17 Display/ clear interface statistics information

Use show statistics interface [interface-num] command in any configuration mode to display information of specified interface or all interfaces：

- 64 Byte receiving
- 65 to 127 Byte packet number

- 128 to 255 Byte packet number
- 256 to 511 Byte packet number
- 512 to 1023 Byte packet number
- 1024 to 1518 Byte packet number
- Total received packet number
- Total received byte number
- Receiving direction dropping packet number
- Received unicast packet number
- Received multicast packet number
- Received broadcast packet number
- Received error packet number
- Received FCS error packet number
- Receiveddata symbolerror packet number
- Detected false carrier times
- Received extra small packet number（smaller than 64 byte）
- Received extra large packet number（larger than 1518 byte）
- Received flow control frame number
- Sent total packet number
- Sent total byte
- Sending direction dropping packet number
- Sent unicast packet number
- Sent multicast packet number
- Sent broadcast packet number
- Sent error packet number
- Delay sending packet number
- Collision times
- late collision times

Use clear interface [interface-num | slot-num] command in global configuration mode to clear information of specified interface or all interfaces in specified slot or all interfaces. Use clear interface command in interface configuration mode to clear information of current interface.

2.2.18 Enable local switching feature of Ethernet interface

In standard switching, packet cannot transmit from the interface it is in, but in some special cases, such as applying downlink WAP, this function is needed. Use this command to enable local switching feature of Ethernet interface. Use the no command to disable it.

local

no local

Example

！Enable local switching feature of e0/1

```
OLT(config-if-ethernet-0/1)#local
```

！Disable local switching feature of e0/5

OLT(config-if-ethernet-0/1)#no local

Display it in any configuration mode:

show local interface [ethernet|pon] [interface-num]

Example：

！Display local switching feature of e0/1

OLT(config-if-ethernet-0/1)#show local interface ethernet 0/1

2.3. Interface mirror

2.3.1 Brief introduction of interface mirror

System provides mirror based on interface, that is, copy packet in a or more specified interface to monitor interface to analyze and monitor packet. For example, copy packet of Ethernet 0/2 to specified monitor interface Ethernet 0/3 so that test and keep record by protocols linked by monitor interface Ethernet 0/3.

2.3.2 Interface mirror configuration

Interface Mirror configuration command includes:

- Configure mirror interface
- Configure monitored interface
- Display interface mirror

Configure mirror interface

Configure mirror destination interface in global configuration mode：

- Configure mirror interface

mirror destination-interface [ethernet|pon] interface-num

This command will cancel original mirror destination interface.

- Remove mirror interface

no mirror destination-interface [ethernet|pon] interface-num

For example:

！Configure Ethernet 0/1 to be mirror interface

OLT(config)# mirror destination-interface ethernet 0/1

Configure mirror source interface

Configure mirror source-interface of switch in global configuration mode:

- Configure mirror source-interface

mirror source-interface { interface-list | cpu } { both | egress | ingress } interface-list is in the form of interface-num [to interface-num], which can be repeated for 3 times. Cpu interface is in the form og character string “cpu”

both means mirroregress and ingress interfaces, egress means mirror interface egress and ingress means mirror interface ingress.

- Remove mirror source interface

no mirror source-interface { interface-list | cpu }

For example:

！Configure Ethernet 0/1 to Ethernet 0/12 to be mirror source interfaces

OLT(config)# mirror source-interface ethernet 0/1 to ethernet 0/12 both

！Remove Ethernet 0/10 to Ethernet 0/12 from mirror source interfaces

OLT(config)#no mirror source-interface ethernet 0/10 to ethernet 0/12

- Display interface mirror

Use show mirror command to display system configuration of current mirror interface, including monitor port and mirrored port list. Use this command in any configuration mode:

show mirror

For example:

！Display monitor port and mirrored port list

OLT#show mirror

2.4. Port LACP convergent configuration

2.4.1 Brief introduction of port convergence

Port convergence is a channel group formed by many ports convergence to realize flow load sharing for each member. When a link cannot be used, flow of this link will be transferred to another link to guarantee the smoothness of the flow.

Basic configurations are:

1 static or dynamic channel groups can be configured and at most 12 interface members can be configured in each group, and at most 8 interfaces can be convergent at the same time in each group which is determined by up/down status, interface number, LACP priority. Each group is defined to be a channel group, and the command line is configured around it.

2 Load balance strategy of each group can be divided into source MAC, destination MAC, source and destination MAC, source IP, destination IP, and source and destination IP. The default strategy is source MAC.

3 System and interface LACP priority can be configured. The default system priority is 32768，and interface priority is 128. To remove system and interface priority is to restore them to default ones.

4 LACP protocol of each interface can be configured. In static mode, interface is static convergent, and LACP protocol does not run; in active mode, interface will initiate LACP negotiation actively; in passive mode, interface only can response LACP negotiation. When interconnecting with other device, static mode only can interconnect with static mode; active can interconnect with active and passive mode, but passive mode only can interconnect with active mode. The default mode of interface is ACTIVE mode.

Each convergent interface need same layer 2 features, so there are following restrictions to interfaces in a channel group:

1 Static convergent interfaces and dynamic convergent interfaces can not be in a same channel group, but there can be static convergent channel as well as dynamic convergent channel.

2 Each interface in a same channel group must possess the same features as following: interface speed rate, working mode of full duplex, STP/GVRP/GMRP function, STP cost, STP interface priority, VLAN features (interface mode, PVID, VLAN belonged to, tag VLAN list of access interface, allowed VLAN list of trunk interface) and layer 2 multicast group belonged to.

3 If modifying the feature of one interface in the channel group, other interfaces will be modified automatically in the same place. The feature refers to point 2.

4 After convergence, static hardware item (ARL, MARL, PTABLE, VTABLE) will be modified, but there will be delay.

5 After convergence, only host interface can send CPU packet. If STP changes status of some interface, the status of the whole channel group will be changed.

6 After convergence, when transferring layer 2 protocol packet, STP/GARP/GNLINK will not transfer packet to the current channel grou. If transferring to other channel group, only one packet will be transferred.

If there are members in the channel group, this channel group cannot be deleted. Delete interface members first.

Influence on choosing link redundancy caused by LACP system and interface priority. LACP provides link redundancy mechanism which needs to guarantee the redundancy consistency of two interconnected switches and user can configure redundancy link which is realized by system and interface priority. The redundancy choosing follows the following steps:

First, determine which switch is the choosing standard. For LACP packets interaction, each of the two switches knows each other’s LACP system priority and system MAC and compares the LACP system priority to choose the smaller one; if the system priority is the same, compare MAC and choose the smaller one.

1、 Then, choose redundancy link according to the interface parameter of the chosen switch. Compare interface LACP priority, and choose the inferior one to be redundant. If the priorities are the same, choose the interface whose interface number is larger to be redundant.

2.4.2 Interface convergent configuration

Port LACP configuration command includes:

- Channel group configuration

Please configure it in global configuration mode:

channel-group channel-group-number

Parameter “channel-group-number” is range from 0 to 5.

For example:

！Create a channel group with the group number being 0

OLT(config)#channel-group 0

- Delete channel group

no channel-group channel-group-number

- Add port members to the group

channel-group channel-group-number mode {active | passive | on}

In interface configuration mode, add current interface to channel group and specify the mode of interface. If the channel group doesn’t exist, create it.

For example:

！Add Ethernet 0/3 to channel-group 3 and specify the port to be active mode

OLT(config-if-ethernet-0/3)#channel-group 3 mode active

- Delete interface member in channel group

no channel-group channel-group-number

In interface configuration mode, delete current interface from channel group.

For example:

！Delete interface Ethernet 0/3 from channel group 3

OLT(config-if-ethernet-0/3)#no channel-group 3

- Configure load balance of switch

channel-group load-balance

{dst-ip|dst-mac|src-dst-ip|src-dst-mac|src-ip|src-mac}

choose physical link program when packet sending.

For example:

！Specify load-balance of channel-group 0 is destination mac

OLT(config)#channel-group load-balance dst-mac

- Configure system LACP priority

lacp system-priority priority

For example:

！Configure LACP system priority is 40000

OLT(config)#lacp system-priority 40000

- Delete system LACP priority

no lacp system-priority

Use this command to restore system default LACP priority to be 32768.

- Configure interface LACP priority

lacp port-priority priority

Use this command in interface configuration mode to configure LACP priority of the current interface

For example:

！Configure lacp port-priority of Ethernet 0/2 to be 12345

OLT(config-if-ethernet-0/2)#lacp port-priority 12345

- Delete interface LACP priority

no lacp port-priority

Use this command to restore interface default LACP priority to be 128.

- Display system LACP ID

show lacp sys-id

System id is in the form of 16 characters of system priority and 32 characters of system MAC address.

For example:

！Display lacp system id

OLT(config)#show lacp sys-id

- Display local information of channel group

show lacp internal [channel-group-number]

Use show lacp interval command to display the information of group members, if the there is no keywords, all groups are displayed.

For example: Display the member information of channel group 2.

OLT#show lacp internal 2

- Display information of neighbour interface of channel group

show lacp neighbor [channel-group-number]

Use show lacp neighbor command to display the information of the neighbour port in the group. If there is no keyword, the neighbor ports of all the groups are displayed.

For example: Display the information of the neighbour port of the group 2

OLT#show lacp neighbor 2

2.5. Interface CAR configuration

2.5.1 Brief introduction of interface CAR

Interface CAR is used to restrict the speed rate impacted CPU of single interface. CPU can make speed rate statistics of each interface. If the speed rate is larger than the configured threshold (it is defaulted to be 300 packet/second), disable this interface and send trap of interface being abnormal. After a certain time (it is defaulted to be 480 seconds), re-enable the interface. If this interface will not be re-disabled by interface CAR in 2 seconds, the storm of impacting CPU by interface is over, and the interface recovers, and sends the trap of interface being normal. Caution: If the re-enabled interface is disable again by impacting CPU packet in 2 seconds, no trap of interface being abnormal is sent.

2.5.2 Port CAR configuration command list

Port CAR configuration command includes:

- Enable/disable interface CAR globally
- Enable/disable interface CAR on a port
- Configure interface CAR re-enable time
- Configure interface CAR
- Display interface CAR status

2.5.3 Enable/disable interface globally

Configure it in global configuration mode

- Enable global interface

port-car

- Disable global interface

no port-car

By default, port-car globally enables

For example:

！Enable port-car globally

OLT(config)#port-car

2.5.4 Enable/disable interface CAR on a port

Please configure it in interface configuration mode:

- Enable interface CAR

port-car

- Disable interface CAR

no port-car

For example:

！Enable port-car of Ethernet 0/8

```
OLT(config-if-ethernet-0/8)#port-car
```

2.5.5 Configure the port-car-rate

Please configure it in global configuration mode:

- Configure the port-car-rate

```
port-car-rate port-car-rate
```

Default port-car-rate is 300 packet/second

For example:

！Configure port-car-rate to be 200 packet/second

```
OLT(config)#port-car-rate 200
```

2.5.6 Display port-car information

Input following command in any configuration mode to display port-car information:

```
show port-car
```

For example:

！Display port-car information

```
OLT(config)#show port-car
```

2.6. Port Alarm Configuration

2.6.1 Brief introduction of port alarm configuration

System can monitor port packet receiving rate. If the rate of receiving packet is beyond the interface flow exceed threshold, send alarm of large interface flow and the interface is in the status of large interface flow. In this status, if the rate of receiving packet is lower than the interface flow normal threshold, send alarm of normal interface flow. This function can actively report the rate of receiving packet to user.

2.6.2 Port alarm configuration list

Port alarm configuration command includes:

- Enable/disable port alarm globally
- Enable/disable port alarm on the port
- Configure the exceed threshold and normal threshold of port alarm
- Display port alarm

2.6.3 Enable/disable port alarm globally

Please configure it in global configuration mode:

- Enable port alarm globally

```
alarm all-packets
```

- Disable port alarm globally

no alarm all-packets

By default, alarm all-packets enable.

For example:

！ Enable global alarm all-packets

OLT(config)#alarm all-packets

2.6.4 Enable/disable port alarm on the port

Please configure it in interface configuration mode:

- Enable port alarm on the port

alarm all-packets

- Disable port alarm on the port

no alarm all-packets

For example:

！Enable alarm all-packets of Ethernet 0/8

OLT(config-if-ethernet-0/8)# alarm all-packets

2.6.5 Display port alarm

- Input following command in any configuration mode to display global interface alarm:

show alarm all-packets

For example:

！Display global alarm all-packets information

OLT(config)#show alarm all-packets interface ethernet 0/1

- Input following command in any configuration mode to display interface alarm on the port:

show alarm all-packets interface [interface-list]

Keyword “interface-list” is alternative. If there is no keyword, the alarm all-packets of all the interfaces are displayed, or the information of specified port is displayed.

For example:

！Display the alarm all-packets interface information of Ethernet 0/1

OLT(config)#show alarm all-packets interface ethernet 0/1

3. VLAN CONFIGURATION

3.1. Brief introduction of VLAN

VLAN （Virtual Local Area Network ）is a technology divided devices in LAN logically not physically into network interfaces to realize virtual workgroup. IEEE promulgated IEEE 802.1Q protocol standard draft to realize standardized VLAN.

VLAN technology allows network administrator to divide a physical LAN into different broadcast domain or VLAN logically. Each VLAN contain a group of computer station with the same need to possess the same attribute with the LAN formed physically. But it is divided logically not physically, so each working station of the same VLAN need not be in the same physical space. Broadcast and unicast flow in a VLAN will not transfer to other VLAN, which is helpful to control the flow, reduce device cost, predigest network management and improve network security. Following are VLAN features:

- Flow control helped by VLAN

In traditional network, large number of broadcast data is sent to all network devices to cause network congestion. VLAN can configure the intercommunicated devices in each VLAN to reduce broadcast to improve network efficiency.

- provides higher security

Device in one VLAN can only intercommunicate with the device in the same VLAN. For example, devices in R&D department can intercommunicate with production department only by the routing device, which greatly improved system security for the two departments cannot intercommunicate directly.

3.2. VLAN interface type

System supports IEEE 802.1Q which possesses two types of VLAN interfaces. One is tagged, and the other is untagged.

Tagged interface can ad VLAN ID, priority and other VLAN information to the head of the packet which is out of the interface. If the packet has included IEEE 802.1Q information when entering the switch, the mark information will not be changed; if the packet has not includes IEEE 802.1Q mark information, system will determine the VLAN it belongs to according to the default VLAN ID of the receiving interface. Network devices supported IEEE 802.1Q will determine whether or not to transmit this packet by the VLAN information in the mark.

Untagged interface can drop the mark information from all the packets which are out of the interface. When a frame is out of a untagged interface, it will not contain IEEE 802.1Q mark information. The function of dropping the mark makes the packet can be transferred from the network device supported mark to the one which doesn’t support it.

Now, only the switch supported IEEE 802.1Q can be recognize IEEE 802.1Q frame so only a port linking to a switch supported IEEE 802.1Q can be configured to be Tagged port.

3.3. Default VLAN

There is a default VLAN of production, which possesses following features:

- The name of this VLAN is Default which can be modified.
- It includes all ports which can be added and deleted.
- All the port mode of default VLAN is untagged which can be modified to be tagged.
- VLAN ID of default VLAN is 1 which cannot be deleted.

3.4. VLAN configuration

3.4.1 VLAN configuration list

Configure VLAN should create VLAN according to the need first, then configure VLAN interface and its parameter.

VLAN configuration list is as following:

- Create/delete VLAN Add/delete
- VLAN interface Specify/delete
- VLAN description Configure
- interface type
- Configure interface default VLAN
- ID Configure tag VLAN
- Display VLAN information

3.4.2 VLAN Create/delete VLAN

Configure it in global configuration mode:

- Enter VLAN configuration mode or create VLAN and enter it

VLAN VLAN-list

- Delete created VLAN or specified VLAN except VLAN 1

no VLAN { VLAN-list | all }

VLAN-ID allowed to configure by system is in the range of 1 to 4094. VLAN-list can be in the form of discrete number, a sequence number, or the combination of discrete and sequence number, discrete number of which is separate by comma, and sequence number of which is separate by subtraction sign, such as: 2,5,8,10-20. Use the VLAN command to enter VLAN configuration mode. If the VLAN identified by the VLAN-id keyword exists, enter VLAN configuration mode. If not, this command creates the VLAN and then enters VLAN configuration mode. For example, if VLAN 2 is not existed, system will create VLAN 2 first, then enter VLAN configuration mode; if VLAN 2 has existed, enter VLAN configuration mode.

When deleting VLAN, if the VLAN-list is specified, delete corresponding VLAN. If choosing all, delete all existed VLAN except default VLAN. If deleting interface in VLAN, and default VLAN id is the same as the VLAN to be deleted, restore interface default VLAN ID to be default VLAN ID.

If the VLAN to be removed exists in the multicast group, remove the related multicast group first.

3.4.3 Add/delete VLAN interface

Use the switchport command to add a port or multiple ports to current VLAN. Use the no switchport command to remove a port or multiple ports from current VLAN. Use following commands in VLAN configuration mode:

- Add interface to specified VLAN

```
switchport { interface-list | all }
```

- Delete some interface from specified VLAN

```
no switchport { interface-list | all }
```

Interface-list is the optioned interface list which means a or more interfaces. If choose all, add all ports to current VLAN; if choosing all when deleting interface, all ports in current VLAN will be deleted. When deleting interface from VLAN 1, if the PVID of interface is 1, modify the PVID to be other VLAN ID before deleting this interface. When deleting interface in other VLAN ID, port PVID should be the same as the VLAN ID, and the port is also in VLAN 1, delete it. If this port is not in VLAN 1, modify port PVID to be other VLAN ID, delete the port.

There are two status of the interface in VLAN, one is tagged and the other is untagged. If the port is access port, add it to VLAN with the status of being untagged. If it is trunk port, change it to be tagged in VLAN.

For example:

！Add Ethernet 1, 3, 4, 5, 8 to current VLAN

```
OLT(config-if-VLAN)#switchport ethernet 0/1 ethernet 0/3 to ethernet 0/5 ethernet 0/8
```

！Remove Ethernet 3, 4, 5, 8 from current VLAN

```
OLT(config-if-VLAN)#no switchport ethernet 0/3 to ethernet 0/5 ethernet 0/8
```

Command switchport access VLAN and its no command can also add and delete port to or from VLAN. Please refer to interface configuration of chapter 2.

3.4.4 Specify/restore VLAN description

The description string is used to distinguish each VLAN. Please configure it in VLAN configuration mode:

- Specify a description string to specified VLAN

```
description string
```

- Delete description string of specified VLAN

```
no description
```

string：It is in the range of 1 to 32 characters to describe the current VLAN. The characters can be printable, excluding such wildcards as '/'、':'、'*'、'?'、'\\'、'<'、'>'、'|'、'"'etc.

For example:

！Specify the description string of the current VLAN as “market”

```
OLT (config-if-VLAN)#description market
```

```
！Delete the description string of VLAN
OLT(config-if-VLAN)#no description
```

3.4.5 Configure interface type

Use switch port mode command to configure port type. Please refer to interface configuration in chapter 2.

3.4.6 Configure interface default VLAN ID

System supports IEEE 802.1Q. When receiving a untagged packet, system will add a tag to the packet, in which the VLAN ID is determined by the default VLAN ID of the receiving port. The command to configure default VLAN of trunk port is switch port trunk native VLAN; for access port, use switch port access VLAN command to configure default VLAN of specified interface. The detailed introduction of the corresponding no command is in chapter 2.

For example:

```
！Configure default VLAN-id of Ethernet interface 1 to be 2
OLT(config-if-ethernet-0/1)#switchport mode access
OLT(config-if-ethernet-0/1)#switchport access
VLAN 2
```

⚠ Caution: To use switch port trunk native VLAN VLAN-id must guarantee the specified interface to be trunk, and belongs to specified VLAN, and the VLAN ID is not 1. Use switch port access VLAN VLAN-id to configure interface default VLAN and add it to the VLAN. The specified interface is access, and the VLAN is existed and is not the default VLAN.

3.4.7 Display VLAN information

VLAN information is VLAN description string, VLAN-id, VLAN status and interface members in it, tagged interfaces, untagged interfaces and dynamic tagged interfaces. Interface members consist of tagged and untagged members.

```
show VLAN [ VLAN-id ]
```

If the VLAN with specified keyword exists, this command displays the information of the specified VLAN. If no keyword is specified, this command displays the list of all the existing VLANs

For example:

```
！Display the information of existed VLAN 2.
OLT(config)#show VLAN 2
```

3.5. PVLAN

PVLAN means private VLAN which is used to realize interface isolation function. These private VLANs are unknown to uplink devices to save the resource of public VLAN. Nowadays, factories in this field use SVL to realize PVLAN and provide corresponding configuration command. But there is some shortage by using SVL, such as: the uplink and downlink interfaces are access, and MAC address wasting. Our company uses redirection technology to realize PVLAN and overcome the shortage of SVL, any interface can be access or trunk, which entirely realize PVLAN. The detailed information of PVLAN configuration can refer to interface isolation configuration.

3.6. GVRP configuration

3.6.1 Brief introduction of GVRP

GVRP, GARP VLAN Registration Protocol is a kind of application of GARP. It is based on GARP working mechanism to maintain VLAN dynamic register information in switch and transfer it to other switch. All switch that support GVRP can receive VLAN register information from other switches and dynamically upgrade local VLAN register information which includes: current VLAN members, and by which interface can reach VLAN members. And all switches supported GVRP can transfer local VLAN register information to other switches to make the consistency of the VLAN information of devices which support GVRP. VLAN register information transferred by GVRP includes local munal configuration of static register information and the dynamic register information of other switch.

3.6.2 GVRP Configuration list

In all configurations, enable global GVRP first before enable GVRP on a port. GVRP must be enabled in the two ends of trunk link which follows IEEE 802.1Q standard.

GVRP Configuration list is as following:

GVRP Configuration list is as following:

- Enable/disable global GVRP
- Enable/disable GVRP on a port
- Display GVRP
- Add/delete VLAN that can be dynamic learnt by
- GVRP Display VLAN that can be learnt by GVRP

3.6.3 Enable/disable global GVRP

Please configure it in global configuration mode:

- Enable global GVRP

gvrp

- Disable global GVRP

no gvrp

By default, GVRP globally disables

For example:

！Enable GVRP globally

OLT(config)#gvrp

3.6.4 Enable/disable GVRP on a port

Please configure it in interface configuration mode:

- Enable GVRP on a port

```
gvrp
```

- Disable GVRP on a port

```
no gvrp
```

For example:

！Enable GVRP on Ethernet port 8

```
OLT(config-if-ethernet-0/8)#gvrp
```

⚠ Caution: Enable global GVRP before enable GVRP on a port. By default, global GVRP disables and GVRP on a port can be enabled in trunk mode interface.

3.6.5 Display GVRP

- Use following command in any configuration mode to display global GVRP：

```
show gvrp
```

- Use following command in any configuration mode to display GVRP on a port：

```
show gvrp interface [ interface-list ]
```

Interface-list keyword is optional. If this keyword unspecified, the command displays GVRP information for all the Ethernet ports. If specified, the command displays GVRP information on specified Ethernet port.

For example:

！Display GVRP information on interface Ethernet 0/1

```
OLT(config)#show gvrp interface ethernet 0/1
```

3.6.6 Add/delete VLAN that can be dynamic learnt by GVRP

Use gvrp permit VLAN command to add configured static VLAN to GVRP module for other switches to learn. Configure it in global configuration mode:

```
gvrp permit VLAN VLAN-list
no garp permit VLAN [ VLAN-list ]
```

For example: !Add VLAN 2, 3, 4 to

GVRP OLT(config)#gvrp permit VLAN

2-4

3.6.7 Display VLAN that can be learnt by GVRP

Use show gvrp permit VLAN command to display current static VLAN permitted learning by

GVRP show gvrp permit VLAN

For example:

Display current static VLAN permitted learning by

GVRP OLT(config)#show gvrp permit VLAN

3.6.8 Examples for GVRP configuration

！Enable GVRP on Ethernet port 2

OLT(config-if-ethernet-0/2)#gvrp

！Disable GVRP on Ethernet port 2

OLT(config-if-ethernet-0/2)#no gvrp

3.7. QinQ configuration

3.7.1 Brief introduction of QinQ

QinQ is used for the communication between discrete client VLAN whose service model is the interconnection of one or more switches supported QinQ by service provider interfaces which are in service provider VLAN. The interface linking client VLAN is called customer interface. Packet with client VLAN tag will add a tag head with the VLAN id being service provider VLAN when passing through the customer interface. The tag head will be stripped when passing through service provider VLAN.

3.7.2 QinQ configuration list

- Configure global QinQ
- Configure global internal/external TPID
- Configure interface QinQ
- Configure interface VLAN
- insert Configure interface
- VLAN swap
  Configure interface VLAN pass-through

3.7.3 Configure global QinQ

Use dtag command to enable/disable QinQ globally in global configuration mode

dtag

no dtag

For example:

!Enable QinQ globally

OLT(config)dtag

3.7.4 Configure global internal/external TPID

For QinQ packet, there are 2 VLAN tags: external VLAN tag (Service tag) and internal VLAN tag (Customer tag). OLT can configure TPID in both internal and external VLAN tag to be other value. These configurations can be effective to the whole switch. The packet is called double tag packet when the external and internal TPID are matching at the same time.

！Configure internal TPID command mode to be global

dtag inner-tpid tpid

no dtag inner-tpid

！Configure external TPID command mode to be interface

dtag outer-tpid tpid

no dtag outer-tpid

Example:

Configure internal TPID to be 0x9100

OLT(config)#dtag inner-tpid 9100

3.7.5 Configure interface QinQ

After booting, it is defaulted to be uplink interface which can be called Service interface and the packet from this interface can be with double tags. It also can configure this interface to be Customer interface, the packet from this interface can only be with internal tag.

Caution: uplink interface needs to be tag member in Service VLAN and customer interface needs to be untag member in Service VLAN.

！Command configuration mode is interface mode

dtag mode [customer | uplink]

no dtag mode [customer | uplink]

Example：

Configure interface 0/1 to be customer

OLT(config-if-ethernet-0/1)#dtag mode customer

3.7.6 Configure interface VLAN insert

Interface is configured to be Customer interface. Add VLAN id of external tag according to internal VLAN id to send tag packet.

Caution： in fixed some interface mode, for a specified VLAN id, only one of VLAN insert,VLAN swap and VLAN pass-through can be configured.

！Configure it in interface configuration mode

dtag insert startVLANid endVLANid

targetVLANid no dtag insert startVLANid

endVLANid Example

：

Configure all VLANs from VLAN1 to VLAN2 in e0/1 to add new tag head with the tag VLAN to be VLAN3

OLT(config-if-ethernet-0/1)#dtag insert 1 2 3

3.7.7 Configure interface VLAN swap

Interface is configured to be Customer interface. Not adding tag head, change to new VLANid according to internal VLANid to send tag packet.

Caution： in fixed some interface mode, for a specified VLANid, only one of VLAN insert,VLAN swap and VLAN pass-through can be configured.

！Configure it in interface configuration mode

dtag swap startVLANid endVLANid newVLANid

no dtag swap startVLANid

endVLANid Example：

Configure tag packet from VLAN1 to VLAN 3 in e0/1 is replaced by

VLAN5 OLT(config-if-ethernet-0/1)#dtag swap 2 4 5

3.7.8 Configure interface VLAN pass-through

Interface is configured to be Customer interface. Not add tag head according to internal VLANid to send tag packet.

Caution： in fixed some interface mode, for a specified VLANid, only one of VLAN insert,VLAN swap and VLAN pass-through can be configured.

！Configure it in interface configuration mode

dtag pass-through startVLANid endVLANid

no dtag pass-through startVLANid

endVLANid Example：

Configure tag packet transparent transmission from VLAN 1 to VLAN 3 in

e0/1. OLT(config-if-ethernet-0/1)#dtag pass-through 1 3

4. LAYER 3 CONFIGURATION

4.1. Brief Introduction of Layer 3

OLT is a GE Intelligent Routing Switch based on ASIC technology which can support transmission in both layer 2 and layer 3. The inter accessing of hosts in the same VLAN is the transmission in layer 2 and the inter accessing of hosts in the different VLAN is the transmission in layer 3.

4.2. Layer 3 Configuration

4.2.1 Layer 3 Configuration list

Configuration list is as following：

- VLAN division and the creation of layer 3 interface
- Transmission mode configuration
- Create VLAN interface for normal VLAN
- Create super VLAN interface and add VLAN to super VLAN
- Configure IP address for VLAN interface or super VLAN interface
- ARP proxy configuration
- Display interface configuration

4.2.2 VLAN division and the creation of layer 3 interface

VLAN division please refers to VLAN configuration chapter.

Layer 3 interface includes normal VLAN interface and super VLAN interface. Normal VLAN interface is the interface in some concrete VLAN; super VLAN interface is created in super VLAN (super VLAN is the VLAN which is not existed and contains no interface) which can contain many sub VLANs (sub VLAN is the existed concrete VLAN). At most 258 layer 3 interfaces can be created, among which super VLAN can be 128 at most.

The total maximum number of VLAN contained by all layer 3 interfaces is 258. Each VLAN only exists in one layer 3 interface. In superVLAN, interface must be untagged member in only one subVLAN, and tagged in other subVLANs.

4.2.3 Transmission mode configuration

OLT supports two types of packet transmission mode: 1）flow transmission ;2）network topology transmission. Searching failed route or host route with the unreached destination in flow transmission mode; these packet will be dropped in network topology trsnamission. It is defaulted to be flow transmission mode.

Please configure it in global configuration mode:

[no] ip def cpu

4.2.4 Create VLAN interface for normal VLAN

Configure VLAN interface for each VLAN which supports layer 3 transmission or add this VLAN to superVLAN.

Create VLAN interface for VLAN 2 and enter VLAN interface configuration mode:

```
OLT(config)#interface VLAN-interface 2
```

4.2.5 Create superVLAN interface and add VLAN to superVLAN

superVLAN interface realizes the intercommunication of hosts which belong to different VLAN but the same network interface. superVLAN interface is realized through ARP proxy.

