CLI Configuration Guide

(GEL-2871, GEL-5271)

Contents

1. **System Management** 9

   1.1. **Command Line Interface Mode** 9

   1.2. **Management IP Address** 9

      1.2.1. **Configuring** 9

      1.2.2. **Examples** 10

   1.3. **Backup/Restore Configuration** 10

   1.4. **System Warm Restart** 10

   1.5. **User Login Management** 11

   1.6. **System Hostname Configuration** 12

   1.7. **Firmware Upgrade** 12

   1.8. **System Data And Time Configuration** 13

2. **Configuring Ethernet Interface** 15

   2.1. **Overview of Interface Types** 15

   2.2. **Configuring** 15

   2.3. **Examples** 17

   2.4. **Display Information** 17

3. **Configuring Storm Control** 20

   3.1. **Overview of Storm Control** 20

   3.2. **Configuring** 20

   3.3. **Examples** 20

3.4. Display information 20

4. Configuring SPAN 21

4.1. Overview of SPAN 21

4.2. Configuring 21

4.3. Examples 22

4.4. Display information 22

5. Configuring Port Aggregation 23

5.1. Overview of Port Aggregation 23

5.2. Overview of LACP 23

5.3. Configuring 24

5.4. Examples 25

5.5. Display information 25

6. Configuring VLAN 29

6.1. Overview of VLAN 29

6.2. Configuring 29

6.3. Display Information 31

7. Configuring QINQ 33

7.1. Overview of QINQ 33

7.1.1. VLAN Stacking 33

7.1.2. VLAN Mapping 33

7.2. Configuring 34

7.3. Examples 36

7.4. Display Information 39
7.5. Configuring ERPS 40
7.6. Overview of ERPS 40
7.7. Introduction to ERPS Rationale 40
7.8. Configuring 42
7.9. Examples 44
7.10. Display Information 49
8. Configuring IGMP Snooping 50
8.1. Overview of IGMP Snooping 50
8.2. Configuring 50
8.3. Examples 51
8.4. Display Information 52
9. Configuring Spanning Tree Protocol 54
9.1. Overview of Spanning Tree Protocol 54
9.2. Configuring 54
9.3. Examples 59
9.4. Display Information 62
10. Configuring MAC Address 63
10.1. Overview of MAC Address 63
10.2. Configuring 63
10.3. Examples 64
10.4. Display Information 64

11. Configuring LLDP 66
1.1. Overview of LLDP 66
1.2. Configuring 69
1.2.1. Configuring Switch and Operating Mode 69
1.2.2. Configuring Optional Basic Parameter 69
1.2.3. Configuring Optional State Machine Parameter 71
1.2.4. Configuring Send Tlv List 72
1.3. Examples 73
1.3.1. LLDP Basic Function Configuration Example 73
1.4. Display Information 73
12. Configuring L3 75
12.1. Overview of L3 75
12.2. Configuring 77
12.3. Examples 80
12.4. Display Information 81
13. Configuring ACL 83
13.1. Overview of ACL 83
13.2. Configuring 83
13.3. Examples 85
13.4. Display Information 85
14. Configuring QoS 87
14.1. Overview of QoS 87
14.2. Configuring 88

14.3. Examples 93
14.4. Display Information 94
15. Configuring DHCP Snooping 97
15.1. Overview of DHCP Snooping 97
15.2. Configuring 97
15.3. Examples 99
15.4. Display Information 99
16. Configuring 802.1X Authentication 101
16.1. Overview of 802.1X Authentication 101
16.1.1. 802.1X Architecture 101
16.1.2. 802.1X Authentication Method 101
16.1.3. 802.1X Basic Concepts 102
16.1.4. Authentication process for 802.1X 103
16.2. Configuring 105
16.3. Examples 108
16.3.1. 802.1X Port Authentication Scenario 108
16.3.2. MAC Authentication Scenario 109
16.4. Display Information 110
17. Configuring Port Security 111
17.1. Overview of Port Security 111
17.2. Configuring 111
17.3. Examples 112

17.4. Display Information 113

18. Configuring Ip Source Guard 115

18.1. Overview of Ip Source Guard 115

18.2. Configuring 115

18.3. Examples 115

18.4. Display Information 116

19. Configuring Arp-check 117

19.1. Overview of Arp-check 117

19.2. Configuring 117

19.3. Examples 117

20. Configuring SNMP Network Management 118

20.1. Overview of SNMP Network Management 118

20.2. Configuring 118

20.3. Examples 119

21. Configuring RMON 120

21.1. Overview of RMON 120

21.2. Rationale 121

21.3. Configuring 122

21.4. Examples 124

21.5. Display Information 124

22. Configuring AAA 126

22.1. Overview of AAA 126

22.2. Configuring 126

22.3. Examples 128

22.3.1. **SSH Login Authentication Using Tacacs+ Method** 128

22.3.2. **Use the None Method to Perform Serial Port Login** 129

22.4. Display Information 130

23. Configuring Serial Device Server 131

23.1. Overview of Serial Device Server 131

23.2. Configuring 131

23.3. Examples 133

23.3.1. **Example for Tcp-client** 133

23.3.2. **Example for Tcp-server** 134

23.4. Display Information 134

24. Fault Diagnosis 136

24.1. Ping/tracerout 136

24.2. Display Port Optical Module DDM Information 136

1. System Management

1.1. Command Line Interface Mode

The command line interface is divided into many different modes, The commands available to you depend on which mode you are currently in. Enter a question mark (?) at the system prompt to obtain a list of commands available for each command mode. Table following describes the main command modes, how to access each one, the prompt you see in that mode, and how to exit the mode. The examples in the table use the hostname SWITCH.

Table Command Mode Summary

Mode	Prompt	Enter Or Exit	About This Mode
User Exec	SWITCH>	Enter exit to quit	Use this mode to: Perform basic tests. Display system information.
Privileged Mode	SWITCH#	While in user EXEC mode, enter the enable command. Enter disable to exit.	Use this mode to: Exec network utilities. Display module information. System management operation.
Global Configuration	SWITCH(config)#	While in Privileged mode, enter the configuration terminal command. Enter exit or end to return.	Use this mode to: configure parameters that apply to the entire switch.
Interface Configuration	SWITCH(config-if)#	While in global configuration mode, e interface command (with a specific interface). Enter exit or end to return.	Use this mode to: configure parameters for the Ethernet ports.

1.2. Management IP Address

1.2.1. Configuring

- **Manually Assigning IPv4 Information**

Command	SWITCH(config)#management vlan VLANID ip address IPADDR/MASKLEN gateway IPADDR SWITCH(config)#no management vlan
Description	Manually assigning switch management IPv4 information.

- **Configuring DHCP-Based IPv4 Information Autoconfiguration**

Command	SWITCH(config)#management vlan VLANID ip address dhcp SWITCH(config)#no management vlan
Description	Configuring DHCP-Based IPv4 information autoconfiguration.

- **Manually Assigning IPv6 Information**

Command	SWITCH(config)#management vlan VLANID ipv6 address IPV6ADDR/MASKLEN gateway IPV6ADDR SWITCH(config)#no management vlan
Description	Manually assigning switch management IPv6 information.

- **Configuring DHCP-Based IPv6 Information Autoconfiguration**

Command	**SWITCH(config)#management vlan VLANID ipv6 address dhcp** **SWITCH(config)#no management vlan**
Description	**Configuring DHCP-Based IPv6 information autoconfiguration.**

- **Display IP Information**

Command	**SWITCH#show management summary**
Description	**Display IP information.**

1.2.2. Examples

Example 1: Manually assigning IPv4 information.

The following examples shows how to configure management IPv4 address, The management VLAN is 1, the management IP is 192.168.64.200/24, and the gateway address is 192.168.64.1.

Manually assigning IPv4 information:

```
SWITCH#configure terminal
SWITCH(config)#management vlan 1 ip address 192.168.64.200/24 gateway 192.168.64.1
```

Display IP information:

```
SWITCH#show management summary
Management interface with Ipv4:
Type:          Static
Vlan:          1
Ip address:    192.168.64.200/24
Gateway:       192.168.64.1
```

1.3. Backup/Restore Configuration

- **Backup Configuration**

Command	**SWITCH#write**
Description	**Save your entries in the configuration file.**

- **Restore Configuration**

Command	**SWITCH#copy default-config startup-config** **SWITCH#reload**
Description	**Restore the system default configuration, which will take effect after the device restarts.**

1.4. System Warm Restart

- **System Warm Restart**

Command	**SWITCH#reload**
Description	**System warm restart.**

1.5. User Login Management

- **Configuring Username and Password**

Command	**SWITCH(config)# username NAME password LINE** **SWITCH(config)# no username NAME**
Description	**If the user name does not exist, add a new user, if it exists, modify the user's password.** **By default, the device has its own user "admin" and password "admin", which supports password modification and deletion operations.** **The device supports up to 8 users, and the length of the user and password is 0-32 bytes.** **Password display is encrypted.** **Password characters are case sensitive.** **The delete operation does not support deleting the user itself; to delete an online user, the user must be kicked off the line first.**

- **Kick Online Users**

Command	**SWITCH# clear line {vty | console} LINE**
Description	**Vty means remote login user.** **Console indicates the serial port login user.** **LINE information can be viewed in the show users command information.** **Does not support kicking the user itself.**

- **Enable WEB Server**

Command	**SWITCH(config)# web-server enable {all | http | https}** **SWITCH(config)# no web-server enable**
Description	**Enable WEB server.** **Disabled by default.** **Support IPv6.**

- **Enable Telnet Server**

Command	**SWITCH(config)# telnet-server enable** **SWITCH(config)# no telnet-server enable**
Description	**Enable Telnet Server.** **Disabled by default.** **Support IPv6.**

- **Enable SSH Server**

Command	**SWITCH(config)# ssh-server enable** **SWITCH(config)# no ssh-server enable**
Description	**Enable SSH Server.** **Disabled by default.** **Support IPv6.**

1.6. System Hostname Configuration

- **Configuring Hostname**

Command	**SWITCH(config)# hostname WORD**
Description	**The name must consist of printable characters and the length cannot exceed 63 bytes.** **This configuration takes effect immediately.**

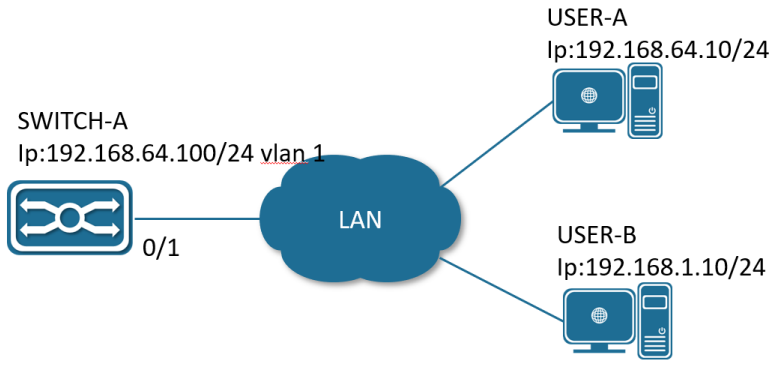
1.7. Firmware Upgrade

- **Firmware Upgrade**

Command	**SWITCH# upgrade tftp tftp://SERVER/FILENAME**
Description	**You need to build a TFTP server on the terminal, and ensure the two-way interconnection between the terminal and the device network.** **SERVER: TFTP server IP and the relative address of the server window and the firmware upgrade file.** **FILENAME: Firmware upgrade file.** **The firmware upgrade process will take 5-6 minutes, reboot the device to complete the firmware upgrade.** **Do not power off the device during the upgrade process.**

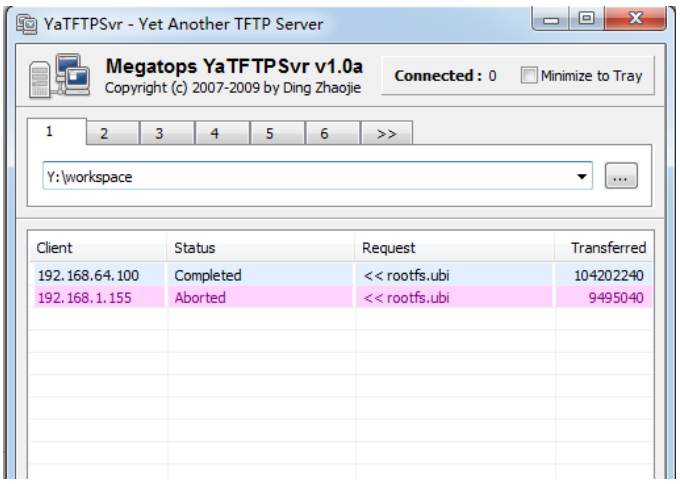
Example 1: The following examples shows firmware upgrade via tftp.

Step 1: As shown in the figure below, SWITCH-A is the device to be upgraded, and the telnet function is enabled; USER-A is the host on the same network segment in the LAN, and USER-B is the management device in the LAN, both of which can log in to SWITCH-A by telnet.



Firmware upgrade connection diagram

Step 2: Select USER-B to perform the version upgrade operation. Open the TFTP server on USER-B and place the upgrade file xcat-release-3.2.0.bin in the Y:/workspace directory.TFTP server as shown in the figure below.



TFTP Server

Step 3: USER-B telnet logs in to SWITCH-A and executes the upgrade command in privileged mode. Upgrade information as shown in the figure below.

```
SWITCH#upgrade tftp tftp://192.168.1.10/xcat-release-3.2.0.bin
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
100 55.5M    0 55.5M    0     0  1016k      0 --:--:--  0:00:55 --:--:-- 1033k
100 55.5M    0 55.5M    0     0  1016k      0 --:--:--  0:00:55 --:--:-- 1016k
Un-packet install file, this will last about 60 seconds.
Check upgrade file success.
Start erase and write bin to flash, this will last about 120 seconds.
Erasing 128 Kibyte @ 680000 --  2 % complete flash_erase: Skipping bad block at 006a0000
Erasing 128 Kibyte @ 12a0000 --  7 % complete flash_erase: Skipping bad block at 012c0000
Erasing 128 Kibyte @ 3580000 -- 21 % complete flash_erase: Skipping bad block at 035a0000
Erasing 128 Kibyte @ f5e0000 -- 100 % complete
Bad block at 6a0000, 1 block(s) from 6a0000 will be skipped
Bad block at 12c0000, 1 block(s) from 12c0000 will be skipped
Bad block at 35a0000, 1 block(s) from 35a0000 will be skipped
Reboot system to finish upgrade? (y/n):
```

Upgrade Information

Step 4: After the upgrade is over, select "y" to restart the device to complete the upgrade, select "n" to continue running the device, and the upgrade operation will be completed after restart.

1.8. System Data And Time Configuration

- **Setting the Systm Clock**

Command	**SWITCH# clock set HH:MM:SS DAY MON YEAR**
Description	**Setting the system clock.** **For example: Clock set 15:30:00 1 october 2017.**

- **Setting Ntp Server**

Command	**SWITCH(config)# ntp server A.B.C.D**
Description	**Configure the IP address of the NTP server (domain name configuration is not supported).** **After the configuration is complete, if the device and the server are connected to the network, the device will automatically synchronize the time information from the server.** **It takes about 4-8 minutes to complete the time synchronization for the first time.**

- **Setting Timezone**

Command	**SWITCH(config)# clock timezone ZONE**

Description	**Configure the system time zone.** **The default timezone is UTC.** **Supports standard time zone configuration, such as Shanghai time zone keyword "Shanghai", Hong Kong time zone keyword "Hong_Kong", etc.**

- **Display System Clock**

Command	**SWITCH# show clock**
Description	**Display system clock.**

- **Display Ntp Status**

Command	**SWITCH# show ntp status**
Description	**Display ntp status.**

2. Configuring Ethernet Interface

2.1. Overview of Interface Types

The interfaces of switch can be divided into the following two categories: Layer 2 interfaces and Layer 3 interfaces.

L2 interface，Including common physical ports (Switch Port) and aggregate ports (Port Channel).

Switch Port consists of a single physical port on the device and only support Layer 2 switching. The port can be an Access Port, Hybrid Port or a Trunk Port.

Port Channel is formed by the aggregation of multiple physical member ports. We can bundle multiple physical links together to form a simple logical link, which we call an aggregate port. For Layer 2 switching, the aggregation port can superimpose the bandwidth of multiple ports to expand the link bandwidth.

L3 interface，Here mainly refers to the SVI port.

SVI is a switching virtual interface, a logical interface used to implement Layer 3 switching. SVI can be used as the local management interface, through which the administrator can manage the device. You can create an SVI with the interface vlan interface configuration command, and then assign an IP address to the SVI to establish routing between VLANs.

2.2. Configuring

- **Interface Range Mode**

Command	**SWITCH(config)# interface IFNAME_RANGE**
Description	**Specify the range of interfaces to be configured, and enter interface-range configuration mode.** **When there are multiple range combinations, separate them with ',' without spaces.** **For example, the command interface range gigabitEthernet 0/1-4, gigabitEthernet 0/9-12 is a valid range.** **You can use the interface range command to configure up to five port ranges;** **Each interface-range must consist of the same port type.**

- **Adding a Description for an Interface**

Command	**SWITCH(config-if)# description DESC**
Description	**Add a description (up to 80 characters) for an interface.**

- **Shutdown the Interface**

Command	**SWITCH(config-if)# shutdown** **SWITCH(config-if)# no shutdown**
Description	**Shut down an interface.**

- **Configuring Interface Speed**

Command	**SWITCH(config-if)# speed {10 | 100 | 1000 | auto}** **SWITCH(config-if)# no speed**
Description	**Enter auto to enable the interface to autonegotiate speed with the connected device.** **If you use the 10, 100, or the 1000 keywords with the auto keyword, the port autonegotiates only at the specified speeds;**

- **Configuring Interface Duplex Mode**

Command	**SWITCH(config-if)# duplex {auto | full | half}** **SWITCH(config-if)# no duplex**
Description	**Enable half-duplex mode (for interfaces operating only at 10 or 100 Mbps). You cannot configure half-duplex mode for interfaces operating at 1000 Mbps**

Attention:

- **When both speed and duplex exit auto mode, port auto-negotiation is disabled.**

- **Configuring Interface Flowcontrol**

Flow control enables connected Ethernet ports to control traffic rates during congestion by allowing congested nodes to pause link operation at the other end. If one port experiences congestion and cannot receive any more traffic, it notifies the other port by sending a pause frame to stop sending until the condition clears. Upon receipt of a pause frame, the sending device stops sending any data packets, which prevents any loss of data packets during the congestion period.

Command	**SWITCH(config-if)# flowcontrol {on | off }**
Description	**Configure the flow control mode for the port.** **on: The port cannot send pause frames but can operate with an attached device that is required to or can send pause frames; the port can receive pause frames.** **off: Flow control does not operate in either direction. In case of congestion, no indication is given to the link partner, and no pause frames are sent or received by either device.**

- **Configuring Interface MTU**

When a port performs high-throughput data exchange, it may encounter a frame larger than the Ethernet standard frame length, which is called a jumbo frame.