Create superVLAN 1 and add VLAN 3, VLAN 4 to be subVLAN of superVLAN 1.

```
OLT(config)#interface superVLAN-interface 1
OLT(config-if-superVLANInterface-
1)#subVLAN 3 OLT(config-if-
superVLANInterface-1)#subVLAN 4 Delete
VLAN 3 and VLAN 4 from superVLAN 1.
OLT(config-if-superVLANInterface-1)#no
subVLAN 3 OLT(config-if-superVLANInterface-
1)#no subVLAN 4
```

4.2.6 Configure IP address for VLAN interface or superVLAN interface

At most 32 IP address can be configured for each VLAN interface or superVLAN interface the IP address of which cannot be in the same network interface. The IP address firstly configured will be the primary IP address. After deleting primary IP address, there will be another to be the primary IP address automatically and it can also configure an IP address to be the primary one manually. For example, if IP address of VLAN interface 1 is 10.11.0.1/16, other interfaces cannot configure the IP address in the same network interface (10.11.0.0/16), such as 10.11.1.1/24.

Configure IP address of VLAN interface 2 to be 10.11.0.1/16：

```
OLT(config-if-VLANInterface-2)#ip address 10.11.0.1
255.255.0.0 Delete IP address of VLAN interface 2：
OLT(config-if-VLANInterface-2)#no ip address
```

Specify an IP address of specified interface to be the primary IP address：

```
OLT(config-if-VLANInterface-2)#ip address primary 10.11.0.1
```

4.2.7 Configure accessing IP address range of VLAN or superVLAN interface

At most 8 accessing range can be configured for each VLAN or superVLAN interface. After configuring accessing range, ARP must learn in this range to restrict user’s accessing. When deleting VLAN or superVLAN interface, related configuration will be deleted.

Use following command in VLAN or superVLAN interface mode：

```
ip address range start ip end ip
```

4.2.8 Display interface configuration

Each created VLAN or superVLAN interface has its own configuration information, including: VLAN number, IP address and netmask. Following command is used to display configuration information of all layer 3 interface, specified normal VLAN or super VLAN interface.

Display all layer 3 interface configuration information：

```
OLT(config)#show ip interface
```

Display VLAN interface 2 configuration information：

```
OLT(config)#show ip interface VLAN-interface 2
```

Display superVLAN interface 3 configuration information：

```
OLT(config)#show ip interface superVLAN-interface 3
```

5. ARP CONFIGURATION

5.1. Brief Introduction of ARP

ARP table is a table of the relationship between IP and MAC, including dynamic and static. Dynamic ARP table item is learnt by ARP protocol. Static ARP table item is added manually.

5.2. ARP configuration

5.2.1 ARP configuration list

Configuration list is as following:

- Add and delete ARP table item
- Display ARP table item
- Configure ARP aging time
- Display ARP aging time
- Configure and delete ARP attack protection
- Display ARP attack protection configuration
- Configure anti-ARP attack rate limit
- Enable user forbidden by anti-ARP attack
- Display anti-ARP attack
- Configure and delete DOS protection
- Display ARP DOS protection configuration

5.2.2 Add and delete ARP table item

Use this command can add or delete a static or dynamic ARP table item. ARP table item not only include corresponding relations of IP and MAC, but also the local VLAN and port number the frame with keyword MAC being destination address has passed.

Add a static ARP table item with the IP address being 192.168.0.100，MAC address being 00:01:02:03:04:05，the corresponded VLAN interface being 1，and port number being 3：

```
OLT(config)#arp 192.168.0.100 00:01:02:03:04:05 1 0/3
```

Delete the corresponded ARP table item of IP address 192.168.0.100：

```
OLT(config)#no arp 192.168.0.100
```

Delete all static ARP table item：

```
OLT(config)#no arp static
```

Delete all dynamic ARP table item:

```
OLT(config)#no arp dynamic
```

Delete all ARP table item:

```
OLT(config)#no arp all
```

5.2.3 Display ARP table item

Use this command to display static, dynamic, specified IP address or all ARP table item.

Display all ARP table item：

OLT(config)#show arp all Display

dynamic ARP table item ：

OLT(config)#show arp dynamic

Display static ARP table item：

OLT(config)#show arp static

Display all ARP table item with the IP address being 192.168.0.100：

OLT(config)#show arp 192.168.0.100

5.2.4 Configure ARP aging time

Use this command to modify ARP aging time:

OLT(config)#arp aging 20

5.2.5 Display ARP aging time

Use this command to display ARP aging time:

OLT(config)#show arp aging

6. DHCP CONFIGURATION

6.1 Brief introduction

DHCP packet is broadcasting packet so in layer 3 network structure and using DHCP to distribute IP address, each broadcasting domain needs a DHCP server. For layer 3 network structure by using OLT to establish a layer 3 network, each VLAN needs a DHCP server which greatly wastes of resources. A better way to solve this problem is to configure DHCP relay in OLT to relay DHCP packet to DHCP server which can need at least only one DHCP server.

Following DHCP functions are supported:

Support DHCP relay function

Support specifying DHCP server for each layer 3 interface

support built-in DHCP server

support at most 12 address pools and at most 8 network interfaces for each address pool

support DHCP client to obtain system IP

6.2 DHCP configuration

6.2.1 DHCP configuration list

DHCP configuration list is as following:

- Enable DHCP relay
- Configure DHCP server
- Specify DHCP server for layer 3 interface
- Display DHCP server configuration
- Hide DHCP server
- Support relay option82

6.2.2 Enable DHCP relay

By default, DHCP relay is disabled. Enable DHCP relay in global configuration mode:

- Enable DHCP relay

```
dhcp-relay
```

- Disable DHCP relay

```
no dhcp-relay
```

Display DHCP relay in any configuration mode:

- Display DHCP relay

```
show dhcp-relay
```

Example:

！Enable DHCP relay

OLT(config)#dhcp

！Disable DHCP relay

OLT(config)#no dhcp

！Display DHCP relay

OLT(config)#show dhcp-relay

6.2.3 Configure DHCP server

After enabling DHCP relay, configure DHCP server and specify it to corresponded interface. If IP address of DHCP server is configured to be IP address of any interface or 127.0.0.1, use built-in DHCP server. Configure IP address pool before using built-in DHCP server.

- Enable DHCP server and specify corresponded interface IP

dhcp-server group-num ip ip-address

- Disable DHCP server

no dhcp-server group-num

Example：

！Configure IP address of DHCP server 1 to be 192.168.0.100

OLT(config)#dhcp-server 1 ip 192.168.0.100

！Disable DHCP server 1

OLT(config)#no dhcp-server 1

6.2.4 Specify DHCP server for layer 3 interface

After creating DHCP server, specify DHCP server for each layer 3 interface, and system will relay DHCP packet to DHCP server of this interface after receiving DHCP packet. Use this command in interface configuration mode.

- Specify DHCP server for layer 3 interface

dhcp-sever group-num

- Delete DHCP server for current layer 3 interface

no dhcp-server

Example：

！Specify DHCP server 1 for VLAN interface 1

OLT(config-if-VLANInterface-1)#dhcp-

server 1 !Delete DHCP server for VLAN

interface 1

OLT(config-if-VLANInterface-1)#no dhcp-server

6.2.5 Display DHCP server configuration

After configuring DHCP server, there are two ways to display DHCP server configuration: one is displaying all DHCP server group, the other is displaying DHCP server of layer 3 interface.

- Display DHCP server configuration of all or specified group

show dhcp-server [group-num]

group-num is DHCP server group number.

- Display DHCP server configuration of layer 3 interface

show dhcp-server inerface [{ superVLAN-interface | VLAN-interface } VLAN-id]

VLAN-id is layer 3 interface number, if there is no keyword after interface, all DHCP server configuration of all layer 3 interface will be displayed.

Example:

！Display all DHCP server

OLT(config)#show dhcp-server

！Display DHCP server 1

OLT(config)#show dhcp-server 1

！Display DHCP server of VLAN interface 1

OLT(config)#show dhcp-server interface VLAN-interface 1

6.2.6 Hide DHCP server

After enabling this function, IP address of DHCP server in IP address information requested by DHCP client cannot be the real IP address of DHCP server, but primary IP address of current interface of OLT to hide DHCP server directory.

When DHCP relay of multi-levels exist and this function enables, all-around relay needs enable this function, or the first or the last relay enables, or the network will be abnormal.

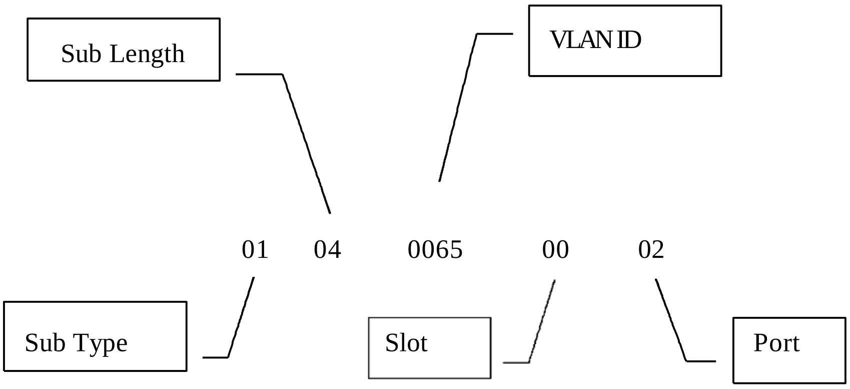
- Hide IP address of DHCP server

dhcp-relay hide server-ip

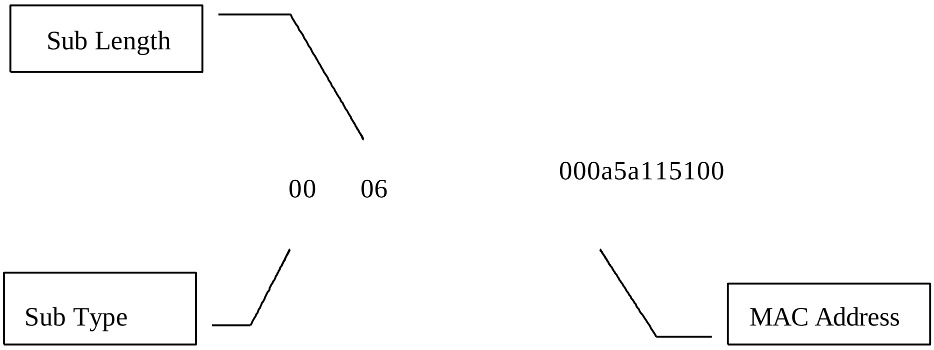
6.2.7 Support relay option82

Option82 is the Relay Agent Information option in DHCP packet defined by rfc 3046. When DHCP client sending require packet to DHCP relay, option82 will be added to packet. Option82 in this chapter supports sub-option1, sub-option2 and sub-option5. sub-option1 is one of sub-option of option82 which is Circuit ID with the content being interface VID and MAC address of receiving packet. sub-option2 is also the sub-option of option82 which is Remote ID and is MAC address of relay devices. sub-option5 is also a sub-option of option82 which is Link Selection and is IP address of interface.

The form of sub-option1is as following：



The form of sub-option2 is as following：



When relay devices receive the DHCP_DISCOVER and DHCP_REQUEST packet sent by client, add option82 and send to server. After receiving the request packet of server, strip option82 before transmitting to client.

- Enable option82 support

dhcp-relay option82

- Disable option82 support

no dhcp-relay option82

- Configure handling strategy of require packet contained option82

dhcp-relay option82 strategy {drop|keep|replace}

- Display configuration of option82

show dhcp

6.3DHCP SNOOPING

It belongs to layer 2 function which allows switch to detect DHCP packet and record user’s IP address information. This function cannot be enabled at the same with DHCP relay. When enabling it, switch will filtrate all DHCP packet to CPU and transmit by layer 2 CPU.

To permit using valid DHCP server to distribute IP address, DHCP SNOOPING will divide interfaces to be trust one and non-trust one. Only trust interface can receive and send DHCP packet transmitted by DHCP server to prevent interference of invalid DHCP server.

In security, DHCP SNOOPING permits configuring the max DHCP client number of some interface or VLAN too prevent malicious requiry attack.

6.3.1 Enable the function

Enable DHCP SNOOPING, which cannot be enabled at the same time with DHCP RELAY.

- Enable DHCP SNOOPING

```
dhcp-snooping
```

6.3.2 Configure trust interface

Specify some interface to be the trust one. Generally, valid DHCP server connects to trust interface.

- Specify interface to be the trusy one

```
dhcp-snooping trust
```

6.3.3 Configure Max client number

Configure max client number of interface or VLAN to prevent malicious user’s IP require DOS attack to protect DHCP server.

- Configure max client number of interface/VLAN

```
dhcp-snooping max-clients num
```

6.3.4 Configure IP source guard

Prevent IP address stolen through IP source guard.

- Configure interface IP source guard

```
ip-source-guard
```

6.3.5 Display configuration

Use this command to display all configuration of DHCP SNOOPING.

- Display related configuration

```
show dhcp-snooping
```

6.3.6 Display user’s information

It can display user’s IP address, MAC address, ingress VLAN and ingress interface information.

- Display user’s information

```
show dhcp-snooping clients
```

7. LOCAL IP ADDRESS POOL CONFIGURATION

7.1. Brief introduction of local IP pool

Local IP pool is the database which records the IP address DHCP server distributed to DHCP clients which can enquire IP address information DHCP server distributed. In local IP address pool configuration mode, configure parameter of DHCP clients distributed by DHCP server. The configuration options are: gateway and netmask of DHCP client, DNS server, WINS server, lease, IP address range distributed to DHCP client and IP address which is forbidden to distribute and specify. It needs configure local IP address pool before system built-in DHCP server distributing IP address to DHCP client. Enable ip-bind before applying specified IP address in dhcp-client configured client.

7.2. Local IP address pool configuration

7.2.1 Local IP address pool configuration list

- Enter IP address pool configuration mode
- Configure gateway and netmask of local IP address pool
- Configure local IP address pool network interface
- Disable/enable specified IP address in IP address pool
- Configure lease
- Configure DNS
- Configure WINS
- Display IP address pool configuration
- Configure ip bind
- Display IP bind
- Add or delete dhcp client
- Display dhcp client

7.2.2 Enter IP address pool configuration mode

Please configure it in global configuration mode：

- Enter ip address pool configuration mode

ip pool ippoolname

If IP address pool specified by ippoolname doesn’t exist, create this pool.

- Delete ip address pool

no ip pool ippoolname

Example：

```
！Enter IP address pool configuration mode
OLT(config)#ip pool nic
！Delete IP address pool nic
OLT(config)#no ip pool nic
```

7.2.3 Configure gateway and netmask of local IP address pool

Use this command in local IP address pool configuration mode：

- Configure gateway and netmask of local IP address pool

gateway ip-address mask

Parameter ip-address is IP address and mask is its netmask.

All IP address in local IP address pool must be in the address domain determined by this gateway and netmask and IP address in address pool cannot contain gateway

Example：

！Configure gateway and netmask of local IP address pool

```
OLT(config-ip-pool-nic)#gateway 192.168.0.100 255.255.255.0
```

7.2.4 Configure local IP address pool network interface

Please configure it in local IP address pool configuration mode：

- Create local IP address pool network interface

section section-id from-ip to-ip

- Delete local IP address pool network interface

no section section-id

section-id is the section id of this address pool which can configure at most 8 groups. from-ip is the start address of this address segment and to-ip is the end address. These two addresses must be in the address domain determined by this gateway and netmask and IP address in address pool cannot contain gateway.

Example：

！Create network interface of local IP address pool nic

```
OLT(config-ip-pool-nic)#section 0 192.168.0.100 192.168.0.200
```

！Delete network interface 0 of local IP address pool nic

```
OLT(config-ip-pool-nic)#no section 0
```

7.2.5 Disable/enable specified IP address in IP address pool

Configure it in local IP address pool configuration mode：

- Disable/enable specified IP address in local IP address pool network interface

ip { disable | enable }

ip-address must contain some network interface of locap IP address pool.

Example：

！Disable specified IP address 192.168.0.100 in local IP address pool network interface

```
OLT(config-ip-pool-nic)#ip disable 192.168.0.100
```

！Enable specified IP address 192.168.0.100 in local IP address pool network interface

```
OLT(config-ip-pool-nic)#ip enable 192.168.0.100
```

7.2.6 Configure lease

Configure it in local IP address pool configuration mode：

- Configure lease

```
lease day:hour:min
```

day:hour:min is the lease time which is accurated to minute. The shortest is 0:0:1 and the longest is 999:23:59. It is defaulted to be 1day.

For example：

！Configure lease time to be 1 day 1 hour 1minute

```
OLT(config-ip-pool-nic)#lease 1:1:1
```

7.2.7 Configure DNS

Configure it in local IP address pool configuration mode：

- Configure primary and second DNS

```
dns { primary-ip | second-ip } ip-address
```

- Delete primary and second DNS

```
no dns { primary-ip | second-ip }
```

- Configure DNS suffix

```
dns suffix suffix-name
```

- Delete DNS suffix

```
no dns suffix
```

Example：

！Configure primary DNS

```
OLT(config-ip-pool-nic)#dns primary-ip 192.168.0.100
```

！Delete primary DNS

```
OLT(config-ip-pool-nic)#no dns primary-ip
```

7.2.8 Configure WINS

Configure it in local IP address pool configuration mode：

- Configure primary and second WINS

```
wins { primary-ip | second-ip } ip-address
```

- Delete primary and second WINS

```
no wins { primary-ip | second-ip }
```

Example：

```
！Configure primary WINS
OLT(config-ip-pool-nic)#wins primary-ip 192.168.0.100
！Delete primary WINS
OLT(config-ip-pool-nic)#no wins primary-ip
```

7.2.9 Display IP address pool configuration

Use this command in any configuration mode：

```
show ip pool [ ippool-name [ section-num ] ]
```

Display configuration information of specified or all IP address pool

Example：

```
！Display all IP address pool configuration
OLT(config)#show ip pool
```

8. STATIC ROUTING CONFIGURATION

8.1. Brief introduction of static routing

OLT is a GE Intelligent Routing Switch based on ASIC technology which maintains a layer 3 transmission routing table to designate the next hop address and related information which can be dynamically learnt and manually configured. Static routing is the route manually designated to some address.

8.2. Static routing configuration

8.2.1 Static routing configuration list

Add/delete static route

Display route table information

8.2.2 Add/delete static route

Use this command to add a route table item to designate the next hop transmission address when communication with some address. Destination address, netmask and next hop address must be designated. If destination address and mask are all 0, the added route is defaulted route.

```
OLT(config)#ip route 192.168.0.100 255.255.255.255 10.11.0.254
```

Add a host route to 192.168.0.100 with the hop address being 10.11.0.254

```
OLT(config)#ip route 192.168.0.100 255.255.255.255 10.11.0.254
```

Delete host route to 192.168.0.100, the next hop address may or may not inputted, if it is input, it must be the same as that in real route table：

```
OLT(config)#no ip route 192.168.0.100 255.255.255.255
```

8.2.3 Display route table information

Use following commands to display existed route table information or specified route.

Display all static route：

```
OLT(config)#show ip route static
```

Display system core route：

```
OLT(config)#show ip route
```

Display system core route from 192.168.0.1 to 192.168.0.255

```
OLT(config)#show ip route 192.168.0.100 255.255.255.0
```

9. RIP CONFIGURATION

9.1. Brief introduction of RIP

RIP is short for Routing Information Protocol. It is a protocol based on D-V（Distance- Vector）algorithm which is widely used in real application. It submits routie information through UDP（User Datagram Protocol）and sends upgrade packet every 30 seconds. If local router hasn't received the upgrade packet from opposite end router after 180 seconds, local router will mark all routing information from the opposite end to be unreachable; if some route information hasn't received upgrade packet from the opposite end in 120 seconds after marking to be unreachable, local router will delete it from the route table.

The distance to the destination measured by Hop Count is Routing Metric. In RIP, the hop between router and the straightly connected network is 0, and the hop will be 1 if passing through a network which router can reach, and the rest may be deduced by analogy. To restrict convergfence time, RIP prescribe Metric is the intergeral number between 0 to 15. The hop larger or equal to 16 is defined to be infinite, that is, the destination host or network is unreachable.

There are such 2 versions as RIP-1 and RIP-2（RIP-2 supports plain text authentication）.

To improve capability and prevent routing ring, RIP supports Split Horizon and Poison Reverse.

Each router run RIP manages a routing database which contains all route item to all reachable desination. These route information includes:

Destination address: IP address of host or network.

Next hop address: the next router address passed when going to the destination.

Output interface: the interface transferring packet.

Metric value: the cost to the destination which is an intergeral number from 0 to 16.

Timer: the time is from the last time the router is modified. Every time when the router is modified, the timer is configured to be 0.

The process of RIP enabling and running is as following:

(1) Enabling RIP, router will send requery packet in the form of broadcast to neighbor routers. After receiving it, neighbor routers (must enable RIP) will send response packet which contains local route table information back.

(2) The router who has sent requery packet modifies local route table after receiving response packet.

(3) At the same time, RIP broadcasts or multicasts local route table every 30 seconds to neighbor routers to maintain local route and choose a best route, and then, broadcast and multicast modify informationto neighbor network to make global efficient of upgrading route. At the same time, RIP adopts overtime system to handle overtime route to guarantee real time of route, As internal route protocol, RIP makes router know the route information of the whole network through this system.

RIP has been one of the standard of delivering router and host route. The theory of switch with layer 3 switching IP packet is the same as that of router, so RIP is also adopted by layer 3 switch manufacturer. It can be used in simple structured, strong continuitydistrict network, such as: residential community network. For complicated large network, it is suggested not using RIP.

9.2. RIP configuration

9.2.1 RIP configuration list

In every configuration, enable RIP and RIP network before configuring other functions. Configuring functions which relates to interface is not restricted by RIP enabling. Caution: after disabling RIP, original parameter still exists, and it will be effective when enable RIP next time.

Configuration list is as following：

- Enable RIP
- Specify IP network to run RIP protocol
- RIP working status of specified interface
- RIP version of specified interface
- Enable host routing
- Enable route convergence
- Configure authentication to RIP packet
- Configure split
- Configure metricin
- Define prefix ACL
- Configure route redistribute
- Configure route filtration
- Display RIP configuration

9.2.2 RIP Enable RIP

By default, RIP is disabled. Enable RIP mode in global configuration mode:

- Enable RIP and enter RIP configuration mode

```
route rip
```

- Disable RIP

```
no route rip
```

9.2.3 Specify IP network to run RIP protocol

By default, after RIP enabling, no interface runs RIP protocol, only when administrator specifies some IP network to run RIP protocol, this interface will send and receive RIP packet. Configure it in RIP protocol configuration mode:

- Specify to run RIP protocol in IP network

```
network ip-address
```

- Cancel to run RIP protocol in IP network

no network ip-address

9.2.4 RIP working status of specified interface

Specify RIP working status in interface configuration mode, such as: run RIP or not in interface, receive and send RIP upgrade packet in interface or not; it can also specify sending (or receiving) RIP upgrade packet.

Configure it in interface configuration mode：

- Enable interface to run RIP

ip rip work

- Disable interface to run RIP

no ip rip work

After disabling interface running RIP, this interface will not send or receive RIP upgrade packet, but other interface still can send and receive route of tjis interface.

- Permit interface to receive RIP packet

ip rip input

- Forbid interface to receive RIP packet

no ip rip input

- Permit interface to send RIP packet

ip rip output

- Forbid interface to send RIP packet

no ip rip output

9.2.5 RIP version of specified interface

RIP has RIP-1 and RIP-2 two versions which can specify RIP packet version handled by interface.

RIP-1 uses broadcast and RIP-2 supports broadcast and multicast and it is defaulted to use multicast. Multicast address in RIP-2 is 224.0.0.9.

The advantage of using multicast is that in the same network interface, the host which is not running RIP can avoid receiving RIP broadcast; using multicast can avoid host which runs RIP-1receiving and handling route with subnet mask in RIP-2. When interface running rip-2, it can also receive RIP-1 packet.

Configure it in interface configuration mode:

- Specify RIP working version of interface to be RIPV1

ip rip version 1

- Specify RIP working version of interface to be RIPV2 multicast

ip rip version 2 mcast

- Specify RIP working version of interface to be RIPV2 broadcast

```
ip rip version 2 bcast
```

- Delete rip version number and configure it to default rip1

```
no ip rip version
```

9.2.6 Enable host routing

In some cases, RIP packet received by router contains host route table item which has little to do with searching address but occupies a lot of resources. Configure it to be sure whether the switch receives it.

Configure it in RIP protocol configuration mode:

- Permit host route

```
host-route
```

- Forbid host route

```
no host-route
```

9.2.7 Enable route convergence

Route convergence means routes of different subnetwork in the same network convergent to be a route with natural netmask when sending to other networks. Route convergence reduces route information volume and switching information volume.

RIP-1 only sends route with natural netmask, that is, send route out by using route convergence. RIP-2 supports network mask. When sending all routes out in the form of broadcasting, disable route convergence of RIP-2.

Configure it in RIP protocol configuration mode:

- Enable RIP-2 route convergence

```
auto-summary
```

- Disable RIP-2 route convergence

```
no auto-summary
```

By default, RIP-2 uses route convergence.

9.2.8 Define prefix list

A prefix-list is marked by prefix list name. Each prefix-list can contain many items and each item can specifies a matching range through sequence-number which shows the matching order in prefix-list.

When matching, switch will check each item according to ascending order. It will filtrate the prefix-list when there is one item matches.

⚠Caution: By default, if at least one prefix list is defined, the matching mode of at least one item is permit. Deny mode item can fast filtrate the route information which is not matched. If all item is in deny mode, any route will not pass the filtration. It can define an item of permit 0.0.0.0 to permit all route information to pass after many deny mode items.

Above situation can be changed by ip prefix-list default command. Details refer to command line configuration manual.

Configure it in global configuration mode：

- Create prefix ACL or adding item

ip prefix-list

- Delete prefix list or some item

no ip prefix-list

- Configure matching mode when prefix does not exist or there is no matching item

ip prefix-list default

- Restore to default matching mode when prefix does not exist or there is no matching item

no ip prefix-list default

9.2.9 Configure redistribution

RIP permits user to introduce other route protocol to RIP.

The route protocol that can be introduced are: connected, static and ospf.

Configure it in RIP protocol configuration：

- Introduce other route protocol

redistribute

- Cancel introduction of other route protocol

no redistribute

9.2.10 Configure distribute-list

Filtrate route through configuring strategy rules for receiving and sending route by specifying address prefix list. In addition, receive specified switch RIP packet by specifying neighbor switch.

Configure it in RIP protocol configuration：

- Configure RIP to filtrate received route

distribute-list prefix-list in

- Configure RIP to filtrate sent route

distribute-list prefix-list out

- Configure RIP to receive specified route

distribute-list gate-way in

- Cancel filtration

no distribute-list

9.2.11 Display RIP configuration

There are 3 commands to display RIP information.

- Display RIP statistics information

show ip rip

- Display RIP interface configuration, such as version, authentication

show ip rip interface

- Display RIP route table

show ip route rip

10. OSPF CONFIGURATION

10.1. Brief introduction of OSPF

OSPF is short for Open Shortest Path First which is an internal route protocol based on link status and the shortest path precedence. In IP network, it searches and transmits route dynamically through collecting and delivering link status of autonomy system; OSPF protocol supports packet authentication based on interface to guarantee the safety of route calculating; OSPF protocol sends and receives packets in the form of IP multicast.

Each router supported OSPF protocol maintains a database which describes the topology of the whole autonomy. This database collects the link states advertise (LSA). Each router broadcasts information describing local states to the whole autonomy. In each multiple accessing network, if there are two or more routers, designated router (DR) and backup designated router (BDR) are selected. Designated router broadcasts network link states advertise out. Introducing this concept can redeuce the number of neighborship between each router in multiple accessing network. OSPF protocol permits autonomy system dividing into areas to be managed. Routing information transmitted between areas will be furtherly abstracted to reduce bandwidth occupation.

OSPF uses 4 types of different routing, according to the precedence are:

- Inter Area Routing
- Area Border Routing
- The first type external routing
- The second type external routing

Inter Area Routing and Area Border Routing describe internal network structure of autonomy system; external routing describes how to select route to the destination out of autonomy system. Generally, the first type routing corresponds to information introduced by other internal routing protocol, the cost of which can be comparable with that of the OSPF itself; the second type of routing corresponds the information introduced by external routing protocol, the cost of which is far beyond that of OSPF itself. So when calculating, only external cost is considered.

According to libk state database, each router establishes a shortest path tree with the root of itself which can give out the routing to each node in autonomy system. External routing information appears in leaf node and it can broadcast its router to mark to keep record the extra information about autonomy system.

Areas of OSPF are connected by BackBone which with the mark of 0.0.0.0. All areas must be continuous logically. BackBone specially introduces virtual connection to guarantee the logical connection when the area is physically divided.

All the routers in the same area must be consensus the parameter configuration of this area. Therefore, when configuring routers in the same area, most configuration data must be considered based on area and error configuration may cause the non-communication of neighbour routers or routing information congestion and self-ring.

10.2. OSPF Configuration

10.2.1 OSPF Configuration list

OSPF Configuration list is as following:

- Enable/disable OSPF
- Configure router ID
- Specify interface and area id
- Configure area authentication type
- Configure interface type
- Configure interface cost
- Configure priority when selecting DR
- Configure Hello time interval
- Configure interface invalid time of neighbour routers
- Configure retransmission LSA time interval of neighbor router
- Configure time needed when interface sending link state update packet
- Configure packet authentication key
- Configure STUB area of OSPF
- Configure route convergence in OSPF
- Configure OSPF virtual connection
- Configure route introduced by OSPF other route protocol
- Configure OSPF introduced default route
- Configure external route parameter received by OSPF
- OSPF monitor and maintain

10.2.2 Enable/disable OSPF

Configure it in global configuration mode:

- Enable OSPF protocol

router ospf

- Disable OSPF protocol

no router ospf

It is defaulted to disable OSPF.