The user can control the maximum frame length that the port is allowed to send and receive by setting the MTU of the port. Frames received or forwarded by the port, if the length exceeds the set MTU, will be discarded.

Due to chip limitations, the MTU value only supports even numbers. If the user configures an odd number, the device will auto-align to even. For example, if the MTU is configured as 127, it actually works as 128.

Command	**SWITCH(config-if)# mtu LENGTH** **SWITCH(config-if)# no mtu**
Description	**Change the MTU size for the interface on the switch. The range is 64 to 10240 bytes; the default is 1526 bytes.**

- **Configuring SFP Interface Mode**

Command	**SWITCH(config-if)# port mode {sgmii | 2500BASE-X | 1000BASE-X | 10G}** **SWITCH(config-if)# no port mode**
Description	**1000BASE-X:The port operate at 1000Mbps, full-duplex only.** **Sgmii: Enables connection to external copper transceivers.** **2500BASE-X: The port operate at 2.5G, full-duplex only.** **10G: The port operate at 2.5G, full-duplex only.**

- **Configuring Interface Isolate**

In some situations, you need to prevent Layer 2 (L2) connectivity between end devices on a switch, you can use the isolate

function.

When some ports are set as isolated ports, the isolated ports cannot communicate with each other, the isolated port and the non-isolated port can communicate normally, and the non-isolated port and the non-isolated port can communicate normally.

Command	**SWITCH(config-if)#switchport isolate** **SWITCH(config-if)# no switchport isolate**
Description	**Setting the port as an isolated port.**

2.3. Examples

- **Enter gigabitEthernet0/1 Interface Configuration Mode:**

```
SWITCH#
SWITCH#configure terminal
Enter configuration commands, one per line.   End with CNTL/Z.
SWITCH(config)#interface gigabitEthernet0/1
SWITCH(config-if)#
```

- **Configure the Port Description Information as "TEST_A"**

```
SWITCH(config-if)#description TEST_A
```

- **No Shutdown Port**

```
SWITCH(config-if)#no shutdown
```

- **Setting the Port Speed 100M, Duplex Full, and Flowcontrol On**

```
SWITCH(config-if)#speed 100
SWITCH(config-if)#duplex full
SWITCH(config-if)#flowcontrol on
```

- **Setting the Port MTU value 1024**

```
SWITCH(config-if)#mtu 1024
```

2.4. Display Information

- **Display Brief Information of All Ports**

```
SWITCH#show interface brief

--------------------------------------------------------------------------------
Ethernet    Type  Status  Reason  Speed  Duplex  Flowcontrol  Autoneg  Port
Interface                                                          Ch #
--------------------------------------------------------------------------------
GiE0/1      ETH   down    none    --     --      --           --       --
GiE0/2      ETH   up      none    1000M  FULL    OFF          ON       --
GiE0/3      ETH   down    none    --     --      --           --       --
GiE0/4      ETH   down    none    --     --      --           --       --
GiE0/5      ETH   down    none    --     --      --           --       --
GiE0/6      ETH   down    none    --     --      --           --       --
GiE0/7      ETH   down    none    --     --      --           --       --
GiE0/8      ETH   up      none    100M   FULL    OFF          ON       --
```

```
GiE0/9      ETH    down     none     --      --      --          --      --
GiE0/10     ETH    down     none     --      --      --          --      --
GiE0/11     ETH    down     none     --      --      --          --      --
GiE0/12     ETH    down     none     --      --      --          --      --
```

- Display Single Port Configuration and Status

```
SWITCH#show interface gigabitethernet0/1
Interface gigabitethernet0/1
  Hardware is eth  current hw addr: 0050.4c82.89a0
  Physical:0050.4c82.89a0
  Description: test_a
  Index 1 metric 0 mtu 1024 speed-unknown duplex-unknown flowcontrol-unknown
  Port mode is invalid
  <up>
    vrf binding: not bound
  Bandwidth -8
  Input packets 0677, bytes 072690,
  Multicast packets 0327 broadcast packets 0350 fcs error 00 undersizeerrors 00 oversizeerrors 00
  Output packets 00, bytes 00,
  Multicast packets 00 broadcast packets 00
```

- Display Port Packet Statistics

```
SWITCH#show interface gigabitEthernet0/1 counters
Interface gigabitEthernet16/1
Good Octets Tx            : 1914949
Good Octets Rx            : 0
Bad Octets Rx             : 0
Mac Tx Err Pkts           : 0
Good Packets Tx           : 1913
Good Packets Rx           : 0
Bad Packets Rx            : 0
Broadcast Packet Tx       : 24
Broadcast Packets Rx      : 0
Multicast Packet Tx       : 55
Multicast Packets Rx      : 0
pkts_64_octets            : 285
pkts_65_127_octets        : 263
pkts_128_255_octets       : 42
pkts_256_511_octets       : 36
pkts_512_1023_octets      : 91
pkts_1024_max_octets      : 1196
Excessive Collisions      : 0
```

```
UnRecg MAC Cntl Pkts Rx : 0
Flow Ctrl Pkts Sent       : 0
Flow Ctrl Pkts Recvd      : 0
Drop Events               : 0
Undersized Pkts Recvd     : 0
Fragments Recvd           : 0
Oversized Pkts Recvd      : 0
Jabber Pkts Recvd         : 0
mac_rcv_error             : 0
Bad CRC                   : 0
Collisions                : 0
Late Collisions           : 0
Bad Flow Ctrl Recv        : 0
```

- **Display Port Isolation Configuration**

```
SWITCH#show switchport isolate
interface        config
GiE0/1             isolated
GiE0/2             normal
GiE0/3             normal
GiE0/4             normal
GiE0/5             normal
GiE0/6             normal
GiE0/7             normal
GiE0/8             normal
GiE0/9             normal
GiE0/10            normal
```

3. Configuring Storm Control

3.1. Overview of Storm Control

Storm control prevents traffic on a LAN from being disrupted by a broadcast, multicast, or unicast storm on one of the physical interfaces. A LAN storm occurs when packets flood the LAN, creating excessive traffic and degrading network performance. Errors in the protocol-stack implementation, mistakes in network configurations, or users issuing a denial-of-service attack can cause a storm.。

Storm control uses bandwidth as a percentage of the total available bandwidth of the port that can be used by the broadcast, multicast, or unicast traffic, to measure traffic activity.

because of hardware limitations and the way in which packets of different sizes are counted, threshold percentages are approximations.

3.2. Configuring

- **Configuring Storm Control**

命令	**SWITCH(config-if)#storm-control {broadcast | multicast | unicast | all | unicast-broadcast | multicast-broadcast} level LINE** **SWITCH(config-if)#no storm-control**
描述	**Configure broadcast, multicast, or unicast storm control. By default, storm control is disabled.** **If you set the threshold to the maximum value (100 percent), no limit is placed on the traffic. If you set the threshold to 0.0, traffic on that port is blocked.** **The range is 0.00 to 100.00.** **Support adaptive port rate change.** **Unicast only containing unknown unicast packets.**

3.3. Examples

3.4. Display information

- **Display All Port Storm Control Configurations**

SWITCH#show storm-control

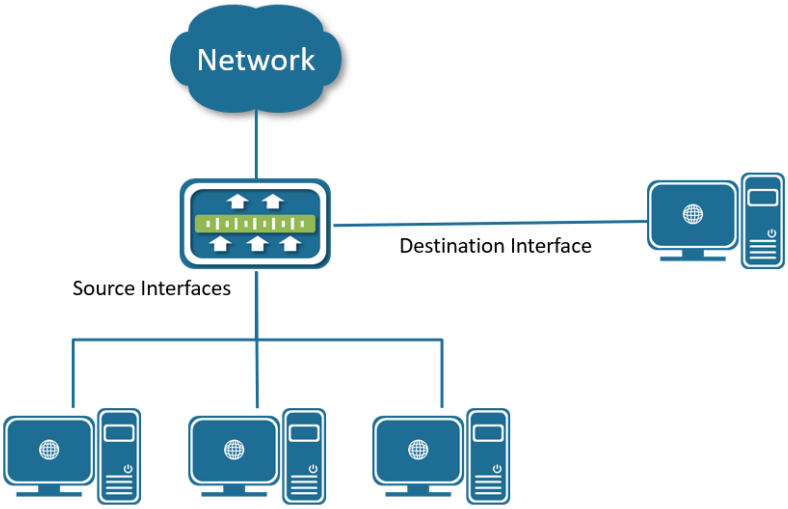
Port	BcastLevel	McastLevel	Unicastlevel
GiE0/1	100.00%	10.00%	100.00%
GiE0/2	100.00%	100.00%	100.00%
GiE0/3	100.00%	100.00%	100.00%
GiE0/4	100.00%	100.00%	100.00%
GiE0/5	100.00%	100.00%	100.00%
GiE0/6	100.00%	100.00%	100.00%
GiE0/7	100.00%	100.00%	100.00%
GiE0/8	100.00%	100.00%	100.00%
GiE0/9	100.00%	100.00%	100.00%
GiE0/10	100.00%	100.00%	100.00%
GiE0/11	100.00%	100.00%	100.00%
GiE0/12	100.00%	100.00%	100.00%

4. Configuring SPAN

4.1. Overview of SPAN

You can analyze network traffic passing through ports by using SPAN (Local Switched Port Analyzer) to send a copy of the traffic to another port on the switch that has been connected to a network analyzer or other monitoring or security device. SPAN copies traffic received or sent (or both) on source ports to a destination port for analysis.

SPAN does not affect the switching of network traffic on the source ports. You must dedicate the destination port for SPAN use. Except for traffic that is required for the SPAN session, destination ports do not receive or forward traffic.



Example of SPAN configuration

SPAN supports a session entirely within one switch. all source ports and destination ports are in the same switch.

SPAN sessions allow you to monitor traffic on one or more ports, and send the monitored traffic to only one destination port.

A SPAN session is an association of a destination port with source ports, all on a single network device.

4.2. Configuring

- **Creating a Session**

Command	**SWITCH(config)#monitor session SESSION-ID** **SWITCH(config)#no monitor session SESSION-ID**
Description	**Create a SPAN session.** **For session_number, the range is 1 to 7**

- **Configuring Session Description**

Command	**SWITCH(config-monitor)#description DESC**
Description	**Add a description (up to 64 characters) for an interface**

- **Configuring Source interface**

Command	**SWITCH(config-monitor)#source interface IFNAME {both | rx | tx}** **SWITCH(config-monitor)#no source interface IFNAME {both | rx | tx}**

Description	**Specify the SPAN session and the source port.**

- **Configuring Destination Interface**

Command	**SWITCH(config-monitor)#destination interface IFNAME** **SWITCH(config-monitor)#no destination interface IFNAME**
Description	**Specify the SPAN session and the destination port.**

4.3. Examples

Example 1: This example shows how to create SPAN session, and configure session source interfaces and destination interface.

Step 1: Create session.

```
SWITCH#configure terminal
Enter configuration commands, one per line.   End with CNTL/Z.
SWITCH(config)#monitor session 1
SWITCH(config-monitor)#
```

Step 2: Configuring session description.

```
SWITCH(config-monitor)#description TRAFFIC_MONITOR
```

Step 3: Configuring session source interfaces.

```
SWITCH(config-monitor)#source interface gigabitEthernet0/1 rx
SWITCH(config-monitor)#source interface gigabitEthernet0/2 both
```

Step 4: Configuring session destination interface.

```
SWITCH(config-monitor)#destination interface gigabitEthernet0/8
```

4.4. Display information

- **Display Single Session**

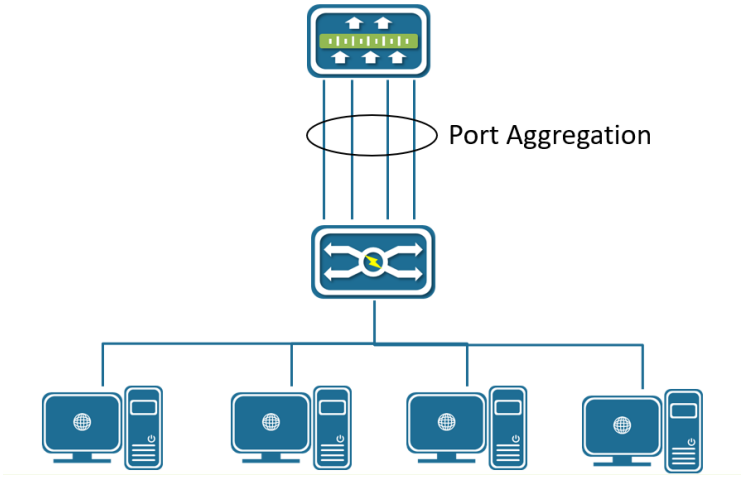
```
SWITCH#show   monitor session 1
session 1
---------------
description          : TRAFFIC_MONITOR
type                 : local
source intf          :
    tx               : gigabitEthernet0/2
    rx               : gigabitEthernet0/1   gigabitEthernet0/2
    both             : gigabitEthernet0/2
source VLANs         :
    rx               :
destination ports : gigabitEthernet0/8
Legend: f = forwarding enabled, l = learning enabled
```

5. Configuring Port Aggregation

5.1. Overview of Port Aggregation

Port aggregation provides fault-tolerant high-speed links between switches, routers, and servers. You can use it to increase the bandwidth between the wiring closets and the data center, and you can deploy it anywhere in the network where bottlenecks are likely to occur. Port aggregation provides automatic recovery for the loss of a link by redistributing the load across the remaining links. If a link fails, port aggregation redirects traffic from the failed link to the remaining links in the channel without intervention.

Port aggregation consists of individual Fast Ethernet or Gigabit Ethernet links bundled into a single logical link called channel, as shown in Figure below.



Typical Port Aggregation application

Each Channel can consist of up to eight compatibly configured Ethernet ports. All ports in each Channel must be configured as Layer 2 ports. The number of Channels is limited to 12.

You can configure an Channel in one of these modes: Manual(Static), Active(LACP), or Passive(LACP).

5.2. Overview of LACP

LACP (Link Aggregation Control Protocol) based on the IEEE802.3ad standard is a dynamic link aggregation protocol. If a port enables the LACP, the port will send LACPDU message to announce its system priority, system MAC, port priority, port number and operation key, etc. After the connected device receives the LACP message from the peer end, it compares the system priorities of the two ends according to the system ID in the message. On the side with the higher system ID priority, the ports in the aggregation group are set to be in the aggregation state according to the order of port ID priority from high to low, and the updated LACP message is sent out. It will also set the corresponding port to the aggregation state, so that the two sides can reach the same agreement when the port exits or joins the aggregation group.

After the LACP member interface link is bound, periodic LACP packet exchange will be carried out. When no LACP packet is received for a period of time, it is considered that the packet reception timed out, the member interface link is unbound, and the port is in a state of non-forwarding again. There are two modes of timeout here: long timeout mode and short timeout mode. In the long timeout mode, the port sends a packet every 30 seconds. If it does not receive a packet from the peer for 90 seconds, it will be in a packet receiving timeout.; In the short timeout mode, the port sends a packet every 1 second. If it does not receive a packet from the peer for 3 seconds, it is in the packet receiving timeout.

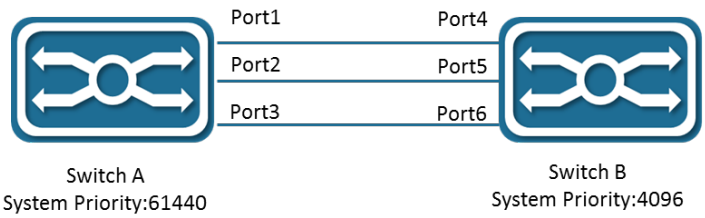


Figure Typical LACP application

As shown Figure, switch A and switch B are connected together through 3 ports. We set the system priority of switch A to 61440, and set the system priority of switch B to 4096. Enable LACP link aggregation on the three directly connected ports of switches A and B.

After receiving the LACP message from the peer, switch B finds that its system ID has a higher priority (switch B has a higher system priority than switch A), so it follows the order of port ID priority (in the case of the same port priority) , in the order of port numbers from small to large) set ports 4, 5, and 6 to be in the aggregation state.

After switch A receives the updated LACP packet from switch B, it finds that the system ID of the peer end has a higher priority, and set the ports 1, 2, and 3 to the aggregation state.

5.3. Configuring

- **Configuring Layer 2 Channels**

Command	**SWITCH(config-if)#channel-group ID mode manual** **SWITCH(config-if)#channel-group ID mode {active | passive}** **SWITCH(config-if)#no channel-group**
Description	**Assign the port to a channel group, and specify the mode.** **For ID, the range is 1 to 12.**

Note

✦ When the first port is added to the aggregation port, a PO port is actively created, and the default attribute of the PO port is the first port attribute.

✦ For Layer 2 Channels:

Ports with different native VLANs cannot form an EtherChannel.

- **Configuring LACP System Priority**

Command	**SWITCH(config)#lacp system-priority SYSTEM-PRIORITY** **SWITCH(config)#no lacp system-priority**
Description	**The system priority range is 1 to 65535, the default value is 32768.** **All dynamic link groups of a device can only have one LACP system priority. Modifying this value will affect all aggregation groups on the switch.**

- **Configuring LACP Interface Priority**

Command	**SWITCH(config-if)#lacp port-priority PORT-PRIORITY** **SWITCH(config-if)#no lacp port-priority**

Description	**The interface priority range is 1 to 65535, the default value is 32768.**

- **Configuring LACP Timeout Mode**

Command	**SWITCH(config-if)#lacp timeout {long | short}** **SWITCH(config-if)#no lacp timeout**
Description	**In long mode, the interval for sending LACP protocol packets is 30S, and the timeout is 90S.** **In short mode, the interval for sending LACP protocol packets is 1S, and the timeout is 3S.** **Default is in long mode.**

- **Configuring Load-balance Method**

Command	**SWITCH(config)#port-channel load-balance {dst-ip | dst-mac | dst-port | src-dst-ip | src-dst-mac | src-dst-port | src-ip | src-mac | src-port}** **SWITCH(config)#no port-channel load-balance**
Description	**Configure an Channel load-balancing method.** **The default is src-mac.** **Select one of these load-distribution methods: •** **dst-ip: Load distribution is based on the destination IP address.** **dst-mac: Load distribution is based on the destination MAC address of the incoming packet.** **Dist-port: Load distribution is based on the destination L4-port of the incoming packet** **src-dst-ip: Load distribution is based on the source-and-destination IP address.** **src-dst-mac: Load distribution is based on the source-and-destination MAC address.** **src-dst-port: Load distribution is based on the source-and-destination L4-port of the incoming packet.** **src-ip: Load distribution is based on the source IP address.** **src-mac: Load distribution is based on the source-MAC address of the incoming packet.**

5.4. Examples

Example 1: This example shows how to assign the ports to a channel, and set load-balance method.