Example：

```
！Enable OSPF protocol
OLT(config)#router ospf
```

10.2.3 Configure router ID

Router ID is a 32 byte intergeral number without symbols wgich is the unique sign of a router in autonomy system and user must configure it. Configuring router ID manually must guarantee the router ID of any two routers are different. Generally, configure router ID to be the same as the IP address of some interface of router.

Configure it in global configuration mode:

- Configure router ID

router id router-id

- Cancel router ID

no router id

To guarantee the stability of running OSPF, when programming network, be sure the division of router ID and configure manually.

By default, choose the smallest IP address from interface IP to be router ID.

Example：

！Configure router ID when switch running OSPF

OLT(config)#router id 10.11.5.2

10.2.4 Specify interface and area id

OSPF protocol divided autonomy into different area which means dividing router to be different group. Some router will belong to different area (this kind of router is called Area Border Router ABR), and a neywork interface delongs to an area or every interface running OSPF protocol must use area ID to demonstrate which area belonged to. Different area uses ABR to transmit routing information.

In addition, all routers in the same area must be consensus the parameter configuration. Therefore, when configuring routers in the same area, most configuration data must be considered based on area and error configuration may cause the non-communication of neighbour routers or routing information congestion and self-ring. Configure it in OSPF protocol configuration mode:

- Specify interface and area number

network address wildcard-mask area area-id

- Cancel interface to run OSPF protocol

no network address wildcard-mask area area-id

After enabling OSPF, it should specifiy to be applied in which network interface and configure the area it belonged to. wildcard-mask can be IP address mask or the wildcard after NON the mask.

Example：

！Specify running OSPF in IP address 10.11.5.2

OLT(config-router-ospf)#network 10.11.5.2 255.255.255.0 area 0.0.0.0

10.2.5 Configure area authentication type

Authentication type of all routers in an area must be the same（support plain text authentication, MD5 encrypt authentication, not authentication）

- Configure area authentication type

area area-id authentication [message-digest]

- Restore interface authentication type to be non-authentication

no area area-id authentication

Example：

！Configure authentication of OSPF area 0 to be MD5

OLT(config-router-ospf)#area 0 authentication message-digest

10.2.6 Configure interface type

OSPF protocol calculating route is based on neighbor network topology of current router. Each router describes the network topology of its neighbor network and transmits it to other routers. According to link layer protocol type, devide network into following 4 types:

- Broadcast: when link layer protocol is Ethernet or FDDI, the network is defaulted to be Broadcast
- Non Broadcast MultiAccess (NBMA）：when link layer protocol is ATM, the network is defaulted to be NBMA.
- Point-to-Multipoint：none link layer protocol will be defaulted to be Point-to-Multipoint. Point-to-Multipoint must be changed from other types of network. Generally, change non-entire connetivity NBMA to Point-to-Multipoint.
- Point-to-Point：when link layer protocol is PPP, LAPB or POS, the network is defaulted to be Point-to-Point.

NBMA network is non-broadcasting, point-to-multipoint network, specially as ATM. Configure poll-interval to send poll-interval Hello packet time range before specifying neighborship established by router and neighbor routers.

In broadcasting network without multiple accessing, configure interface to be nonbroadcast.

If in NBMA network, not all routers can reach each other. Configure interface to be point-to-multipoint.

If there is one opposite end in NBMA network, configure interface to be point-to-point.

The difference between NBMA and point-to-multipoint:

- In OSPF protocol, NBMA is connectivity, non-broadcasting, multipoint reaching network. Point-to-multipoint network need not entire connectivity.
- In NBMA, it needs selecting DR and BDR，while in point-to-multipoint, there is no DR and BDR.
- NBMA is a default network, such as: if link layer protocol is ATM，OSPF will defaulted to think the interface is NBMA（no matter this network is entire connectivity or not）. Point-to-multipoint is not default network type. None link protocol is thought to be point-to-multipoint. Point-to-multipoint must be forced to be changed from other network type. Generally, change non-entire connectivity to be point-to-multipoint.

- NBMA uses unicast sending packet which needs configure neighbor manually. Point-to-multipoint uses multicast sending packet.

The link layer protocol of switch is Ethernet, OSPF thinks network type is broadcast. Generally, not change its network type,

Configure it in interface configuration mode.

- Configure network type of interface

ip ospf network { broadcast | non-broadcast | point-to-multipoint | point-to-point }

- Restore dewfault network type of interface

no ip ospf network

Example：

！Configure VLAN interface 4 to be broadcast

OLT(config-if-VLANInterface-4)#ip ospf network broadcast

10.2.7 Configure interface cost

User can configure cost of interface sending packet, or OSPF defaults cost to be 1. Configure it in interface configuration mode:

- Configure cost of VLAN interface to send packet

ip ospf cost cost

- Restore the default cost of VLAN interface to send packet

no ip ospf cost

Example：

！Configure cost of VLAN interface 3 to be 10

OLT(config-if-VLANInterface-3)#ip ospf cost 10

10.2.8 Configure priority when selecting DR

The priority of router interface determines the competency in selecting“designated router”. The superior priority is firstly considered in conflict. Designated router (DR) is not determined by human, but selected by all routers in the network interface. The router in this network interface whose Priority > 0 can be the candidate. Choose the one with the superior priority to be the so called DR. If the priority is the same, choose the one with larger router ID. The vote is the Hello packet. Each router writes its own DR into Hello and sends it to each router in the network interface. When two of them declairing that they are the DR, choose the one with superior priority. If they have the same priority, choose the one with the larger router ID. The one with the priority being 0, he will not be selected to be DR or BDR.

If DR is failure because of some fault, routers must select DR again at the same time. It costs a long time. During this time, the calculation of router is not correct. In order to shorten it, BDR（ Backup Designated Router）is brought up. BDR is a abackup for DR. Select BDR at the same time as DR. It establishes neighborship and exchange routing information with the routers in the network interface. After the failure of DR, BDR is about to be DR because the neighborship has been established. There will be reselected a new BDR which will not be effected the calculation of router though it needs a long time.

Caution:

- DR is not always the router with the superlative priority and BDR is not always the one with the second superlative priority. After selecting DR and BDR, a new router adds, no matter how superlative its priority is, it will not be DR.
- DR is the definition in a network interface which is for router interface. A router may be DR in an interface and may be BDR or DRother in another interface.
- Selecting DR in broadcast or NBMA interface, it is unnecessary to select DR in poit-to-poit or poit-to-multipoit interface.

Configure it in interface configuration mode:

- Configure the priority of interface to select “designated router”

```
ip ospf priority value
```

- Restore the default value

```
no ip ospf priority
```

By default, the priority of VLAN interface to select “designated router” is in the range of 0 ~ 255

Example：

```
！Configure priority of VLAN interface 3 to be 100
OLT(config-if-VLANInterface-3)#ip ospf priority 100
```

10.2.9 Configure Hello time interval

Hello packet is a geneally used packet which is periodically sent to neighbor router to search and maintain neighborship and select DR and BDR. User can configure time interval of sending Hello packet. The smaller the hello-interval is, the faster the changes of network is found. The hello-interval of routers in the same network must be the same.

After enabling a router, it sends Hello packet to the neighbor node whose priority is larger than 0 (the routers can be selected as DR or BDR). After selecting of DR and BDR, they will send Hello packet to all neighbors to set up neighborship. If neighborship fails, router periodically send Hello packet according to the time interval of poll-interval command until neighbor router can be used again. The value of poll-interval is three times of the value of hello-interval. When the time interval of sending Hello packet is changed, configure the value of poll-interval. Configure it in interface configuration mode:

- Configure time interval of sending hello packet

```
ip ospf hello-interval seconds
```

- Restore the default time interval of sending hello packet

```
no ip ospf hello-interval
```

By default, the time interval of point-to-point, broadcast interface sending Hello packet to be 10 seconds and point-to-nultipoint, nonbroadcast interface sending Hello packet to be 30 seconds.

Example：

！Configure time interval of VLAN interface 3 sending hello packet to be 15

```
OLT(config-if-VLANInterface-3)#ip ospf hello-interval 15
```

10.2.10 Configure interface invalid time of neighbour routers

The dead interval of OSPF neighbor is: in the time interval, if the Hello packet hasn’t received, it is thought the neighbor is ineffective. dead-interval seconds must be 4 times of Hello-interval seconds, and the dead-interval must be the same in the same network interface.

Configure it in interface configuration mode:

- Configure dead interval of neighbor routers.

```
ip ospf dead-interval seconds
```

- Restore the default dead interval

```
no ip ospf dead-interval
```

The default dead interval of OSPF neighbor for Point-to-point and broadcast is 40 seconds; The default dead interval of OSPF neighbor for point-to-multipoint, non-broadcast is 120seconds.

Example:

！Configure the dead interval of interface 3 to be 60seconds

```
OLT(config-if-VLANInterface-3)#ip ospf dead-interval 60
```

⚠Caution: After modifying network type, hello-interval and dead-interval are restore to the default value.

10.2.11 Configure retransmission LSA time interval of neighbor router

When a router sending “Link Status Advertisement”（LSA）, it needs to receive the confirm. If the confirm hasn’t received in LSA retransmit interval, this LSA will be retransmit. User can configure retransmit-interval value.

Configure it in interface configuration mode:

- Configure the retransmit interval of sending LSA between neighbour routers

```
ip ospf retransmit-interval seconds
```

- Restore the default value of retransmit interval of sending LSA between neighbor routers

```
no ip ospf retransmit-interval
```

By default, the retransmit interval of sending LSA between neighbour routers is 5 seconds.

Example：

！Configure LSA retransmit interval of VLAN interface 3 to be 3 seconds.

```
OLT(config-if-VLANInterface-3)#ip ospf retransmit-interval 3
```

10.2.12 Configure time needed when interface sending link state update packet

In LSU packet, the aging time of LSA will add a transmit-delay before sending. LSA will be aging (1 more minute per second) with time in Link Status DateBase (LSDB) of this router but it will not be aging in network transmission, so it is necessary to add the configured time before sending LSA. This configuration is very important in network with low speed.

Configure it in interface configuration mode:

- Configure the time of sending LSU

```
ip ospf transmit-delay seconds
```

- Restore the default LSU time

```
no ip ospf transmit-delay
```

By default, the time of sending LSU is 1 second.

Example：

！Configure LSA delay interval of VLAN interface 3 to be 3 seconds.

```
OLT(config-if-VLANInterface-3)#ip ospf transmit-delay 3
```

10.2.13 Configure packet authentication key

OSPF supports simple or MD5 encryption authentication between neighbour routers.

Configure it in interface configuration mode:

- Configure interface simple authentication key

```
ip ospf authentication-key password
```

- Cancel interface simple authentication key

```
no ip ospf authentication-key
```

- Configure interface MD5 authentication key

```
ip ospf message-digest-key key-id md5 key
```

- Cancel interface MD5 authentication key

```
no ip ospf message-digest-key
```

By default, non-authentication is configured.

Password is a character string of 1 ~ 8 bytes;

key-id is intergeral number between 0 ~ 255；

key is a character string of 1 ~ 16 bytes.

Example：

！Configure simple authentication key of VLAN interface 3 to be abc123

```
OLT(config-if-VLANInterface-3)#ip ospf authentication-key abc123
```

10.2.14 Configure STUB area of OSPF

Stub area is special LSA area. ABR in stub area doesn't transmit the router outside of autonomy system. The scale of routing table and transmission number of routing packet in these areas will greatly reduced.

Stub area is optional configuration attribution, but not every area can suit the configuration condition. Generally, stub area locates in the edge of autonomy system which is the non-backbone area with one ABR; or there are many ABRs, but no virtual connection is configured between ABRs.

To guarantee the reachable of router out of autonomy system, ABR in this area will generate a default route (0.0.0.0) and distribute it to other non-ABR router in this area.

Pay attention to followings when configuring Stub area：

- Backbone area cannot configure to be Stub area and virtual connection cannot pass through Stub area.
- If configuring an area to be Stub area, all routers in this area must configure this attribution.
- There cannot be ASBR in Stub area, that is, external router cannot transmit in this area.

Configure it in OSPF protocol configuration mode:

- Configure an area to be Stub area

area area-id stub [no-summery]

- Cancel configured Stub area

no area area-id stub

- Configure the cost to default router of Stub area

area area-id default-cost cost

- Cancel the cost to default router of Stub area

no area area-id default-cost

By default, Stub area is not configured; the cost to default router of Stub area is 1.

There are two configuration command in STUB area: area stub and area default-cost. All routers connected to STUB area must use area stub command to configure to be STUB attribution. Command area default-cost only be effective in ABR configuration. This command can specify the cost for ABR to send default routing to STUB area.

For reducing the number of Link State Advertisement (LSA) sent to STUB,configure no-summary in ABR to forbid ABR to send summary LSAs（LSA type 3）to STUB area.

Example:

！Configure area 1.1.1.1 to be stub area and configure the cost to default router of Stub area to be 10

```
OLT(config-router-ospf)#area 1.1.1.1 stub
OLT(config-router-ospf)#area 1.1.1.1 default-cost 10
```

10.2.15 Configure route convergence in OSPF

Route convergence is: ABR can convergent the route information with the same prefix together and distribute one route to other area. One area can configure many convergent network interface so that OSPF can convergent many network interface. ABR sends route information to other area to generate Sum_net_Lsa（Type 3 LSA）with the unit of network interface. If there are some continuous network interface in area, use area range command to convergent these continous network interface to be one network interface. ABR sends one convergent LSA and LSA located in specified convergent network will not be sent separately which can reduce the scale of LSDB in other areas.

Convergent them to be one network interface：202.38.0.0 255.255.0.0

Once adding convergent network interface of some network interface to area, the internal route whose IP address locates in this network interface will not be broadcasted to other area but broadcast the abstract information of the whole convergent network route. If the network interface is restricted by keyword not-advertise, the abstract information to this network route will not be broadcasted. This network is demonstrated by IP address/ mask. Receiving convergent network and restricting it will reduce the exchange volume of route information in areas.

Caution: Route convergence is effective in ABR configuration.

Configure it in OSPF protocol configuration mode:

- Configure OSPF area route convergence

```
area area-id range address mask [ advertise | not advertise]
```

- Cancel OSPF area route convergence

```
no area area-id range address mask
```

By default, route in areas will not be convergent.

Example：

！Convergent 202.38.160.0 255.255.255.0 and 202.38.180.0 255.255.255.0to be one route

202.38.0.0 255.255.0.0

```
OLT(config-router-ospf)#area 1.1.1.1 range 202.38.0.0 255.255.0.0
```

10.2.16 Configure OSPF virtual connection

After dividing SOPF areas, not all areas are equal. One area with the area-id being 0.0.0.0 is different which is called BackboneArea. The update of OSPF route in non- BackboneArea is through BackboneArea. OSPF protocol regulates: all non- BackboneArea must be connected with BackboneArea, that is, there must be at least one interface of ABR in area 0.0.0.0. If there is an area which is not physically connected with BackboneArea 0.0.0.0, there must establish a virtual connection.

If the physical connection cannot be proved because of the restriction of network topology, create virtual connection. Virtual connection means two ABRs set up a physical connection through interbal route area of a non-Back Bone Area. The ends must be ABR and it can be effective when configuring at both two sides. Virtual connection is marked by route ID of the opposite end. The internal area supported a non-Back Bone Area for the two ends of the virtual connection is called Transit Area and its area number must be demonstrated when configuring.

Virtual connection is activated after the calculation of transmitting area route which equals to form point-to-point link between two ends, so in this connection, it can also configure interface parameter as physical interface, such as sending HELLO packet interval.

"Logical channel" means serval routers running OSPF between two ABRs which only transmit packet (the destination address of protocol packet are not these routers, so packet is transmitted as general IP packet) and two ABRs can straightly transmit router information. Here, router information means type 3 LSA generated by ABR, so the synchronization of routers in area do not changed.

Caution: If autonomy system is divided to be one or more areas, there must be one Back Bone area to guarantee the straightly or logically connection between other areas and Back Bone area and Back Bone area itself must be connected.

Configure it in OSPF protocol configuration mode:

- Create and configure virtual connection

area area-id virtual-link router-id [hello-interval seconds] [retransmit- interval seconds] [transmit-delay seconds] [dead-interval seconds] { [authentication-key key] | [message- digest-key keyid md5 key] }

- Cancel created virtual connection

no area area-id virtual-link router-id [hello-interval seconds] [retransmit- interval seconds] [transmit-delay seconds] [dead-interval seconds] { [authentication-key key] | [message- digest-key keyid md5 key] }

By default, area-id and router-id has no default value；the value of hello-interval is 10 seconds ；the value of retransmit-interval is 5 seconds；the value of transmit-delay is 1 second；the value of dead-intervalis 40 seconds.

Example：

！Configure a virtual connection with the transmission area being 1.1.1.1，router-id of the opposite end being 10.11.5.2

OLT(config-router-ospf)#area 1.1.1.1 virtual-link 10.11.5.2

10.2.17 Configure route introduced by OSPF other route protocol

Each dynamic routing protocol can share routing information. Because of OSPF, router found by other routing protocol always be handled as external routing information of autonomy.

OSPF uses following 4 kinds of different router which as priority order are:

- Inter Area Routing
- Area Border Routing
- The first category external routing

- The second category external routing

The description of routing in or between area is for network structure in Autonomy system. External routing describes how to choose destination routing out of Autonomy system.

The first category external routing is received IGP router (such as: RIP and STATIC). This kind of router is more credible, so the cost volume of external router and autonomy system is the same and can compare with the router of OSPF itself, that is, the cost to external router= the cost to its ASBR +the cost of ASBR to destination address.

The second category external routing is the received EGP router. This kind of router is less credible, so the cost volume of ASBR to the outside of autonomy system is far more expensive than that of autonomy system to ASBR, so the former is mainly considered, that is, the cost to the second external router = the cost of ASBR to destination address. If the cost is the same, consider the cost of this router to corresponded ASBR.

Configure it in OSPF protocol configuration mode:

- Introduce route information of other protocol

redistribute protocol [metric metric] [type 1 | 2] [tag tag-value]

- Cancel route information of other protocol

no redistribute protocol

By default，OSPF doesn’t introduce route information of other protocol.

protocol means introduced source routing protocol which can be connected, rip, static, RIP, IS-IS and BGP.

Example：

！Configure OSPF introduce RIP router

```
OLT(config-router-ospf)#redistribute rip
```

10.2.18 Configure OSPF introduced default route

Use redistribute static command cannot introduce default routing. Use default-information originate command to introduce default router to OSPF routing domain.

Configure it in OSPF protocol configuration mode:

- Introduce default route to OSPF

default-information originate [always] [metric metric-value] [type type-value]

- Cancel introduced default route

no default-information originate

By default，OSPF will not introduce any default route.

Example：

！Configure OSPF introduce default route

```
OLT(config-router-ospf)#default-information originate always
```

10.2.19 Configure external route parameter received by OSPF

When OSPF introducing route information found by other route protocol to autonomy system, configure some extra parameter, such as the default cost and mark of introduced router. Route mark can used to mark protocol related information,, such as the number to distinguish autonomy system when OSPF receiving BGP.

Configure it in OSPF protocol configuration mode:

- Configure default cost when OSPF receiving external route

```
default redistribute metric metric
```

- Restore metric of received external route

```
no default redistribute metric
```

- Configure default type when OSPF receiving external route

```
default redistribute type { 1 | 2 }
```

- Restore default type of received external route

```
no default redistribute type
```

By default, the metric of received external route is 1 and type is 2.

Example：

！Configure the metric of received external route to be 10

```
OLT(config-router-ospf)#default redistribute metric 10
```

10.2.20 OSPF monitor and maintain

Followings are display command:

show ip ospf	Display OSPF information.
show router id	Display configured router ID
show ip ospf neighbor	Display OSPF neighbor.
show ip ospf database	Display OSPF LSDB.
show ip ospf virtual-link	Display OSPF virtual link
show ip ospf border-routers	Display OSPF edge router
show ip ospf interface	Display OSPF interface
show ip route ospf	Display OSPF routing table.
show ip ospf cumulative	Display OSPF statistic.
show ip ospf error	Display OSPF error
show ip ospf request-list	Display OSPF request list.
show ip ospf retrans-list	Display OSPF retransmit list

These commands can be used in any configuration mode.

Example：

！Display OSPF information

```
show ip ospf
```

```
OLT(config-router-ospf)#show ip ospf
！Display OSPF neighbor information
show ip ospf neignbor
OLT(config-router-ospf)#show ip ospf neighbor
！Display OSPF virtual link information
show ip ospf virtual-link
OLT(config-router-ospf)#show ip ospf virtual-link
！Display LSDB information
show ip ospf database
OLT(config-router-ospf)#show ip ospf database
```

11. MULTICAST PROTOCOL CONFIGURATION

11.1. Brief introduction of GMRP

GMRP（GARP Multicast Registration Protocol） is a kind of application of GARP（Generic Attribute Registration Protocol）, which is based on GARP working mechanism to maintain the dynamic multicast register information in switch. All switches supported GMRP can receive multicast register information from other switches and upgrade local multicast register information dynamically and transfer it to other switches to make the consistency of multicast information of devices supported GMRP in the same switching network. Multicast register information transferred by GMRP includes local manual configuration of static multicast register information and the dynamic multicast register information of other switch.

11.2. GMRP Configuration

11.2.1 GMRP Configuration list

In all configurations, enable global GMRP first before enable GMRP on a port. GMRP Configuration list is as following: :

- Enable/disable global GMRP
- Enable/disable GMRP on a port
- Display GMRP
- Add/delete multicast that can be dynamic learnt by GMRP
- Display multicast that can be learnt by GMRP

11.2.2 Enable/disable global GMRP

Please configure it in global configuration mode:

- Enable global GMRP

```
gmrp
```

- Disable global GMRP

```
no gmrp
```

By default, GMRP globally disables

For example:

```
! Enable GMRP globally
OLT(config)#gmrp
```

11.2.3 Enable/disable GMRP on a port

Enable global GMRP before enable GMRP on a port. Please configure it in interface configuration mode:

- Enable GMRP on a port

```
gmrp
```

- Disable GMRP on a port

no gmrp

For example:

！Enable GMRP on Ethernet port 3

OLT(config-if-ethernet-0/3)#gmrp

⚠ Caution: Enable global GMRP before enable GMRP on a port. By default, global GMRP deisables and GMRP on a port can be enabled in trunk mode interface.

11.2.4 Display GMRP

- Use following command in any configuration mode to display global GMRP：

show gmrp

- Use following command in any configuration mode to display GMRP on a port：

show gmrp interface [interface-list]

Interface-list keyword is optional. If this keyword unspecified, the command displays GMRP information for all the Ethernet ports. If specified, the command displays GMRP information on specified Ethernet port.

For example:

！Display GMRP information of Ethernet 0/2 to ethernet 0/4 ethernet 2/1

OLT(config)#show gmrp interface ethernet 0/2 to ethernet 0/4 ethernet 2/1

11.2.5 Add/delete multicast that can be dynamic learnt by GMRP

Add configured static multicast group to GMRP for other switches to dynamically learn.

garp permit multicast [mac-address mac VLAN VLAN-id]

Example：

Add 01:00:5e:00:01:01 VLAN 1 to GMRP

OLT(config)#garp permit multicast mac-address 01:00:5e:00:01:01 VLAN 1

11.2.6 Display multicast that can be learnt by GMRP

Display multicast group can be statically learnt by GMRP.

show garp permit multicast

For example: Display multicast group that can be statically learnt by GMRP.

OLT(config)#show garp permit multicast

11.3. IGMP Snooping Configuration

11.3.1 Brief introduction of IGMP Snooping

IGMP（Internet Group Manangement Protocol）is a part of IP protocol which is used to support and manage the IP multicast between host and multicast router. IP multicast allows transferring IP data to a host collection formed by multicast group. The relationship of multicast group member is dynamic and host can dynamically add or exit this group to reduce network load to the minimum to realize the effective data transmission in network.

IGMP Snooping is used to monitor monitor IGMP packet between host and routers. It can dynamically create, maintain and delete multicast address table according to the adding and leaving of the group members. At that time, multicast frame can transfer packet according to his own multicast address table.

11.3.2 IGMP Snooping configuration

Use following command to control IGMP Snooping to establish the MAC address multicast transmission table in layer 2.

Use following command in global configuration mode:

- Enable IGMP Snooping

```
igmp-snooping
```

- Disable IGMP Snooping

```
no igmp-snooping
```

By default，IGMP Snooping disables.

- Display IGMP Snooping

Use following command in any mode to see IGMP Snooping:

```
show igmp-snooping
```

For example:

！Display IGMP snooping information

```
OLT(config)#show igmp-snooping
```

11.3.3 IGMP Snooping multicast interface aging time configuration

Use following command in global configuration mode to configure host-aging-time dynamic multicast group learnt by igmp-snooping：

```
igmp-snooping host-aging-time
```

Use following command to display host-aging-time dynamic multicast group learnt by igmp-snooping：

```
show igmp－snooping
```

For example:

！Configure host-aging-time of the dynamic multicast group learnt by igmp-snooping to be 10 seconds

```
OLT(config)#igmp-snooping host-aging-time 10
```

11.3.4 IGMP Snooping max-response-time configuration

Configure the max response time to delete group interface when receiving a leave packet:

```
igmp-snooping max-response-time seconds
```

Use this command in global configuration mode.

For example:

！Configure the max-response-time of igmp-snooping is 13 seconds

```
OLT(config)#igmp-snooping max-response-time 13
```

11.3.5 IGMP Snooping interface fast-leave configuration

Configure interface fast-leave when fast-leave enables, if the fast-leave packet is received, the interface leaves the aging group, or the time to leave is determined by the max-response- time ：

```
igmp-snooping fast-leave
```

Use this command in interface configuration mode.

For example:

！Enable igmp-snooping fast-leave

```
OLT(config-if-ethernet-0/1)#igmp-snooping fast-leave
```

11.3.6 Configure the number of the multicast group allowed learning

Use igmp-snooping group-limit command to configure the number of the multicast group allowed learning.

```
igmp-snooping group-limit limit
```

Use this command in global configuration mode.

For example:

！Configure the igmp-snooping group-limit to be 10

```
OLT(config-if-ethernet-0/1)#igmp-snooping group-limit 10
```

11.3.7 IGMP Snooping permit/deny group configuration

Configure igmp-snooping permit/deny group and default group learning regulation.

Configure igmp-snooping permit/deny group in interface configuration mode:

```
igmp-snooping permit/deny group group-address
```

Configure igmp-snooping default group learning regulation in global configuration mode：

igmp-snooping deny/permit group all

For example:

！Configure Ethernet 0/1 not to learn multicast 01:00:5e:00:01:01

OLT(config-if-ethernet-0/1)#igmp-snooping deny group 01:00:5e:00:01:01

！Configure the learning regulation of default group to allow all multicast group

OLT(config)#igmp-snooping permit group all

11.3.8 IGMP Snooping route-port forward configuration

Multicast routers interface is the interface received IGMP inquiring packet (It is also called mix router interface.).

Use igmp-snooping route-port forward command to configure whether to add router interface to IGMP snooping learning group. By default, router interface to IGMP snooping learning group is not added.

Use following command in global configuration mode:

igmp-snooping route-port forward

no igmp-snooping route-port forward

For example:

！Enable igmp-snooping route-port forward

OLT(config)#igmp-snooping route-port forward

11.3.9 IGMP Snooping multicast VLAN configuration

Use igmp-snooping multicast VLAN command to specify a VLAN for a port to learn and transmit multicast packet. IGMP packet intercepted by IGMP Snooping will modify its VID to be specified VLAN to transmit. Descendent multicast packet is transmitted in VLAN, and separated with unicast packet VLAN.

It will be effective as soon as the creation of multicast VLAN of interface. Use this command in interface configuration mode:

igmp-snooping multicast VLAN

VLAN-id no igmp-snooping

multicast VLAN

For example:

！Configure multicast VLAN of Ethernet 0/1 to be VLAN 2 OLT(config-if-ethernet-0/1)#igmp- snooping multicast VLAN 2

11.4. Static Multicast Configuration

11.4.1 Brief introduction of Static Multicast

Static multicast configuration command is used to crewate multicast group and add interfaces to it. If the switch supports multicast, when receiving multicast packet, detect whether there is multicast group. If it doesn’t exist, transfer the multicast packet as broadcast packet. If it exists, transfer the multicast packet to all interface members of this multicast group.

11.4.2 Static Multicast Configuration

Static Multicast Configuration list

Configure static multicast in following turns:

- Create multicast group
- Add interfaces to multicast group
- Display multicast group information
- Delete interface members from multicast group
- Delete multicast group

Create multicast group

Use following command in global configuration mode to create a multicast group:

multicast mac-address mac VLAN VLAN-id

mac：The mac address of multicast group displayed in the form of multicast address, such as: 01:00:5e:**:**:**.VLAN-id ranges from 1 to 4094. If the VLAN doesn’t exist, the multicast group adding fails.

Example:

！Create a multicast group to VLAN 1 with the mac address being 01:00:5e:01:02:03

OLT(config)#multicast mac-address 01:00:5e:01:02:03

VLAN 1 Add interfaces to multicast group

Use multicast mac-address VLAN interface command in global configuration mode to add interface to existed multicast group:

multicast mac-address mac VLAN VLAN-id interface { all | interface-list }

mac：Means mac address of existed multicast which is in the form of multicast mac-address, such as: 01:00:5e:**:**:**. VLAN-id ranges from 1 to 4094. Multicast group is assembled by VLAN-id and mac-address. Interface-list is optional. If all is chosen, all interfaces in system in multicast mac-address VLAN interface command. If the VLAN doesn’t exist, the multicast group adding fails.

For example：

！Add interface Ethernet 0/2 to ethernet 0/4 ethernet 0/8 to existed multicast group

OLT(config)#multicast mac-address 01:00:5e:01:02:03 VLAN 1 interface ethernet 0/2 to ethernet 0/4 ethernet 0/8

Display multicast group information

Use show multicast command to display the information of the specified or all existed multicast group which includes multicast group interface information, IGMP interface list information:

```
show multicast [ mac-address mac ]
```

Mac is the mac address existed in multicast group. If mac-address is not specified, input show multicast command, information of the entire multicast group is displayed.