- **Assign the gigabitEthernet0/5, gigabitEthernet0/6 to PO 1, set load-balance to src-ip:**

```
SWITCH(config)#interface gigabitEthernet0/5
SWITCH(config-if)#channel-group 1 mode manual
SWITCH(config-if)#exit
SWITCH(config)#interface gigabitEthernet0/6
SWITCH(config-if)#channel-group 1 mode manual
SWITCH(config-if)#exit
SWITCH(config)#port-channel load-balance src-ip
```

5.5. Display information

- **Display Channels Configuration and Status**

```
SWITCH#show port-channel
Load balance: Source and Destination Mac address
```

```
Interface po3
  Type: static
  Member:
    gigabitEthernet0/18       link down       Disable

Interface po8
  Type: LACP
  Member:
    gigabitEthernet0/19       link up         Enable
    gigabitEthernet0/17       link up         Enable

SWITCH#show port-channel 8
Interface po8
  Type: LACP
  Member:
    gigabitEthernet0/19       link up         Enable
    gigabitEthernet0/17       link up         Enable

SWITCH#show port-channel load-balance
Source and Destination Mac address
```

- **Display LACP Summary**

```
SWITCH#show lacp summary
% Aggregator po8 1008
% Aggregator Type: Layer2
% Admin Key: 0008 - Oper Key 0008
%    Link: gigabitEthernet0/17 (17) sync: 1 status: Bundled
%    Link: gigabitEthernet0/19 (19) sync: 1 status: Bundled

SWITCH#show lacp detail
% Aggregator po8 1008
% Aggregator Type: Layer2
%   Mac address: 74:b9:eb:ee:25:46
%   Admin Key: 0008 - Oper Key 0008
%   Actor LAG ID- 0x8000,74-b9-eb-ee-25-46,0x0008
%   Receive link count: 2 - Transmit link count: 2
%   Individual: 0 - Ready: 1
%   Partner LAG ID- 0x8000,00-01-a0-00-10-10,0x0032
%    Link: gigabitEthernet0/17 (17) sync: 1 status: Bundled
%    Link: gigabitEthernet0/19 (19) sync: 1 status: Bundled

SWITCH#show lacp 8
% Aggregator po8 1008 Admin Key: 0008 - Oper Key 0008
% Partner LAG ID: 0x8000,00-01-a0-00-10-10,0x0032
% Partner Oper Key 0050
```

```
SWITCH#show lacp sys-id
% System 8000,74-b9-eb-ee-25-46

SWITCH#show lacp port gigabitEthernet0/19
% LACP link info: gigabitEthernet0/19 - 19
% LAG ID: 0x8000,74-b9-eb-ee-25-46,0x0008
% Partner oper LAG ID: 0x8000,00-01-a0-00-10-10,0x0032
% Actor Port priority: 0x8000 (32768)
% Admin key: 0x0008 (8) Oper key: 0x0008 (8)
% Physical admin key:(1)
% Receive machine state : Current
% Periodic Transmission machine state : Slow periodic
% Mux machine state : Collecting/Distributing
% Oper state: ACT:1 TIM:0 AGG:1 SYN:1 COL:1 DIS:1 DEF:0 EXP:0
% Partner oper state: ACT:1 TIM:0 AGG:1 SYN:1 COL:1 DIS:1 DEF:0 EXP:0
% Partner link info: admin port 0
% Partner oper port: 20
% Partner admin LAG ID: 0x0000-00:00:00:00:0000
% Admin state: ACT:1 TIM:0 AGG:1 SYN:0 COL:0 DIS:0 DEF:1 EXP:0
% Partner admin state: ACT:0 TIM:0 AGG:1 SYN:0 COL:0 DIS:0 DEF:1 EXP:0
% Partner system priority - admin:0x0000 - oper:0x8000
% Partner port priority - admin:0x0000 - oper:0x8000
% Aggregator ID: 1008
```

- **Display Only One Channel Information**

```
SWITCH#show int po8
Interface po8
  Hardware is AGG   Current HW addr: 74b9.ebee.2546
  Logical:(not set)
  Port Mode is access
  interface configure:
    medium-fiber mtu 1526 speed-auto duplex-auto flowcontrol-off autonego-off
  interface status:
    link-up bandwidth-2g
  Aggregate Members:(LACP)
    gigabitEthernet0/19      link up         Enable
    gigabitEthernet0/17      link up         Enable
  input packets:
    Good Octets Rx           : 18986
    Good Packets Rx          : 104
    Broadcast Packets Rx     : 0
    Multicast Packets Rx     : 104
  ouput packets:
    Good Octets Tx           : 38529
```

```
    Good Packets Tx             : 359
    Broadcast Packet Tx         : 4
    Multicast Packet Tx         : 355
  un-normal packets:
    Drop Events                 : 0
    Undersized Pkts Recvd       : 0
    Oversized Pkts Recvd        : 0
Bad CRC                         : 0
```

6. Configuring VLAN

6.1. Overview of VLAN

A VLAN is a switched network that is logically segmented by function, project team, or application, without regard to the physical locations of the users. VLANs have the same attributes as physical LANs, but you can group end stations even if they are not physically located on the same LAN segment. Any switch port can belong to a VLAN, and unicast, broadcast, and multicast packets are forwarded and flooded only to end stations in the VLAN. Each VLAN is considered a logical network, and packets destined for stations that do not belong to the VLAN must be forwarded through a router or a switch supporting fallback bridging.

The port link types of Ethernet switches can be divided into three types: Access, Trunk, and Hybrid. These three ports will be processed differently when they join VLAN and forward packets.

Access: An access port can belong to one VLAN and is manually assigned to that VLAN.

Trunk: A trunk port is a member of all VLANs by default, but membership can be limited by configuring the allowed-VLAN list.A trunk port have a native vlan, the switch forwards untagged traffic in the native VLAN configured for the port. The native VLAN is VLAN 1 by default.

Hybrid: A hybrid port is a member of all VLANs by default, but membership can be limited by configuring the allowed-VLAN list.A hybrid port allow users to configure traffic of a vlan forwards tagged or untagged. A trunk port have a hybrid vlan, The hybrid VLAN is VLAN 1 by default.

6.2. Configuring

- **Creating VLAN**

Command	**SWITCH(config)#vlan (<vlan-id> | <vlan-range>)** **SWITCH(config)#no vlan (<vlan-id> | <vlan-range>)**
Description	**Create a VLAN, vlan-id 1-4094, vlan-range example: 2-10.**

- **Configuring the Interface as a Access Port**

Command	**SWITCH(config)#interface IFNAME** **SWITCH(config-if)#switchport mode access**
Description	**Configure the interface port mode access.**

Command	**SWITCH(config-if)#switchport access vlan VLANID** **SWITCH(config-if)#no switchport access vlan**
Description	**Specify the default VLAN of the interface, which is used if the interface is access mode.** **Default vlan is 1.**

- **Configuring the Interface as a Trunk Port**

Command	**SWITCH(config)#interface IFNAME** **SWITCH(config-if)#switchport mode trunk**

Description	**Configure the interface port mode trunk.**

Command	**SWITCH(config-if)#switchport trunk allowed vlan { all | VLAN_LIST | none}** **SWITCH(config-if)#no switchport trunk allowed vlan VLAN_LIST**
Description	**Configure the list of VLANs allowed on the trunk, which is used if the interface is trunk mode.** **All: Adds all VLANs in available in the VLAN table,New VLANs added to the VLAN table are added automatically.** **None: Removes all VLANs.** **VLAN_LIST: It will manually set the Allowed VLAN list, If it belongs to ALL , the Allowed VLAN list will be cleared first, and then the new VLAN list will be added;vlan-list parameter is either a single VLAN number from 1 to 4094 or a range of VLANs described by two VLAN numbers, the lower one first, separated by a hyphen. Do not enter any spaces between comma-separated VLAN parameters or in hyphen-specified ranges. Only created VLANs can be added to the Allowed VLAN list; when a VLAN is deleted, the corresponding VLAN in the Allowed VLAN list will be automatically deleted.** **All VLANs are allowed by default.**

Command	**SWITCH(config-if)#switchport trunk native vlan VLANID** **SWITCH(config-if)#no switchport trunk native vlan**
Description	**Configure the VLAN that is sending and receiving untagged traffic on the trunk port. For VLANID, the range is 1 to 4094.** **Native VLAN has nothing to do with whether the Allowed VLAN contains this VLAN, or even whether the VLAN is created.** **Default vlan is 1.**

Note:

✦ The default VLAN ID of the trunk port of the local device must be the same as the default VLAN ID of the trunk port of the connected device, otherwise the packets of the default VLAN will not be transmitted correctly.

- **Configure the Interface as a Hybrid Port**

Command	**SWITCH(config)#interface IFNAME** **SWITCH(config-if)#switchport mode hybrid**
Description	**Configure the interface port mode hybrid.**

Command	**SWITCH(config-if)#switchport hybrid allowed vlan { all | VLAN_LIST | none}** **SWITCH(config-if)#no switchport hybrid allowed vlan VLAN_LIST**
Description	**Configure the list of VLANs allowed on the trunk, which is used if the interface is hybrid mode.** **All: Adds all VLANs in available in the VLAN table,New VLANs added to the VLAN table are added automatically.**

	None: Removes all VLANs. VLAN_LIST: It will manually set the Allowed VLAN list, If it belongs to ALL , the Allowed VLAN list will be cleared first, and then the new VLAN list will be added;vlan-list parameter is either a single VLAN number from 1 to 4094 or a range of VLANs described by two VLAN numbers, the lower one first, separated by a hyphen. Do not enter any spaces between comma-separated VLAN parameters or in hyphen-specified ranges. Only created VLANs can be added to the Allowed VLAN list; when a VLAN is deleted, the corresponding VLAN in the Allowed VLAN list will be automatically deleted. All VLANs are allowed by default.

Command	SWITCH(config-if)#switchport hybrid vlan VLANID SWITCH(config-if)#no switchport hybrid vlan
Description	Configure the default VLAN that is sending and receiving untagged traffic on the hybrid port. For VLANID, the range is 1 to 4094. Native VLAN has nothing to do with whether the Allowed VLAN contains this VLAN, or even whether the VLAN is created. Default vlan is 1.

Command	SWITCH(config-if)#switchport hybrid untagged vlan VLAN_LIST SWITCH(config-if)#no switchport hybrid untagged vlan VLAN_LIST
Description	Configure the list of untagged VLANs, which is used if the interface is hybrid mode. The default VLAN must be untagged output, therefore, it is not maintained by the untagged VLAN list. By default the untagged VLAN list is empty. The Untagged VLAN list must be in the Allowed VLAN list of the Hybird port, Therefore, when a VLAN is deleted from the Allowed VLAN, it will also be deleted from the Untagged VLAN list. Since the untagged VLAN list does not maintain the default VLAN, if a VLAN in the previous list is set as the default VLAN, it will be deleted from the untagged VLAN list.

Note

✦ The default VLAN ID of the hybrid port of the local device must be the same as the default VLAN ID of the hybrid port of the connected device, otherwise the packets of the default VLAN will not be transmitted correctly.

6.3. Display Information

Displays the VLAN table, includes VLAN VID, VLAN status, VLAN member ports, and VLAN configuration information.

- Display VLAN Information

```
VLAN ID   Name          State    H/W Status   Member ports
                                                (u)-Untagged, (t)-Tagged
======= ============ ======= ========== ============================
1         default       ACTIVE   Up           gigabitEthernet0/2(u)
                                                gigabitEthernet0/3(u)
```

7. Configuring QINQ

7.1. Overview of QINQ

QINQ technology also known as Stacked VLAN. The standard is derived from IEEE 802.1ad, which means that the public network VLAN Tag of a service provider network is encapsulated before the user packet enters the service provider network, and the private network user VLAN Tag in the user packet is regarded as data, so that the packet carries Two-layer VLAN tag traversal of service provider network.

In the metropolitan area network, a large number of VLANs are required to isolate users. The 4094 VLANs supported by the IEEE 802.1Q protocol are far from meeting the requirements. Through the double-layer Tag encapsulation of QINQ technology, in the service provider network, the packets are only transmitted according to the unique outer VLAN Tag allocated on the public network, so that the VLANs of different private network users can be reused, and the number of VLAN tags available to users is expanded. At the same time, it provides a simple Layer 2 VPN function, so QINQ technology is actually a VLAN VPN technology. In addition to QINQ, common VLAN VPN technologies also include VLAN Mapping. The only difference between the two is that QINQ is for stacking VLANs, and VLAN Mapping is for VLAN mapping.

7.1.1. VLAN Stacking

VLAN Stacking: From the user network to the provider network, a single-layer tag becomes a double-layer tag, and the C-Tag remains in the packet as an inner-layer tag; reverse, from a double-layer tag to a single-layer tag.

VLAN Stacking QINQ is divided into three categories:

- **Type A: Basic QINQ, which is enabled and disabled based on the interface. When an interface with basic QINQ enabled receives a packet, it is treated as an un-tagged packet. On the basis of the original packet, a VLAN tag of the default VLAN of the port is added.**
- **Type B: Flexible QINQ based on C-tag, according to the C-VLAN Tag on the user side, according to the configured mapping policy, an S-VLAN tag is added to the original packet. There are two optional configuration methods for this type of QINQ, and only one of them can be selected. One way is to configure the mapping relationship between C-VLAN and S-VLAN directly on the interface; the other way is to configure VLAN VPN globally (which includes the mapping relationship between C-VLAN and S-VLAN), and then associate the VPN on the interface. When using the same mapping policy for multiple interfaces, generally choose the latter configuration method. For this type of QINQ, if the packets received by the interface are un-tagged, the C-tag is the default VLAN Tag of the interface.**
- **Class C: ACL-based flexible QINQ, adding outer tags according to the configured traffic policy. The configuration of this type of QINQ is placed in the "QOS" module. For details, please refer to the "Configuring QOS" chapter. The policy pair between Policy-map and Class-map: "nest vlan <1-4094>" is used to configure ACL-based Flexible QINQ.**

The above three types of QINQ can be enabled at the same time on the same port, and their priority relationship is: Type C > Type B > Type A.

7.1.2. VLAN Mapping

VLAN Mapping: From the user network to the provider network, it is still a single-layer Tag, but the C-Tag becomes S-Tag; in reverse, from S-Tag to C-Tag.

VLAN Mapping is divided into 1:1 VLAN Mapping and 1:N VLAN Mapping (the reverse is N:1). Currently, only 1:1 VLAN Mapping is supported. VLAN Mapping is configured by configuring VLAN VPN globally, and then associating VPN on interface. VLAN

Mapping only takes effect on tag packets, which is very different from the QINQ function.

The following points should be noted when configuring QINQ and VLAN Mapping.

VLAN Mapping takes effect only for tagged packets. Upstream, original packets must carry tags to implement CVLAN-to-SVLAN mapping; for downstream, the VLAN output rule on downlink interfaces must be tag output to implement SVLAN-to-SVLAN mapping. Mapping of CVLANs.

Note

Only physical interfaces support the configuration of QINQ and VLAN Mapping, but aggregated interfaces do not

When using the QINQ function or the VLAN Mapping function, it needs to be used in conjunction with the VLAN configuration. In the input and output directions, the filtering function of the VLAN, and the rules for whether the VLAN carries tags are all subject to the VLAN configuration. Specific requirements are as follows:

- **Both CVLAN and SVLAN need to be added to the allow list of the downlink interface (connected to the Customer network), otherwise the flow will be filtered.**
- **The SVLAN needs to be added to the allow list of the uplink interface (connected to the provider network), otherwise the flow will be filtered.**
- **For QINQ, on the downlink interface, SVLAN should be configured with untag output, so as to strip the outer tag of QINQ downstream.**
- **For VLAN-Map, since it only takes effect for untag packets, for downlink interfaces, SVLAN should be configured with tag output, otherwise the downstream flow cannot complete the mapping from SVLAN to CVLAN.**

The globally configured VLAN VPN is either used for VLAN Stacking (QINQ) or VLAN Mapping, but not both.

VLAN Mapping only supports 1:1 mapping. Therefore, if there are VLAN VPNs with N:1 mapping, they cannot be associated with the interface as the VPN of VLAN mapping. Similarly, if the VPN has been associated with the interface as the VLAN mapping, the mapping relationship Cannot change to N:1

The mapping relationship of VLAN Mapping must be consistent globally. Therefore, different interfaces can only be associated with the same VLAN VPN.

On the same interface, if you need to apply VLAN Mapping and QINQ at the same time, it should be noted that the two functions need to control different CVLANs and SVLANs. The specific constraints are as follows.

- **If VLAN Mapping is used together with basic QINQ, the basic QINQ will take effect and VLAN Mapping will be invalid.**
- **If VLAN Mapping and flexible QINQ are used together, if a flow passes through the SVLAN mapped by VLAN Mapping and can be used as CVLAN to match the mapping policy of flexible QINQ, the final packet will take effect with flexible QINQ, adding SVLAN as external Layer TAG, the inner layer TAG remains unchanged (not the VLAN mapped by VLAN Mapping).**
- **Due to the above constraints, when two applications are enabled on the same interface, it is necessary to pay attention that the VLANs controlled by the two do not overlap. Invalid.**

For Type B QINQs, you can either choose to configure the mapping policy directly under the interface, or choose to associate with VPN, but cannot be configured at the same time.

7.2. Configuring

- **Creating VLAN VPN**

Command	**SWITCH(config)#vlan-vpn VPN-NAME** **SWITCH(config)#no vlan-vpn VPN-NAME**
Description	**There can be multiple VPNs in the system, and each VPN maintains the mapping relationship between independent CVLANs and SVLANs. A VPN will only actually take effect when applied to an interface. A VPN can be applied to VLAN Stacking (QINQ) or VLAN Mapping, but only one of the two can be selected.**

- **Adding VPN Mapping Relations**

Command	**SWITCH(config-vlan-vpn)#cvlan VLAN_LIST svlan VLANID** **SWITCH(config-vlan-vpn)#no cvlan VLAN_LIST** **SWITCH(config-vlan-vpn)#no cvlan**
Description	**The valid range of VLAN_LIST and VLANID is <1,4094>, VLAN_LIST supports standard multi-vlan representation method ("-" and "," and combination of both).** **no cvlan without any parameters, clear all the mapping relationships in the VPN.**

- **Configuring Port-based QINQ**

Command	**SWITCH(config-if)#switchport vlan-stacking basic** **SWITCH(config-if)#no switchport vlan-stacking basic**
Description	**After basic QINQ is enabled, all incoming packets from this interface match the QINQ rules, and the mapped SVLAN is the default VLAN ID of the interface.**

- **Configuring Mapping Relationship of QINQ on the interface**

Command	**SWITCH(config-if)#switchport vlan-stacking cvlan VLAN_LIST svlan VLANID** **SWITCH(config-if)#no switchport vlan-stacking cvlan VLAN_LIST** **SWITCH(config-if)#no switchport vlan-stacking cvlan**
Description	**Similar to the mapping relationship configuration under VPN. Only when the interface is not associated with a VPN, can the mapping relationship be configured directly.**

- **Attaching QINQ VPN on the Interface**

Command	**SWITCH(config-if)#switchport vlan-stacking vpn VPN-NAME** **SWITCH(config-if)#no switchport vlan-stacking vpn**
Description	**An interface can only be associated with one VPN. The VPN association configuration can be performed only when the interface is not configured with a mapping relationship.**

- **Clearing QINQ Configuration on the Interface**

Command	**SWITCH(config-if)#no switchport vlan-stacking**
Description	**Equivalent to three commands:** **no switchport vlan-stacking basic** **no switchport vlan-stacking cvlan** **no switchport vlan-stacking vpn**

- **Attaching VLAN Mapping VPN on the Interface**

Command	**SWITCH(config-if)#switchport vlan-mapping vpn VPN-NAME** **SWITCH(config-if)#no switchport vlan-mapping**
Description	**VLAN mapping configured on different interfaces must be associated with the same VPN. And the mapping relationship in the corresponding VPN must be 1:1.**

7.3. Examples

Example 1: This example shows how to configure L2 VPN service.

Service Provider provides VPN for Enterprise A and Enterprise B:

- **Enterprise A and enterprise B belong to different VLANs on the public network, and communicate through their own public network VLANs.**
- **The VLANs in enterprise A and enterprise B are transparent to the public network, and the user VLANs in enterprise A and enterprise B can be reused without conflict.**
- **Tunnel encapsulates a layer of VLAN Tag of Native VLAN to user data packets. In the public network, user data packets are transmitted in the native VLAN, which does not affect the use of VLANs in different enterprise user networks, and implements a simple Layer 2 VPN.**

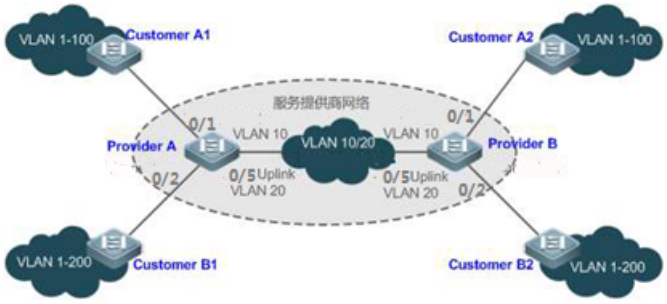


Illustration:

- **Customer A1, Customer A2, Customer B1 and Customer B2 are the edge devices of the network where enterprise user A and enterprise user B are located, respectively. Provider A and Provider B are edge devices of the service provider network, and enterprise A and enterprise B access the public network through the edge devices of the provider.**
- **The VLAN range of the office network used by enterprise A is VLAN 1-100.**
- **The VLAN range of the office network used by enterprise B is VLAN 1-200.**

ProviderA and ProviderB are completely symmetrical and have exactly the same configuration:

- **Configuring VLAN**

```
SWITCH(config)#vlan 2-200
SWITCH(config)#interface gigabitEthernet0/1
SWITCH(config-if)#switchport mode trunk
SWITCH(config-if)#switchport trunk allowed vlan 1-100
SWITCH(config-if)#switchport trunk native vlan 10
SWITCH(config)#interface gigabitEthernet0/2
SWITCH(config-if)#switchport mode trunk
```

```
SWITCH(config-if)#switchport trunk native vlan 10
SWITCH(config-if)#interface gigabitEthernet0/5
SWITCH(config-if)#switchport mode trunk
```

- **Configuring Base QINQ**

```
SWITCH(config)#interface gigabitEthernet0/1-2
SWITCH(config-if)#switchport vlan-stacking basic
SWITCH(config-if)#exit
```

Example 2: This example shows how to Implement Layer 2 VPN and service flow management based on Flexible QINQ.

Basic QinQ can only encapsulate user data packets in the outer tag of a native VLAN, that is, the encapsulation of the outer tag depends on the native VLAN of the tunnel port. Flexible QinQ provides flexible encapsulation of external tags (S-Tags) of service providers (ISPs) according to the tags of user packets (ie C-Tags), so as to flexibly implement VPN transparent transmission and service flow QoS policies.

- **Broadband Internet access and IPTV services are an important part of the services carried by the MAN. The MAN service provider network divides VLANs for different service flows to differentiate management, and provides QoS policy settings for these VLANs. You can use QinQ based on C-Tag on the edge device of the service provider to encapsulate the relevant VLAN of the user's business flow, and use the QoS policy of the service provider network for guaranteed transmission while transparent transmission.**
- **Unified VLAN planning is implemented between enterprise branches, and important services and general services are in different VLAN ranges. The enterprise network can use the flexible QinQ based on C-Tag to transparently transmit the internal services of the company, and can also use the service provider network. The QOS strategy of the company gives priority to ensuring the data transmission of important services.**

As shown in the figure below, the client devices in the metropolitan area network are aggregated through the corridor switches in the community, and broadband Internet access and IPTV services are differentiated by assigning different VLANs to enjoy different QoS service policies.

- **In the public network, different service flows of broadband Internet access and IPTV are transmitted in different VLANs to realize transparent transmission of user services.**
- **The ISP network sets the QoS policy for VLAN, and the corresponding VLAN can be encapsulated for the user service on the edge device of the service provider, so that the IPTV service is transmitted preferentially in the ISP network.**

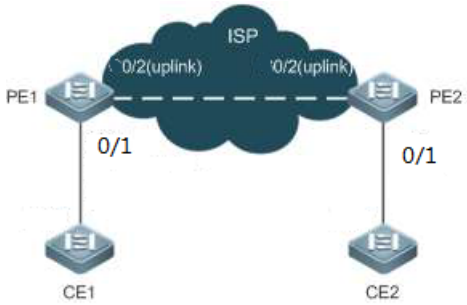


Illustration:

- **CE1 and CE2 are edge devices that connect to the user's network, and PE1 and PE2 are edge devices that the provider serves on the network.**

- **VLAN 1-100 and VLAN 101-200 on CE1 and CE2 devices are the broadband Internet service flow for users, and the IPTV service flow for users.**
- **PE1 and PE2 devices package different s-tags for vlans of different businesses to distinguish different business data. VLAN 1-100 package VLAN100, vlan101-200 package VLAN200.**

PE1 and PE2 are configured exactly the same:

- **Configuring VLAN**

```
SWITCH(config)#vlan 2-200
SWITCH(config)#interface gigabitEthernet0/1
SWITCH(config-if)#switchport mode hybrid
SWITCH(config-if)#switchport hybrid untagged vlan 100,200
SWITCH(config-if)#switchport hybrid vlan 100
SWITCH(config-if)#interface gigabitEthernet0/2
SWITCH(config-if)#switchport mode trunk
SWITCH(config-if)#exit
```

- **Configuring Flexible QINQ**

```
SWITCH(config)#vlan-vpn isp
SWITCH(config-vlan-vpn)# cvlan 1-100 svlan 100
SWITCH(config-vlan-vpn)# cvlan101-200 svlan 200
SWITCH(config-vlan-vpn)# interface gigabitEthernet0/1
SWITCH(config-if)#switchport vlan-stacking vpn isp
SWITCH(config-if)#exit
```

Example 3: This example shows how to Implement Layer 2 VPN and service flow management based on VLAN Mapping.

Similar to Case 2, the broadband Internet access service and the IPTV service of the user are distinguished. For example, the broadband Internet access service is VLAN2, and the IPTV service is VLAN3. In the ISP network, VLAN200 and VLAN300 are respectively used to represent broadband Internet access services and IPTV services. All ports 1-10 of the PE device are connected to the CE device, and the uplink interface is gigabitEthernet0/11.

PE1 and PE2 are configured exactly the same:

- **Configuring VLAN**

```
SWITCH(config)#vlan2-3,200,300
SWITCH(config)#interface gigabitEthernet0/1-10
SWITCH(config-if)#switchport mode trunk
SWITCH(config-if)#interface gigabitEthernet0/11
SWITCH(config-if)#switchport mode trunk
SWITCH(config-if)#exit
```

- **Configuring VLAN Mapping**

```
SWITCH(config)#vlan-vpn isp-map
SWITCH(config-vlan-vpn)#cvlan 2 svlan 200
SWITCH(config-vlan-vpn)#cvlan 3 svlan 300
SWTICH(config-vlan-vpn)#interface gigabitEthernet0/1-10
SWITCH(config-if)#switchport vlan-mapping vpn isp-map
SWITCH(config-if)#exit
```

7.4. Display Information

- **Display a VPN Information**

```
SWITCH#show vlan-vpn test
------------------------------------------------------------
VLAN VPN: test
Class: vlan-stacking
Mapping attributes:
 cvlan 1-25,73,75-80 svlan 3
 cvlan 200 svlan 4
Applied interfaces:
 gigabitEthernet0/17
 gigabitEthernet0/18
```

2) Display all VPN Information

```
SWITCH#show vlan-vpn
------------------------------------------------------------
VLAN VPN: test
Class: vlan-stacking
Mapping attributes:
 cvlan 1-25,73,75-80 svlan 3
 cvlan 200 svlan 4
Applied interfaces:
 gigabitEthernet0/17
 gigabitEthernet0/18
------------------------------------------------------------
VLAN VPN: test-map1
Class: vlan-mapping
Mapping attributes:
 cvlan 100 svlan 1
 cvlan 200 svlan 2
 cvlan 800 svlan 8
 cvlan 900 svlan 9
Applied interfaces:
 gigabitEthernet0/18
 gigabitEthernet0/19
------------------------------------------------------------
VLAN VPN: test1
Class: unkown
Mapping attributes:
 cvlan 800 svlan 8
 cvlan 900 svlan 9
Applied interfaces:
 empty!
```

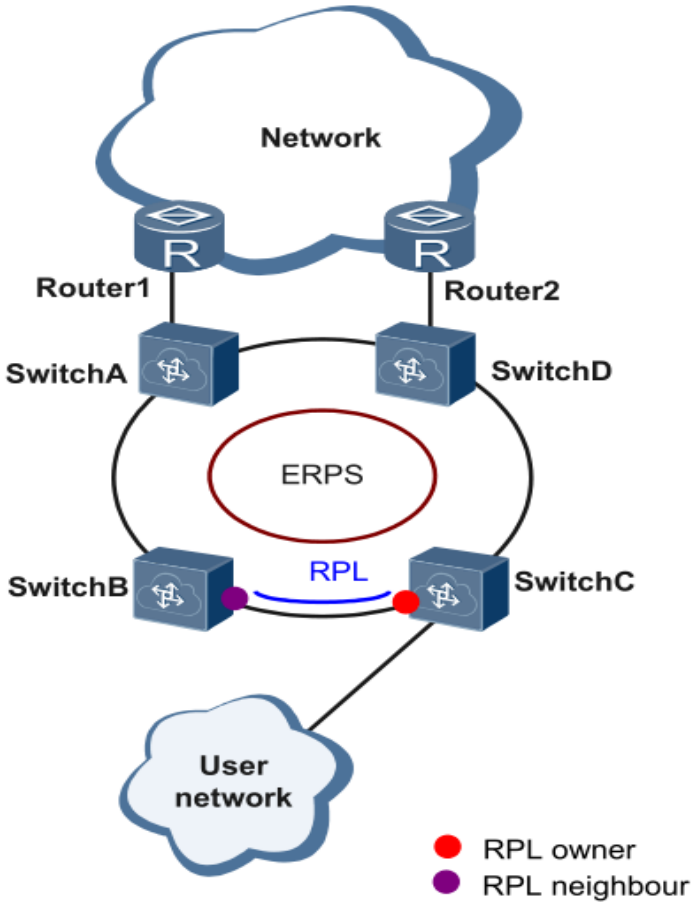
7.5. Configuring ERPS

7.6. Overview of ERPS

ERPS (Ethernet Ring Protection Switching) was developed by ITU, also known as G.8032.It is a link layer protocol specifically applied to Ethernet.It can prevent the broadcast storm caused by the data loop when the Ethernet ring network is complete, and can quickly restore the communication between each node on the ring network when a link on the Ethernet ring is disconnected.

At present, the technology to solve the Layer 2 network loop problem is STP.STP is more mature to use, but its convergence time is longer (seconds).ERPS is a link layer protocol that is specially applied to Ethernet and has a faster rate than STP for convergence, up to 50ms.

ERPS typical scenario:



7.7. Introduction to ERPS Rationale

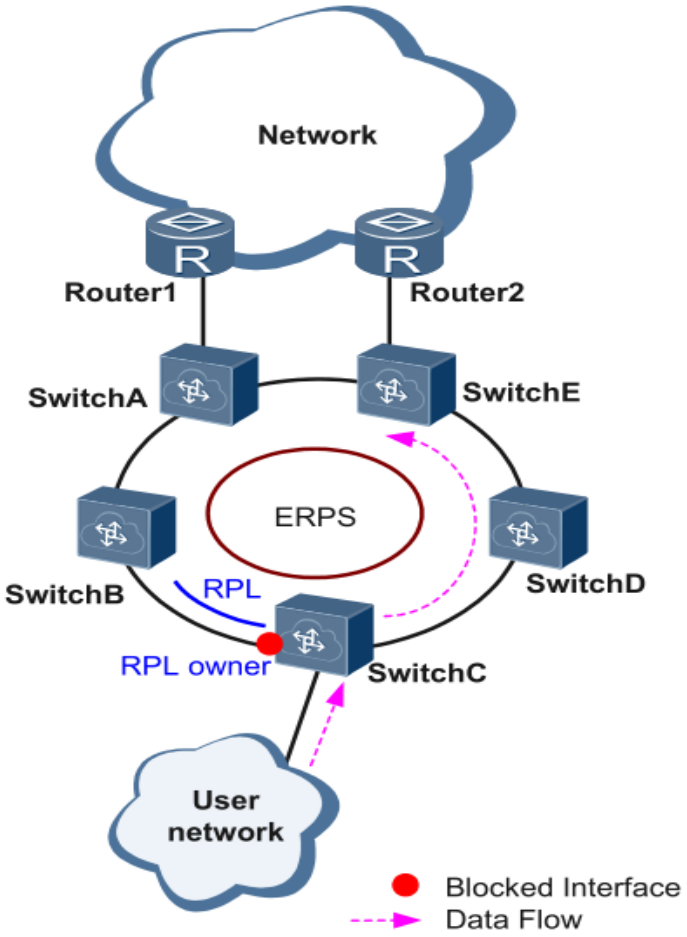
ERPS is a standard ring network protocol dedicated to the Ethernet link layer, with the ERPS ring as the basic unit.Only two ports on each layer 2 switch can be added to the same ERPS ring.In the ERPS, in order to prevent network loop, a break-down mechanism can be launched, blocking the RPL owner port and eliminating the ring route.When the ring connection fails, the equipment running the ERPS protocol can quickly forward the blocked port, make the link protection replacement, and restore

link communication between various nodes on the ring network.This section mainly presents the rationale for the implementation of ERPS under the basic network based on the normal ->link failure->link recovery process (including protection switch operations).

Link OK

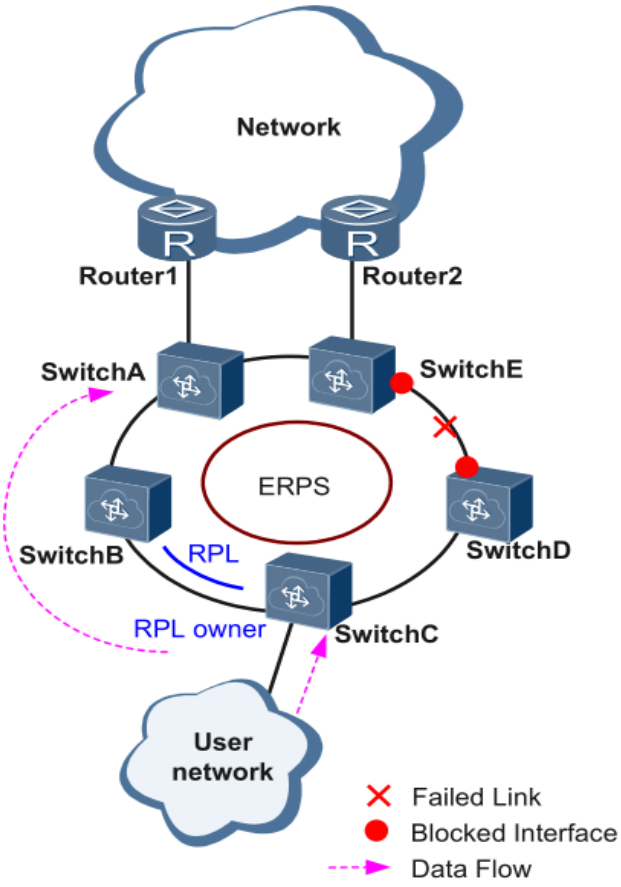
As shown in the diagram below, the equipment on the ring consisting of SwitchA~SwitchE is in good condition.

To prevent loops, ERPS first blocks the RPL owner port. If the RPL neighbor port is configured, the port will also be blocked, and other ports can forward traffic normally.



Link Failure

As shown in the diagram, when the link between SwitchD and SwitchE fails, the ERPS protocol starts the protection switching mechanism, blocks the ports on both ends of the faulty link, and then forward the RPL owner port, and the two ports resume user traffic. receiving and sending, thus ensuring uninterrupted traffic.



Link Restore

After the link returns to normal, if the ERPS ring is configured in revert mode, the device where the RPL owner port resides will block the traffic on the RPL link again, and the faulty link will be used again to transmit user traffic.

7.8. Configuring

- **Creating Ring**

Command	**SWITCH(config)#erps ring <1-255> east-interface IFNAME west-interface IFNAME** **SWITCH(config)#no erps ring <1-255>**
Description	**Create/delete ERPS ring.** **The ERPS ring is made up of the same set of VLAN and interconnected layer 2 switch, which is the basic unit of the ERPS protocol and needs to be configured on each device in the ring.** **The ring number is the unique identifier for the ERPS ring.**

- **Creating ERPS Instance**

Command	**SWITCH(config)#erps instance NAME** **SWITCH(config)#no erps instance NAME**
Description	**Create/remove ERPS instances; Create an instance to go into instance configuration mode.** **For the layer 2 switch operating an ERPS protocol, VLAN transmitting ERPS and data articles must be mapped into a protective instance so that ERPS protocol can be forwarded or blocked in accordance with their blocking**

	principles.Otherwise, user traffic could cause broadcast storms in a ring network that could make the network unavailable.