For example:

！Display the information of multicast group with the MAC address to be 00:00:00:00:00:00

```
OLT(config)#show multicast mac-address 00:00:00:00:00:00
show multicast table information

MAC Address      : 00:00:00:00:00:00
VLAN ID          : 1
Static port list : e0/2,e0/3.
IGMP port list
Dynamic port list
Total entries: 1
```

Delete interface members from multicast group

Use following command in global configuration mode to delete multicast interface member:

```
no multicast mac-address mac VLAN VLAN-id interface { all | interface-list }
```

The meaning of mac, VLAN-id and interface-list is the same as that in adding interfaces. Interface in interface-list means the interface member existed in multicast group. All means all the members in multicast group.

For example:

！Delete interface ethernet 5, 6 from existed multicast group.

```
OLT(config)#no multicast mac-address 00:00:00:00:00:00 VLAN 1 interface ethernet 0/5 ethernet 0/6
```

Delete multicast group

Use following command in global configuration mode to delete specified mac address and the multicast group of specified VLAN ID or all multicast groups:

```
no multicast [ mac-address mac VLAN VLAN－id ]
```

The meaning of mac, VLAN-id and interface-list is the same as that above. They are corresponded to be existed multicast group.

For example：

！Delete multicast group with the mac address being 00:00:00:00:00:00and VLAN ID being 1

```
OLT(config)#no multicast mac-address 00:00:00:00:00:00 VLAN 1
```

11.5. Brief Introduction of IGMP

IGMP defines the establishement and maintenance of the multicast membership between host and switch which is the base of the whole IP group. Host adds to multicast group by sending IGMP packet. Multicast router uses IGMP to know whether there is multicast group member in the subnet connected to router.

If there is one user in LAN declaring adding to some multicast group through IGMP, multicast router in LAN will transmit this information through multicast route protocol and add this LAN to multicast tree (the collection of multicast information distributing paths) as a branch. Host in multicast tree branch starts sending and receiving multicast information as the member of the multicast group. The multicast router connected with this branch will periodically query this multicast group to see whether there is any member in it. If there is a host taking part in sending and receiving multicat information, multicast router will continue to send and receive multicast data; when all users leave this multicast group, this branch will be deleted.

Now, Version 1 and Version 2 of IGMP is widely used: IGMP Version 2 specifies three types of packet: multicast member query packet, report packet and leave packet.

Multicast member query packet: There are general query packet and special group query packet according to multicast address. It uses general query packet to know the multicast group; special group query packet is used to query the member of some special multicast group to avoid members of other multicast group to send response packet.

Multicast member report packet: after host received a general or special group member query packet, it will multicast group member report to switch which supports multicast. After receiving group member packet, switch add members in report to member listof the network where the switch locates. If in special response time, switch do not receive the response of any member which means there is no member, it will not transmit multicast packet to the network it connected.

Multicast member leave packet: when a host leaving a multicast group, IGMP will send a leave packet to all switches which support multicast.

IGMP is asymmetricbetween host and switch: host need response IGMP query packet (response in the form of member report packet); switch need send general query packet timely and be sure whether there is host to add to some specified multicast group in its subnet according to the received response packet.

11.6. IGMP configuration

11.6.1 IGMP configuration list

Enable multicast route before configuring IGMP.

IGMP configuration list is as following:

- Enable multicast protocol
- Specify interface running IGMP protocol
- Specify interface running IGMP version
- Configure the time interval switch sending query packet
- Configure switch sending the last member query interval
- Configure switch robustness-variable
- Configure the number of the multicast group restricted switch interface to add
- Configure IGMP the max response time of query packet
- Configure interface accessing control list
- Configure switch interface to add to multicast group
- Configure ingress VLANid of static multicast group
- members IGMP monitor and maintenance

11.6.2 Enable multicast protocol

Only after enabling multicast protocol, other configuration related to multicast can be effective.

Configure it in global configuration mode:

- Enable multicast protocol

ip multicast-routing

- Dsiable multicast protocol

no ip multicast-routing

By default, multicast protocol disables

11.6.3 Specify interface running IGMP protocol

Enable IGMP protocol in interface before switch sending multicast packet.

Configure it in interface mode（ include VLAN and SuperVLAN interface

）：

Run IGMP in specified interface

ip igmp

Disable IGMP in interface

no ip igmp

fault, IGMP is run in any interface.

Caution: Enable IGMP protocol in interface before switch sending multicast packet.

11.6.4 Specify interface running IGMP version

All system run in the same subnetwork must support the same IGMP version switch can find the switch with other version automatically and inform sys-log, but it cannot shift it automatically.

Configure it in interface mode（include VLAN and Super VLAN interface）：

- Configure the version of run IGMP in switch interface

```
ip igmp version { 1 | 2 | 3}
```

- Restore the default version of run IGMP in switch interface

```
no ip igmp version
```

By default, switch interface runs IGMP Version 2.

Caution: Before configuring interface IGMP, interface must run IGMP protocol. Following commands which configure interface attribution should be attention.

11.6.5 Configure the time interval switch sending query packet

Switch need periodically send Membership Query Message to the network it connected. The time interval id determined by Query Interval timer. User can modify the time interval of IGMP host sending query packet by configuring Query Interval timer.

Configure it in interface mode（include VLAN and SuperVLAN interface）：

- Configure the time interval of IGMP host sending query packet.

```
ip igmp query-interval seconds
```

- Restore default time interval of IGMP host sending query packet.

```
no ip igmp query-interval seconds
```

By default, time interval of IGMP host sending query packet is 125 seconds.

11.6.6 Configure switch sending the last member query interval

When switch receives leave packet, it will send special group query packet to know whether there is group member. User can modify the time interval of switch sending special group query packet.

Configure it in interface mode（include VLAN and SuperVLAN interface）：

- Configure the time interval of switch sending last member query packet

```
ip igmp last-member-query-interval seconds
```

- Restore default time interval of switch sending last member query packet

```
no ip igmp last-member-query-interval
```

By default, time interval of switch sending last member query packet is 1 second.

⚠ Caution: Only when switch interface running IGMP V2/V3，this configuration iseffective.（though running IGMP Version 1 this command can be configured.）

11.6.7 Configure switch robustness-varible

The robustness-varible is a very important parameter to express the operation of IGMP which is used to control the numberof sending packetto prevent the loss of the packet in network to strengthen the operation of network protocol.

Configure it in interface mode（include VLAN and SuperVLAN interface）：

- Configure switch robustness-variable

```
ip igmp robustness-variable num
```

- Restore default robustness-variable

```
no ip igmp robustness-variable
```

By default, robustness-variable is 2.

11.6.8 Configure the number of the multicast group restricted switch interface to add

Use this command to restrict the number of IGMP group added in interface, the router will not handle IGMP adding packet if it is beyond the restriction. By default, the max number of IGMP group added in interface is the max number of multicast group number (that is max hardware table item, considering it can use up all hareware table items through one interface). In configuration, if the added number of IGMP group is beyond the configuration, the added IGMP group will not be deleted. Repeat this command, the new configuration will cover the original.

Configure it in interface mode（include VLAN and SuperVLAN interface）:

- Configure the number of the multicast group restricted switch interface to add.

```
ip igmp limit-group num
```

- Restore the default number of the multicast group restricted switch interface to add.

```
no ip igmp limit-group
```

By default, the number of the multicast group restricted to add is 1024.

11.6.9 Configure IGMP the max response time of query packet

After host receiving the query packet from switch, it will enable a Delay Timers for each multicast group it added to, and use a random number between (0，Max Response Time] to be the start value, and Max Response Time is the max response time specified by query packet (the max response time of IGMP Version 1 is 10 seconds). Host should inform switch multicast group members before the time is up. If switch hasn’t received any multicast member report after the max response time, it thought there is no members in local group and it will never transmit multicast packet it received to network.

Configure it in interface mode（include VLAN and SuperVLAN interface）

- Configure the max response time of query packet of host members

```
ip igmp query-max-response-time seconds
```

- Restore the default max response time.

no ip igmp query-max-response-time

By default, the max response time in query packet of host member is 10 seconds.

⚠ Caution: Only when switch interface running IGMP V2/V3 , this configuration is effective (though running IGMP Version 1 this command can be configured.)

11.6.10 Configure interface accessing control list

Multicast switch makes sure which multicast group contains local group members which connected to switch by sending IGMP query packet. Configure a filtration in interface to make host add to multicast group regulated by IP standard ACL.

Configure it in interface mode (include VLAN and SuperVLAN interface)

- Control switch receiving the addition of multicast group

ip igmp access-group access-list-number [port-list]

- Cancel addition of configured multicast group

no ip igmp access-group access-list-number [port-list]

By default, host can add to any multicast group.

11.6.11 Configure switch interface to add to multicast group

Configure Ethernet switch interface to add to multicast group to make switch transmit multicast packet to it and specify source address list.

Configure it in interface mode (including VLAN interface and superVLAN interface) :

- Configure switch interface to add to multicast group

ip igmp static-group groups-address port-list sourcelist sourcelist

- Cancel interface to add to multicast group

no ip igmp static-group groups-address port-list sourcelist sourcelist

11.6.12 VLANid Configure ingress VLANid of static multicast group members

This command is used with ip igmp static-group command. This command specifies ingress VLAN id and creates a complete static multicast member table to realize the packet transmission of static multicast members.

Configure it in interface mode (include VLAN and SuperVLAN interface)

In VLAN interface mode:

- Configure ingress VLANid of static multicast group members of Ethernet

switch. ip igmp create-group groups-address

- Cancel ingress VLANid of static multicast group members of Ethernet

switch. no ip igmp create-group groups-address

In SuperVLAN interface mode:

ip igmp create-group groups-address VLAN VLANid

- Cancel ingress VLANid of static multicast group members of Ethernet switch. no ip igmp create-group groups-address VLAN VLANid

11.6.13 IGMP monitor and maintenance

Display IGMP configuration and running in command line configuration：

Display IGMP interface information：

- show ip igmp interface

[{ VLAN-interface vid } | { superVLAN-interface number }]

Display static configuration and multicast group information learnt by IGMP：

- show ip igmp groups [multicast-ip]

Display IGMP proxy information

- show ip igmp groups [multicast-ip]

11.7. Brief introduction of PIM

PIM-DM（Protocol Independent Multicast-Dense Mode）is intensive multicast route protocol. PIM-DM suits small scaled network and multicast members are intensive.

11.7.1 Working theory of PIM-DM

The working process of PIM-DM are: Neighbor Discovering, DM forwarding to pruning and grafting.

(1) Neighbor Discovering

When enabling PIM-DM router, it needs Hello packet to be neighbor discovering. Each network node running PIM-DM uses Hello packet to keep connection. PIM-DM sends Hello packet periodically.

(2) Forwarding &Pruning

PIM-DM supposes all hosts in network are ready to receive multicast data. When some multicast source S sends data to multicast group G, router will be RPF examining after receiving multicast packet. If the examination is passed, router will create a (S,G) item and forward data to all downlink PIM-DM nodes. If the examination fails, that is, multicast packet inputted from error interface, the packet is dropped. After this process, a (S,G) item will be created in PIM- DM multicast area.

If there is no multicast member in downlink node, Prune packet will be sent to uplink node which informs the uplink not to transmit data to downlink node. After receiving Prune packet, uplink node will delete corresponded interface from the outputting interface list of its multicast transmission item (S,G) to set up a SPT (Short Path Tree) with the source S being the root. Prune is originated by leave router.

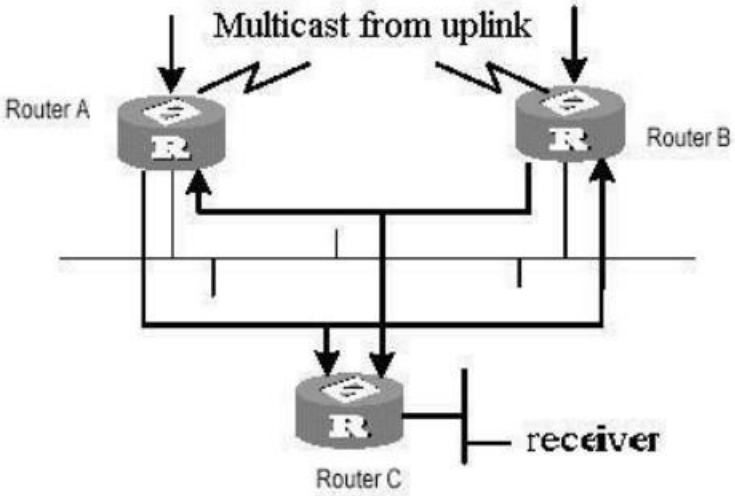
This process is called Forwarding and Pruning. Each pruned node provides overtime mechanism. When pruning is overtime, each router restarts Forwarding and Pruning. The process of PIM-DM Forwarding and Pruning is periodically running.

In this process, PIM-DM adopts RPF examination to establish a multicast transmission tree originated with data source by using current unicast route table. When a multicast packet arrives, router will judge the correctness of arrival path. If arrival interface is the one to multicast source demonstrated by unicast route, the multicast packet is from the correct path; or, this multicast packet will be dropped as redundant packet without transmission. The unicast route information as path judging can be from any unicast route protocol, such as RIP or route information found by OSPF, but not dependent on specified unicast route protocol.

(3) Assert mechanism

As following picture, if there are two multicast routers A and B in a LAN network interface and they have their own receiving paths to multicast source S, they will transmit this multicast packet to LAN after receiving multicast packet from multicast source S. multicast router C in downlink node will receive two same multicast packet.

Multicast packet router from uplink node detect this situation, it needs Assertmechanism to select a unique transferrer. By sending Assert packet, select a best path. If the priority and metric of the two or more paths are the same, the one with larger IP address will be the uplink neighbor of (S, G) item, which is responsible for the transmission of (S, G) multicast packet.



Picture for Assert Mechanism

(4) Graft

When the pruned downlink node needs to restore to transmission state, this node uses graft packet to inform uplink node. Enable multicast route before configuring IGMP protocol.

(5) SRM

To avoid repeat forwarding –pruning, new protocol standard adds this mechanism. Router connected to multicast source timely sends SRM, and PIM will refresh pruning state after receiving it.

11.7.2 Working theory of PIM-SM

The working process of PIM-SM are: Neighbor Discovering, RP sharing tree generating, multicast source register and SPT shift. Neighbor Discovering is the same as that of PIM-DM.

(1) RP sharing tree（RPT）generating

When host adding to a multicast group G, leave router connected with this host know there is receiver of multicast group G through IGMP packet, it will calculate the corresponded convergent point RP and send join packet to the upper node. Passing each router from leave router to RP, （*，G）item will be generated in transmission table. No matter where it sending from, it was sent to multicast group G. When RP received the packet to multicast group G, packet will arrive leave router along the established path to host. Above forms RPT with the root of RP.

(2) Multicast source register

When multicast source S sends a multicast packet to multicast group G, PIM-SM multicast router will encapsulate received multicast packet to register packet and send it to corresponded RP in the form of unicast. If there are many PIM-SM multicast router in a network interface, DR（Designated Router）will send this multicast packet.

11.8. PIM configuration

11.8.1 PIM configuration list

Configuring PIM needs following operation: when router runs in PIM-DM protocol domain, it is suggested enabling PIM-DM in all interface of non-border router. PIM-SM need not enable PIM-SM in all interface.

Basic configuration of PIM：

- Enable multicast protocol
- Enable PIM-DM or PIM-SM protocol

Advanced configuration of PIM：

- Configure Hello packet sending interval
- Configure BSR bordor
- Enter PIM mode
- Configure multicast source (group) filtrate
- Configure PIM neighbor filtrate
- Configure max number of PIM neighbor
- Configure static RP
- Specify candidate BSR
- Specify candidate RP

11.8.2 Specified interface to run PIM-DM protocol

PIM-DM protocol needs enabling in each interface.

After configuring PIM-DM, it will send Hello packet timely and handle protocol sent by PIM neighbor.

Configure it in VLAN interface configuration mode:

- Specified interface to run PIM-DM protocol

```
ip pim dense-mode
```

- Disable PIM-DM protocol

```
no ip pim dense-mode
```

By default, not any interface run PIM-DM protocol. Generally, it is suggested each interface configure PIM-DM. This configuration must be effective in global configuration mode. After enabling PIM-DM, it cannot enable PIM-SM, vice versa.

⚠ Caution: Enable multicast protocol before enabling PIM-DM.

11.8.3 Specified interface to run PIM-SM protocol

PIM-SM protocol needs enabling in each interface.

After configuring PIM-SM, it will send Hello packet timely and handle protocol sent by PIM neighbor.

Configure it in VLAN interface configuration mode:

- Specified interface to run PIM-SM protocol

```
ip pim sparse-mode
```

- Disable PIM-SM protocol

```
no ip pim sparse-mode
```

By default, not any interface run PIM-SM protocol. Generally, it is suggested each interface configure PIM-SM. This configuration must be effective in global configuration mode. After enabling PIM-SM, it cannot enable PIM-DM, vice versa.

⚠ Caution: Enable multicast protocol before enabling PIM-SM.

11.8.4 Configure Hello packet sending interval

After enabling PIM, Hello packet will be sent timely. The time interval sending Hello packet can be modified according to the bandwidth and type of network.

Configure it in VLAN interface configuration mode:

- Configure sending interval of Hello packet

```
ip pim query-interval seconds
```

- Restore the default time interval

```
no ip pim query-interval
```

Default sending time interval of Hello packet is 30 seconds. User can configure it according to the different network environment.

Generally, this parameter need not modify.

⚠ Caution: Enable interface running PIM before configuring PIM attribution. Following commands should pay attention to it.

11.8.5 Configure BSR border

Configure interface to be BSR border of PIM. After configuring this command in some interface, all Bootstrap Message cannot be through the border, but other PIM packets can. Through this, user can divide the network operating PIM-SM into many areas and use different Bootstrap Router in each area. Caution: This command cannot establish multicast border but a PIM Bootstrap Router border.

Configure it in interface configuration mode (including VLAN interface and superVLAN interface)

- Configure interface to be BSR border

ip pim bsr-border

- Delete BSR border

no ip pim bsr-border

By default, bsr-border disables.

11.8.6 Configure PIM neighbor filtrate

Configure basic ACL to restrict all passed routers to be the neighbor of current PIM.

Configure it in VLAN interface configuration:

- Filtrate PIM neighbor

ip pim neighbor-policy acl-number

- Cancel neighbor no

ip pim neighbor-policy By
default, non-filtration.

11.8.7 Configure max number of PIM neighbor

To prevent establishing large number of PIM neighbourship to occupy router's memory and lead to router's failure, it can restrict the number of PIM neighbour in router's interface. The restriction of PIM neighbor is defined by system, user cannot change it by command.

Configure it in VLAN interface configuration mode:

- Configure restriction of PIM neighbor number

ip pim neighbor-limit limit

- Restore default configuration

no ip pim neighbor-limit

By default, the max number of PIM neighbor is 128.

When configuring, PIM neighbor number in interface is beyond the configured value, the original PIM neighbor will not be deleted.

11.8.8 Monitor and maintenance of PIM

Display interface information of running PIM in global configuration mode：

- show ip pim interface [VLAN-interface vid]

Display PIM neighbor information

- show ip pim neighbor

Display multicast route table learnt by PIM

- show ip mroute group-address

Display PIM current RP information, including dynamic learnt RP and configured static RP.

- show ip pim rp-info group-address

Display BSR information, including: selected BSR and information about local configured candidate BSR.

show ip pim bsr

12. ACL CONFIGURATION

12.1. Brief introduction of ACL

12.1.1 Introduction of ACL

In order to filtrate data packet, it needs configuring a series of matching rules to recognize the object which needs filtration. After recognizing special object, it can configure to permit or deny corresponded data packet passing according to the scheduled strategy. Access Control List (ACL) is used to realize this function.

ACL can classifies data packet according to a series of matching condition which can be source address, destination address and interface number. Switch detects data packet according to the specified condition of ACL to determine to transmit or drop.

Data packet matching rules defined by ACL can be introduced to other situation which needs distinguish flow, such as the flow classification in QoS.

12.1.2 Matching order configuration

An ACL rule consists of many “permit | deny” syntax, and the range of data packet specified by each syntax is different. When matching a data packet and ACL rule, there should be order. Use following command to configure ACL matching order:

access-list access-list-number match-order { config | auto }

Parameter：

access-list-number：the number of ACL rule which is in the range of 1 to 399.

config：Specify user configured order when matching this rule.

auto：Specify auto-sequencing when matching this rule. (according to the deep precedency) It is defaulted to specify user configured order, that is “config”. Once user configures the matching order of an ACL rule, it cannot be changed unless delete the content of the rule and re-configure its order.

The deep precedency used by auto means locating the syntax with the smallest data range at the end, which can be realized by comparing address wildcard. The smaller the wildcard value is, the smaller range the host has. For example, 192.168.3.1 0 specifies a host：192.168.3.1，while 192.168.3.1 0.0.255.255 specifies a network interface：192.168.3.1 ~ 192.168.255.255. The former is before the latter in ACL. The concrete rule is: For standard ACL syntax, compare source address wildcard, if their wildcard is the same, use config order; for layer 2 ACL, the rule with “any” is in the front, others use config order; for extended ACL, compare source address wildcard, if they are the same, compare destination address wildcard, if they are the same, compare interface number range, the smaller is in the back, if the interface number range is the same, use config order; for user-defained ACL, compare the length of mask, the longer is in the back, if they are the same, use config order.

12.1.3 ACL support

ACL can be classified as following:

ACL is the command control list applied to switch. These command is used to tell switch which data packet to receive and which to refuse. It consists of a series of judging syntax. After activating an ACL, switch will examine each data packet entering switch according to the judging condition given by ACL. The one which satisfies the ACL will be permit or dropped according to ACL. QOS introduces the permit rule configuration.

In system, the ACL can be classified as following:

- Standard ACL based on number ID
- Standard ACL based on name ID
- Extended ACL based on number ID
- Extended ACL based on name ID
- Layer 2 ACL based on number ID
- Layer 2 ACL based on name ID

The restriction to every ACL and number of QOS action is as following table：

Table 13-1 ACL number restriction

Standard ACL based on number ID	1-99	99
Extended ACL based on number ID	100-199	100
Layer 2 ACL based on number ID	200-299	100
Standard ACL based on name ID	--	1000
Extended ACL based on name ID	--	1000
Layer 2 ACL based on name ID	--	1000
Sub-rule number which can be configured by an ACL	0-127	128
The max sub-rule number which can be configured	--	3000
Time range	--	128
The absolute time range which can be configured by a time range	--	12
The periodic time range which can be configured by a time range	--	32
Sub-item of activating ACL	--	1373

12.2. ACL configuration

12.2.1 Configuration list

ACL configuration includes:

- Configure time range
- Define ACL
- Activate ACL

Above three steps should be in order. Configure time range at first, then defaine ACL which will introduce defined time range and activate ACL.

12.2.2 Configure time range

- Enter time-range configuration mode

Use time-range command to enter time-range configuration mode. In this mode, you can configure time range.

Configure it in global configuration mode.

Command:

time-range time-range-name

There are two kinds of configuration: configure absolute time range and periodic time range. Configuring absolute is in the form of year, month, date, hour and minute. Configuring periodic time range is in the form of day of week, hour and minute.

- Create absolute time range

Use following command to configure it.

Configure it in time-range configuration mode.

Configure absolute time range：

absolute [start time date] [end time date]

Delete absolute time range:

no absolute [start time date] [end time date]

If the start time is not configured, there is no restriction to the start time.; if endtime is not configured, the end time can be the max time of system. The end time must be larger than start time.

Absolute time range determines a large effective time and restricts the effective time range of periodic time. It can configure 12 absolute time range.

- Create periodic time range

Use following command to configure periodic time range.

Configure it in time-range configuration mode. Command:

periodic days-of-the-week hh:mm:ss to [day-of-the-week] hh:mm:ss no periodic days-of-the-week hh:mm:ss to [day-of-the-week] hh:mm:ss

The effective time range of periodic time is a week. It can configure at most 32 periodic time range.

12.2.3 Define ACL

Switch supports many ACL. Followings are how to define it:

- Define standard ACL

Switch can defaine at most 99 standard ACL with the number ID (the number is in the range of 1 to 99), at most 1000 standard ACL with the name ID and totally 3000 sub-rules. It can define 128 sub-rules for an ACL (this rule can suit both ACL with name ID and number ID). Standard ACL only classifies data packet according to the source IP information of IP head of data packet and analyse the matching data packet. The construction of IP head refers to RFC791.

(1) Define standard ACL based on number ID

Standard ACL based on number ID is using number to be ID of standard ACL. Use following command to define standard ACL based on number ID.

Configure it in global configuration mode.

Command：

access-list access-list-number { deny | permit } { source-addr source-wildcard | any } [fragments] [time-range time-range-name]

Define the matching order of ACL:

access-list access-list-number match-order { config | auto }

Delete all the subitems or one subitem in one ACL with number ID or name ID or all ACLs.

no access-list { all | { access-list-number | name access-list-name } [subitem] }

Use access-list command repeatedly to define more rules for the same ACL.

If parameter time-range is not used, this ACL will be effective at any time after activation.

Concrete parameter meaning refers to corresponded command line.

(2) Define standard ACL with name ID.

Standard ACL with name ID is using name ID to identify standard ACL.

Instruction：

Defining standard ACL with name ID should enter specified configuration mode: use access-list standard in global configuration mode which can specify matching order of ACL. Use exit command to be back from this mode.

Use following commands to define standard ACL with name ID. Configure it incorresponded mode.

Command：

Enter standard ACL with name ID configuration mode（global configuration mode） access-list standard name [match-order { config | auto }]

Defining standard ACL rule（standard ACL with name ID configuration mode）

{ permit | deny } { source-addr source-wildcard | any } [fragments] [time-range time-range-name]

Delete all the subitems or one subitem in one ACL with number ID or name ID or all ACLs.（global configuration mode）

no access-list { all | { access-list-number | name access-list-name } [subitem] }

Use { permit | deny } command repeatedly to define more rules for the same ACL. Specifying matching order cannot be modified.

By default, the matching order is user configured order (config).

Concrete parameter meaning refers to corresponded command line.

- Define extended ACL

Switch can defaine at most 100 extended ACL with the number ID (the number is in the range of 100 to 199), at most 1000 extended ACL with the name ID and totally 3000 sub-rules. It can define 128 sub-rules for an ACL (this rule can suit both ACL with name ID and number ID). Extended ACL classifies data packet according to the source IP, destination IP, used TCP or UDP interface number, packet priority information of IP head of data packet and analyse the matching data packet. Extended ACL supports three types of packet priority handling: TOS(Type Of Service) priority, IP priority and DSCP. The construction of IP head refers to RFC791.

(1) Define extended ACL with number ID

Extended ACL based on number ID is using number to be ID of extended ACL. Use following command to define extended ACL based on number ID.

Configure it in global configuration mode.

Define extended ACL based on number ID

access-list access-list-number2 { permit | deny } [protocol] [established] { source-addr source-wildcard | any } [port [portmask]] { dest-addr dest-wildcard | any } [port [portmask]] [icmp-type [icmp-code]] [fragments] { [precedence precedence] [tos tos] | [dscp dscp] } [time-range time-range-name]

Define the matching order of ACL

access-list access-list-number match-order { config | auto }

Delete all the subitems or one subitem in one ACL with number ID or name ID or all ACLs.

no access-list { all | { access-list-number | name access-list-name } [subitem] }

Use access-list command repeatedly to define more rules for the same ACL.

Number ID of extended ACL is in the range of 100 to 199.

Caution: parameter port means TCP or UDP interface numberused by all kinds of superior levels. For some common interface number, use corresponded mnemonic symbol to replace the real number, such as using “bgp” to instead of the TCP interface number 179 of BGP protocol. Details refer to corresponded command line.

(2) Define extended ACL with name ID

Extended ACL with name ID is using name ID to identify extended ACL.

Instruction：

Defining standard ACL with name ID should enter specified configuration mode: use access-list extended in global configuration mode which can specify matching order of ACL. Use exit command to be back from this mode.

Configure it in corresponded mode. Enter extended ACL with name ID (global configuration mode).

access-list extended name [match-order { config | auto }]

Define extended ACL (extended ACL with name ID configuration mode)

{ permit | deny } [protocol] [established] { source-addr source-wildcard | any } [port [portmask]] { dest-addr dest-wildcard | any } [port [portmask]] [icmp-type [icmp-code]] { [precedence precedence] [tos tos] | [dscp dscp] } [fragments] [time-range time-range- name]

Delete all the subitems or one subitem in one ACL with number ID or name ID or all ACLs.（global configuration mode）

no access-list { all | { access-list-number | name access-list-name } [subitem] }

Use { permit | deny } command repeatedly to define more rules for the same ACL. Specifying matching order cannot be modified.

Caution: parameter port means TCP or UDP interface number used by all kinds of superior levels. For some common interface number, use corresponded mnemonic symbol to replace the real number, such as using “bgp” to instead of the TCP interface number 179 of BGP protocol. Details refer to corresponded command line.

- Define layer 2 ACL

Switch can define at most 100 layer 2 ACL with the number ID (the number is in the range of 200 to 299), at most 1000 layer 2 ACL with the name ID and totally 3000 sub-rules. It can define 128 sub-rules for an ACL (this rule can suit both ACL with name ID and number ID). Layer 2 ACL only classifies data packet according to the source MAC address, source VLAN ID, layer protocol type, layer packet received and retransmission interface and destination MAC address of layer 2 frame head of data packet and analyze the matching data packet.

(1) Define layer 2 ACL based on number ID

Layer 2 ACL based on number ID is using number to be ID of layer 2 ACL. Use following command to define layer 2 ACL based on number ID.

Configure it in global configuration mode.