- **Associating ERPS Instances and Rings**

Command	**SWITCH(config-erps-inst)#ring <1-255>**
Description	**Configure the corresponding relationships between ERPS instances and rings.**

- **Configuring ERPS Instance Level**

Command	**SWITCH(config-erps-inst)#level <0-7>**
Description	**Configure ERPS instance level.**

- **Configuring the Configuration Profile Used by ERPS Instances**

Command	**SWITCH(config-erps-inst)#profile NAME**
Description	**Configure the ERPS configuration profile name.**

- **Configuring RPL Roles in ERPS Instance**

Command	**SWITCH(config-erps-inst)#rpl-role NAME**
Description	**Configure the ERPS instance RPL role;** **An ERPS ring has only one RPL owner port, which is determined by user configuration. The RPL owner port is blocked from forwarding user traffic to prevent loops in the ERPS ring.**

- **Configuring Raps VLAN for Instance**

Command	**SWITCH(config-erps-inst)#vlan <2-4094> raps-channel** **SWITCH(config-erps-inst)#no raps-channel**
Description	**Configuration/delete raps VLAN for ERPS instances;** **Each ERPS ring must be configured with a raps VLAN.Different ERPS rings cannot use the same raps VLAN ID.**

- **Configuring VLAN Instance**

Command	**SWITCH(config-erps-inst)#id <0-255>**
Description	**Configure VLAN Instance;** **The relationship between VLAN and Instance can be configured in MST mode; by default, all VLANs belong to Instance 0; the default id is 0.** **Note: Multi-instance is currently not supported in intersecting rings!**

- **Configuring Intersecting Sub-ring Block Port**

Command	**SWITCH(config-erps-inst)#sub-ring block (east-interface | west-interface)**
Description	**Configure the ERPS instance as a sub-ring instance and specify a sub-ring block port.**

- **Configuring Sub-ring Virtual Channels and Non-virtual Channels**

Command	**SWITCH(config-erps-inst)#virtual-channel attached-to-instance NAME** **SWITCH(config-erps-inst)# non-virtual-channel**
Description	**Configure the type of ERPS intersecting sub-ring: virtual channel and associated main ring; or non-virtual channel type.** **Note: The position displayed by this command in show running-config must be after the displayed position of the associated instance.Normally only need to ensure that the sub-ring ID and instance name are larger than the main ring ID and instance name.**

- **Creating ERPS Configuration Profile**

Command	**SWITCH(config)#erps profile NAME** **SWITCH(config)#no erps profile NAME**
Description	**Create/Remove ERPS configuration profile; Enter ERPS profile configuration mode after creating it.**

- **Configuring ERPS Revert Mode**

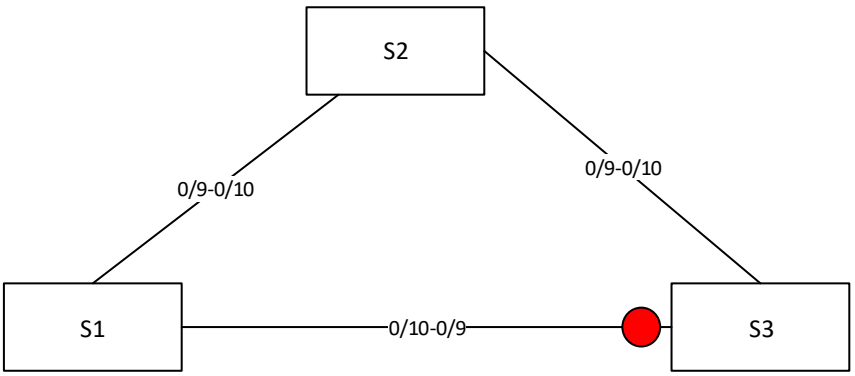
Command	**SWITCH(config-erps-prof)#revertive | non-revertive**
Description	**Configure ERPS revertive/non-revertive.**

- **Configuring ERPS Timer Parameters**

Command	**SWITCH(config-erps-prof)#timer (wait-to-restore (<1-12> | default) | hold-off (<0-100> | default) | guard-timer (<1-200> | default))**
Description	**Configure ERPS timer parameters.** **<1-12>: in minutes; revert time after recovery, default is 5 minutes.** **<0-100>: in 100 milliseconds; hold time before port forwarding, the default is 0, direct forwarding without delay.** **<1-200>: in 10 milliseconds; protection window when state changes, avoid receiving messages from previous state leading to protocol errors, default is 50: 500 ms.** **guard-timer parameters limit network size. It is conservatively recommended that when there are more than 300 nodes in the ring network, directly configure this parameter to the maximum value to avoid the failure of old packets to be discarded due to the large network size; no special configuration is required for nodes within 300 nodes.**

7.9. Examples

1. Single-ring case requirements: As shown in the figure, the configuration blocks the direct links of S1 and S2 by default, and restores the link in time to ensure the availability of the network in case of failure.Where the data VLANs are 1, 2 and 3.



S1/S2:

- **Enter global configuration mode, create ERPS and set related parameters, command reference list below:**

Create vlan 2,3;vlan 1 default exists

```
SWITCH(config)#vlan 2,3
```

Change the interface mode to trunk. By default, trunk mode will add all data vlans and management vlans to the interface for forwarding.

```
SWITCH(config)#interface gigabitEthernet0/9-10
SWITCH(config-if)#switchport mode trunk
```

Create ERPS ring 1

```
SWITCH(config)#erps ring 1 east gigabitEthernet0/9 west gigabitEthernet0/10
```

Create ERPS instance 1, associated with ring 1, and associated details configuration

```
SWITCH(config)#erps instance 1
SWITCH(config-erps-inst)#ring 1
SWITCH(config-erps-inst)#rpl-role non-owner
SWITCH(config-erps-inst)#vlan 1000 raps-channel
```

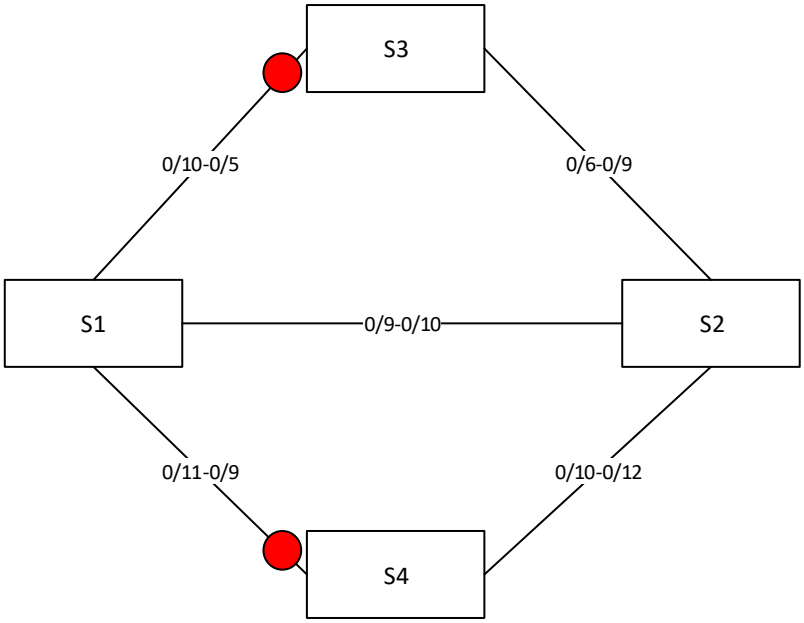
S3:

- **Enter global configuration mode, create ERPS and set related parameters, command reference list below:**

```
SWITCH(config)#Vlan 2,3
SWITCH(config)#interface gigabitEthernet0/9,gigabitEthernet0/10
SWITCH(config-if)#switchport mode trunk
SWITCH(config)#Erps ring 1 east gigabitEthernet0/9 west gigabitEthernet0/10
SWITCH(config)#Erps instance 1
SWITCH(config-erps-inst)#ring 1
SWITCH(config-erps-inst)#rpl-role owner east
SWITCH(config-erps-inst)#vlan 1000 raps-channel
```

2. Intersection ring case requirements

As shown in the following topology, S1, S2, S3, and S4 form intersecting rings, and the data vlans are 1, 2, 3, and 4. It is required to achieve fast convergence when a single point of failure occurs in each ring; a maximum of two faults can occur in the network Points (different rings), without user disconnection, to achieve optimal reliability.



Typical configuration examples:

S1:

```
Vlan 2,3,4
interface gigabitEthernet0/9-12
switchport mode trunk
Erps ring 1 east gigabitEthernet0/9 west gigabitEthernet0/10
Erps instance 1
 ring 1
 vlan 1000 raps-channel

Erps ring 2 east gigabitEthernet0/9 west gigabitEthernet0/11
Erps instance 2
 ring 2
  sub-ring block east-interface
  vlan 1100 raps-channel
  virtual-channel attached-to-instance 1
```

S2:

```
Vlan 2,3,4
interface gigabitEthernet0/9-12
switchport mode trunk
Erps ring 1 east gigabitEthernet0/9 west gigabitEthernet0/10
Erps instance 1
 ring 1
 vlan 1000 raps-channel

Erps ring 2 east gigabitEthernet0/12 west gigabitEthernet0/10
Erps instance 2
 ring 2
```

```
 sub-ring block east-interface
 vlan 1100 raps-channel
 virtual-channel attached-to-instance 1
```

S3:

```
Vlan 2,3,4
interface gigabitEthernet0/5-6
switchport mode trunk
Erps ring 1 east gigabitEthernet0/5 west gigabitEthernet0/6
Erps instance 1
 ring 1
 rpl-role owner east
 vlan 1000 raps-channel
```

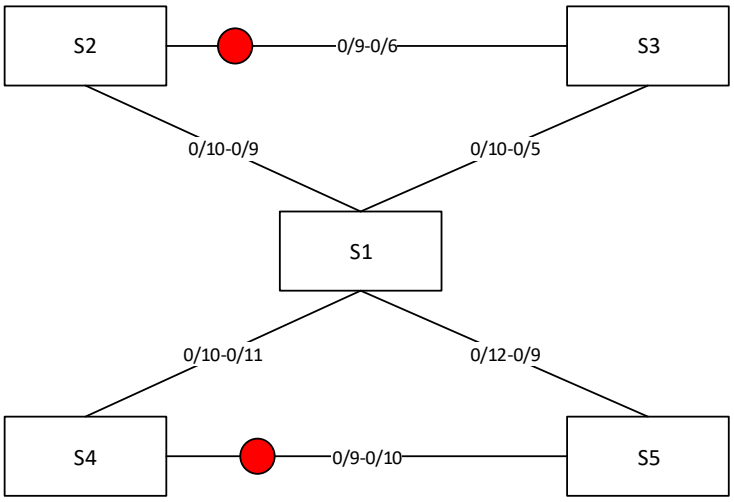
S4:

```
Vlan 2,3,4
interface gigabitEthernet0/9-12
switchport mode trunk
Erps ring 2 east gigabitEthernet0/9 west gigabitEthernet0/10
Erps instance 2
 ring 2
 rpl-role owner east
 vlan 1100 raps-channel
```

3. Tangent ring case requirements

The topology diagram is shown below. S1 is located in the central computer room, which can be supervised and maintained by the administrator in real time, and has high reliability; S2-S5 are distributed in various deployment points, in order to improve the reliability of the network and avoid the occurrence of single-link external connection The single-point failure risk is avoided, and the single-machine failure risk that may occur in a dual-link external connection is avoided, and the dual-link external connection is used to form a ring network.

It is required that each ring network can converge quickly when a single point of failure occurs to avoid user network interruption.



Typical configuration examples:

S1:

```
Vlan 2,3,4
interface gigabitEthernet0/9-12
switchport mode trunk
Erps ring 1 east gigabitEthernet0/9 west gigabitEthernet0/10
Erps instance 1
 ring 1
 vlan 1000 raps-channel

Erps ring 2 east gigabitEthernet0/11 west gigabitEthernet0/12
Erps instance 2
 ring 2
  vlan 1100 raps-channel
```

S2:

```
Vlan 2,3,4
interface gigabitEthernet0/9-12
switchport mode trunk
Erps ring 1 east gigabitEthernet0/9 west gigabitEthernet0/10
Erps instance 1
 ring 1
 rpl-role owner east
 vlan 1000 raps-channel
```

S3:

```
Vlan 2,3,4
interface gigabitEthernet0/5-6
switchport mode trunk
Erps ring 1 east gigabitEthernet0/5 west gigabitEthernet0/6
Erps instance 1
 ring 1
 vlan 1000 raps-channel
```

S4:

```
Vlan 2,3,4
interface gigabitEthernet0/9-12
switchport mode trunk
Erps ring 2 east gigabitEthernet0/9 west gigabitEthernet0/10
Erps instance 2
 ring 2
 rpl-role owner east
 rpl-role owner east
```

S5:

```
Vlan 2,3,4
interface gigabitEthernet0/9-12
switchport mode trunk
Erps ring 2 east gigabitEthernet0/9 west gigabitEthernet0/10
```

```
Erps instance 2
 ring 2
 vlan 1100 raps-channel
```

7.10. Display Information

- **Show ERPS Ring Information**

```
SWITCH#show erps ring 1
Ring       : 1
==========
Bridge     : 1
East       : gigabitEthernet0/9
West       : gigabitEthernet0/10
ERP Inst :1,
```

- **Show ERPS Instances**

```
SWITCH#
SWITCH#show erps instance 1
Inst Name          : 1
Inst Id            : 0
State              : ERPS_ST_IDLE
Last Priority      : RAPS-NR-RB
Phy Ring           : 1
Role               : NON-OWNER
East Link          : Link_Unblocked(up)(00-D0-FA-0A-10-06, 1)
East Link          : Link_Unblocked(up)(00-D0-FA-0A-10-06, 1)
TCN Propagation : Disabled
Attached           : -
Attached To        : -
Virtual ID         : -:-
------------------------------------------------------------
      Channel          |          Interface                  |   Profile
 (LEVL, VID, RID)     | (east,ver) ,    (west,ver)          |
============================================================
 (0, 1000,      1)      | (gigabitEthernet0/9, V=1), (gigabitEthernet0/10, V=1)       | Default
```

- **Show ERPS Profile**

```
SWITCH#show erps profile 1
Profile : 1
=========
 Wait-To-Restore : 5 mins
 Hold Off Timer   : 0 secs
 Guard Timer        : 500 ms
 Wait-To-Block     : 5500 ms
 Protection Type : Revertive
```

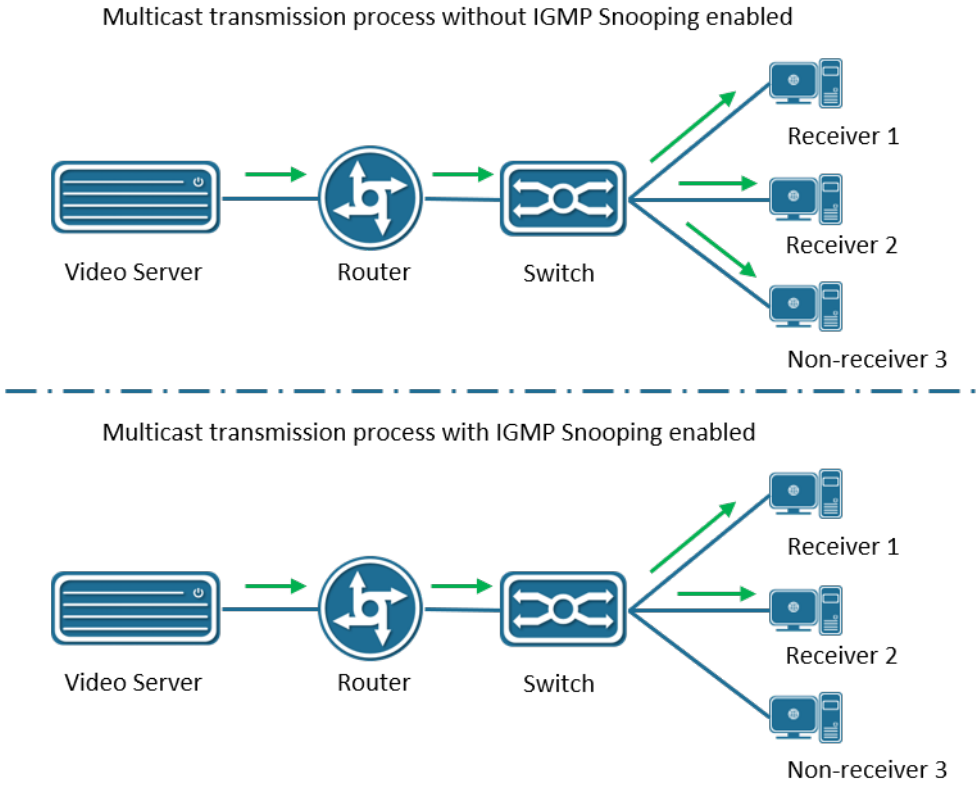
8. Configuring IGMP Snooping

8.1. Overview of IGMP Snooping

IGMP Snooping is a short term for Internet Group Management Protocol Snooping, a mechanism running on a layer 2 device for managing and controlling multicast groups.

A Layer 2 device running IGMP Snooping analyzes the received IGMP packets, establishes a mapping relationship between ports and MAC multicast addresses, and forwards multicast data according to the mapping relationship.When the Layer 2 device does not run IGMP Snooping, the multicast data is broadcast at Layer 2; when the Layer 2 device runs IGMP Snooping, the multicast data of the known multicast group will not be broadcast at Layer 2, but at Layer 2.

As shown in the figure below, when the Layer 2 multicast device does not run IGMP Snooping, the IP multicast packets are broadcast in the VLAN; when the Layer 2 multicast device runs IGMP Snooping, the IP multicast packets are only sent to the group members recipient.