Define layer 2 ACL based on number ID

access-list access-list-number3 { permit | deny } [protocol] [cos VLAN-pri] ingress { { [source- VLAN-id] [source-mac-addr source-mac-wildcard] [interface interface-num] } | any } egress { { [dest-mac-addr dest-mac-wildcard] [interface interface-num | cpu] } | any } [time-range time-range-name]

Define the matching order of ACL:

access-list access-list-number match-order { config | auto }

Delete all the subitems or one subitem in one ACL with number ID or name ID or all ACLs.

no access-list { all | { access-list-number | name access-list-name } [subitem] }

Use access-list command repeatedly to define more rules for the same ACL.

The number ID of layer 2 ACL is in the range of 200 to 299.

Interface parameter in above command specifies layer 2 interface, such as Ethernet interface. Concrete parameter meaning refers to corresponded command line.

(2) Define layer 2 ACL with name ID.

Layer 2 ACL with name ID is using name ID to identify layer 2 ACL.

Instruction：

Defining layer 2 ACL with name ID should enter specified configuration mode: use access-list link in global configuration mode which can specify matching order of ACL. Use exit command to be back from this mode.

Use following commands to define layer 2 ACL with name ID. Configure it in corresponded mode.

Enter layer 2 ACL with name ID configuration mode（global configuration mode）

access-list link name [match-order { config | auto }]

Defining layer 2 ACL rule（layer 2 ACL with name ID configuration mode）

{ permit | deny } [protocol] [cos VLAN-pri] ingress { { [source-VLAN-id] [source-mac-addr source- mac-wildcard] [interface interface-num] } | any } egress { { [dest-mac-addr dest-mac-wildcard] [interface interface-num | cpu] } | any } [time-range time-range-name]

Delete all the subitems or one subitem in one ACL with number ID or name ID or all ACLs.（global configuration mode）

no access-list { all | { access-list-number | name access-list-name } [subitem] }

Use { permit | deny } command repeatedly to define more rules for the same ACL. Specifying matching order cannot be modified.

By default, the matching order is user configured order (config).

Concrete parameter meaning refers to corresponded command line.

12.2.4 Activate ACL

After activating ACL, it can be effective. Use access-group command to activate accessing control list.

Configure it in global configuration mode.

Activate ACL

access-group { [ip-group { access-list-number | access-list-name } [subitem subitem]] [link-group { access-list-number | access-list-name } [subitem subitem]] } }

Cancel activating ACL

no access-group { all | { [ip-group { access-list-number | access-list-name } [subitem subitem]] [link-group { access-list-number | access-list-name } [subitem subitem]] } }

Instruction:

This command supports activating accessing control list of layer 2 and layer 3 at the same time, but the action of each accessing control list should not be conflict, if there is conflict (such as one is permit, the other is deny), the activation fails. Switch uses straight through to activate layer 2 and layer 3 ACL, that is, subitem 1 of layer 2 ACL and layer 3 ACL combine together, and the rest may be deduced by analogy; if the number of two groups of ACL is not the same, the rest subitem can activate separately.

12.3. Monitor and maintanence of ACL

Configure followings in any configuration mode except user mode.

Display time information

show time-range [all | statistic | name time-range-name]

Display detail information of ACL

show access-list config { all | access-list-number | name access-list-name }

Display statistic information of ACL

show access-list config statistic

Display runtime information of ACL

show access-list runtime { all | access-list-number | name access-list-name }

Display runtime statistic information of ACL

show access-list runtime statistic

Concrete configuration refers to command line configuration.

13. QOS CONFIGURATION

13.1. Brief introduction of QOS

In traditional packet network, all packets are equal to be handled. Each switch and router handles packet by FIFO to make best effort to send packets to the destination and not to guarantee the transmission delay and delay variation.

With the fast development of computer network, the requirement of network is higher. More and more voice, image and important data which are sensitive about bandwidth, delay and jittering transferred through network, which greatly enrich network service resources and the requirement of quality of service is higher for the network congestion. Now, Ethernet becomes the leading technology in every independent LAN, and many LAN in the form of Ethernet have become a part of internet. With the development of Ethernet technology, Ethernet connecting will become one of main connecting for internet users. To realize end-to-end QoS solution has to consider the service guarantee of Ethernet QoS, which needs Ethernet device applies to Ethernet technology to provide different levels of QoS guarantee for different types of service flow, especially the service flow highly requiring delay and jitter.

1. Flow

Flow is traffic which means all packets through switch.

2. Traffic classification

Traffic classification means adopting certain regulation to recognize packet with some features. Clasification rule means the filtration regulation configured by the administrator according to managing need which can be simple, such as realizing flow with the feature of different priority according to the ToS field of IP packet head and can be complicated, such as information of integrated link layer (layer 2), network layer (layer 3), transmission layer (layer 4), such as MAC address, IP protocol, source address, destination address or application program interface number to classify packet. General classification is limited in the head of encapsulation packet. Use packet content to be classification standard is singular.

3. Access control list

To classify flow is to provide service distinctively which must be connected resource distributing. To adopt which kind of flow control is related to the stage it is in and the current load of the network. For example: monitor packet according to the promised average speed rate when the packet is in the network and queue scheduling manage the packet before it is out of the node.

4. Packet filtration

Packet filtration is to filtrate service flow, such as deny, that is, deny the service flow which is matching the traffic classification and permit other flows to pass. System adopts complicated flow classification to filtrate all kinds of information of service layer 2 packets to deny useless, unreliable, and doubtable service flow to strengthen network security.

Two key points of realizing packet filtration:

Step 1: Classify ingress flows according to some regulation;

Step 2: Filtrate distinct flow by denying. Deny is default accessing control.

5. Flow monitor

In order to serve customers better with the limited network resources, QoS can monitor service flow of specified user in ingress interface, which can adapt to the distributed network resources.

6. Interface speed limitation

Interface speed limitation is the speed limit based on interface which limits the total speed rate of interface outputting packet.

7. Redirection

User can re-specify the packet transmission interface based on the need of its own QoS strategies.

8. Priority mark

Ethernet switch can provide priority mark service for specified packet, which includes: TOS, DSCP, 802.1p. These priority marks can adapt different QoS model and can be defined in these different models.

9. Choose interface outputting queue for packet

Ethernet switch can choose corresponding outputting queue for specified packets.

10. Queue scheduler

It adopts queue scheduler to solve the problem of resource contention of many packets when network congestion. There are three queue scheduler matchings: Strict-Priority Queue (PQ), Weighted Round Robin (WRR) and WRR with maximum delay.

(1)PQ

PQ (Priority Queueing) is designed for key service application. Key service possesses an important feature, that is, require the precesent service to reduce the response delay when network congestion. Priority queue divides all packets into 4 levels, that is, superior priority, middle priority, normal priority and inferior priority (3, 2, 1, 0), and their priority levels reduce in turn.

When queue schedulerimg, PQ precedently transmits the packets in superior priority according to the priority level. Transmit packet in inferior priority when the superior one is empty. Put the key service in the superior one, and non-key service (such as email)in inferior one to guarantee the packets in superior group can be first transmitted and non-key service can be transmitted in the spare time.

The shortage of PQ is: when there is network congestion, there are more packets in superior group for a long time, the packets in inferior priority will wait longer.

(2)WRR

WRR queue scheduler divides a port into 4 or 8 outputting queues (S2926V-O has 4 queues, that is, 3, 2, 1, 0) and each scheduler is in turn to guarantee the service time for each queue. WRR can configure a weighted value (that is, w3, w2, w1, w0 in turn) which means the percentage of obtaining the resources. For example: There is a port of 100M. Configure its WRR queue scheduler value to be 50, 30, 10, 10 (corresponding w3, w2, w1, w0 in turn) to guarantee the inferior priority queue to gain at least 10Mbit/s bandwidth, to avoid the shartage of PQ queue scheduler in which packets may not gain the service.

WRR possesses another advantage. The scheduler of many queues is in turn, but the time for service is not fixed——if some queue is free, it will change to the next queue scheduler to make full use of bandwidth resources.

(3) WRR with maximum delay

Compared with WRR, WRR with maximum delay can guarantee the maximum time from packets entering superior queue to leaving it will not beyond the configured maximum delay.

11. The cos-map relationship of hardware priority queue and priority of IEEE802.1p protocol

System will map between 802.1p protocol priority of packet and hardware queue priority. For each packet, system will map it to specified hardware queue priority according to 802.1p protocol priority of packet.

12. Flow mirror

Flow mirror means coping specified data packet to monitor interface to detect network and exclude failure.

13. Statistics based on flow

Statistics based on flow can statistic and analyse the packets customer interested in.

14. Copy packet to CPU

User can copy specified packet to CPU according to the need of its QoS strategies.

System realizes QoS function according to accessing control list, which includes: flow monitor, interface speed limit, packet redirection, priority mark, queue scheduler, flow mirror, flow statistics and coping packet to CPU.

13.2. QOS Configuration

13.2.1 QoS Configuration list

QOS Configuration includes:

- Flow monitor
- line rate
- Packet redirection configuration
- Priority configuration
- Queue-scheduler configuration

- The cos-map relationship of hardware priority queue and priority of IEEE802.1p protocol
- The cos-map relationship of DSCP and priority of IEEE802.1p protocol
- Flow mirror configuration
- Flow statistic configuration
- Copy packet to CPU configuration

Define corresponded ACL before configuring QoS.

13.2.2 Flow monitor

Flow monitor is restriction to flow speed which can monitor the speed of a flow entering switch. If the flow is beyond specified specification, it will take actions, such as dropping packet or reconfigure their priority.

Use following command to configure flow monitor.

Configure it in global configuration mode.

Rate-limit configuration based on flow

rate-limit input { [ip-group { access-list-number | access-list-name } [subitem subitem]] [link-group { access-list-number | access-list-name } [subitem subitem]] } } target-rate [exceed-action action]

Cancel rate-limit configuration based on flow

no rate-limit input { [ip-group { access-list-number | access-list-name } [subitem subitem]] [link-group { access-list-number | access-list-name } [subitem subitem]] } }

Define corresponded ACL before configuring. Configure the flow monitor with the same configuration in the same interface mode, such as configuring the flow monitor of ACL rule which introduces filtrating source IP address in the same interface mode.

The aim of this configuration is matching data flow of ACL to realize flow monitor: take action when data flow is beyond configured flow, such as dropping packet.

Details of this command refers to corresponded command.

13.2.3 Packet redirection configuration

Packet redirection configuration is redirecting packet to be transmitted to some egress.

Use following command to configure it.

Configure it in global configuration mode.

Redirection

traffic-redirect { [ip-group { access-list-number | access-list-name } [subitem subitem]] [link-group { access-list-number | access-list-name } [subitem subitem]] } } { interface interface-num }

Cancel redirection

no traffic-redirect { [ip-group { access-list-number | access-list-name } [subitem subitem]] [link-group { access-list-number | access-list-name } [subitem subitem]] } }

Instruction:

Use this command to redirect the data packet which matched specified accessing list regulations (it is only be effective for permit rules of accessing list).

Details of this command refers to corresponded command.

13.2.4 Priority configuration

Traffic priority configuration is the strategy of remark priority for matching packet in ACL, and the marked priority can be filled in the domain which reflect priority in packet head.

Use following command to configure priority mark configuration.

Configure it in global configuration mode.

Mark packet priority

traffic-priority { [ip-group { access-list-number | access-list-name } [subitem subitem]] [link-group { access-list-number | access-list-name } [subitem subitem]] } } { [dscp dscp-value | precedence { pre-value | from-cos }] [cos { pre-value | from-ipprec }] [local-precedence pre-value] }

Cancel packet priority configuration

no traffic-priority { [ip-group { access-list-number | access-list-name } [subitem subitem]] [link-group { access-list-number | access-list-name } [subitem subitem]] } }

System will mark IP priority（precedence specified value of traffic-priority command）, DSCP（dscp specified value of traffic-priority command）, 802.1p priority（that is cos value of traffic-priority command). User can mark different priority for packet according to real QoS strategy. Switch can locate packet to interface outputting queue according to the 802.1p priority and also can locate packet to corresponding outputting queue according to the specified local priority in traffic-priority command (local-precedence specified value). If both 802.1p priority and local priority are configured, 802.1p priority will be precedent to use.

Details of this command refers to corresponded command.

13.2.5 Queue-scheduler configuration

When network congestion, it must use queue-scheduler to solve the problem of resource competition.

Use following command to configure queue-scheduler.

Configure it in global configuration mode.

Configure queue-scheduler

queue-scheduler { strict-priority | wrr queue1-weight queue2-weight queue3-weight queue4-weight queue5-weight queue6-weight queue7-weight queue8-weight | sp-wrr queue1-weight queue2-weight queue3-weight }

Disable queue-scheduler

no queue-scheduler

System supports three types of queue-scheduler mode: Strict-Priority Queue, Strict-Priority Queue and Weighted Round Robin (SP+WRR) and Weighted Round Robin (WRR).

By default, switch uses Strict-Priority Queue.

The detailed command refers to the corresponding command line reference.

13.2.6 The cos-map relationship of hardware priority queue and priority of IEEE802.1p protocol

There are 4 hardware priority queues which are from 0 to 3, of which 3 is the

The default mapping is the mapping defined by 802.1p：

```
802.1p:          0  1  2  3  4  5  6  7
packed-priority：  0  0  1  1  2  2  3  3
```

Use queue-scheduler cos-map command to configure 4 cos-map relationship of hardware priority queue and 8 priority of IEEE802.1p protocol

Use following command in global configuration moide.

```
queue-scheduler cos-map [ queue-number ] [ packed-priority ]
```

Use following command to display the priority cos-map.

```
show queue-scheduler cos-map
```

For example:

```
！Configure packed-priority 1 to mapped priority 6 of IEEE 802.1p
OLT(config)#queue-scheduler cos-map 1 6
```

13.2.7 Configure the mapping relationship between DSCP and 8 priority in IEEE 802.1p

DSCP is the high 6 byte in ToS bit which is in the range of 0-63. The default mapping relationship is that all DSCP map to priority 0.

Use this command to configure the mapping relationship between DSCP and 8 priority in IEEE 802.1p.

Configure it in global configuration mode：

```
queue-scheduler dscp-map [ dscp-value ] [ packed-priority ]
```

Example

```
！Configure dscp 2 to map to priority 5
OLT(config)#queue-scheduler dscp-map 2 5
```

13.2.8 Flow mirror configuration

Flow mirror is copying the service flow which matches ACL rules to specified monitor interface to analyse and monitor packet.

Use following command to configure flow mirror.

Configure it in interface configuration mode.

Flow mirror configuration

mirrored-to { [ip-group { access-list-number | access-list-name } [subitem subitem]] [link-group { access-list-number | access-list-name } [subitem subitem]] } } [interface interface- num]

Cancel flow mirror configuration

no mirrored-to { [ip-group { access-list-number | access-list-name } [subitem subitem]] [link-group { access-list-number | access-list-name } [subitem subitem]] } }

Details of this command refers to corresponded command.

13.2.9 Flow statistic configuration

Flow statistic configuration is used to statistic specified service flow packet.

Use following command to configure it.

Configure it in global configuration mode.

Flow statistic configuration

traffic-statistic { [ip-group { access-list-number | access-list-name } [subitem subitem]] [link-group { access-list-number | access-list-name } [subitem subitem]] } }

Clear statistic information

clear traffic-statistic { all | [ip-group { access-list-number | access-list-name } [subitem subitem]] [link-group { access-list-number | access-list-name } [subitem subitem]] } }

Cancel flow statistic configuration

no traffic-statistic { [ip-group { access-list-number | access-list-name } [subitem subitem]] [link-group { access-list-number | access-list-name } [subitem subitem]] } } If

reconfiguring flow statistics, the corresponded information will be cleared.

Details of this command refers to corresponded command.

13.2.10 Copy packet to CPU

Copy packet to CPU is copying a packet to be transmitted to CPU.

Use following command to configure it. Configure it in interface configuration mode.

Copy packet to CPU.

traffic-copy-to-cpu { [ip-group { access-list-number | access-list-name } [subitem subitem]] [link-group { access-list-number | access-list-name } [subitem subitem]] } }

Cancel copy packet to CPU

no traffic-copy-to-cpu { [ip-group { access-list-number | access-list-name } [subitem subitem]] [link-group { access-list-number | access-list-name } [subitem subitem]] } }

Instruction:

Copying packet to CPU is only be effected to permit rule in ACL.

Details of this command refers to corresponded command.

13.3. Monitor and maintenance of QoS

Configure it in corresponded configuration mode. Show command can be used in any configured mode except user mode.

Display all QoS information:

show QoS-info all

Display all QoS statistic information

show QoS-info statistic

Display flow mirror configuration

show QoS-info mirrored-to

Display queue scheduler and parameter

show queue-scheduler

Display the cos-map relationship of hardware priority queue and priority of IEEE802.1p protocol

show queue-scheduler cos-map

Display QOS configuration of all interface

show QoS-interface [interface-num] all

Display parameter configuration of flow limit

show QoS-interface [interface-num] rate-

limit Display line limit configuration

show QoS-interface [interface-num] line-rate

Display QOS statistic information of all interface

show QoS-interface statistic

Display priority configuration

show QoS-info traffic-priority

Display redirection configuration

show QoS-info traffic-redirect

Display flow statistic configuration

show QoS-info traffic-statistic

Display configuration of copying to CPU.

show QoS-info traffic-copy-to-cpu

Details of this command refers to corresponded command.

13.4. Configuration example of QACL

13.4.1 Use QACL to realize user isolation

1．Brief introduction of isolation

Use user isolation to bind some interface and some IP address. Only the packet with the source IP address being this one can be transmitted, or it will be dropped. This can fix specified user to some interface to realize user management.

There are two types of mode: one is transmitting all ARP packet, the other is not transmitting all ARP packet. In transmitting all ARP mode, after enabling user isolation, all ARP packet can be transmitted. In not transmitting all ARP mode, after enabling user isolation, only after configuring user binding rules (such as ip +port+mac), corresponded ARP packet can be transmitted.

Followings are the configuring examples of two user isolation. Example 1 can use QACL to realize user isolation of all ARP packet; example 2 uses QACL to realize user isolation of not transmitting ARP packet.

2．Example 1

Example 1 uses QACL to realize user isolation of transmitting all ARP packet. This example can realize following function:

1) Enable user isolation (prevent all packet and permit ARP packet with VLAN id being 4016);

2) Configure Ethernet interface 1 to be uplink interface (permit all packet from uplink interface 1)

3) Configure binding rules of three users:

1> ip+port：ip is 192.168.0.1 and port to be Ethernet interface 2

2> ip+port+vid：ip is 192.168.0.2，port is Ethernet interface 2 and vid is 2

3> ip+port+mac；ip is 192.168.0.3，port is Ethernet interface 2 and mac is 00:00:00:00:00:03

The configuration is as following:

（1）Define needed ACL

！Define to deny all packet ACL

```
OLT(config)#access-list 200 deny ingress any egress any
```

！Define to transmit ACL to transmit packet from uplink interface 1

```
OLT(config)#access-list 200 permit ingress interface ethernet 0/1 egress any
```

！Define ACL to transmit packet with VLAN ID being 4016 and from non-uplinkinterface 2

```
OLT(config)#access-list 200 permit ingress 4016 interface ethernet 0/2 egress any
```

！Define ACL to transmit all ARP packet

```
OLT(config)#access-list 200 permit arp ingress any egress any
```

！Define ip+port user to bind ACL with ip being 192.168.0.1，port being Ethernet interface 2. This ip+port user bound rule can be divided into 2 ACLs：one is ACL to transmit packet with source address being 192.168.0.1, the other is ACL to transmit packet from Ethernet interface 2

```
OLT(config)#access-list 1 permit 192.168.0.1 0
OLT(config)#access-list 201 permit ingress interface ethernet 0/2 egress any
```

！Define ip+port+vid user to bind ACL with ip being 192.168.0.2，port being Ethernet interface 2 and vid being 2. This ip+port+vid user bound rule can be divided into 2 ACLs：one is ACL to transmit packet with source address being 192.168.0.2, the other is ACL to transmit packet with vid being 2 from Ethernet interface 2

```
OLT(config)#access-list 1 permit 192.168.0.2 0
OLT(config)#access-list 201 permit ingress 2 interface ethernet 0/2 egress any
```

！Define ip+port+mac user to bind ACL with ip being 192.168.0.3，port being Ethernet interface 2 and mac being 00:00:00:00:00:03. This ip+port+mac user bound rule can be divided into 2 ACLs：one is ACL to transmit packet with source address being 192.168.0.3, the other is ACL to transmit packet with mac being 00:00:00:00:00:03 from Ethernet interface 2

```
OLT(config)#access-list 1 permit 192.168.0.3 0
OLT(config)#access-list 201 permit ingress 00:00:00:00:00:03 0:0:0:0:0:0 interface ethernet
0/2 egress any
```

（2）Activate ACL

```
OLT(config)#access-group link-group 200
OLT(config)#access-group ip-group 1 link-group 201
```

3． Example 2

Example 2 uses QACL to realize user isolation of not transmitting all ARP packet. This example can realize following function:

1) Enable user isolation (prevent all packet and permit packet with VLAN id being 4016);

2) Configure Ethernet interface 1 to be uplink interface (permit all packet from uplink interface 1)

3) Configure binding rules of three users:

1> ip+port：ip is 192.168.0.1 and port to be Ethernet interface 2

2> ip+port+vid：ip is 192.168.0.2，port is Ethernet interface 2 and vid is 2

3> ip+port+mac；ip is 192.168.0.3，port is Ethernet interface 2 and mac is 00:00:00:00:00:03

The configuration is as following:

（1）Define needed ACL

！Define to deny all packet ACL

```
OLT(config)#access-list 200 deny ingress any egress any
```

！Define to transmit ACL to transmit packet from uplink interface 1

```
OLT(config)#access-list 200 permit ingress interface ethernet 0/1 egress any
```

！Define ACL to transmit packet with VLAN ID being 4016 and from non-uplinkinterface 2

```
OLT(config)#access-list 200 permit ingress 4016 interface ethernet 0/2 egress any
```

！Define ACL to transmit all ARP packet

！Define ip+port user to bind ACL with ip being 192.168.0.1，port being Ethernet interface 2. This ip+port user bound rule can be divided into 2 ACLs：one is ACL to transmit packet with source address being 192.168.0.1, the other is ACL to transmit packet from Ethernet interface 2

```
OLT(config)#access-list 1 permit 192.168.0.1 0
OLT(config)#access-list 201 permit ingress interface ethernet 0/2 egress any
```

！Define ip+port+vid user to bind ACL with ip being 192.168.0.2，port being Ethernet interface 2 and vid being 2. This ip+port+vid user bound rule can be divided into 3 ACLs：one is ACL to transmit packet with source address being 192.168.0.2, the other is ACL to transmit packet with vid being 2 from Ethernet interface 2 and the last is ACL transferring ARP packet from Ethernet interface 2 with sending protocol being 192.168.0.1 and vid being 2.

```
OLT(config)#access-list 1 permit 192.168.0.2 0
OLT(config)#access-list 201 permit ingress 2 interface ethernet 0/2 egress any
```

！Define ip+port+mac user to bind ACL with ip being 192.168.0.3，port being Ethernet interface 2 and mac being 00:00:00:00:00:03. This ip+port+mac user bound rule can be divided into 2 ACLs：one is ACL to transmit packet with source address being 192.168.0.3, the other is ACL to transmit packet with mac being 00:00:00:00:00:03 from Ethernet interface 2 and the last is ACL transferring ARP packet from Ethernet interface 2 with sending protocol being 192.168.0.1 and mac being 00:00:00:00:00:03.

```
OLT(config)#access-list 1 permit 192.168.0.3 0
OLT(config)#access-list 201 permit ingress 00:00:00:00:00:03 0:0:0:0:0:0 interface ethernet 0/2 egress any
```

（2）Activate ACL

```
OLT(config)#access-group link-group 200
OLT(config)#access-group ip-group 1 link-group 201
OLT(config)#access-group user-group 300
```

13.4.2 Use QACL to realize bandwidth control

Brief introduction

Bandwidth control means restricting the uplink and downlink speed rate of special flow. Using QACL to realize this function.

- Configuration example

Use QACL to realize the flow bandwidth control with source mac address being 00:01:02:03:04:05, uplink interface being 1, downlink interface being 8, uplink speed being 3 Mbps and downlink speed being 5 Mbps.

Configuration is as following:

（1）Define needed ACL

！Define ACL transmitting packet with source interface to be Ethernet interface 8，destination interface to be wthernet interface 1，source MAC address to be 00:01:02:03:04:05

```
OLT(config)#accesss-list 200 permit ingress 00:01:02:03:04:05 0:0:0:0:0:0 interface ethernet
0/8 egress egress interface ethernet 0/1
```

！Define ACL transmitting packet with source interface being Ethernet interface 1，destination interface being Ethernet interface 8，source MAC address being 00:01:02:03:04:05

```
OLT(config)#accesss-list 201 permit ingress 00:01:02:03:04:05 0:0:0:0:0:0 interface fast-
ethenet 1 egress egress interface ethernet 0/8
```

（2）Configure flow monitor of uplink and downlink interface

！Enter interface configuration mode of uplink interface 1

```
OLT(config)#interface ethernet 0/1
```

！Configure corresponded flow monitor of uplink interface 1

```
OLT(config-if-ethernet-0/1)##rate-limit input link-group 201 3
```

！Enter interface configuration mode of downlink interface 8

```
OLT(config)#interface ethernet 0/8
```

！Configure corresponded flow monitor of downlink interface 8

```
OLT(config-if-ethernet-0/8)##rate-limit input link-group 200 5
```

13.4.3 Use QACL to realize deny all packet expect

Brief introduction of deny all packet expect

deny all packet expect is used to drop all packet except needing transmitting. This function can be realized by configuring QACL.

Configuration example

Configuring deny all packet expect PPPoE, the protocol number of PPPoE is 0x8863（decimal is 34915）and 0x8864（decimal is 34916）

1）Drop all packets

2）Transmit PPPoE packet

Configuration is as following:

（1）Define needed ACL

！Configure deny ACL of all packet

OLT(config)#access-list 200 deny ingress any egress any

！Configure ACL of transmitting PPPoE packet OLT(config)#access-

list 200 permit 34915 ingress any egress any OLT(config)#access-list

200 permit 34916 ingress any egress any

（2）Activate ACL

OLT(config)#access-group link-group 200

13.4.4 Use QACL to prevent virus

Brief introduction of QACL anti-virus

Reasonable configured QACL can be used as firewall to prevent virus to be spread through network to reduce the influence to the network. Different virus has different attacking (such as attack different interface). Configure different QACL rules for different virus, which can do effective protection. For all kinds of virus attacking, it can be obtained from professional anti-virus company (Kingsoft Company).

Configuration example

Use QACL to prevent bow wave virus

Bow wave virus will attack TCP 135 interface and infect through UDP 69 INTERFACE, TCP 4444 interface. Configuring switch to prevent QACL of this packet can effectively prevent this virus.

The configuring is as following:

（1）Define needed ACL

！Configure ACL to prevent TCP packet of interface 135

OLT(config)#access-list 100 deny tcp any any eq 135

！Configure ACL to prevent UDP packet of interface 69

OLT(config)#access-list 100 deny udp any any eq 69

！Configure ACL to prevent TCP packet of interface 4444

OLT(config)#access-list 100 deny tcp any any eq 4444

（2）Activate ACL

OLT(config)#access-group ip-group 100

13.5. Port isolation

13.5.1 Brief introduction of port isolation

Forbid intercommunication of users in different interfaces by port isolation configuration.

There are two kinds of interfaces in port isolation function. One is uplink port, and the other is downlink port. Uplink port can transmit any packet, but downlink port can only transmit the packet whose destination is uplink port. Connect user’s computer to downlink port, and advanced devices connect to uplink port to shield intercommunication bwtween users and not influence user accessing exterior network through advanced switching devices.

13.5.2 Port isolation configuration

Use port-isolation command in global configuration mode to add a or a group of descendent isolation port. Use no port-isolation command to remove a or a group of descendent isolation port:

- Add port isolation downlink port

```
port-isolation { interface-list }
```

- Delete port isolation downlink port

```
no port-isolation { interface-list | all }
```

interface-list is the optioned interface list which means one or more Ethernet interfaces. When adding port isolation downlink ports, not all ports can be added to be port isolation downlink ports. Choose all only when delete port isolation downlink ports. Choose “all” to remove all downlink isolation ports. By default, all ports are port isolation uplink ports.

For example:

！Add Ethernet 0/1, Ethernet 0/3, Ethernet 0/4, Ethernet 0/5, Ethernet 0/8 to be downlink isolation port.

```
OLT(config)#port-isolation ethernet 0/1 ethernet 0/3 to ethernet 0/5 ethernet 0/8
```

！Remove ethernet 0/3, Ethernet 0/4, Ethernet 0/5, ethernet 0/8 from downlink isolation port.

```
OLT(config)#no port-isolation ethernet 0/3 to ethernet 0/5 ethernet 0/8
```

13.6. Storm control

13.6.1 Brief introduction of strom control

Restrict the speed rate of port receiving broadcast, known multicast/ unknown unicast packets by storm control configuration.

13.6.2 Strom control configuration

Use storm-control command in interface configuration mode to configure storm-control. Use show interface command to display storm-control information.

- Configure the speed rate of storm control

storm-control rate target-rate

- Enable storm control

storm-control { broadcast | multicast | dlf }

- Disable storm control

no storm-control { broadcast | multicast | dlf }

For example：

！Configure storm control of e0/1 with the speed rate being 2Mbps

OLT(config-if-ethernet-0/1)#storm-control broadcast 2

！Configure known multicast storm control of e0/3 with the speed rate being 5Mbps

OLT(config-if-ethernet-0/3)#storm-control multicast 5

14. STP CONFIGURATION

14.1. Brief introduction of STP Configuration

STP（Spanning Tree Protocl） is a part of IEEE 802.1D network bridge. The realization of standard STP can eliminate network broadcast storm caused by network circle connection and the circle connection caused by misplaying and accidence, and it also can provide the possibility of network backup connection.