8.2. Configuring

- **Enabling IGMP Snooping**

Command	**SWITCH(config)# igmp snooping** **SWITCH(config)# no igmp snooping**
Description	**Enable/disable IGMP Snooping function; disabled by default.** **Global configuration mode.**

- **Configuring IGMP Snooping Upstream Ports**

Command	**SWITCH(config-if)# igmp snooping mrouter interface IFNAME** **SWITCH(config-if)# no igmp snooping mrouter interface IFNAME**
Description	**Configure/delete IGMP Snooping upstream port; optional configuration.** **SVI interface mode.**

- **Configuring IGMP Snooping Static Groups**

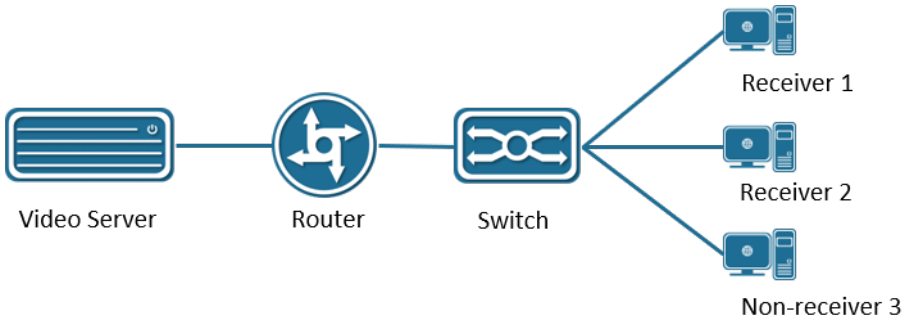
Command	**SWITCH(config-if)# igmp snooping static-group IPADDR source IPADDR interface IFNAME** **SWITCH(config-if)# no igmp snooping static-group IPADDR source IPADDR interface IFNAME**
Description	**Configure/delete IGMP Snooping static group; optional configuration.** **SVI interface mode.**

- **Configuring IGMP Snooping Fast Leave**

Command	**SWITCH(config-if)# igmp snooping fast-leave** **SWITCH(config-if)# no igmp snooping fast-leave**
Description	**Configure/delete IGMP Snooping fast leave function; optional configuration.** **SVI interface mode.**

8.3. Examples

Simplified topology:



Basic configuration /roles: (top down)

server:

During the test, VLC is used as the multicast server to provide the multicast service: udp://225.0.0.1:1234, the server IP is 3.3.3.10

router:

Run the multicast routing protocol and enable IGMP, and use Ruijie S57 Layer 3 switch to simulate the test. The main configurations are as follows:

Enable multicast routing

```
ip multicast-routing
```

Configure the uplink port , connect to the server, here is simply to select the PIM dense mode, the actual network scale is large, and the multicast use is less, it is recommended to use the sparse mode

```
interface GigabitEthernet 0/23
 no switchport
 no ip proxy- arp
 ip pim dense-mode
ip address 3.3.3.3 255.255.255.0
```

Configure the downlink port. The PIM dense mode is simply selected here. The actual network scale is large and the multicast usage is small. It is recommended to use the sparse mode

```
interface VLAN 1
no ip proxy- arp
 ip pim dense-mode
ip address 2.2.2.1 255.255.255.0
```

SWITCH:

Multicast can be enabled

```
igmp snooping
```

Client:

Watch server multicast video through udp://225.0.0.1:1234, IP 2.2.2.10

8.4. Display Information

- View IGMP Snooping Multicast Groups

```
SWITCH#show igmp snooping groups
```

- Viewing IGMP Snooping Interface Information

```
SWITCH#show igmp snooping interface {ifname}
Example:
IGMP Snooping information for vlan1
 IGMP Snooping enabled
 Snooping Querier none
 IGMP Snooping other querier timeout is 255 seconds
 Group Membership interval is 260 seconds
 IGMPv2 fast-leave is disabled
 IGMPv1/v2 Report suppression enabled
 IGMPv3 Report suppression enabled
 Router port detection using IGMP Queries
 Number of router-ports: 2
 Number of Groups: 2
 Number of Joins: 891
 Number of Leaves: 4
 Active Ports:
  gigabitEthernet0/1
  gigabitEthernet0/2
```

- Viewing IGMP Snooping Routing Port Information

```
SWITCH#show igmp snooping mrouter vlan1
Example:
```

```
SWITCH#show igmp snooping mrouter vlan1
VLAN Interface IP-address Expires
1 gigabitEthernet0/18(dynamic) 2.2.2.1 00:03:34
        gigabitEthernet0/20(static) -- --
```

- **Viewing IGMP Snooping Interface Statistics**

```
SWITCH#show igmp snooping statistics interface vlan1
IGMP Snooping statistics for vlan1
 Group Count : 2
 IGMP reports received : 893
 IGMP leaves received : 4
 IGMPv1 query warnings : 0
 IGMPv2 query warnings : 456
 IGMPv3 query warnings : 0
```

9. Configuring Spanning Tree Protocol

9.1. Overview of Spanning Tree Protocol

Spanning Tree Protocol is a layer 2 management protocol, which eliminates layer 2 loops by selectively blocking redundant links in the network, and also has the function of link backup.

Like the development process of many protocols, the Spanning Tree Protocol is constantly updated with the development of the network, from the original STP (Spanning Tree Protocol) to RSTP (Rapid Spanning Tree Protocol), and then to the latest MSTP (Multiple Spanning Tree Protocol).

For layer 2 Ethernet, there can only be one active path between two LANs, otherwise a broadcast storm will occur. However, in order to strengthen the reliability of a local area network, it is necessary to establish redundant links, some of which must be in a backup state. If the network fails and another link fails, the redundant link must be upgraded to Active status. Controlling such a process manually is obviously a very hard job, and the STP protocol does this automatically. It enables devices on a local area network to:

Find and start an optimal tree topology for the LAN.

Faults are detected and then recovered, automatically updating the network topology so that the best possible tree structure is selected at any time.

9.2. Configuring

- **Configuring STP Mode**

Command	**SWITCH(config)# spanning-tree mode { stp | rstp | mstp }**
Description	**stp: Spanning tree protocol (IEEE 802.1d)** **rstp: Rapid spanning tree protocol (IEEE 802.1w)** **mstp: Multiple spanning tree protocol (IEEE 802.1s)** **The default is rstp mode. After the mode is switched, the spanning tree protocol is disabled by default and needs to be re-enabled.** **Global configuration mode.**

- **Enabling Spanning Tree Protocol**

Command	**SWITCH(config)# spanning-tree enable** **SWITCH(config)# no spanning-tree enable**
Description	**Enables/disables STP function; disabled by default.** **Global configuration mode.**

- **Configuring Device Priority**

Command	**SWITCH(config)# spanning-tree priority <0-61440>** **SWITCH(config)# no spanning-tree priority** **SWITCH(config)# spanning-tree instance <1-63> priority <0-61440>**

	SWITCH(config) #no spanning-tree instance <1-63> priority
Description	**Configure/delete STP system priority; default 32768.Optional.** **Global configuration mode.**

- **Configuring Hello Time**

Command	**SWITCH(config)# spanning-tree hello-time <1-10>** **SWITCH(config)# no spanning-tree hello-time**
Description	**Configure/reset BPDU packet period, in seconds; the default is 2s. Optional.** **Global configuration mode.**

- **Configure Forward-Delay Time**

Commands	**SWITCH(config)# spanning-tree forward-time <4-30>** **SWITCH(config)# no spanning-tree forward-time**
Description	**Configure/reset STP port forwarding state delay time, in seconds.** **the default is 15s. Optional.** **Global configuration mode.**

- **Configure Max-Age Time**

Command	**SWITCH(config)# spanning-tree max-age <6-40>** **SWITCH(config)# no spanning-tree max-age**
Description	**Configure/reset the lifetime of BPDUs, in seconds; the default is 20s.Optional.** **Hello Time, Forward-Delay Time, Max-Age Time need to follow the conditions: 2*(Hello Time + 1.0 seconds) <= Max-Age Time <= 2*(Forward-Delay – 1.0seconds), otherwise it may lead to topology unstable.** **The longest path of the STP/RSTP network is affected by this parameter. The default longest path is 20 devices. When there are more than 20 devices, the configuration needs to be modified (forward-delay 21s, max-age 40s can be configured), and the maximum supported longest path is 40.** **Global configuration mode.**

- **Configure Max-Hops**

Command	**SWITCH(config)# spanning-tree max-hops <1-40>** **SWITCH(config)# no spanning-tree max-hops**
Description	**Configure/reset the maximum number of hops for BPDU packets; the default is 20. Optional.** **The longest path of the MSTP network is affected by this parameter. When there are more than 20 devices, the configuration needs to be modified, with a maximum of 40.** **MSTP is compatible with the max-age function, and the max-age parameter needs to be adjusted at the same time. Refer to the corresponding command.** **Global configuration mode.**

- **Configuring Transmit-Holdcount**

Command	**SWITCH(config)# spanning-tree transmit-holdcount <1-10>**

	SWITCH(config)# no spanning-tree transmit-holdcount
Description	**Configure/reset the maximum number of BPDUs sent per second; default is 6.Optional.** **Global configuration mode.**

- **Entering MST Mode**

Command	**SWITCH(config)# spanning-tree mst configuration**
Description	**Enter MST mode.** **Global configuration mode.**

- **Configuring the Mapping Between MST VLAN and Instance**

Command	**SWITCH(config-mst)# instance <1-63> vlan VLANID** **SWITCH(config-mst)# no instance <1-63> vlan VLANID**
Description	**Configure/delete the association between MST instances and VLANs; optional configuration.** **MST mode.**

- **Configuring the MST Area Name**

Command	**SWITCH(config-mst)# region NAME** **SWITCH(config-mst)# no region NAME**
Description	**Configure/delete the MST area name; optional configuration.** **MST mode.**

- **Configuring the MST Version Number**

Command	**SWITCH(config-mst)# revision <0-65535>**
Description	**Configure/delete the MST version number, the default is 0; optional configuration.** **MST mode.**

- **Configuring the Association Between Ports and Instances**

Command	**SWITCH(config-if)# spanning-tree instance <1-63>** **SWITCH(config-if)# no spanning-tree instance <1-63>**
Description	**Configure/remove association of ports and instances; optional configuration.** **By default, when configuring the relationship between an instance and a VLAN, the system automatically generates data about the relationship between the port and the instance based on the VLAN and port relationship, and no manual configuration is required.** **After the instance is configured, if the relationship between ports and VLANs is manually modified, such as adding/exiting all VLANs of an instance to the ports, you need to manually maintain the relationship between ports and instances through this command.** **When major configuration changes occur, it is recommended to automatically generate port and instance data by reconfiguring the instance-VLAN relationship or restarting the device.** **MST mode.**

- **Configuring Port Priority**

Command	**SWITCH(config-if)# spanning-tree priority <0-240>** **SWITCH(config-if)# spanning-tree instance <1-63> priority <0-240>**
Description	**Configure the port STP priority; the default is 128.Optional.** **Interface configuration mode.**

- **Configuring Port Path Cost**

Command	**SWITCH(config-if)# spanning-tree path-cost <1-200000000>** **SWITCH(config-if)# no spanning-tree path-cost**
Description	**Path cost to configure/reset port; optional configuration.** **Interface configuration mode.**

- **Configuring Link-Type**

Command	**SWITCH(config-if)# spanning-tree link-type { auto | point-to-point | shared }** **SWITCH(config-if)# no spanning-tree link-type**
Description	**Configure/reset the link type, the default is auto. Optional.** **auto: Automatic setting mode based on the duplex capability of link negotiation, full duplex is a point-to-point connection.** **point-to-point: Enable fast forwarding.** **shared: Disable fast forwarding.** **Global configuration mode.**

- **Configuring Protocol Migration Processing**

Command	**SWITCH(config-if)# clear spanning-tree detected protocols**
Description	**Force version checking on all ports.** **Privileged mode.**

- **Enable Portfast**

Command	**SWITCH(config-if)# spanning-tree portfast** **SWITCH(config-if)# no spanning-tree portfast**
Description	**Configure/delete port portfast; the port will be forwarded directly after portfast is enabled. However, the Port Fast Operational State will be disabled due to the receipt of BPDUs, so that it can normally participate in the STP algorithm and forwarding; it is disabled by default; optional configuration.** **Interface configuration mode.**

- **Configuring Edge Ports**

Command	**SWITCH(config-if)# spanning-tree {edgeport | autoedge}** **SWITCH(config-if)# no spanning-tree {edgeport | autoedge}**

Description	**Configure/delete a port Edge Port; if configured as edgeport, it means that the device directly connected to the port is not a bridge device and can be forwarded quickly; if configured as autoedge, it means that the port automatically identifies whether it is an edge port according to the BPDU; it is disabled by default; optional configuration.** **Interface configuration mode.**

- **Configuring Root Guard**

Command	**SWITCH(config-if)# spanning-tree guard root** **SWITCH(config-if)# no spanning-tree guard root**
Description	**Configure/delete port root guard; when the root guard function is enabled on an interface, its port role on all instances is forced to be the designated port. Once the port receives configuration information with a higher priority, the root guard function will set the interface to the designated port. blocked state; closed by default; optional configuration.** **Interface configuration mode.**

- **Configuring BPDU Guard**

Command	**SWITCH(config)# spanning-tree portfast bpdu-guard** **SWITCH(config)# no spanning-tree portfast bpdu-guard** **SWITCH(config-if)# spanning-tree portfast** **SWITCH(config-if)# no spanning-tree portfast** **or:** **SWITCH(config-if)# spanning-tree bpdu-guard enable** **SWITCH(config-if)# spanning-tree bpdu-guard disable**
Description	**Configure/delete BPDU Guard; after the port has BPDU Guard enabled, if a BPDU is received on the port, it will enter the Error-disabled (blocked) state; optional configuration.** **Interface configuration mode.**

- **Configuring BPDU Filter**

Command	**SWITCH(config)# spanning-tree portfast bpdu-filter** **SWITCH(config)# no spanning-tree portfast bpdu-filter** **SWITCH(config-if)# spanning-tree portfast** **SWITCH(config-if)# no spanning-tree portfast** **or:** **SWITCH(config-if)# spanning-tree bpdu-filter enable** **SWITCH(config-if)# spanning-tree bpdu-filter disable**
Description	**Configure/delete BPDU Filter; after enabling BPDU Filter, the port neither sends BPDU nor receives BPDU packets; optional configuration.** **Interface configuration mode.**

- **Configuring TC Topology Change Notification**

Command	**SWITCH(config-if)# spanning-tree restricted-tcn**

	SWITCH(config-if)# no spanning-tree restricted-tcn SWITCH(config-if)# spanning-tree instance <1-63> restricted-tcn SWITCH(config-if)# no spanning-tree instance <1-63> restricted-tcn
Description	Configure/reset the topology change notification limit. After configuration, the port will not forward TC BPDUs, nor refresh the address table; optional configuration. Interface configuration mode.

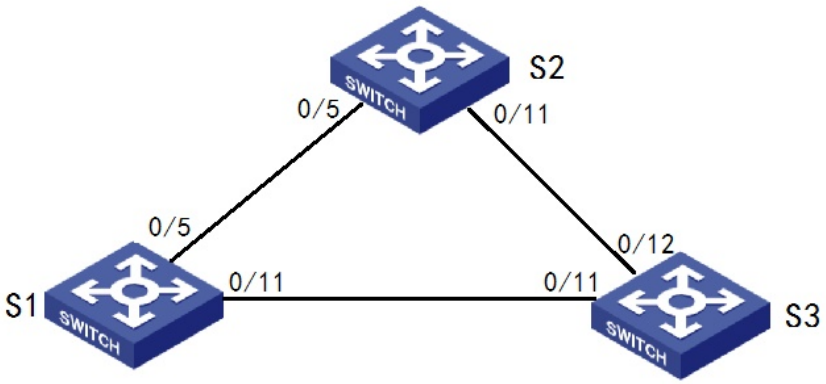
- Configuring the Wrong Port Timeout Function

Command	SWITCH(config)# spanning-tree errdisable-timeout enable SWITCH(config)# no spanning-tree errdisable-timeout enable SWITCH(config)# spanning-tree errdisable-timeout interval <10-1000000> SWITCH(config)# no spanning-tree errdisable-timeout interval
Description	Configure/reset error port timeout feature. By default, the error port timeout function is not enabled, that is, the error port will never timeout and automatically recover, and must be recovered manually. The timeout unit is seconds, the default is 300 seconds; Optional. Global configuration mode.

9.3. Examples

1. RSTP anti-loop to realize link redundancy scheme.

Simplified topology:



Typical configuration:

S1/S2/S3:

- Enter the global configuration mode, configure the rstp mode, and enable the stp switch:

use rstp mode

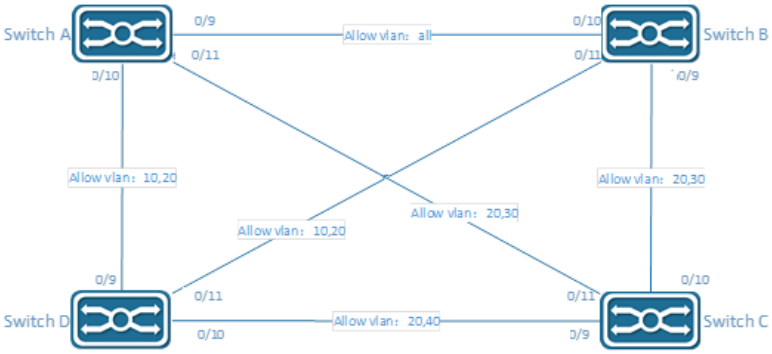
```
spanning-tree mode rstp
```

enable stp

```
spanning-tree enable
```

2. MSTP implements domain- and instance-based anti-loop and link redundancy.

Simplified topology:



Configuration plan:

The devices belong to the same domain, the default 'Default' domain is used here, no additional configuration is required.

VLAN 20 is a shared vlan and is directly assigned to CST.

Example	VLAN
0	20
1	10
3	30
4	40

Typical configuration:

Switch A:

 # Configure VLANs and ports

```
SWITCH(config)#vlan 10,20,30,40
SWITCH(config)#interface gigabitEthernet0/9
SWITCH(config-if)#switchport mode trunk
SWITCH(config)#interface gigabitEthernet0/10
SWITCH(config-if)#switchport mode trunk
SWITCH(config-if)#switchport trunk allowed vlan 10,20
SWITCH(config)#interface gigabitEthernet0/11
SWITCH(config-if)#switchport mode trunk
SWITCH(config-if)#switchport trunk allowed vlan 20,30
```

 # Configure MSTP instance

```
SWITCH(config)#spanning-tree mode mstp
SWITCH(config)#spanning-tree mst configuration
SWITCH(config-mst)#instance 1 vlan 10
SWITCH(config-mst)#instance 3 vlan 30
SWITCH(config-mst)#instance 4 vlan 40
```

 # enable MSTP

```
SWITCH(config)#spanning-tree enable
```

Switch B:

 # Configure VLANs and ports

```
SWITCH(config)#vlan 10,20,30,40
SWITCH(config)#interface gigabitEthernet0/9
SWITCH(config-if)#switchport mode trunk
SWITCH(config-if)#switchport trunk allowed vlan 20,30
SWITCH(config)#interface gigabitEthernet0/10
SWITCH(config-if)#switchport mode trunk
SWITCH(config)#interface gigabitEthernet0/11
SWITCH(config-if)#switchport mode trunk
SWITCH(config-if)#switchport trunk allowed vlan 10,20
```

#Configure MSTP instance

```
SWITCH(config)#spanning-tree mode mstp
SWITCH(config)#spanning-tree mst configuration
SWITCH(config-mst)#instance 1 vlan 10
SWITCH(config-mst)#instance 3 vlan 30
SWITCH(config-mst)#instance 4 vlan 40
```

 # enable MSTP

```
SWITCH(config)#spanning-tree enable
```

Switch C:

 # Configure VLANs and ports

```
SWITCH(config)#vlan 10,20,30,40
SWITCH(config)#interface gigabitEthernet0/9
SWITCH(config-if)#switchport mode trunk
SWITCH(config-if)#switchport trunk allowed vlan 20,40
SWITCH(config)#interface gigabitEthernet0/10
SWITCH(config-if)#switchport mode trunk
SWITCH(config-if)#switchport trunk allowed vlan 20,30
SWITCH(config)#interface gigabitEthernet0/11
SWITCH(config-if)#switchport mode trunk
SWITCH(config-if)#switchport trunk allowed vlan 20,30
```

 # Configure MSTP instance

```
SWITCH(config)#spanning-tree mode mstp
SWITCH(config)#spanning-tree mst configuration
SWITCH(config-mst)#instance 1 vlan 10
SWITCH(config-mst)#instance 3 vlan 30
SWITCH(config-mst)#instance 4 vlan 40
```

 # enable MSTP

```
SWITCH(config)#spanning-tree enable
```

Switch D:

 # Configure VLANs and ports

```
SWITCH(config)#vlan 10,20,30,40
SWITCH(config)#interface gigabitEthernet0/9
```

```
SWITCH(config-if)#switchport mode trunk
SWITCH(config-if)#switchport trunk allowed vlan 10,20
SWITCH(config)#interface gigabitEthernet0/10
SWITCH(config-if)#switchport mode trunk
SWITCH(config-if)#switchport trunk allowed vlan 20,40
SWITCH(config)#interface gigabitEthernet0/11
SWITCH(config-if)#switchport mode trunk
SWITCH(config-if)#switchport trunk allowed vlan 10,20
```

 # Configure MSTP instance

```
SWITCH(config)#spanning-tree mode mstp
SWITCH(config)#spanning-tree mst configuration
SWITCH(config-mst)#instance 1 vlan 10
SWITCH(config-mst)#instance 3 vlan 30
SWITCH(config-mst)#instance 4 vlan 40
```

#enable MSTP

```
SWITCH(config)#spanning-tree enable
```

9.4. Display Information

- **View STP Status**

```
SWITCH#show spanning-tree
```

- **View MSTP Instance Status**

```
SWITCH#show spanning-tree mst instance <1-63>
```

10. Configuring MAC Address

10.1. Overview of MAC Address

The MAC address table contains address information that the switch uses to forward traffic between ports. The switch sends packets between any combination of ports, based on the destination address of the received packet. Using the MAC address table, the switch forwards the packet only to the port associated with the destination address. If the destination address is on the port that sent the packet, the packet is filtered and not forwarded.