STP protocol with IEEE 802.1D standard provides network dynamic redundancy transferring mechanism and prevents circle connection in bridge network. It determines which interface of the network bridge can transmit data packet. After executing STP matching, switch in the LAN will form a STP dynamic topology which prevents the loop existing between any two working station to prevent broadcast storm in LAN. At the same time, STP matching is responsible to detect the change of physical topology to establish new spanning tree after the changes of topology. For example: when there is a break in the switch or a channel, it can provide certain error tolerance to re-configure a new STP topology.

14.2. STP Configuration

14.2.1 STP Configuration list

The configuration can be effective only after STP enables. Configure related parameter of devices or Ethernet interface before enabling STP and these configurations will be saved after disabling STP. And the parameter will be effective after re-enabling STP. STP configuration list is as following:

- Enable/disable interface STP
- Configure STP mode
- Configure STP priority
- Configure Forward Delay
- Configure Hello Time
- Configure Max Age
- Configure path cost of specified interfaces
- Configure STP priority od specified port
- Configure interface to force to send rstp packet
- Configure link type of specified interface
- Configure the current port as an edge port
- Configure the speed limit of sending BPDU of specified interface
- STP monitor and maintainenance

14.2.2 Enable/disable STP

Configure it in global configuration mode:

- Enable/disable STP of the devices

spanning-tree

- Disable STP of the devices

no spanning-tree

By default, switch STP disables.

For example：

！Enable STP

OLT(config)#spanning-tree

14.2.3 Enable/disable interface STP

Disable STP of specified interface to make the interface not to attend STP calculating. Use following command in interface configuration mode:

- Enable STP on specified interface

spanning-tree

- Disable STP on specified interface

no spanning-tree

By default, interface STP enables.

For example:

！Disable STP on Ethernet 01

OLT(config-if-ethernet-0/1)#no spanning-tree

14.2.4 Configure STP mode

Configure it in global configuration mode:

- Configure switch running STP

spanning-tree mode stp

- Configure switch running RSTP

spanning-tree mode rstp

- Configure switch running MSTP

spanning-tree mode mstp

It is defaulted to run rstp.

Example:

！Configure switch running STP

OLT(config)#spanning-tree mode stp

14.2.5 Configure STP priority

Configure STP priority when STP enables, and the inferior priority of the switch can be the root bridge. Use following command in global configuration mode:

- Configure STP priority

spanning-tree priority bridge-priority

- Restore default STP priority

no spanning-tree priority

For example：

！Configure the priority of the switch in spanning tree to 36864

OLT(config)#spanning-tree priority 36864

⚠ Caution: If the priorities of all network bridge in switching network are the same, choose the one with the smallest MAC address to be the root. If STP enables, configuring network bridge may cause the re-accounting of the STP. By default, the network bridge priority is 32768 and ranges from 0 to 61440 and should be the integrity of 4096.

14.2.6 Configure switch Forward Delay

When this switch is the root bridge, port state transition period is the Forward Delay time, which is determined by the diameter of the switched network. The longer the diameter is, the longer the time is. Configure it in global configuration mode:

- Configure Forward Delay

spanning-tree forward-time seconds

- Restore default Forward Delay

no spanning-tree forward-time

For example:

！Configure forward delay to 20 seconds

OLT(config)#spanning-tree forward-time 20

⚠ Caution: If Forward Delay is configured too small, temporary redundancy will becaused; if Forward Delay is configured too large, network will not be restored linking for a long time. Forward Delay ranges from 4 to 30 seconds. The default forward delay time, 15 seconds is suggested to use. Forward Delay≥Hello Time + 2.

14.2.7 Configure Hello Time

Suitable Hello Time can guarantee network bridge noticing link failure in time without occupying too much resources. Configure it in global configuration mode:

- Configure Hello Time

spanning-tree hello-time seconds

- Restore default Hello Time

no spanning-tree hello-time

For example:

！Configure Hello Time to 5 seconds

```
OLT(config)#spanning-tree hello-time 5
```

⚠ Caution: Too large Hello Time may cause link failure thought by network bridge for losing packets of the link to restart accounting STP; too smaller Hello Time may cause network bridge frequently to send configuration packet to strengthen the load of network and CPU. Hello Time ranges from 1 to 10 seconds. It is suggested to use the default time of 2 seconds. Hello Time ≤ Forward Delay – 2

14.2.8 Configure Max Age

Max Age is used to judge whether the packet is outdate. User can configure it according to the real situation of the network in global configuration mode:

- Configure Max Age

```
spanning-tree max-age seconds
```

- Restore the default Max Age

```
no spanning-tree max-age
```

For example:

！Configure the Max Age to 10 seconds

```
OLT(config)#spanning-tree max-age 10
```

⚠Caution：Max Age is used to configure the longest aging interval of STP. Lose packet when overtiming. The STP will be frequently accounts and take crowded network to be link fault, if the value is too small. If the value is too large, the link fault cannot be known timely. Max Age is determined by diameter of network, and the default time of 20 seconds is suggested. 2*(Hello Time + 1) ≤ Max Age ≤ 2*(ForwardDelay – 1)

14.2.9 Configure path cost of specified interfaces

Configure interface STP path cost and choose the path with the smallest path cost to be the effective path. The path cost is related to the link speed rate. The larger the speed rate is, the less the cost is. STP can auto-detect the link speed rate of current interface and converse it to be the cost. Configure it in interface configuration mode:

- Configure path cost of specified interface

```
spanning-tree cost cost
```

- Restore the default path cost of specified interface

```
no spanning-tree cost
```

Confiure path cost will cause the re-acounting of the STP. Interface path cost ranges from 1 to 65535. It is suggested to use the default cost to make STP calculate the path cost of the current interface. By default, the path cost is determined by the current speed.

In IEEE 802.1D, the default path cost is determined by the speed of the interface. The port with the speed 10M have the cost of 100， 100M, 19; and 1000M, 4.

14.2.10 Configure STP priority od specified port

Specify specified port in STP by configuring port priority. Generally, the smaller the value is, the superior the priority is, and the port will be more possible to be included in STP. If the priorities are the same, the port number is considered. Configure it in interface configuration mode:

- Configure port priority

spanning-tree port-priority port-priority

- Restore the default port priority

no spanning-tree port-priority

The smaller the value is, the superior the priority is, and the port is easier to be the root interface. Change the port priority may cause the re-calculating of the STP. The port priority ranges from 0 to 255. the default port priority is 128.

For example:

```
！Configure the port priority of Ethernet 0/1 in STP to 120
OLT(config-if-ethernet-0/1)#spanning-tree port-priority 120
```

14.2.11 Configure interface to force to send rstp packet

This configuration is used to check whether there is traditional network bridge running STP.

Configure it in interface configuration mode:

- Configure interface to force to send rstp packet

spanning-tree mcheck

For example:

```
！Configure Ethernet 0/1 to send RSTP packet
OLT(config-if-ethernet-0/1)#spanning-tree mcheck
```

14.2.12 Configure link type of specified interface

In rstp, the requirement of interface quickly in transmission status is that the interface must be point to point link not media sharing link. It can specified interface link mode manually and can also judge it by network bridge.

Configure it in interface configuration mode:

- Configure interface to be point-to-point link

spanning-tree point-to-point forcetrue

- Configure interface not to be point-to-point link

spanning-tree point-to-point forcefalse

- Configure switch auto-detect whether the interface is point-to-point link

spanning-tree point-to-point auto

For example:

！Configure the link connected to Ethernet 0/1 as a point-to-point link

OLT(config-if-ethernet-0/1)#spanning-tree point-to-point forcetrue

14.2.13 Configure the current port as an edge port

Edge port is the port connecting to the host which can be in transmission status in very short time after linkup, but once the port receiving STP packet, it will shift to be non-edge port.

Configure it in interface configuration mode:

- Configure the port to be edge port

spanning-tree port fast

- Configure the port to be non-edge port

no spanning-tree portfast

For example:

！Configure Ethernet 0/1 as a non-edge port.

OLT(config-if-ethernet-0/1)#spanning-tree portfast

14.2.14 Configure the speed limit of sending BPDU of specified interface

Restrict STP occupying bandwidth by restricting the speed of sending BPDU packet. The speed is determined by the number of BPDU sent in each hello time.

Configure it in interface configuration mode:

- Configure the maximum number of configuration BPDUs sent by interface in each Hello time to be 2

spanning-tree transit-limit 2

For example:

！Configure the maximum number of configuration BPDUs that can be transmitted by the Ethernet 0/1 in each Hello time to 2

OLT(config-if-ethernet-0/1)#spanning-tree transit-limit 2

14.2.15 STP monitor and maintainenance

The displaying information is as following:

- STP status
- BridgeID
- Root BridgeID
- All kinds of configuration parameter of STP

show spanning-tree interface

Use following command in any configuration mode to display STP status globally or on a port：

show spanning-tree interface

For example：

！Display STP configuration of e0/1

```
OLT(config)#show spanning-tree interface ethernet 0/1
```

14.2.16 Enable/disable STP remote-loop-detect

When multi-layer cascading, if switch in media layer shut down STP, the BPDU packet sent by upper switch will be cut by switch in media layer. When there is loop in the network below the media layer, upper switch cannot detect the loop. Remote loop detect is the complementary for this situation.

Enable STP remote-loop-detect

In interface configuration mode

```
spanning-tree remote-loop-detect
```

In global configuration mode

```
spanning-tree remote-loop-detect interface
```

Use no command to disable this function.

For example:

！Enable spanning-tree remote-loop-detect interface of Ethernet 0/1

```
OLT(config)#spanning-tree remote-loop-detect interface ethernet 0/1
```

！Disable remote-loop-detect of Ethernet 0/1

```
OLT(config-if-ethernet-0/1)#no spanning-tree remote-loop-detect
```

14.3. Brief introduction of MSTP

Multiple spanning tree (IEEE802.1S) is the update for SST (Single spanning tree, IEEE8021.D/8021,W). SST can realize link redundant and eliminate loop, but all VLANs share a tree may cause the waste of effective bandwidth and the overload of some link and backup of the rest. MST can supply the gap of above which can map different VLAN to different spanning tree example to realize all functions of SST and the balance of load, that is, different spanning tree example can form different topology and data of different VLAN can choose different transmission channel according to the spanning tree example where the VLAN locates.

14.4. MSTP configuration

14.4.1 MSTP configuration list

Each parameter configured by MSTP can be effective in MSTP mode when spanning tree is enable. The configuration will be saved when MSTP is disable and it will be effective when MSTP is enable. The configuration list is as following:

- Configure timer value of MSTP
- Configure MSTP configuration mark
- Configure MSTP net bridge privilege

- Configure edge interface status of MSTP interface
- Configure MSTP interface link type
- Configure MSTP interface path cost
- Configure MSTP interface privilege
- Display MSTP configuration information

14.4.2 Configure timer value of MSTP

MSTP timer value includes: forward delay, hello time, max age and max hops.

Configure it in global configuration mode

- Configure forward delay

spanning-tree mst forward-time forward-time

- Configure hello time

spanning-tree mst hello-time hello-time

- Configure max age

spanning-tree mst max-age max-age

- Configure max hops

spanning-tree mst max-hops max-hops

Example：

！Configure max hops to be 10

```
OLT(config)#spanning-tree mst max-hops 10
```

14.4.3 Configure MSTP configuration mark

MSTP configuration mark includes: MSTP configuration name, MSTP modify level and the relations of MSTP example and VLAN. MSTP will treat interconnected net bridge with the same configuration mark as a virtual net bridge.

Configure it in global configuration mode:

- Configure MSTP configuration mark name

spanning-tree mst name

- Configure MSTP configuration mark modify level

spanning-tree mst revision revision-level

- Configure mapping relation of MSTP example and VLAN of MSTP configuration mark

spanning-tree mst instance instance-num VLAN VLAN-list

Example：

！Configure MSTP configuration mark name to be nicnet

```
OLT(config)#spanning-tree mst name nicnet
```

！Configure MSTP configuration mark modify level to be 10

OLT(config)#spanning-tree mst revision 10

！Configure VLAN2~7 mapping to spanning tree example 5

OLT(config)#spanning-tree mst instance 5 VLAN 2-7

14.4.4 Configure MSTP net bridge privilege

In MSTP, the privilege of net bridge is based on the parameter of each STP example. net bridge privilege as well as interface privilege and interface path cost determine the topology of each STP example to construct the base of link load balance.

Configure it in global configuration mode:

- Configure privilege of net bridge in MSTP example

spanning-tree mst instance instance-num priority

Example：

！Configure privilege of net bridge in MSTP example 4 to be 4096

OLT(config)#spanning-tree mst instance 4 priority 4096

14.4.5 Configure edge interface status of MSTP interface

As SST, after linking up of interface with edge interface attribution, if it hasn’t received any packet in two packet-sending periods, interface will be in forwarding status.

Configure it in interface configuration mode：

- Configure interface to be edge interface

spanning-tree mst portfast

！Example：

Configure interface 2 to be edge interface

OLT(config-if-ethernet-0/2)#spanning-tree mst portfast

14.4.6 Configure MSTP interface link type

Interface link type are two kinds: one is sharing medium (linking through hub), the other is point-to-point. Link type is used in suggestion-aggression mechanism. Only the interface of point-to-point can shift fast. Link type can be specified manually or self-detect by STP.

！Example

Configure link type of interface 2 to be point-to-point for cefalse

OLT(config-if-ethernet-0/2)#spanning-tree mst link-type point-to-point for cefalse

14.4.7 Configure MSTP interface path cost

Interface path cost are internal cost and external cost. The former is based on each MSTP example configured parameter to determine topology of different example in each MSTP region. The latter is the parameter which has nothing to do with example and determine the CST topology formed by each region.

Configure it in interface configuration mode：

- Configure the path cost of interface in some instance

spanning-tree mst instance instance-num cost

- Configure the external path cost of interface

spanning-tree mst external cost

Example：

！Configure the path cost of interface 2 in instance 1 to be 10

```
OLT(config-if-ethernet-0/2)#spanning-tree mst instance 1 cost 10
```

！Configure the external path cost of interface 2 to be 10

```
OLT(config-if-ethernet-0/2)#spanning-tree mst external cost 10
```

14.4.8 Configure MSTP interface privilege

In MSTP, interface privilege is the parameter based on each STP instance.

Configure it in interface configuration mode：

- Configure interface privilege in some instance

spanning-tree mst instance instance-num port-priority priority

！Configure privilege of interface 2 in instance 1 to be 16

```
OLT(config-if-ethernet-0/2)#spanning-tree mst instance 1 port-priority 16
```

14.4.9 Display MSTP configuration information

The basic information of MSTP includes: MSTP configuration mark information (includes configuration name, modify level and the mapping relations between VLAN and MSTP instance); the configuration information of STP instance and interface.

Use this command in any configuration mode：

- Display MSTP configuration mark information

show spanning-tree mst config-id

- Display interface information of some instance

show spanning-tree mst instance instance-num interface [interface-list]

！Example：

Display MSTP configuration mark information

```
OLT(config)#show  spanning-tree  mst  config-id
```

Display information of interface 2 in instance 1

```
OLT(config)#show spanning-tree mst instance 1 interface ethernet 0/2
```

15. 802.1X CONFIGURATION COMMAND

15.1. Brief introduction of 802.1X configuration

IEEE 802.1X is the accessing management protocol standard based on interface accessing control passed in June, 2001. Traditional LAN does not provide accessing authentication. User can access the devices and resources in LAN when connecting to the LAN, which is a security hidden trouble. For application of motional office and CPN, device provider hopes to control and configure user's connecting. There is also the need for accounting.

IEEE 802.1X is a network accessing control technology based on interface which is the accessing devices authentication and control by physical accessing level of LAN devices. Physical accessing level here means the interface of LAN Switch devices. When authentication, switch is the in-between (agency) of client and authentication server. It obtains user's identity from client of accessing switch and verifies the information through authentication server. If the authentication passes, this user is allowed to access LAN resources or it will be refused.

System realizes IEEE 802.1X authentication. Use IEEE 802.1X authentication needs: RADIUS server which system can access to make the authentication informayion to send to; IEEE 802.1X authentication client software installed in accessing user's device (such as PC).

15.2. 802.1X Configuration

Configure system or interface related parameter before enabling 802.1X authentication and these configurations will be saved after disabling 802.1X. And the parameter will be effective after re-enabling 802.1X.

802.1X configuration list is as following：

- Configure RADIUS project
- Configure domain
- Configure 802.1X

15.2.1 AAA configuration mode

Finish necessary configuration of domain and RADIUS project of 802.1X authentication.

Use aaa command in global configuration mode to enter AAA configuration mode.

For example:

！Enter AAA configuration mode

```
OLT(config)#aaa
OLT(config-aaa)#
```

15.2.2 RADIUS Server Configuration

RADIUS server saves valid user's identity. When authentication, system transfers user's identity to RADIUS server and transfer the validation to user.

User accessing to system can access LAN resources after authentication of RADIUS server.

RADIUS server configurations are as following:

- radius host
- primary-auth-ip primary-acct-ip
- realtime-account
- second-auth-ip second-acct-ip
- auth-secret-key acct-secret-key
- username-format
- show radius host

The order of configuration can be as following:

（1）In AAA mode, use radius host command to enter RADIUS server configuration mode (if the RADIUS server does not exist, create it first), use no radius command to remove specified RADIUS server. The name of RADIUS server ranges from 1 to 32 charaters with no difference in upper-case type and lower case letters and without space.

For example：

！Enter RADIUS server nic

OLT(config-aaa)#radius host nic

OLT(config-aaa-radius-nic)#

（2）In RADIUS server configuration mode, use primary-acct-ip & primary-auth-ip command to configure ip address and authentication of current primary authentication server (the default authentication port is 1812 and accounting port is 1813). Use no primary-acct-ip & primary-auth-ip command to remove ip address of primary server.

For example:

！ Configure ip address of primary authentication server to be 192.168.0.100，and authentication port to be 1812, accounting port to be 1813

OLT(config-aaa-radius-nic)#primary-auth-ip 192.168.0.100 1812

OLT(config-aaa-radius-nic)#primary-acct-ip 192.168.0.100 1813

（3）In RADIUS server configuration mode, use realtime-account command to enable realtime accounting. Use no realtime-account command to disable it. It is defaulted to enable and the interval of sending accounting packet is 12 minutes.

Example：

！Configure the interval of sending accounting packet to be 10 minutes

OLT(config-aaa-radius-nic)#realtime-account interval 10

！Disable realtime accounting

OLT(config-aaa-radius-nic)#no realtime-account

（4）In RADIUS server configuration mode, use second-ip command to configure ip adress and authentication and accounting port of second authentication server (the default authentication port is 1812 and the accounting port is 1813). Use no second-ip command to remove it.

For example:

！Configure the ip address of the second authentication server of the RADIUS server with the name of nic to be 192.168.0.200， and authentication port to be 1812 and accounting port to be 1813

```
OLT(config-aaa-radius-nic)#second-auth-ip 192.168.0.200 1812
 OLT(config-aaa-radius-nic)#second-acct-ip 192.168.0.200 1813
```

（5）Use secret-key command to configure a shared key for the RADIUS server. Use no secret-key command to restore the default shared key Switch.

For example:

！Configure the shared key for the RADIUS server with the name of nic to be nicnet

```
OLT(config-aaa-radius-nic)#acct-secret-key nicnet
OLT(config-aaa-radius-nic)#auth-secret-key nicnet
```

（6）Use username-format command to configure the format of the usernames to be sent to RADIUS servers. With-domain means user name with domain name. Without-domain means user name without domain name.

For example:

！Configure the username sent to the RADIUS server with the name of nic not to carry domain name.

```
OLT(config-aaa-radius-nic)#username-format without-domain
```

（7）Use show radius host command to display RADIUS server information.

For example:

！Display RADIUS server information

```
OLT(config-aaa-radius-nic)# show radius host nic
```

15.2.3 Domain Configuration

Client need provide username and password when authentication. Username contains user's ISP information, domain and ISP corresponded. The main information of domain is the RADIUS server authentication and accounting the user should be.

The main configuration command of domain is as following:

- domain
- radius host binding
- access-limit
- state
- default domain-name
- show domain

The order of configuration can be as following:

(1) In AAA configuration mode, use domain command to enter AAA configuration mode. If it doesn’t exist, create it. Use no domain command to remove the domain. The name of the domain ranges from 1 to 24 charaters, no difference in upper-case type and lower case letters, and without space.

For example:

！Create domain with the name of nic.com

```
OLT(config-aaa)#domain nic.com
OLT(config-aaa-nic.com)#
```

（2）Use radius host command to choose a RADIUS server for current domain. Administrator specifies a existed RADIUS server to configure to be the RADIUS server of current domain.

For example:

！Configure current domain to use RADIUS configuration of “nic”

```
OLT(config-aaa-nic.com)#radius host nic
```

（3）Use access-limit to enable command to configure the maximum number of access user that can be contained in current domain.

For example:

！Configure the maximum number of access user that can be contained in domain nic.com to 100

```
OLT(config-aaa-nic.com)#access-limit enable 100
```

（4）Use state command to configure the state of the domain to be active or block.

For example:

！Activate nic.com

```
OLT(config-aaa-nic.com)#state active
```

（5）Use default domain-name to enable command to configure a existed domain to be default domain. If the domain doesn’t exist, the configuration fails. Use default domain-name disable command to disable the default domain.

When the default domain name is disabled, switch will not deal with the invalid packet, if the username goes without the domain name. After the default domain name is enabling, switch will add @ and default domain name to a username wothout a domain name to authenticate. To configure a default domain which must be existed, or the configuration fails.

For example:

！Configure default domain name to be nic.com and enable the default domain

```
OLT(config-aaa)#default domain-name enable nic.com
```

（6）Use show domain command to display the configuration of the domain.

For example:

```
！Display the configuration of the domain
OLT(config-aaa-nic.com)#show domain
```

15.2.4 802.1X Configuration

Related command of 802.1X configuration is as following:

- dot1x
- dot1x daemon
- dot1x eap-finish
- dot1x eap-transfer
- dot1x re-authenticate
- dot1x re-authentication
- dot1x timeout re-authperiod
- dot1x timeout re-authperiod interface
- dot1x port-control
- dot1x max-user
- dot1x user cut

（ 1 ）Use dot1x command to enable 802.1x. Domain and RADIUS server configurations can be effective after this function enabling. Use no dot1x command to disable 802.1x. Use show dot1x command to display 802.1x authentication information.

After enabling 802.1X, user accessed to system can access VLAN resources after authentication. By default, 802.1X disables.

For example:

```
！Enable 802.1X
OLT(config)#dot1x
！Display 802.1x authentication information
OLT(config)#show dot1x
```

（ 2 ）When 802.1x enables, use this command to configure whether a port send 802.1x daemon and sending period.

By default, 802.1x daemon is not sent by default. When 802.1x enables, default interval to send daemon is 60seconds.

For example:

```
！Enable dot1x daemon on ethernet 0/5 with the period time of 20 seconds
OLT(config-if-ethernet-0/5)#dot1x daemon time 20
```

（ 3 ）Use dot1x eap-finish and dot1x eap-transfer command to configure protocol type between system and RADIUS server:

After using dot1x eap-transfer command, 802.1 authentication packet encapsulated by EAP frame from user is sent to RADIUS server after transfering to data frame encapsulated by other high level protocol. After using dot1x eap-transfer command, 802.1 authentication packet encapsulated by EAP frame from user is sent to RADIUS server without any changes.

For example:

```
！Configure authentication packet tramsitting to be eap-finish
OLT(config)#dot1x eap-finish
```

（4）Use dot1x re-authenticate command to re-authenticate current interface. Use dot1x re-authentication command to enable 802.1x re-authentication. Use no dot1x re-authentication command to disable 802.1x re-authentication. Use dot1x timeout re-authperiod command to configure 802.1x re-authperiod. Use dot1x timeout re-authperiod interface command to configure 802.1x re-authperiod of a specified interface. Please refer to command line configuration to see the details.

（5）Use dot1x port-control command to configure port control mode.

After 802.1X authentication enables, all interfaces of the system default to be needing authentication, but interfaces of uplink and connecting to server need not authentication. Use dot1x port-control command to configure port control mode. Use no dot1x port-control command to restore the default port control. Use show dot1x interface command to display configuration of interface.

Configure it in interface configuration mode:

```
dot1x port-control { auto | forceauthorized | forceunauthorized }
```

For example:

```
！Ethernet 0/5 is RADIUS server port. Configure port-control mode of ethernet 0/5 to be
forceauthorized in interface configuration mode
OLT(config-if-ethernet-0/5)#dot1x port-control forceauthorized
！Display 802.1X configuration of ethernet 0/5
OLT(config)#show dot1x interface ethernet 0/5
port ctrlmode        Reauth   ReauthPeriod(s) MaxHosts
e0/5   forceauthorized disabled   3600          160
Total [26] item(s), printed [1] item(s).
```

（6）Use dot1x max-user command to configure the maximum number of supplicant systems an ethernet port can accommodate. Use no dot1x max-user command to configure the maximum number to be 1.

Configure it by using following command:

```
dot1x max-user user-num
```

For example:

！Configure the max-user of ethernet 0/5 is 10 in interface configuration mode

```
OLT(config-if-ethernet-0/5)#dot1x max-user 10
```

（7）Use dot1x user cut command to remove specified online user.

Remove specified online user by specified username and MAC address.

For example:

！Remove user with username of aaa@OLT.br

```
OLT(config)#dot1x user cut username aaa@OLT.br
```

16. SNTP CLIENT CONFIGURATION

16.1. Brief introduction of SNTP protocol

The working theory of SNTP is as following:

SNTPv4 can be worked in three modes: unicast, broadcast (multicast) and anycast.

In unicast mode, client actively sends requirement to server, and server sends response packet to client according to the local time structure after receiving requirement.

In broadcast and multicast modes, server sends broadcast and multicast packets to client timing, and client receives packet from server passively.

In anycast mode, client actively uses local broadcast or multicast address to send requirement, and all servers in the network will response to the client. Client will choose the server whose response packet is first received to be the server, and drops packets from others. After choosing the server, working mode is the same as that of the unicast.

In all modes, after receiving the response packet, client resolves this packet to obtain current standard time, and calculates network transmit delay and local time complementary, and then adjusts current time according them.

16.2. SNTP client configuration

SNTP client configuration command includes：

- Enable/disable SNTP client
- SNTP client working mode configuration
- SNTP client unicast server configuration
- SNTP client broadcast delay configuration
- SNTP client multicast TTL configuration
- SNTP client poll interval configuration
- SNTP client retransmit configuration
- SNTP client valid server configuration
- SNTP client MD5 authentication configuration

16.2.1 Enable/disable SNTP client

Use sntp client command in global configuration mode to enable SNTP client. Use no sntp client command to disable SNTP client. After SNTP enabling, switch can obtain standard time through internet by SNTP protocol to adjust local system time.

Enable SNTP client using following command：

- sntp client
- no sntp client

For example:

```
！Enable SNTP client
OLT(config)#sntp client
```

16.2.2 SNTP client working mode configuration

SNTPv4 can work in three modes: unicast, broadcast (multicast), anycast. In unicast and anycast, client sends requirement and gets the response to adjust system time. In broadcast and multicast, client waits for the broadcast packet sent by server to adjust system time.

- sntp client mode { broadcast | unicast | anycast [key number] | multicast }
- no sntp client mode

For example:

！Configure SNTP client to operate in anycast

```
OLT(config)#sntp client mode anycast
```

16.2.3 SNTP client unicast server configuration

In unicast ode, SNTP client must configure server address. The related command is as following：

- sntp server ip-address [key number]
- no sntp server

Only in unicast, configured server address can be effective.

For example:

！Configure unicast server ip-address to be 192.168.0.100

```
OLT(config)#sntp server 192.168.0.100
```

16.2.4 SNTP client broadcast delay configuration

SNTP client broadcast delay configuration is as following：

- sntp client broadcastdelay milliseconds
- no sntp client broadcastdelay

Only in broadcast (multicast), configured transmit delay can be effective. After configuration, SNTP client can add transmit delay after obtaining time from server to adjust current system time.

For example:

！Configure broadcastdelay to be 1 second

```
OLT(config)#sntp client broadcastdelay 1000
```

16.2.5 SNTP client multicast TTL configuration

Use following command to configure ttl-value of multicast packet：

- sntp client multicast ttl ttl-value
- no sntp client multicast ttl

This command should be effective by sending packet through multicast address in anycast operation mode. In order to restrict the range of sending multicast packet, TTL-value setting is suggested. The default ttl-value is 255.

For example:

！Configure TTTL-value of sending multicast packet to be 5

```
OLT(config)#sntp client multicast ttl 5
```

16.2.6 SNTP client poll interval configuration

Use following command to configure poll-interval of SNTP client in unicast or anycas. ：

- sntp client poll-interval seconds
- no sntp client poll-interval

Only in unicast and anycast mode, configured poll interval can be effective. SNTP client sends requirement in a poll interval to the server to adjust current time.

For example:

！Configure poll-interval to be 100 seconds

```
OLT(config)#sntp client poll-interval 100
```

16.2.7 SNTP client retransmit configuration

Uses following command to configure retransmit times inunicast and anycast operation mode. ：

- sntp client retransmit times
- no sntp client retransmit
- sntp client retransmit-interval seconds
- no sntp client retransmit-interval

This command is effective in unicast and anycast operation mode. SNTP requirement packet is UDP packet, overtime retransmission system is adopted because the requirement packet cannot be guaranteed to send to the destination. Use above commands to configure retransmit times and the interval.

For example:

！Configure overtime retransmission to be twice and the interval to be 5

```
OLT(config)#sntp client retransmit-interval 5
OLT(config)#sntp client retransmit 2
```

16.2.8 SNTP client valid server configuration

In broadcast and multicast mode, SNTP client receives protocol packets from all servers without distinction. When there is malice attacking server (it will not provide correct time), local time cannot be the standard time. To solve this problem, a series of valid servers can be listed to filtrate source address of the packet.

Corresponded command is as following ：

- sntp client valid-server
- no sntp client valid-server

For example:

！Configure servers in network interface 10.1.0.0/16 to be valid servers

```
OLT(config)#sntp client valid-server 10.1.0.0 0.0.255.255
```

16.2.9 SNTP client MD5 authentication configuration

SNTP client can use valid server list to filtrate server, but when some malice attackers using valid server address to forge server packet and attack switch, switch can use MD5 authentication to filtrate packet, and authenticated packet can be accepted by client.

Configuration command is as following：

- sntp client authenticate
- no sntp client authenticate
- sntp client authentication-key number md5 value
- no sntp client authentication-key number
- sntp trusted-key number
- no sntp trusted-key number

For example:

！Configure SNTP client MD5 authentication-key, with the key ID being 12，and the key being abc and trusted-key being 12

```
OLT(config)#sntp client authenticate OLT(config)#sntp
client authentication-key 12 md5 abc OLT(config)#sntp
trusted-key 12
```

17. SYSLOG CONFIGIRATION

17.1. Brief introduction of Syslog

Syslog is system information center, which handles and outputs information uniformly.

Other modules send the information to be outputted to Syslog, and Syslog confirms the form of the outputting of the information according to user's configuration, and outputs the information to specified displaying devices according to the information switch and filtration rules of all outputting directions.

Because of Syslog, information producer——all modules of outputting information need not care where the information should be send at last, console, telnet terminal or logging host (Syslog server). They only need send information to Syslog. The information consumer—— console, Telnet terminal, logging buffer, logging host and SNMP Agent can choose the information they need and drop what they needn't for suitable filtration rules.

Syslog information level reference:

severe level	Description	corresponded explanation
0 : emergencies	the most emergent error	need reboot
1 : alerts	need correct immediately	self-loop, hardware error
2 : critical	key error	memory, resources distribution error
3 : errors	non-key errors need cautions	general error; invalid parameter which is hard to restore
4 : warnings	Warning for some error which may exist	alarm; losing packet which is not important; disconnect with the exterior server
5 : notifications	information needs cautions	Trap backup outputting
6 : informational	general prompt information	command line operation log; set operation for MIB node
7 : debugging	debug information	debugging outputting; process, data of service protocol

17.2. Syslog Configuration

Syslog configuration command includes:

- Enable/disable Syslog
- Syslog sequence number configuration
- Syslog time stamps configuration
- Syslog terminal outputting configuration
- Syslog logging buffered outputting configuration
- Syslog Flash storage outputting configuration

- Syslog logging host outputting configuration
- Syslog SNMP Agent outputting configuration
- Module debug configuration

17.2.1 Enable/disable Syslog

Use logging command in global configuration mode to enable Syslog. Use no logging command to disable Syslog and no information will be displayed.

Configuration command is as following：

- logging
- no logging

For example:

！Enable Syslog

```
OLT(config)#logging
```

17.2.2 Syslog sequence number configuration

Use logging sequence-numbers command to configure global sequence number to be displayed in Syslog. Use no logging sequence-numbers command to configure global sequence number not to be displayed in Syslog.

- logging sequence-numbers
- no logging sequence-numbers

For example:

！Configure global sequence number to be displayed in Syslog outputting information.

```
OLT(config)#logging sequence-numbers
```

17.2.3 Syslog time stamps configuration

Use following command to configure the type of timestamps in Syslog. There 3 types of timestamps: timestamps are not displayed, uptime is the timestamps, and datatime is the timestamps.

Configure command is as following：

- logging timestamps { notime | uptime | datetime }
- no logging timestamps

For example:

！Configure datetime to be the timestamps

```
OLT(config)#logging timestamps datetime
```

17.2.4 Syslog terminal outputting configuration

Use following command in global configuration mode to enable monitor logging and configure filter regulation.

(1) Logging monitor configuration command is as following：

- logging monitor { all | monitor-no }
- no logging monitor { all | monitor-no }

monitor-no: 0 means console, and 1 to 2 means Telnet terminal.

For example:

！Enable monitor logging

OLT(config)#logging monitor 0

(3) Logging monitor configuration command is as following：

- logging monitor { all | monitor-no } { level | none | level-list { level [to level] } &<1-8> } * module , xxx | … - * +
- no logging monitor { all | monitor-no } filter

xxx：means the name of the module. … means other modules are omitted

For example:

！Configure filter regulations of all terminals to allow all modules of levels 0 to 7 to output information

OLT(config)#logging monitor 0 7

17.2.5 Syslog logging buffered outputting configuration

Use logging buffered command in global configuration mode to enable buffered logging and configure filter regulations. Use no logging buffered command to disable buffered logging and restore to default filter regulations.

(1) Logging buffered configuration command is as following：

- logging buffered
- no logging buffered

For example:

！Enable buffered logging

OLT(config)# logging buffered

(2) Filtration rules configuration command is as following：

- logging buffered { level | none | level-list { level [to level] } &<1-8> - * module , xxx | … } *]
- no logging buffered filter

xxx: means the name of the module. … means other modules are omitted.

For example:

！Configure filter regulations of all terminals to allow all module of level 0 to 6 to output information

OLT(config)#logging buffered 6

17.2.6 Syslog Flash storage outputting configuration

Use logging flash command in global configuration command to enable flash logging and configure filter regulations.

(1) Logging buffered configuration command is as following

- logging flash
- no logging flash

For example:

! Enable flash logging

OLT(config)# logging flash

(2) Filtration rules configuration command is as following：

- logging flash { level | none | level-list { level [to level] } &<1-8> - * module , xxx | … - * +
- no logging flash filter

xxx: means the name of the module. … means other modules are omitted.

For example:

! Configure filter regulations of all terminals to allow all modules to output information with the level of 0, 1, 2, 6

OLT(config)#logging flash level-list 0 to 2 6

17.2.7 Syslog logging host outputting configuration

Use following command to configure host ip address, and enable host logging, and configure filter regulation of Syslog server.

(1) Server address configuration command is as following：

- logging ip-address
- no logging ip-address

At most 15 logging hosts are allowed to configure.

For exaple：

! Configure server address to be 1.1.1.1：

OLT(config)#logging 1.1.1.1

(2) Logging buffered configuration command is as following:

- logging host { all | ip-address }
- no logging host { all | ip-address }

For example:：

! Enable logging host 1.1.1.1

OLT(config)#logging host 1.1.1.1

(3) Filtration rules configuration command is as following：

- logging host { all | ip-address } { level | none | level-list { level [to level] } &<1-8> } [module , xxx | … - * +
- no logging host { all | ip-address } filter

xxx: means the name of the module. … means other modules are omitted.

For example:

！Configure filter regulations of logging host 1.1.1.1 to allow module VLAN of level 7 to output information

OLT(config)#logging host 1.1.1.1 none OLT(config)#logging

host 1.1.1.1 level-list 7 module VLAN (4) Logging facility

configuration command is as following：

- logging facility , xxx | … -
- no logging facility

xxx：The name of logging facilities.… means other logging facilities are omitted.

For example：

！Configure logging facility to be localuse7

OLT(config)#logging facility localuse7

(5) Fixed source address configuration command is as following：

- logging source ip-address
- no logging source

ip-address must be an interface address of a device.

For example:

！Configure logging host outputting to use fixed source address 1.1.1.2：

OLT(config)#logging source 1.1.1.2

17.2.8 Syslog SNMP Agent outputting configuration

Use logging snmp-agent command to enable SNMP Agent logging and configure filter configuration. Use no logging snmp-agent command to disable SNMP Agent logging and restore to default filter configuration.

Configure Trap host ip address for Syslog information to send to SNMP Workstation by Trap packet. (refer to SNMP configuration)

(1) Logging buffered configuration command is as following：

- logging snmp-agent
- no logging snmp-agent

For example：

！Enable SNMP Agent logging

OLT(config)#logging snmp-agent

(2) Filtration rules configuration command is as following：

- logging snmp-agent { level | none | level-list { level [to level] } &<1-8> } [module { xxx | … - * +
- no logging snmp-agent filter

xxx: means the name of the module. … means other modules are omitted.

For example：

！Configure SNMP Agent filtrate rules to be permitting information with the level 0 ~ 5

OLT(config)#logging snmp-agent 5

17.2.9 Module debug configuration

Use debug command to enable debug of a module. Use no debug command to disable debug of a module：

- debug , all | , xxx | … - * -
- no debug , all | , xxx | … - * -

xxx: means the name of the module. … means other modules are omitted.

For example:

！Enable debug of module VLAN

OLT(config)#debug VLAN

18. SSH CONFIGURATION

18.1. Brief introduction of SSH

SSH is short for Secure Shell. Users can access to the device via standard SSH client, and sent up safe connection with device. The Data that transmitted via SSH connection are encrypt, which assure the transmitted sensitive data, management data and configuration data, such as password, between the users and devices will not be wiretapped or acquired illegally by the third party.

SSH can replace Telnet, providing users with means of safely management and device configuration.

18.2. SSH Configuration

The configuration task list of SSH is as follows:

- Enable/disable SSH function of the device
- SSH secret key configuration
- Others

18.2.1 Enable/disable SSH function of the device

Enable/disable SSH function of the device in global mode, users can not access to the devices via SSH client when SSH function is closed. To access to the device via SSH client, users need to configure correct secret key and upload the secret key in the device besides opening up the SSH function.

Configuration command is as following：

- ssh
- no ssh

Example：

```
！Enable SSH
OLT(config)#ssh
```

18.2.2 SSH key configuration

Use SSH secret key in privileged mode. User cannot use SSH client to log in if there is no secret key or the key is incorrect or the key is not load. In order to log in by SSH client, configure correct key and load it with SSH enabling.

The configured secret key should be RSA. There are two kinds of keys: public and private. It can use the default key and also can download keyfile to device by tftp and ftp. Configured key can be used after loading. Configured key is stored in Flash storage which will be load when system booting. It also can load the key stored in Flash storage by command line when system booting.

If configured key is not ESA key or public and private key are not matched, user cannot log in by SSH.

Keyfile contains explanation and key explain line and the key. Explain line must contain “:” or space. Key contains the key coded by Base64, excluding “:”and space. Private keyfile cannot contain public key. Private keyfile cannot use password to encrypt.

(1) Configure default key. The command is as following:

- Crypto key generate rsa

Example：

！Configure SSH key to be default key

OLT#crypto key generate rsa

(2) Download or upload key by tftp or ftp. The command is as following:

- load keyfile { public | private } tftp server-ip filename
- load keyfile { public | private } ftp server-ip filename username passwd
- upload keyfile { public | private } tftp server-ip filename
- upload keyfile { public | private } ftp server-ip filename username passwd

Example:

！Download keyfile pub.txt from tftp server 1.1.1.1 to be SSH public key

OLT#load keyfile public tftp 1.1.1.1 pub.txt

(3) Clear configured key. This command will clear all keyfiles storaged in Flash storage. The configuration command is as following:

- crypto key zeroize rsa

Example：

！Clear configured SSH key

OLT#crypto key zeroize rsa

(4) Load new key. After configuring new SSH key, it restored in Flash storage without loading. This command can read configured key from Flash storage and update the current key. When system booting, it will detect Flash storage, if SSH key is configured, it will load automatically. The configuration command is as following:

- crypto key refresh

Example：

！Load new SSH key：

OLT#crypto key refresh

18.2.3 Others

(1) Use following command to display SSH configuration

- show ssh

This command is used to display SSH version number, enabling/disabling SSH and SSH keyfile. The SSH keyfile is “available” when the key is configured and loaded.

(2) Use following command to display configured keyfile

- show keyfile { public | private }

(3) Use following command to display logged in SSH client

- show users

This command is used to display all logged in Telnet and SSH client.

(4) Use following command to force logged in SSH client to stop

- stop username

This command can force logged in SSH client to stop. Username is the logged in user name.

(5) It allows at most 5 SSH clients to logged in. If Telnet client has logged in, the total number of SSH and Telnet clients is no more than 5. For example, if there are 2 Telnet clients in device, at most 3 SSH clients can log in.

19. VRRP CONFIGURATION

19.1. Brief introduction of VRRP

In network based on TCP/IP, specify route to guarantee the communication of non-physical connection devices. The common ways of specifying route are: one is through dynamic of learning of route protocol (such as internal route protocol of RIP and OSPF), the other is static configuration. It is unrealistic to run dynamic route protocol in each terminal and operation system of most of clients doesn't support dynamic route protocol, though some supports, it is restricted by managing cost, convergence and security. It is widely using static route configuration for terminal IP devices to specify one or more default gateway. Static route simples the complicity of network management and reduces communication cost of terminal devices. It has a shortage: if the router of defaulted gateway is damaged, the communication of the host which uses this gateway to be the next hop will be cut off. Using Virtual Router Redundancy Protocol (VRRP) can avoid the shortage of statically specified gateway.

In VRRP protocol, there are two important concept: VRRP router and virtual router, master router and backup router. VRRP router is the router run VRRP which is the physical entity. Virtual router is created by VRRP protocol which is a logical concept. A group of VRRP routers work together to construct a virtual router (also called a backup group). This virtual router is a logical router with unique and fixed IP and MAC address. The routers in the same VRRP group are in two roles: master router and backup router. There is one master router and one or more backup router. VRRP uses selecting strategy to select a router too be master to response ARP and transfer IP data packet. Other routers in the group are backup. When master routers is failure, backup router will become master router in several seconds. This conversion is very fast without changing IP address and MAC address. It is clear for all terminal users.

19.2. VRRP Configuration

VRRP configuration list is as following：

- Add or delete virtual IP address
- Configure priority of backup group
- Configure preeptible way and delay time of backup group
- Configure timer of backup group
- Enable ping of virtual IP

19.2.1 Add or delete virtual IP address

Specify IP address of this network interface to a virtual switch (also called a backup group), or remove a virtual IP address from a backup group.

Configure it in VLAN interface configuration mode.

- ip vrrp vrid vip
- no ip vrrp vrid [vip]

Backup id is in the range of 1 to 255. Virtual address can be undistributed IP address in the interface where the backup group is in, and also can be IP address of backup group interface.

At most 8 backup groups can be configured. If this address is the one the switch has used, it also can be configured. Now, this switch is called an IP Address Owner. When specify the first IP address to a backup group, system will create this backup group, and add virtual IP address to this backup group from that on, system will only add the address to the backup group. At most 8 IP address can be configured to each backup group.

When deleting the last IP address, the backup group will be deleted at the same time, that is, there is no this backup group in this interface and all configurations are not valid.

19.2.2 Configure priority of backup group

In VRRP, determine the position of each switch in backup group according to priority. The one with the superior will be the Master.

The priority value is in the range of 0 to 255 (the larger the number is, the superior the priority level is) and the configured range is 1 to 254. Priority 0 is reserved for special uses and 255 is reserved to IP address owner.

Configure it in VLAN interface configuration mode.

- vrrp priority vrid priority
- no vrrp priority vrid

By default, the priority is in the range of 100.

⚠Caution: For IP address owner, the priority cannot be configured. It is 255 all the time.

19.2.3 Configure preempt way and delay time of backup group

Once there is a Master in the backup group, and there is no failure, and other switch though has configured to process superior priority, It will not be Master unless the preemption is configured. If the switch is configured to be preempt, once it processes its priority is superior than the Master, it will be the Master. Accordingly, the original Master will be the backup. The delay time can be configured at the same time as the preemption, which can delay backup being Master. The aim of delay time is: In unstable network, if Backup doesn’t receive the packet from Master on time, it will become Master (the reason why Backup cannot receive the packet is because of the congestion of the network, not the abnormal working of Master). So waiting for a certain time, the packet will be received from Master, which avoids frequent changes.

The delay time is in the unit of second which is in the range of 0 to 255.

Configure it in VLAN interface configuration mode.

- vrrp preempt vrid [delay]
- no vrrp preempt vrid

It is defaulted to be preempt with the delay time being 0.

⚠ Caution: Cancelling preemption of backup group, the delay time will be 0.

19.2.4 Configure timer of backup group

Master switch in VRRP backup group can timely send VRRP packet (the time interval is adver_interval) to inform other switches it works normally. If backup hasn’t received VRRP packet from master switch after a certain time (master_down_interval), it will think master is abnormal and turn itself to be master.

User can adjust VRRP packet sending time interval adver_interval by using configuration command. The time interval of master_down_interval is 3 times of adver_interval. The large traffic and different timer in switch will cause the abnormal of master_down_interval to shift status. For this, you can prolong adver_interval and configure delay time. The unit of adver_interval is second.

- vrrp timer vrid adver-interval
- no vrrp timer vrid

Configure it in VLAN interface configuration mode.

- vrrp timer vrid adver-interval
- no vrrp timer vrid

By default, adver_interval is 1 second.

19.2.5 Enable ping of virtual IP

To test the reachability of main switch, enable ping function of virtual IP, that is, received destination address to be virtual IP and switch is the main switch which can response ping packet, and host can ping virtual gateway.

Configure it in global configuration mode：

- vrrp ping-enable
- no vrrp ping-enable

It is defaulted to disable ping of virtual IP

19.2.6 VRRP monitor and maintenance

User can display VRRP information by following command.

Use it in any configuration mode:

- show vrrp [VLAN-interface VLAN-id [vrid]]

20. SWITCH MANAGE AND MAINTENANCE

20.1. Configuration Files Management

20.1.1 Edit configuration files

Configuration files adopts text formatting which can be upload to PC feom devices by FTP and TFTP protocol. Use text edit tool (such as windows nootbook) to edit uploaded configuration files.

System is defaulted to execute configuration files in global configuration mode, so there are two initial commands: “enable”, and “configure terminal”. There is entering symbol after each command.

20.1.2 Modify and save current configuration

User can modify and save system current configuration by command line interface to make current configuration be initial configuration of system next booting. Copy running-config startup-config command is needed to save current configuration. When executing configuration files, if there is un-executed command, it will be displayed as “*Line:xxxx+invalid: commandString”. If there is command with executing failure, it will be displayed as “*Line:xxxx+failed: commandString”. If there is a command beyond 512 characters, it will be displayed as “*Line:xxxx+failed: too long command: commandString”, and only first 16 characters of this command will be displayed, and end up with …, in which “xxxx”means the line number of the command, and commandString means command character string. Un-executive command includes command with grammar fault and un-matching pattern. Use following command in privileged mode.

```
OLT#copy running-config startup-config
```

20.1.3 Erase configuration

Use clear startup-config command to clear saved configuration. After using this command to clear saved configuration and reboot switch. The switch will restore to original configuration. Use this command in privileged mode.

```
OLT#clear startup-config
```

20.1.4 Save minmum manageable configuration of network administration

Use command line interface to save minmum manageable configuration of network administration. Minimum manageable configuration of network administration only contains configuration of one VLAN interface. Use copy nm-interface-config startup-config command to save minmum manageable configuration of network administration.

Example:

```
！Save configuration of VLAN interface 1 which has been configured IP address
OLT#copy nm-interface-config startup-config
！Save configuration of VLAN interface 1 which has been configured IP address
```

```
OLT#copy nm-interface-config startup-config 2
！Save configuration of user-defined VLAN interface 2
OLT#copy nm-interface-config startup-config 2 192.168.0.100 255.255.255.0 192.168.0.1
```

20.1.5 Execute saved configuration

User can restore saved configuration by commang line interface by using copy startup-config running-config command in privileged mode to execute saved configuration.

```
OLT#copy startup-config running-config
```

20.1.6 Display saved configuration

User can display syatem saved configuration information in the form of text by command line interface. Use following command to display system saved configuration：

show startup-config [module-list]

module-list: Optional module. If the module name is unoptioned, all information of configuration files will be displayed. If choose one or same of the modules, the specified information will be displayed. This command can be used in any configuration mode.

For example:

```
！Display all saved configuration
OLT#show running-config
！Display saved configuration of GARP and OAM module
OLT#show running-config garp oam
```

20.1.7 Display current configuration

User can display syatem current configuration information in the form of text by command line interface. Use following command to display system current configuration：

show running-config [module-list]

module-list: Optional module. If the module name is unoptioned, all information of configuration files will be displayed. If choose one or same of the modules, the specified information will be displayed.

For example:

```
！Display all configurations
OLT#show running-config
！Display configuration of GARP and OAM module
OLT#show running-config garp oam
```

20.1.8 Configure file executing mode shift

User can change executing mode of configuration file by command line interface. System saved configuration filescan be executed in stop and continue mode. When coming across errors, the executing will not stop; it will display errors and continue executing. It is defaulted to be non-stop mode. Use buildrun mode stop to configure executing mode to be stopped. Use buildrun mode continue command to configure buildrun mode to be continue. Use these commands in privileged mode.

For example:

！Configure buildrun mode to be stop.

OLT#buildrun mode stop

！Configure buildrun mode to be continune

OLT#buildrun mode continue

20.2. Online Loading Upgrade Program

System can upgrade application program and load configuration files on line by TFTP, FTP, Xmodem, and can upload configuration files, logging files, alarm information by TFTP and FTP.

20.2.1 Upload and download files by TFTP

Use following command to upload files by TFTP ：

upload { alarm | configuration | logging } tftp tftpserver-ip filename

Use following command to download files by TFTP ：

load {application | configuration | whole-bootrom } tftp tftpserver-ip filename

tftpserver-ip is the IP address of TFTP server. Filename is the file name to be loaded which cannot be system key words (such as con cannot be file name in windows operation system). Open TFTP server and set file upload path before use this command.

Suppose IP address of TFTP server is 192.168.0.100, file name is abc. Open TFTP server to configure upload and download path in privileged mode.

For example:

！Upload configuration to 192.168.0.100 by FTP and saved as abc

OLT#upload configuration ftp 192.168.0.100 abc username password

Configuration information saved when uploading is successful.

！Download configuration program abc to 192.168.0.100 by TFTP

OLT#load configuration ftp 192.168.0.100 abc

Reboot the switch after successful download and run new configuration program.

！Upload alarm to 192.168.0.100 by TFTP and saved as abc

OLT#upload alarm tftp 192.168.0.100 abc

！Upload logging to 192.168.0.100 by TFTP and saved as abc

```
OLT#upload logging tftp 192.168.0.100 abc
```

！Download application program app.arj to 192.168.0.100 by TFTP

```
OLT#load application tftp 192.168.0.100 app.arj
```

Reboot the switch after successful download and run new application program.

！Download whole-bootrom abc to 192.168.0.100 by TFTP

```
OLT#load whole-bootrom tftp 192.168.0.100 rom3x26.bin
```

20.2.2 Upload and download files by FTP

Use following command to upload files by FTP：

```
upload { alarm | configuration | logging } ftp ftpserver-ip filename username userpassword
```

Use following command to download files by FTP：

```
load { application | configuration | whole-bootrom} ftp ftpserver-ip filename username userpassword
```

ftpserver-ip is the IP address of FTP server. Filename is the file name to be loaded which cannot be system key words (such as con cannot be file name in windows operation system). Open FTP server and set username, password and file upload path before use this command.

Suppose IP address of TFTP server is 192.168.0.100, file name is abc. Open TFTP server to configure username to be user, password to be 1234 and file download path in privileged mode.

For example：

！Upload configuration to 192.168.0.100 by FTP and saved as abc

```
OLT#upload configuration ftp 192.168.0.100 abc user 1234
```

Configuration information saved when uploading is successful.

！Download configuration program abc to 192.168.0.100 by FTP

```
OLT#load configuration ftp 192.168.0.100 abc user 1234
```

Reboot the switch after successful download and run new configuration program.

！Download application program abc to 192.168.0.100 by FTP

```
OLT#load application ftp 192.168.0.100 abc user 1234
```

Reboot the switch after successful download and run new application program.

！Upload alarm to 192.168.0.100 by FTP and saved as abc

```
OLT#upload alarm ftp 192.168.0.100 abc user 1234
```

！Upload logging to 192.168.0.100 by FTP and saved as abc

```
OLT#upload logging ftp 192.168.0.100 abc user 1234
```

！Download whole-bootrom abc to 192.168.0.100 by FTP

OLT#load whole-bootrom ftp 192.168.0.100 abc user 1234

20.2.3 Download files by Xmodem

Use load application xmodem command to load application program by Xmodem protocol.

load application xmodem

Input following command in privileged mode：

OLT#load application xmodem

Choose “send” -> “send file” in super terminal, and input full path and filename of the file in filename dialog box, and choose Xmodem protocol in “protocol” , then click 【send】.

Reboot the switch after successful download and run new application program.

Use load configuration xmodem command to load configuration program by Xmodem protocol.

load configuration xmodem

Input following command in privileged mode：

OLT#load configuration xmodem

Choose “send” -> “send file” in super terminal, and input full path and filename of the file in filename dialog box, and choose Xmodem protocol in “protocol”, then click 【send】.

Reboot the switch after successful download and run new application program.

Use load whole-bootrom xmodem command to load whole bootrom by xmodem protocol.

load whole-bootrom xmodem

Input following command in privileged mode：

OLT#load whole-bootrom xmodem

Choose “send” -> “send file” in super terminal, and input full path and filename of the file in filename dialog box, and choose Xmodem protocol in “protocol”, then click 【send】.

Reboot the switch after successful download and run new BootRom program.

20.3. Facility management

20.3.1 MAC address table management

Brief introduction of MAC address table management

System maintains a MAC address table which is used to transfer packet. The item of this table contains MAC address, VLAN ID and interface number of packet entering. When a packet entering switch, switch will look up the MAC address tablke according to destination MAC and VLAN ID of the packet. If it is found out, send packet according to the specified interface in the item of MAC address table, or the packet will be broadcasted in this VLAN. In SVL learning mode, look up the table only according to MAC in packet and neglect VLAN ID.

System possesses MAC address learning. If the source MAC address of the received packet does not existed in MAC address table, system will add source MAC address, VLAN ID and port number of receiving this packet as a new item to MAC address table.

MAC address table can be manual configured. Administrator can configure MAC address table according to the real situation of the network. Added or modified item can be static, permanent, blackhole and dynamic.

System can provide MAC address aging. If a device does not receive any packet in a certain time, system will delete related MAC address table item. MAC address aging is effective on (dynamic) MAC address item which can be aging by learning or user configuration.

MAC address table management list

MAC address table management

- Configure system MAC address aging time
- Configure MAC address item
- Enable/disable MAC address learning
- Modify MAC address learning mode
- Configure system MAC address aging time
- Configure system MAC address aging time

Use mac-address-table age-time command in global configuration mode to configure MAC address aging time. Use no mac-address age-time command to restore it to default time.

```
mac-address-table age-time { agetime | disable }
```

```
no mac-address-table age-time
```

Agetime means MAC address aging time which ranges from 1 to 1048575 seconds. Default MAC address aging time is 300 seconds. Disable means MAC address not aging. Use no command to restore the default MAC address aging time.

For example:

！Configure MAC address aging time to be 3600 seconds

```
OLT(config)#mac-address-table age-time 3600
```

！Restore MAC address aging time to be 300 seconds

```
OLT(config)#no mac-address-table age-time
```

- Display MAC address aging time

```
show mac-address-table age-time
```

Use show mac-address-table age-time command to display MAC address aging time.

```
show mac-address-table age-time
```

For example:

！Display MAC address aging time.

```
OLT(config)#show mac-address-table aging-time
```

Configure MAC address item

- Add MAC address

mac-address-table { dynamic | permanent | static } mac interface interface-num VLAN VLAN-id

- Add MAC address

MAC address table can be added manually besides dynamically learning.

mac-address-table { dynamic | permanent | static } mac interface interface-num VLAN VLAN-id

Parameter mac, VLAN-id and interface-num corresponded to the three attributions of the new MAC address table item.

MAC address attribution can be configured to be dynamic, permanent and static. Dynamic MAC address can be aging; permanent MAC address will not be aging and this MAC address will exist after rebooting; static MAC address will not be aging, but it will be lost after rebooting.

For example:

！Add mac address 00:00:00:00:00:00 to be static address table.

OLT(config)#mac-address-table static 00:00:00:00:00:00 interface ethernet 0/1 VLAN 1

- Add black hole MAC address

System can configure MAC address table item to be black hole item. When the source address or destination address is black hole MAC address, it will be dropped.

mac-address-table black hole mac VLAN VLAN-id

For example:

！When tagged head of the packet is VLAN 1， forbid packet with its source address or destination address being 00:01:02:03:04:05 to go through system

OLT(config)#mac-address-table blackhole 00:01:02:03:04:05 VLAN 1

- Delete MAC address item

Use no mac-address-table command to remove mac address table.

no mac-address-table [blackhole | dynamic | permanent | static] mac VLAN VLAN-id

no mac-address-table [dynamic | permanent | static] mac interface interface-num VLAN VLAN- id

no mac-address-table [dynamic | permanent | static] interface interface-num

no mac-address-table [blackhole | dynamic | permanent | static] VLAN

VLAN-id no mac-address-table

VLAN means delete MAC address table item according to VLAN-id; mac means deleting a specified MAC address table item; interface-num means delete MAC address table item according to interface number; command no mac-address-table means delete all MAC address.

For example：

！Delete all MAC address table item

```
OLT(config)#no mac-address-table
```

- Display MAC address table

Use show mac-address command to display MAC address table.

```
show mac-address-table
show mac-address-table { interface-num [ VLAN VLAN-id ] |
cpu } show mac-address-table mac [ VLAN VLAN-id ]
show mac-address-table { blackhole | dynamic | permanent | static } [ VLAN VLAN-id ]
show mac-address-table { blackhole | dynamic | permanent | static } interface interface-num [ VLAN VLAN-id ]
show mac-address-table VLAN VLAN-id
```

The parameter meaning is the same as that of add/delete MAC address table item.

Enable/disable MAC address learning

This command is a batch command in global configuration mode to configure all interfaces to be the same; in interface configuration mode, it can configure interface MAC address learning. When MAC address learning is forbidden in an interface, packet with unknown destination address received from other interface will not be transmitted to this interface; and packet from this interface whose source address is not in this interface will not be transmitted. By default, all interface MAC address learning enable.

```
mac-address-table learning
no mac-address-table learning
```

For example:

！Enable MAC address learning on interface Ethernet 0/7.

```
OLT(config-if-ethernet-0/7)#no mac-address-table learning
```

- Display MAC address learning

```
show mac-address learning [ interface [ interface-num ] ]
```

Use show mac-address-table learning command to display MAC address learning.