The MAC address table includes these types of addresses:

Dynamic address: a source MAC address that the switch learns and then ages when it is not in use.

Static address: a manually entered unicast address that does not age and that is not lost when the switch resets.

Filter address: Also a static MAC address, but drop the packet with the specified source or destination unicast filter address.

All addresses are associated with a VLAN. An address can exist in more than one VLAN and have different destinations in each. Each VLAN maintains its own logical address table. A known address in one VLAN is unknown in another until it is learned or statically associated with a port in the other VLAN.

Dynamic addresses are source MAC addresses that the switch learns and then ages when they are not in use. You can change the aging time setting for all VLANs or for a specified VLAN. Setting too short an aging time can cause addresses to be prematurely removed from the table. Then when the switch receives a packet for an unknown destination, it floods the packet to all ports in the same VLAN as the receiving port. This unnecessary flooding can impact performance. Setting too long an aging time can cause the address table to be filled with unused addresses, which prevents new addresses from being learned.

10.2. Configuring

- **Changing MAC Address Aging Time**

Command	**SWITCH(config)#mac-address-table aging-time <0-600>** **SWITCH(config)#no mac-address-table aging-time**
Description	**Set the length of time that a dynamic entry remains in the MAC address table.** **The range is 1 to 600 seconds.** **The default is 300 seconds.** **You can also enter 0, which disables aging.**

- **Adding Static MAC Address Entries**

Command	**SWITCH(config)#mac-address-table static MAC_ADDR vlan VLANID interface IFNAME** **SWITCH(config)#no mac-address-table static MAC_ADDR vlan VLANID interface IFNAME**
Description	**Add a static address to the MAC address table.** **MAC_ADDR: specify the destination MAC unicast address to add to the address table. Packets with this destination address received in the specified VLAN are forwarded to the specified interface.** **VLANID: specify the VLAN for which the packet with the specified MAC address is received, Valid VLAN IDs are 1 to 4094.** **IFNAME: specify the interface to which the received packet is forwarded, Valid interfaces include physical ports or port channels.**

- **Adding Filter MAC Address Entries**

Command	**SWITCH(config)#mac-address-table filter MAC_ADDR vlan VLANID** **SWITCH(config)#no mac-address-table filter MAC_ADDR vlan VLANID**
Description	**Add a filter address to the MAC address table.** **VLANID: specify the VLAN for which the packet with the specified MAC address is received, Valid VLAN IDs are 1 to 4094.** **IFNAME: specify the interface to which the received packet is dropped, Valid interfaces include physical ports or port channels.**

- **Clearing Dynamic MAC Address Entries**

Command	**SWITCH#clear mac-address-table dynamic** **SWITCH#clear mac-address-table dynamic vlan VLANID** **SWITCH#clear mac-address-table dynamic interface IFNAME**
Description	**Clear Dynamic Mac Address Entries.** **Support all, based on vlan or based on interface options.**

10.3. Examples

Example 1: This example shows how to change MAC Address aging time to 60 seconds.

Step1: Enter configuration mode:

```
SWITCH#configure terminal
Enter configuration commands, one per line.   End with CNTL/Z.
```

Step2: Change MAC Address aging time to 60 seconds.

```
SWITCH(config)#mac-address-table aging-time 60
```

Example 2: This example shows how to add a static MAC Address entry.

Step1: Enter configuration mode:

```
SWITCH#configure terminal
Enter configuration commands, one per line.   End with CNTL/Z.
```

Step2: Add a static MAC Address entry.

```
SWITCH(config)#mac-address-table static 000E.C6C1.C8AB vlan 1 interface gigabitEthernet0/1
```

Example 3: This example shows how to add a filter MAC Address entry.

Step1: Enter configuration mode:

```
SWITCH#configure terminal
Enter configuration commands, one per line.   End with CNTL/Z.
```

Step2: Add a filter MAC Address entry

```
SWITCH(config)#mac-address-table filter 000E.C6C1.C8AB vlan 1
```

Example 4: This example shows how to clear dynamic MAC Address entries.

Step1: Clear MAC Address entries by interface.

```
SWITCH#clear mac-address-table dynamic interface gigabitEthernet0/1
```

10.4. Display Information

- **Display MAC Address Table Entries**

```
SWITCH#show   mac-address-table
 VLAN       MAC Address       Type         Ports
```

```
-----+----------------+---------+----------------------+
20      0000.0000.0009    filter     drop
20      0000.0000.000a    filter     drop
```

- **Display MAC Address Table Statistics**

```
SWITCH#show  mac-address-table count
Static Address Count: 0
Filter Address Count: 2
Dynamic Address Count: 0
```

11. Configuring LLDP

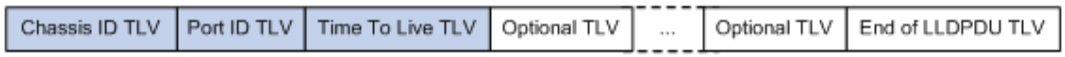
1.1. Overview of LLDP

LLDP (Link Layer Discovery Protocol) provides a standard link layer discovery method, enabling devices of different manufacturers to discover each other in the network and exchange their system and configuration information.LLDP encapsulates the information of the local device (including main capabilities, management address, device identification, interface identification, etc.) in LLDPDU (Link Layer Discovery Protocol Data Unit) It is released to the neighbors directly connected to itself. After receiving the information, the neighbors save it in the form of standard MIB up for the network management system to query and judge the communication status of the link.

LLDPDU

LLDPDU is a data unit encapsulated in the data part of an LLDP message.Before forming an LLDPDU, the device first encapsulates the local information into a TLV format, and then combines several TLVs into one LLDPDU and encapsulates it in the data part of the LLDP packet for transmission.

Figure 1 LLDPDU encapsulation format



As shown in Figure 1, the blue Chassis ID TLV, Port ID TLV, and Time To Live TLV must be carried by each LLDPDU, and the remaining TLVs are optional. Each LLDPDU can carry up to 32 TLVs.

TLV

TLV is the unit that makes up LLDPDU, and each TLV represents a piece of information.The TLVs that LLDP can encapsulate include basic TLVs, 802.1 organization-defined TLVs, 802.3 organization-defined TLVs, and LLDP-MED (Link Layer Discovery Protocol Media Endpoint Discovery, Link Layer Discovery Protocol Media Endpoint Discovery) TLVs.

Basic TLV

Basic TLVs are a set of TLVs that are the basis for network device management. 802.1 organization-defined TLVs, 802.3 organization-defined TLVs, and LLDP-MED TLVs are TLVs defined by standards organizations or other organizations to enhance the management of network devices. Need to choose whether to send in LLDPDU.

Among the basic TLVs, there are several TLVs that are mandatory for implementing the LLDP function, that is, they must be published in the LLDPDU, as shown in Table 1.

Table 1 Basic TLV

TLV name	instruction	Must be published
Chassis ID	Bridge MAC address of the sending device	Yes

TLV name	instruction	Must be published
Port ID	Identifies the port of the sender of the LLDPDU.If LLDP-MED TLV is carried in LLDPDU, its content is the MAC address of the port; otherwise, its content is the name of the port	Yes
Time To Live	The survival time of this device information on the neighbor device	Yes
End of LLDPDU	The end identifier of the LLDPDU, which is the last TLV of the LLDPDU	no
Port Description	Description of the port	no
System Name	the name of the device	no
System Description	description of the system	no
System Capabilities	The main functions of the system and the function items that have been turned on	no
Management Address	Management address, as well as the interface number and OID (Object Identifier) corresponding to the address	no

802.1 Organization-Defined TLV

The content of TLV defined by IEEE 802.1 organization is shown in Table2.

Currently, H3C devices do not support sending Protocol Identity TLV and VID Usage Digest TLV, but can receive these two types of TLVs.

Layer 3 Ethernet interfaces only support Link Aggregation TLVs.

Table2 IEEE 802.1Organization defined TLV

TLV name	instruction
Port VLAN ID (PVID)	Port VLAN ID
Port and protocol VLAN ID (PPVID)	Port Protocol VLAN ID
VLAN Name	The name of the VLAN to which the port belongs
Protocol Identity	The type of protocol supported by the port
DCBX	Data Center Bridging Exchange Protocol
EVB module	(Not currently supported) Edge Virtual Bridging module, including EVB TLV and CDCP (S-Channel Discovery and Configuration Protocol, S-Channel Discovery and Configuration Protocol) TLV.For the detailed introduction of these two TLVs, please refer to "EVB Configuration Guide"
Link Aggregation	Whether the port supports link aggregation and whether link aggregation is enabled

TLV name	instruction
Management VID	management VLAN
VID Usage Digest	Data containing a summary of VLAN ID usage
ETS Configuration	Enhanced Transmission Selection configuration
ETS Recommendations	Enhanced transfer selection recommendation
PFC	Priority-based Flow Control
APP	Application Protocol
QCN	(Not currently supported) Quantized Congestion Notification

802.3 Organization-Defined TLV

The content of TLV defined by Table3.

The Power Stateful Control TLV was defined in the IEEE P802.3at D1.0 version, and later versions no longer support this TLV.The H3C device will only send this type of TLV after receiving the Power Stateful Control TLV.

Table3 IEEE 802.3Organization defined TLV

TLV name	instruction
MAC/PHY Configuration/Status	The rate and duplex status supported by the port, whether it supports port rate auto-negotiation, whether the auto-negotiation function is enabled, and the current rate and duplex status
Link Aggregation	Whether the port supports link aggregation and whether link aggregation is enabled
Maximum Frame Size	Maximum frame length supported by the port
Power Stateful Control	Power status control of ports, including the type of power used by the PSE/PD, the priority of supplying/receiving power, and the power supplied/received
Energy-Efficient Ethernet	Energy Efficient Ethernet

management address

The management address is an address for the network management system to identify and manage network devices.The management address can clearly identify a device, which facilitates the drawing of network topology and facilitates network management.The management address is encapsulated in the Management Address TLV of the LLDP packet and advertised.

LLDP Mode

Under the specified type of LLDP proxy, LLDP has the following four working modes:

- TxRx: Both send and receive LLDP packets.
- Tx: Only sends and does not receive LLDP packets.
- Rx: only receives and does not send LLDP packets.
- Disable: Neither sends nor receives LLDP packets.

When the LLDP working mode of the port changes, the port will initialize the protocol state machine.To prevent the port from continuously performing initialization operations due to frequent changes in the working mode of the port, you can configure the port initialization delay time.

Protocol Specification

The protocol specifications related to LLDP are:

- **IEEE 802.1AB-2005: Station and Media Access Control Connectivity Discovery.**
- **IEEE 802.1AB 2009: Station and Media Access Control Connectivity Discovery.**
- **ANSI/TIA-1057: Link Layer Discovery Protocol for Media Endpoint Devices.**
- **IEEE Std 802.1Qaz-2011 : Media Access Control (MAC) Bridges and Virtual Bridged Local Area Networks-Amendment 18: Enhanced Transmission Selection for Bandwidth Sharing Between Traffic Classes.**

1.2. Configuring

1.2.1. Configuring Switch and Operating Mode

- **Enabling/disabling the LLDP Function Globally**

Command	**SWITCH(config)# lldp run** **SWITCH(config)# no lldp run**
Description	**Global configuration mode.** **Enable/disable LLDP function.** **required.**

- **Entering LLDP Interface Proxy Configuration Mode**

Command	**SWITCH(config-if)# lldp -agent** **SWITCH(lldp-agent)# exit**
Description	**Interface configuration mode.** **Enter the LLDP interface proxy configuration mode.** **Optional.**

- **Configuring the Working Mode of an LLDP Interface**

Command	**SWITCH(lldp-agent)# lldp enable { rxonly | txonly | txrx }** **SWITCH(lldp-agent)# lldp disable**
Description	**LLDP interface proxy configuration mode.** **Configure the working mode of the LLDP interface.** **Optional.**

1.2.2. Configuring Optional Basic Parameter

- **Configuring System Name**

Command	**SWITCH(config)# lldp system-name NAME** **SWITCH(config)# no lldp system-name**
Description	**Global configuration mode.** **Configure/reset the system name.** **Optional.**

- **Configuring System Descriptor**

Command	**SWITCH(config)# lldp system-description LINE** **SWITCH(config)# no lldp system-description**
Description	**Global configuration mode.** **Configure /reset system descriptors.** **Optional.**

- **Configuring the Device Locally-assigned**

Command	**SWITCH(config)# lldp chassis locally-assigned NAME** **SWITCH(config)# no lldp chassis locally-assigned**
Description	**Global configuration mode.** **Configure/reset the device locally-assigned .** **Optional.**

- **Configuring Interface Locally-assigned**

Command	**SWITCH(config-if)# lldp locally-assigned NAME** **SWITCH(config-if)# no lldp locally-assigned**
Description	**Interface configuration mode.** **Configure/reset the interface locally-assigned .** **Optional.**

- **Configuring Interface Proxy Cable Identification**

Command	**SWITCH(config-if)# lldp agt-circuit-id V A L E** **SWITCH(config-if)# no lldp agt-circuit-id**
Description	**Interface configuration mode.** **Configuration/reset interfaceagt-circuit-id.can be used as a value for port-id-tlv.** **Optional.**

- **Configuring Interface Port Descriptor**

Command	**SWITCH(config-if)# lldp port-description LINE** **SWITCH(config-if)# no lldp port-description**
Description	**Interface configuration mode.** **Configure/reset interface port descriptors.**

	Optional.

- **Configuring the Device ID Type of LLDP Interface**

Command	**SWITCH(lldp-agent)# lldp chassis-id-tlv { if-alias | if-name | ip-address | locally-assigned | mac-address }** **SWITCH(lldp-agent)# no lldp chassis-id-tlv**
Description	**LLDP interface proxy configuration mode.** **Configure the device identification type of the LLDP interface.** **Optional.**

- **Configuring the Management Address Type of LLDP Interface**

Command	**SWITCH(lldp-agent)# lldp management-address-tlv { ip-address | mac-address }** **SWITCH(lldp-agent)# no lldp management-address-tlv**
Description	**LLDP interface proxy configuration mode.** **Configure the management address type of the LLDP interface.** **Optional.**

- **Configuring the Port ID Type of LLDP Interface**

Command	**SWITCH(lldp-agent)# lldp port-id-tlv { agt-circuit-id | if-alias | if-name | ip-address | locally-assigned | mac-address }** **SWITCH(lldp-agent)# no lldp port-id-tlv**
Description	**LLDP interface proxy configuration mode.** **Configure the port ID type of the LLDP interface.** **Optional.**

1.2.3. **Configuring Optional State Machine Parameter**

- **Configuring the MsgTxHold Parameter of an LLDP Interface**

Command	**SWITCH(lldp-agent)# lldp msg-tx-hold <1-100>** **SWITCH(lldp-agent)# no lldp msg-tx-hold**
Description	**LLDP interface proxy configuration mode.** **This variable is used as a multiplier for msgTxInterval to determine the value of txTTL carried in LLDP frames transmitted by the LLDP proxy.The default msgTxHold is 4. Administrators can change this value to any value in the range 1 to 100.TTL= msgTxInterval * msgTxHold + 1 .** **Optional.**

- **Configuring the TxFastInit Parameter of the LLDP Interface**

Command	**SWITCH(lldp-agent)# lldp tx-fast-init <1-8>** **SWITCH(lldp-agent)# no lldp tx-fast-init**
Description	**LLDP interface proxy configuration mode.**

	This variable is used as the initial value of the txFast variable. This value determines the number of LLDPDUs transmitted during the fast transmission period.The default value of txFastInit is 4. Administrators can change this value to any value between 1 and 8. **Optional.**

- **Configuring the TxCredit Parameter of the LLDP Interface**

Command	**SWITCH(lldp-agent)# lldp tx-max-credit <1-8>** **SWITCH(lldp-agent)# no lldp tx-max-credit**
Description	**LLDP interface proxy configuration mode.** **Configure the maximum value of txCredit.The default value is 5. Administrators can change this value to any value in the range 1 to 10.** **Optional.**

- **Configuring the msgFastTx Parameter of the LLDP Interface**

Command	**SWITCH(lldp-agent)# lldp timer msg-fast-tx <1-3600>** **SWITCH(lldp-agent)# no lldp timer msg-fast-tx**
Description	**LLDP interface proxy configuration mode.** **This variable defines the time interval of the timer interval between two transfers in a fast transfer period (i.e. txFast is not zero). The default value for msgFastTx is 1; administrators can change this value to any value between 1 and 3600.** **Optional.**

- **Configuring the MsgTxInterval Parameter of the LLDP Interface**

Command	**SWITCH(lldp-agent)# lldp timer msg-tx-interval <5-3600>** **SWITCH(lldp-agent)# no lldp timer msg-tx-interval**
Description	**LLDP interface proxy configuration mode.** **This variable defines the timer interval between normal transfers (i.e. txFast is zero). The default value for msgTxInterval is 30 s; admin can change this value to any value between5and 300.** **Optional.**

- **Configuring the ReinitDelay Parameter of an LLDP Interface**

Command	**SWITCH(lldp-agent)# lldp timer reinit-delay <1-10>** **SWITCH(lldp-agent)# no lldp timer reinit-delay**
Description	**LLDP interface proxy configuration mode.** **This parameter represents the amount of delay between when adminStatus becomes "disabled" and when reinitialization is attempted. The default value of reinitDelay is 2 s.** **Optional.**

1.2.4. **Configuring Send Tlv List**

- **Configuring Tlv Selection for LLDP Interfaces**

Command	**SWITCH(lldp-agent)# [no] lldp tlv-select basic-mgmt { management-address | port-description | system-capabilities | system-description | system-name}** **SWITCH(lldp-agent)# [no] lldp tlv-select ieee-8021-org-specific { link-agg | mgmt-vid | port-ptcl-vlanid | port-vlanid | ptcl-identity | vid-digest | vlan-name }** **SWITCH(lldp-agent)# [no] lldp tlv-select ieee-802 3 -org-specific { mac-phy | max-mtu-size }**
Description	**LLDP interface proxy configuration mode.** **tlvs can be selected with multiple commands.** **Optional.** **Note: When there are many VLAN configurations on the device, the VLAN-related tlv may cause the packet length to exceed the MTU, resulting in packet sending errors. It is necessary to configure not to send this type of tlv.**

1.3. Examples

1.3.1. LLDP Basic Function Configuration Example

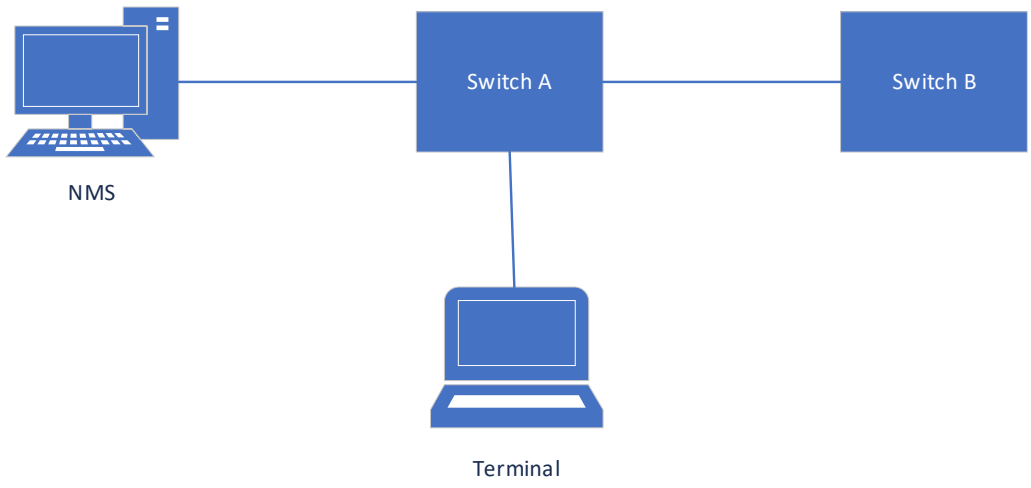
Requirements

NMS (Network Management System, network management system) is connected to Switch A, and Switch A is connected to the Terminal device and Switch B respectively.