Modify MAC address learning mode

System suppoets SVL and IVL learning modes. The default one is SVL. User can configure MAC learning mode in global configuration mode. It will be effective after rebooting.

```
mac-address-table learning mode { svl | ivl }
show mac-address-table learning mode
```

For example:

！Modify MAC address to be IVL OLT(config)#mac-

address-table learning mode ivl

！Display MAC address learning mode. OLT(config)#show

mac-address-table learning mode Configure the number of

port MAC address allowed learning

Use mac-address-table max-mac-count command to configure the number of port MAC address allowed learning. The maximum of MAC address allowed learning is 8191.

mac-address-table max-mac-count 5

no mac-address-table max-mac-count

For example:

！Configure the maximum of MAC address allowed learning of Ethernet 0/7 to be 5

OLT(config-if-ethernet-0/7)#mac-address-table max-mac-count 5

- Display the number of port MAC address allowed learning

show mac-address max-mac-count [interface [interface-num]]

Use show mac-address-table max-mac-count command to display the number of port MAC address allowed learning.

20.3.2 Reboot

Use reboot command in privileged mode to reboot switch:

OLT#reboot

20.4. System Maintenance

20.4.1 Use show command to check system information

show command can be divided into following categories:

- Command of displaying system configuration
- Command of displaying system opeation
- Command of displaying system statistics

Show command related to all protocols and interfaces refers to related chapters. Followings are system show commands.

Use following commands in any configuration mode：

show version	Display system version
show username	Display administrator can be logged in
show users	Display administrators logged in
show system	Display system information show
memory	Display memory
show clock	Display system clock
show cpu	Display cpu information

For example:

！Display system version

```
OLT# show version
```

Version number and date are different with different version.

20.4.2 Basic Configuration and Management

System basic configuration and management includes:

- Configure host name

Use hostname command in global configuration mode to configure system command line interface prompt. Use no hostname command to restore default host name.

Configure system command line interface prompt.

```
hostname hostname
```

hostname：character strings range from 1 to 32, these strings can be printable, excluding such wildcards as '/'、 ':'、 '*'、 '?'、 '\\'、 '<'、 '>'、 '|'、 '"'etc.

Use no hostname command in global configuration mode to restore default host name to be OLT.

For example:

！Configure hostname to be OLTXXXX18

```
OLT(config)#hostname
OLTXXXX18
 OLTXXXX18 (config)#
```

Configure system clock

Use clock set command in privileged mode to configure system clock.

configure system clock

```
clock set HH:MM:SS YYYY/MM/DD
```

For example:

！Configure system clock to be 2001/01/01 0:0:0

```
OL  clock set 0:0:0 2001/01/01
```

Configure clock timezone

Use clock timezone command in privileged mode to configure clock timezone.

configure clock timezone

```
clock timezone name hour minute
```

For example:

！Configure the clock time zone to be UTC 3 0

```
OLT(config)#clock time zone UTC 3 0
```

20.4.3 Network connecting test command

Use ping command in privileged mode or user mode to check the network connection.

```
ping [-c count] [-s packetsize] [-t timeout] host
```

Parameter:

-c count：The number of packet sending.

-s packetsize：The length of packet sending, with the unit of second

-t timeout：the time of waiting for replying after packet is sent，with the unit of second

For example:

```
！Ping 192.168.0.100
OLT#ping 192.168.0.100
PING 192.168.0.100: with 32 bytes of data:
reply from 192.168.0.100: bytes=32 time<10ms TTL=127
reply from 192.168.0.100: bytes=32 time<10ms TTL=127
reply from 192.168.0.100: bytes=32 time<10ms TTL=127
reply from 192.168.0.100: bytes=32 time<10ms TTL=127
reply from 192.168.0.100: bytes=32 time<10ms TTL=127
----192.168.0.100 PING Statistics----
5 packets transmitted, 5 packets received, 0% packet loss
round-trip (ms) min/avg/max = 0/0
```

20.4.4 Loopback test command

In global configuration mode, loopback command is used to test exterior of all interfaces; in interface configuration mode, loopback command is used to test whether the interface is normal, and it can be divided into interior and exterior. When exterior testing, exterior wire must be inserted (receiving and sending lines of RJ 45 connected directly). Use 4 different wires when the speed is less than 100M.

Using loopback command to do the loopback test, interface cannot transmit data packet correctly, and it will be automatically ended after a certain time. If shutdown command is executed, loopback test fails; when loopback test is executing, speed, duplex, mdi, vct and shutdown operations are forbidden. After exterior test, pull out the exterior wire to avoid abnormal communication.

Loopback on all interfaces:

```
loopback { internal | external }
```

Loopback on specified interface:

```
loopback { external | internal }
```

External means external loopback and internal means internal loopback

For example:

！Loopback on interface Ethernet 0/1

OLT(config-if-ethernet-0/1)#loopback external

！Loopback on all interfaces

OLT(config)#loopback internal

20.4.5 Administration IP address restriction

Managed ip address restriction can restrict host IP address or some network interface of switch by restricting web, telnet and snmp agent, but other IP address without configuration cannot manage switch. By default, three server possess an address interface of 0.0.0.0, so users of any IP address can manage switch. Different IP address and mask mean different information. The mask in reverse which is 0.0.0.0 means host address, or it means network interface. 255.255.255.255 means all hosts. When enabling a configuration, an item of 0.0.0.0 must be deleted. When receiving a packet, judge the IP address whether it is in the range of managed IP address. If it does not belong to it, drop the packet and shutdown telnet connection.

login-access-list { web | snmp | telnet } ip-address wildcard

Web means accessing IP address restriction of web server; snmp means accessing IP address restriction of snmp agent; telnet means accessing IP address restriction of telnet; ipaddress means IP address; wildcard means mask wildcard which is in the form of mask in reverse. 0 means mask this bit, and 1 meams does not mask this bit. When mask in reserve is 0.0.0.0, it means host address, and 255.255.255.255 means all hosts. Use the no command to delete corresponding item.

For example:

！Configure ip address allowed by telnet management system to be 192.168.0.0/255.255.0.0

OLT(config)#login-access-list telnet 192.168.0.0 0.0.255.255

OLT(config)#no login-access-list telnet 0.0.0.0 255.255.255.255

Use show login-access-list command to display all ip address allowed by web, snmp, telnet management system.

show login-access-list

20.4.6 The number of Telnet user restriction

Configure the max number of Telnet users. This function can restrict the number of Telnet user (0-5) to enter privileged mode at the same time. The user logged in without entering privileged mode will not be restricted but restricts by the max number. Administrator and super user will not be restricted and can be logged in through series interface. Display the configuration by show users command.

Configure it in global configuration mode:

login-access-list telnet-limit limit-no

no login-access-list telnet-limit

Example：

！Configure only 2 Telnet users can enter privileged mode

```
OLT(config)#login-access-list telnet-limit 2
```

20.4.7 Routing tracert command

Tracert is used for routing detecting and network examination. Configure it in privileged mode：

```
tracert [ -u | -c ] [ -p udpport | -f first_ttl | -h maximum_hops | -w time_out ] target_name
```

Parameter：

-u means sending udp packet，-c means sending echo packet of icmp. It is defaulted to be -c；

udpport：destination interface address for sending udp packet which is in the range of 1 to 65535 and defaulted to be 62929；

first_ttl：initial ttl of sending packet which is in the range of 1 to 255 and defaulted to be 1；

maximum_hops：the max ttl of sending packet which is in the range of 1 to 255 and defaulted to be 30；

time_out：the overtime of waiting for the response which is in the range of 10 to 60 with the unit of second and default to be 10 seconds；

target_name：destination host or router address

Example：

！Tracert 192.168.1.2

```
OLT#tracert 192.168.1.2
```

20.5. Monitor system by SNMP

20.5.1 Brief introduction of SNMP

SNMP（Simple Network Management Protocol）is an important network management protocol in TCP/IP network. It realizes network management by exchanging information packets. SNMP protocol provides possibility of concentrated management to large sized network. Its aim is guaranteeing packet transmission between any two points to be convenient for network administrator to search information, modify and search fault, finish fault diagnosising, capacity planning and creation reporting at any network node. It consists of NMS and Agent. NMS(Network Management Station)，is the working station of client program running，and Agent is server software running in network devices. NMS can send GetRequest, GetNextRequest and SetRequest packet to Agent. After receiving requirement packet of NMS, Agent will Read or Write management variable according to packet type and create

Response packet, and return it to NMS. On the other hand, the Trap packet of abnormity of cold boot or hot boot of devices will send to NMS.

System supports SNMP version of v1, v2c and v3. v1 provides simple authentication mechanism which does not support the communication between administrator to administrator and v1 Trap does not possess authentication mechanism. V2c strengthens management model (security), manages information structure, protocol operation, the communications between managers, and it can create and delete table, and strengthen communication capacity of managers, and reduce the storage operation of agency. V3 realizes user distinguishing mechanism and packet encryption mechanism, and greatly improves security of SNMP protocol.

20.5.2 Configuration

SNMP configuration command list:

SNMP configuration command list includes:

- Configure community
- Configure sysContact
- Configure Trap destination host adress
- Configure sysLocation
- Configure sysName
- Configure notify
- Configure engine id
- Configure view
- Configure group
- Configure user

Configure community

SNMP adopts community authentication. The SNMP packets which are not matching the authenticated community name will be dropped. SNMP community name is a character string. Different community can possess the accessing right of read-only or read-write. Community with the riht of read-only can only query system information, but the one with the right of read-write can configure system. System can configure at most 8 community names. It is defaulted to configure without community name. Configure it in global configuratiob mode.

- Configure community name and accessing right. This command can also used to modify community attribution with character string community-name being the same.

snmp-server community community-name { ro | rw } { deny | permit } [view view-name]

community-name is a printable character string of 1 to 20 characters；ro、rw means read only or can be read and write；permit、deny means community can or cannot be activated; View-name is view configured for community，The default configuration view is iso.

- Delete community name and accessing right

no snmp-server community community-name

community-name is existed community name.

For example:

！Add community nic，and configure privilege to be rw，and permit

```
OLT(config)#snmp-server community nic rw permit
```

！Remove community nic

```
OLT(config)#no snmp-server community nic
```

- Display community name in any mode

```
show snmp community
```

For example:

！Display SNMP community information

```
OLT(config)#show snmp community
```

Configure sysContact

sysContact is a managing variable in system group in MIB II , the content of which is the contact way of the administrator. Configure it in global configuration mode:

```
snmp-server contact syscontact
no snmp-server contact
```

syscontact：Contact way to administrator ranges from 1 to 255 printable characters. Use the no command to restore default way of contacting to administrator.

For example:

！Configure administrator contact way to be support@OLT.br。

```
OLT(config)#snmp-server contact support@OLT.br
```

⚠Caution: Use quotation mark to quote space in charater string.

Use show snmp contact command in any configuration mode to display how to contact to administrator：

```
show snmp contact
```

For example:

！Display how to contact with administrator

```
OLT(config)#show snmp contact
manager contact information : support@OLT.br
```

Configure Trap destination host adress

Use this configuration to configure or delete IP address of destination host. Configure it in global configuration mode.

- Configure notify destination host address snmp-server host host-addr [version {1 | 2c | 3 [auth | noauth | priv]}] community-string [udp-port port] [notify-type [notifytype-list]]

- Delete notify destination host address

no snmp-server host ip-address community-string { 1 | 2c | 3 }

ip-address and snmp-server means IP address in SNMP server notify sending list. community-string means the security name IP corresponded in snmp-server notify table item. Security name is the community name for snmpvi and snmp v2c, and username for snmpv3. 1, 2c, 3 mean SNMP versions. Port means the port number sent to. Notifytype-list means optional notify list. If it is unoptioned, default to choose all type. Only optionaed type will be sent to destination host.

For example:

！Configure SNMP server, the IP address is configured to be 192.168.0.100，and SNMP version to be 2c，and community name to be user

OLT(config)#snmp-server host 192.168.0.100 version 2c user

！Delete the item with the notify destination host being 192.168.0.100 and community name being user

OLT(config)#no snmp-server host 192.168.0.100 user

- Display snmp-server notify item in any configuration mode:：

show snmp host

！Display Trap information of snmp

OLT(config)#show snmp host

Configure sysLocation

sysLocation is a managing variable in system group of MIB which is used to denote location of devices be managed. Configure it in global configuration mode:

snmp-server location syslocation

Syslocation is the charater string of system location ranges from 1 to 255 printable characters.

For example:

！Configure system location to be sample sysLocation factory。

OLT(config)#snmp-server location “sample sysLocation factory”

Use quotation mark to quote space in charater string.

Use show snmp location command in any configuration mode to display system location：

show snmp location

Configure sysName

sysName is a managing variable in system group of MIB II which is switch name. Configure it in global configuiration mode:

```
snmp-server name sysname
no snmp-server name
```

Sysname means the charater string of system name ranges from 1 to 255 printable characters.

For example:

！Configure system name to be OLT S2926V

```
OLT(config)#snmp-server name "OLT S2926V"
```

⚠ Caution: Use quotation mark to quote space in charater string.

Configure notify

Enable/disable sending all kinds of notify types by configuring notify sending. The defaulted notify sending is trap. After disabling notify sending, trap will not be sent. Notify sending is defaulted to disable. Configure it in global configuration mode:

```
snmp-server enable traps [ notificationtype-list ]
no snmp-server enable traps [ notificationtype-list ]
```

notificationtype-list：Notificationtype list defined by system. To enable or disable specified notification type by choose one or serval type. If the keyword is vacant, all types of notification are enabled or disabled.

Notify types are as following: bridge：

Enable/disable STP interfaces：

interface LinkUp/LinkDown

snmp：accessing control; cold boot/heat boot of system

gbnsavecfg：save configuration

rmon：RMON trap

gbn：self-define Trap, such as GN-Link Trap，interface Blocking，CAR， loopback detect

For example:

！Enable notificationtype gbn

```
OLT(config)# snmp-server enable traps gbn
```

Configure engine id

This configuration is used to configure local engine-id or recognizable remote engine-id.

Default local engine id is 1346400000000000000000000 which cannot be deleted but modified. It is defaulted to have no recognizable remote engine-id which can be added and deleted. Once delete a recognizable remote engine the corresponded user can also be deleted. At most 32 engines can be configured. Use no snmp-server engineID command to restore default local engine-id or remove remote engine-id. Configure it in global configuration mode:

snmp-server engineID { local engineid-string | remote ip-address [udp-port port-number] engineid-string }

no snmp-server engineID { local | remote ip-address [udp-port port-number] }

Display current engine configuration in any configuration mode:

show snmp engineID [local | remote]

engineid-string is an engine id that can only be recognized in a network. This system only supports printable characters of engine id which excludes space.

Ip-address is remote engine ip address. Local ip address is not allowed to input.

Port-number is remote engine port number. Default port number is 162

For example:

！Configure local engine id to be 12345

OLT(config)# snmp-server engineid local 12345

！Configure remote engine that can be recognized locally. Configure remote engine ip to be 1.1.1.1，and port number to be 888，and id to be 1234

OLT(config)# snmp-server engineid remote 1.1.1.1 udp-port 888 1234

！Display local engine configuration

OLT(config)# show snmp engineid local

Configure view

Use snmp-server view command to configure view and its subtree. Iso、internet and sysview are the default views. At most 64 views can be configured. View Internet must not delete and modify. Configure it in global configuration mode:

snmp-server view view-name oid-tree { included | excluded }

no snmp-server view view-name [oid-tree]

View-name means the name of the view to be added. It ranges from 1 to 32，excluding space.

Oid-tree means the subtree of the view which corresponds to such a mib node as "1.3.6.1"；The substring of OID must be the integer between 0 and 2147483647.

The sum of the number of characters in view name string and the number of oid nodes should not be more than 64.

When configuring view subtree to be exclude, the node in this subtree cannot be accesed which does not mean the node excluded this subtree can be accessed. When configuring notify destination host, if the security name is the community, sending notify is not effected on view; if the user with the security name being SNMPv3, sending notify is controlled by notify view of this user. What this notify view controlled is the accessing of the node that variable belongs to and it is not influence accessing attribution of trap OID that notify belonged to. If notify does not contain binded variable, sending notify is not effected on view.

For example:

```
！Add view “view1”，and configure it to have a subtree “1.3.6.1”
OLT(config)# snmp-server view view1 1.3.6.1 include
！Add a subtree “1.3.6.2” for existed view “view1”
OLT(config)# snmp-server view view1 1.3.6.2 include
！Remove existed view “view1”
OLT(config)# no snmp-server view view1
！Display configured view
OLT(config)# show snmp view
```

Configure group

Use this configuration to configure a accessing conreol group. Folowing groups are default to exist: (1) security model is v3，the security level is differentiated group initial ; (2) security model is v3，the security level is differentiated encrypt group initial. At most 64 groups can be configured. Configure it in global configuiration mode:

```
snmp-server group groupname { 1 | 2c | 3 [auth | noauth | priv] [context context-name]} [read readview]
[ wrete writeview] [notify notifyview]
no snmp-server group groupname {1 | 2c | 3 [auth | noauth | priv] [context context-name]}
```

Display configured group in any configuration mode:

```
show snmp group
```

groupname means group name, which ranges from 1 to 32 characters，excluding space.

Readview is a view name, which means the right to read in the view. If the keyword is vacant, it is default not to include readable view.

Writeview is a view name, which means the right to read and write in the view. If the keyword is vacant, it is default not to include readable and writable view.

Notifyview is a view name, which means the right to send notification in the view. If the keyword is vacant, it is default not to include notify sending view.

Context-name is facility context. If the keyword is vacant, it is default to be local facility.

For example:

```
！Add group “group1” to local facility，using security model 1, and configure read, write, and notify view to be internet
OLT(config)# snmp-server group group1 1 read internet write internet notify Internet
！Remove group “group1” from local facility
OLT(config)# no snmp-server group group1 1
！Display current group configuration.
OLT(config)# show snmp group
```

Configure user

Use this configuration to configure user for local engine and recognizable remote engine. Following users are default to exist: (1)initialmd5（required md5 authentication）, (2) initialsha（required sha authentication）, (3) initialnone（non- authentication）. The above three users are reserved for system not for user. The engine the user belonged to must be recognizable. When deleting recognizable engine, contained users are all deleted. At most 64 users can be configured. Configure it in global configuration mode:

snmp-server user username groupname [remote host [udp-port port]] [auth { md5 | sha } { authpassword { encrypt-authpassword authpassword | authpassword } | authkey { encrypt-authkey authkey | authkey } } [priv des { privpassword { encrypt-privpassword privpassword | privpassword } | privkey { encrypt-privkey privkey | privkey } }]

no snmp-server user username [remote host [udp-port port]]

Display configured user in any configuration mode:

show snmp user

Username is the username to be configured. It ranges from 1 to 32 characters，excluding space.

Groupname is the groupname that user going to be added. It ranges from 1 to 32 characters，excluding space.

Host is remote engine ip address. If it is vacant, it is default to be local engine.

Port is the port number of remote engine. If it is vacant, it is default to be 162.

Authpassword is authentication password. Unencrypted password ranges from 1 to 32 characters. To avoid disclosing, this password should be encrypted. To configured encrypted password needs client-side which supports encryption to encrypt password, and use encrypted cryptograph to do the configuration. Cryptograph is different by different encryption. Input cryptograph in the form of hexadecimal system, such as “a20102b32123c45508f91232a4d47a5c”

Privpassword is encryption password. Unencrypted password ranges from 1 to 32 characters. To avoid disclosing, this password should be encrypted. To configured encrypted password needs client-side which supports encryption to encrypt password, and use encrypted cryptograph to do the configuration. Cryptograph is different by different encryption. Input cryptograph in the form of hexadecimal system, such as “a20102b32123c45508f91232a4d47a5c”

Authkey is authentication key. Unauthenticated key is in the range of 16 byte (using md5 key folding) or 20 byte (using SHA-1 key folding). Authenticated key is in the range of 16 byte (using md5 key folding) or 24 byte (using SHA-1 key folding).

Privkey is encrpted key. Unencypted key ranes from 16 byte, and encrypted key ranes from 16 byte.

Keyword encrypt-authpassword、encrypt-authkey、encrypt-privpassword、encrypt-privkey are only used in command line created by compile to prevent leaking plain text password and key. When deconfiguring SNMP, user cannot use above keywords.

For example：

！Add user “user1” for local engine to group “grp1”，and configure this user not to use authentication and encryption.

```
OLT(config)# snmp-server user user1 grp1
```

！Add user “user2” for local engine to group “grp2”，and configure this user to use md5 authentication and non-encryption with the auth-password to be 1234

```
OLT(config)# snmp-server user user2 grp2 auth md5 auth-password 1234
```

！Add user “user3” for local engine to group “grp3”，and configure this user to use md5 authentication and des encryption with the auth-password to be 1234 and privpassword to be 4321

```
OLT(config)# snmp-server user user3 grp3 auth md5 auth-password 1234 priv des priv-password 4321
```

20.6. Enable/disable broadcast suppression

Use broadcast-suppression command to configure the broadcast flow allowed by switch. When broadcast flow is beyond the limit, it will be dropped to guarantee network to reduce broadcast flow to a resonable range. Use no broadcast-suppression command to disable broadcast storm suppression to configure the broadcast flow allowed by switch to be the maximum of 200000 per second, which means no suppression on broadcat. The default broadcast flow allowed by switch is at most 5000 per second.

Use following command in global configuration mode：

```
broadcast-suppression packet-number
no broadcast-suppression
```

For example:

！Allow at most 300 packets per second.

```
OLT(config)#broadcast-suppression 300
```

！Non broadcast suppression

```
OLT(config)#no broadcast-suppression
```

20.7. Enable/disable dlf forword packet

Use dlf-forward command to enable dlf forword.

```
dlf-forward { multicast | unicast }
no dlf-forward { multicast | unicast }
```

Use dlf-forward command in global configuration mode or interface configuration mode to enable dlf forword. Use no dlf-forward command to disable dlf forward：

dlf-forward { multicast | unicast }

no dlf-forward { multicast | unicast }

For example:

！Disable dlf forward for unicast

OLT(config)#no dlf-forward unicast

！Disable dlf forward for multicast

OLT(config)#no dlf-forward multicast

20.8. Enable/disable dropping BPDU packet

Use this command to control enable/disable dropping specified typed BPDU packet.

Configure it in global configuration mode:

discard-bpdu

no discard-bpdu

Example：

！Disable dropping bpdu packet

OLT(config)#no discard-bpdu

！Enable dropping bpdu packet

OLT(config)#discard-bpdu

20.9. Telnet client

Logging in switch by control terminal, enable Telnet client in switch to log in other switch or Telnet server of other standard.

Enable Telnet client in privileged mode:

telnet ip-addr [port-num] [/localecho]

ip-addr is IP address of Telnet server. port-num is Telnet server port which is defaulted to be 23. /localecho means enable local echo options. It is defaulted to disable. Generally, Telnet client will not echo but Telnet server will echo.

Display Telnet client running information in any configuration mode.

show telnet client

Using user name “admin” in following command to force running Telnet client to stop in privileged mode.

stop telnet client { all | term-id }

All means stop all Telnet client. term-id means the terminal number of Telnet client which is in the range of 0-5，0 means console ，1-5 means Telnet terminal 1-5.

20.10. CPU Alarm Configuration

20.10.1 Brief introduction of CPU alarm configuration

System can monitor CPU usage. If CPU usage rate is beyond cpu busy threshold, cpu busy alarm is sent because the cpu is busy. In this status, if cpu is below cpu unbusy threshold, cpu unbusy alarm is sent. This function can report current CPU usage to user.

20.10.2 CPU alarm configuration list

CPU alarm configuration command includes：

- Enable/disable CPU alarm
- Configure CPU busy or unbusy threshold
- Display CPU alarm information

20.10.3 Enable/disable CPU alarm

Configure it in global configuration mode：

- Enable CPU alarm

alarm cpu

- Disable CPU alarm

no alarm cpu

by default, CPU alarm enables.

For example:

！Enable CPU alarm

OLT(config)#alarm cpu

20.10.4 Configure CPU busy or unbusy threshold

Use alarm cpu threshold command in global configuration mode to configure CPU busy or unbusy threshold.：

- Configure CPU busy or unbusy threshold

alarm cpu threshold [busy busy] [unbusy unbusy]

busy > unbusy. Default CPU busy threshold is 90%，and CPU unbusy threshold is 60%.

For example:

！Configure CPU busy threshold to be 30%，and CPU unbusy threshold to be 10%

OLT(config)#alarm cpu threshold busy 30 unbusy 10

20.10.5 Display CPU alarm information

- Use show alarm cpu command in any mode to display cpu alarm information：

show alarm cpu

For example:

！Display CPU alarm information

```
OLT(config)#show alarm cpu
```

20.11. Mail Alarm Configuration

Mail alarm configuration includes:

- Configure enable/disable mailalarm
- Configure mailalarm server
- Configure mailalarm receiver
- Configure mailalarm ccaddr
- Configure enable/disable mailalarm smtp authentication
- Configure mailalarm logging level

Configure enable/disable mailalarm

Configure enable/disable mailalarm in global configuration mode:

- mailalarm
- no mailalarm

Example：

！Configure enable mailalarm：

OLT(config)#mailalarm Configure

mailalarm server

Configure it in global configuration mode:

- mailalarm server server-addr
- no mailalarm server

Example：

！Configure smtp server address to be 10.11.0.252：

```
OLT(config)#mailalarm server 10.11.0.252
```

Configure mailalarm receiver

Configure it in global configuration mode:

- mailalarm receiver receiver-addr
- no mailalarm receiver

Example：

！Configure email of mail receiver to be ：system@switch.net

```
OLT(config)#mailalarm receiver system@switch.net
```

Configure mailalarm ccaddr

Configure it in global configuration mode:

- mailalarm ccaddr cc-addr
- no mailalarm ccaddr cc-addr

At most 4 carbon copy addresses can be configured.

Example:

！Configure mail address of carbon copy receiver to be system2@switch.net

```
OLT#mailalarm ccaddr system2@switch.net
```

Configure enable/disable mailalarm smtp authentication

Configure it in global configuration mode:

- mailalarm smtp authentication username username { passwd passwd | encrypt-passwd encrypt-passwd }
- no mailalarm smtp authentication

Keyword encrypt-passwd can only be used in the command generated by decompilation.

Example:

！Enable smtp authentication with the username to be system，and password to be 123

```
OLT#mailalarm smtp authentication username system passwd 123
```

Configure mailalarm logging level

Configure it in global configuration mode:

- mailalarm logging level level
- no mailalarm logging level

When the level of syslog information is lower than the configured value, the syslog information will be encapsulated to the mail and sent to the specified mail box.

Example:

！Configure the syslog level of sending mail alarm to be 4

```
OLT#mailalarm logging level 4
```

20.12. Anti-DOS Attack

20.12.1 IP segment anti-attack

The IP segment packet number which can be received by system do not occupy resources of all receiving packets, which can normally handle other non-segment packets when receiving IP segment attack and the range of IP segment receiving number can be configured. 0 means system will not handle IP segment packet so that system can avoid the influence on segment attack.

- Configure it in global configuration mode

```
anti-dos ip fragment maxnum
```

- Display related information

```
show anti-dos
```

20.12.2 Enable/disable global TTL

System can enable or disable receiving the packet with TTL=0.

- Configure it in global configuration mode

```
anti-dos ip ttl
```

- Display corresponded information

```
show anti-dos
```

21. LLDP CONFIGURATION

21.1. Brief introduction of LLDP protocol

LLDP（Link Layer Discovery Protocol）is the new protocol defined by IEEE 802.1AB. It realizes proclaiming information about itself to other neighbor devices through network and receives the bulletin information from neighbor devices and stores it to standard MIB of LLDP. It is convenient for user to check the device model and linked interfaces of downlink neighbor devices and maintains central office and manage network. Network administrator can know the link of network layer 2 by accessing MIB.

21.2. LLDP configuration

21.2.1 LLDP configuration list

The configuration can be effective only after LLDP enables. Configure related parameter of devices or Ethernet interface before enabling LLDP and these configurations will be saved after disabling LLDP. And the parameter will be effective after re-enabling LLDP. LLDP configuration list is as following:

- Enable/disable global LLDP
- Configure LLDP hello-time
- Configure LLDP hold-time
- Interface LLDP packet receiving/sending mode configuration
- Display LLDP information

21.2.2 Enable/disable global LLDP

Use following command in global configuration mode：

- Enable global LLDP

lldp

- Disable global LLDP

no lldp

By default, global LLDP disables.

For example：

！Enable global LLDP

OLT(config)#lldp

21.2.3 Configure LLDP hello-time

Use following command in global configuration mode：

- Configure LLDP hello-time

lldp hello-time <5-32768>

- Restore default LLDP hello-time

no lldp hello-time

The default LLDP hello-time is 30 seconds

For example：

！Configure LLDP hello-time to be 10

OLT(config)#lldp hello-time 10

21.2.4 Configure LLDP hold-time

Use following command in global configuration mode:

- Configure LLDP hold-time

lldp hold-time <2-10>

- Restore default LLDP hold-time

no lldp hold-time

The default LLDP hold-time is 4

For example：

！Configure LLDP hold-time to be 2

OLT(config)#lldp hold-time 2

21.2.5 Interface LLDP packet receiving/sending mode configuration

Use following command in interface configuration mode:

- Configure interface LLDP packet receiving/sending mode

lldp { rx | tx | rxtx }

Parameter：

rx：only receive LLDP packet tx：
only send LLDP packet rxtx：
receiving/sending LLDP packet

- Disable interface LLDP packet receiving/sending

no lldp

By default, interface LLDP packet receiving/sending mode is rxtx

For example:

！Configure e 0/1 only to send LLDP packet

OLT(config-if-ethernet-0/1)#lldp tx

21.2.6 Display LLDP information

Display followings in any configuration mode: Enable/disable

global LLDP Related parameter of

global LLDP

Interface packet receiving/sending mode

Interface packet receiving/sending statistics

Neighbor devices information found

show lldp interface [<interface-list>]

For example：

！Display LLDP information of interface Ethernet 0/1

OLT(config)#show lldp interface ethernet 0/1