By configuring the LLDP function on Switch A and Switch B, the NMS can judge the communication status of the link between Switch A and the terminal device, and between Switch A and Switch B.

Network diagram

Figure2 LLDP basic function configuration network diagram



Typical configuration example

Switch A/B:

```
Lldp run
```

1.4. Display Information

- **Display the Status of the LLDP Interface**

```
#show lldp interface gigabitEthernet0/2

Agent Mode : Nearest bridge
Enable (tx/rx): Y/Y
Message fast transmit time:1
Message transmission interval: 30
Reinitialisation delay: 2
MED Enabled:Y
Device Type: NOT_DEFINED
LLDP Agent traffic statistics:
Total frames transmitted: 4608
Total entries aged: 0
Total frames received: 150
Total frames received in error: 0
Total frames discarded: 0
Total discarded TLVs: 0
Total unrecognised TLVs: 0
```

- **Show LLDP Interface Neighbors**

```
#show lldp interface gigabitEthernet0/2 neighbor
Nearest bridge Neighbors
Interface Name : gigabitEthernet0/2
System Name :
System Description :
Port Description :
TTL: 3601
System Capabilities : Routing
Mandatory TLVs :
CHASSIS ID TYPE :
Chassis MAC Address: 000e.c6c1.3841
PORT ID TYPE :
Port MAC Address: 000e.c6c1.3841
8021 ORIGIN SPECIFIC TLV
Port Vlan id :0
PP Vlan id :0
Remote Protocols Advertised :
Remote VID Usage Digest : 0
Remote Management Vlan : 0
Link Aggregation Status : Disabled
Link Aggregation Port ID : 0
8023 ORIGIN SPECIFIC TLV
AutoNego Support : Supported Enabled
AutoNego Capability : 1
Operational MAU Type : 0
Max Frame Size : 0
```

MED Capabilities : Capabilities

MED Capabilities Dev Type : End Point Class-1

MED Application Type : Reserved

MED Vlan id : 0

MED Tag/Untag: Untagged

MED L2 Priority : 0

MED DSCP Val : 0

12. Configuring L3

12.1. Overview of L3

L3 functions include :Layer 3 port management, ARP management and Routing management.

- Layer 3 Port Management:

Layer 3 ports are generally divided into routing ports (physical ports switched to Layer 3 ports) or SVI ports (Switch Virtual Interface, corresponding to a VLAN).

The SVI port is a logical interface, which is constructed on top of all the member ports included in the corresponding VLAN, Unlike the routing port, the packets that are forwarded through the SVI at Layer 3 will first pass through Layer 2 (such as VLAN filtering, address learning, etc.) and then go through three layers, and then go through three layers and then two layers when outputting (such as VLAN output rules).

At the network layer, routing devices use IP addresses to complete packet forwarding. (Protocol specification: RFC 1918: Address Allocation for Private Internets, RFC 1166: Internet Numbers).

Layer 3 port management includes IP address maintenance for Layer 3 ports.

An IP address is composed of 32-bit binary. For the convenience of writing and description, it is generally expressed in dotted decimal. When expressed in dotted decimal, it is divided into four groups, each with 8 digits, ranging from 0 to 255. The groups are separated by ".", for example, "192.168.1.1" is the IP address expressed in decimal.

The IP address, as the name suggests, is naturally the interconnection address of the IP layer protocol. A 32-bit IP address consists of two parts:

1) the network address part, which indicates which network it is;

2) the host address part, which indicates which host in the network.

The network address part and the host address part of the IP address are divided by the network mask. The network mask is also a 32-bit value, consisting of several bits "1" in the front and several bits "0" in the back. The IP address is related to the network.

The mask and the obtained is the corresponding part of the network address. Likewise, the netmask can also be directly represented by the mask length.

For example, "192.168.1.1 255.255.255.0" and "192.168.1.1/24" represent the same IP address.

The device supports the configuration of the second IP address, that is, a Layer 3 port can be configured with at most one IP address.

When a Layer 3 port is configured with an IP address, a network segment is determined.

Different Layer 3 ports of the same device must belong to different network segments, and IP addresses configured with different Layer 3 ports must belong to different network segments.

The Layer 3 port represented by the SVI, and the corresponding VLAN is used as the unique identifier of the Layer 3 port.

After the different Layer 3 ports of the device are divided into different network segments, the forwarding between these different network segments (such as VLAN1 and VLAN2) is called "Layer 3 forwarding" (across network segments, or across

different VLANs).

- **ARP Management:**

In a local area network, each IP network device has two addresses:

1) The local address, since it is included in the frame header of the data link layer, should be more precisely the data link layer address, but in fact the local address is processed by the MAC sublayer in the data link layer, Therefore, it is customarily called a MAC address, and a MAC address represents an IP network device on a local area network.

2) The network address represents the IP network device on the Internet, and it also indicates the network to which the device belongs.

To communicate between two IP devices on the LAN, they must know each other's 48-bit MAC address. The process of learning the MAC address from the IP address is called address resolution.

There are two types of address resolution methods:

1) Address Resolution Protocol (ARP).

2) Proxy Address Resolution Protocol (Proxy ARP).

About ARP and Proxy ARP, they are described in RFC 826 and RFC 1027 documents respectively.

ARP (Address Resolution Protocol) is used to bind a MAC address and an IP address. Taking the IP address as an input, ARP can know its associated MAC address. Once the MAC address is known, the IP address to MAC address correspondence is stored in the device's ARP cache. With the MAC address, the IP device can encapsulate the link layer frame, and then send the data frame to the LAN. The encapsulation of IP and ARP on Ethernet is Ethernet II type.

ARP entries are divided into two categories: dynamic entries generated by the ARP protocol and static entries derived from static configuration. Dynamic ARP entries are formed by triggering the opening of IP packets. The opening process is an ARP request/response process. If the ARP entries formed after opening are unreachable, they will automatically age out. Static ARP entries do not need to be opened and will not age out.

- **Routing Management:**

Routing management is responsible for managing routing tables, integrate routes issued by various routing protocols to select the optimal route.

According to different sources, the routing table is usually divided into the following three categories:

  - **Directly connected route: The route discovered by the link layer protocol is also called the interface route. A direct route is automatically generated when an IP address is configured on a Layer 3 port, and the route prefix is the network directly connected to the Layer 3 port.**
  - **Static route: manually configured by the network administrator.**
  - **Prefix: It is represented by an IP address and network mask (or mask length), which refers to the destination network or host determined by the routing table entry (when the mask length is 32, it means the host).**
  - **Direct connection or next hop: Direct connection means that the destination network or host belongs to the directly connected network, and the direct connection route belongs to this situation. When configuring a static route, specifying a Layer 3 port instead of an IP address will also generate such a routing table item; the next hop is represented by an IP host address, indicating that to reach the destination network or host, it needs to be forwarded to the IP network device indicated by the IP address.**

When forwarding IP packets according to the routing table entry, if the routing table entry specifies the next hop, when the link layer encapsulates the ARP query, the IP of the next hop is used, that is, the destination MAC address of the link layer encapsulation is the next hop. The destination MAC address of the hop. If the routing table entry is directly connected, the destination IP address of the packet is directly used for ARP query, that is, the destination MAC address encapsulated at the link

layer is the final destination MAC address of the packet. Either way, if the ARP query fails, the route will be opened (a dynamic ARP entry will be generated). If the connection cannot be made, the IP packet cannot be forwarded and will be discarded.

There may be an inclusion relationship between routing table entries (depending on the length of the mask), so the route lookup process satisfies the LPM (Longest Prefix Match). That is, when IP packets are forwarded for route lookup, if multiple routing entries are hit at the same time, the routing entry with the longest prefix mask length is selected.

12.2. Configuring

- **Configuring SVI Port IP/IPv6 Address**

Command	**Configure SVI Port IP:** **SWITCH(config)#int vlan10** **SWITCH(config-if)#ip address *IPADDR/MASKLEN [secondary]*** **SWITCH(config-if)#ipv6 address *IP(X:X::X:X/M)*** **Or** **SWITCH(config-if)#ip address *IPADDR MASK [secondary]*** **Delete SVI Port IP:** **SWITCH(config)#int vlan10** **SWITCH(config-if)#no ip address *IPADDR/MASKLEN [secondary]*** **SWITCH(config-if)#no ipv6 address *IP(X:X::X:X/M)*** **Or** **SWITCH(config-if)#no ip address *IPADDR MASK [secondary]*** **Show the IP/IPv6 address of the Layer 3 port:** **SWITCH#show ip interface brief** **SWITCH#show ipv6 interface brief**
Description	**Configure in the interface mode of the SVI.** **When a VLAN is created, the SVI is automatically created, and when the VLAN is deleted, the SVI is automatically deleted. int vlanXX is to enter the interface mode of the SVI. Therefore, when the SVI does not exist (the corresponding VLAN does not exist), entering the interface mode of the SVI will fail. At the same time, when the SVI is deleted, the IP address configured on it will be automatically cleared.** **Layer 3 ports support IP/IPv6 address configuration update, which has the same effect as deleting and reconfiguring. The IP addresses configured on different Layer 3 ports must belong to different network segments.** **SVI supports the configuration of the second ip. When configuring the second ip, you need to configure the primary ip first. When deleting the primary ip, if the second ip already exists, you need to delete all the second ip before deleting the primary ip, otherwise it cannot be deleted.** **Note: After this command is configured, the system will clear the management IP configuration (refer to: Configuring Management IP), and use the Layer 3 port IP address as the device management IP instead.**

- **Configuring Routing Port IP/IPv6 Address**

Command	**Configure Routing Port IP:** **SWITCH(config)#interface gigabitEthernet0/1**

	SWITCH(config-if)#no switchport **SWITCH(config-if)#ip address *IP(A.B.C.D/M) [secondary]*** **SWITCH(config-if)#ipv6 address *IP(X:X::X:X/M)*** **Or** **SWITCH(config-if)#ip address IP(A.B.C.D) MASK(A.B.C.D) *[secondary]*** **Delete Routing Port IP:** **SWITCH(config)# interface gigabitEthernet0/1** **SWITCH(config-if)#no ip address IP(A.B.C.D/M)** **SWITCH(config-if)#no ipv6 address IP(X:X::X:X/M)** **Or** **SWITCH(config-if)#no ip address IP(A.B.C.D) MASK(A.B.C.D)** **SWITCH(config-if)#switchport**
Description	**Configure in interface mode.** **Before configuring the routing port IP, since the default attribute of the interface is the Layer 2 port attribute, you need to use the no switchport command to switch the port from the Layer 2 port attribute to the Layer 3 routing port attribute, and then use the ip address command to configure the routing port attribute. IP configuration, otherwise, switch the routing port to the Layer 2 port attribute, use the switchport command.** **Layer 3 ports support IP address configuration update, which has the same effect as deleting and reconfiguring. The IP addresses configured on different Layer 3 ports must belong to different network segments.** **The Layer 3 interface supports the configuration of the second ip. When configuring the second ip, you need to configure the primary ip first.** **When deleting the primary ip, if the second ip already exists, you need to delete all the second ip before deleting the primary ip, otherwise it cannot be deleted.**

- **Configuring Static ARP Entries**

Command	**SWITCH(config)#arp IPADDR MACADD** **SWITCH(config)#no arp IPADDR**
Description	**Configure in global configuration mode.** **The IP address configured with static ARP must belong to the directly connected network segment, otherwise the configuration fails.** **Static ARP has a higher priority than dynamic ARP. When the two conflict, static ARP takes effect.** **When the IP address of the Layer 3 port is deleted or the Layer 3 port is deleted, if the IP address of the static ARP belongs to the directly connected network segment of the Layer 3 port, the static ARP will be invalid (you can see that the entry does not exist through show arp, but show run, you can see that the configuration is still there); Similarly, when a Layer 3 port is configured with an IP address, the ARP entry of the directly connected network segment whose IP address belongs to the Layer 3 port will change from an invalid state to a valid state. (You can see the existence of ARP entries through show arp).**

- **Clearing ARP Cache**

Command	**SWITCH#clear arp-cache**

Description	**Clear the ARP cache in privileged mode.** **This Command only clears dynamic ARP entries, and static ARP entries will not be cleared.**

- **Configuring Static IPv6 Neighbor Entries**

Command	**SWITCH(config)# ipv6 neighbor *IPv6(X:X::X:X) IFNAME MAC(XXXX.XXXX.XXXX)*** **SWITCH(config)#no ipv6 neighbor *IPv6(X:X::X:X) IFNAME***
Description	**Configure in global configuration mode.** **The IPv6 address configured with the static ipv6 neighbor must belong to the directly connected network segment, otherwise the configuration fails.** **The static ipv6 neighbor has a higher priority than the dynamic ipv6 neighbor. When the two conflict, the static ipv6 neighbor takes effect.** **When the IPv6 address of the Layer 3 port is deleted or the Layer 3 port is deleted, if the IPv6 address of the static ipv6 neighbor belongs to the directly connected network segment of the Layer 3 port, the static ipv6 neighbor will be invalid (you can see that the table does not exist through show ipv6 neighbors Item, but show run can see that the configuration is still there); Similarly, when a Layer 3 port is configured with an IPv6 address, the ipv6 neighbor entry whose IPv6 address belongs to the directly connected network segment of the Layer 3 port will change from an invalid state to valid state. (You can see that the neighbors table entry exists by show ipv6 neighbors).**

- **Configuring Static Routes**

Command	**SWITCH(config)#ip route {IPADDR/MASKLEN) | IPADDR MASK} {NH_IPADDR | IFNAME}** **SWITCH(config)#no ip route {IPADDR/MASKLEN | IPADDR MASK} {NH_IPADDR | IFNAME}** **SWITCH(config)#ipv6 route *[IPv6(X:X::X:X/M) [NH_IPv6(X:X::X:X) | IFNAME]*** **SWITCH(config)#no ip v6 route *[IPv6(X:X::X:X/M) [IPv6(X:X::X:X) | IFNAME]***
Description	**Configure in global configuration mode.** **Recursive routing is not supported (the configured next-hop IP must belong to the directly connected network segment);** **The route prefix cannot belong to the directly connected network segment (that is, the directly connected route is automatically generated and cannot be statically configured).** **When a Layer 3 port is configured with an IP address, if the prefix of a static routing entry belongs to the directly connected network segment of the Layer 3 port, the static route will be automatically deleted and a LOG prompt will be displayed;** **When the IP address of a Layer 3 port is deleted or the Layer 3 port is deleted, if the next hop IP of a static routing entry belongs to the directly connected network segment of the Layer 3 port, the static route is automatically deleted and a LOG prompt is displayed.**

- **Configuring ECMP**

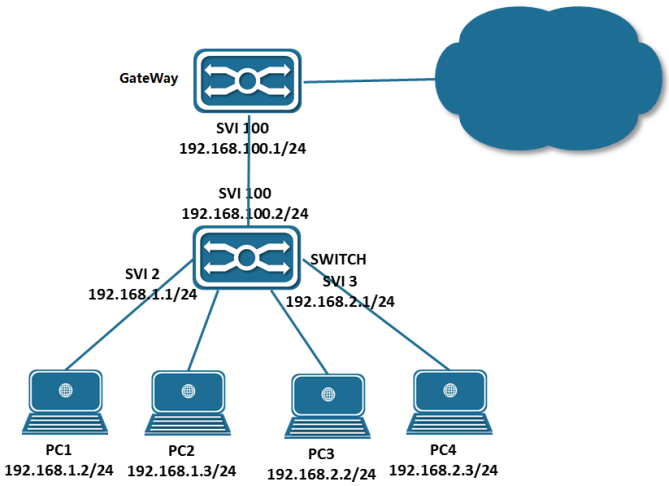
If there are redundant links in the network environment, that is, there are multiple next hops for the route to the same destination address. On devices that support ECMP technology, multiple next hops can work at the same time, so that redundant links can be fully utilized, and when a link failure occurs on a redundant link, traffic can be switched to other redundant links. Network reliability and stability.

ECMP (Equal-Cost Multipath Routing), this technology enables the device to use multiple next-hop links of the corresponding route concurrently, and balance the traffic among the multiple next-hop links according to the set balance factor distribution;

and supports fast switchover of faulty links.

12.3. Examples

Case 1: Weak Layer 3 Gateway



As a weak Layer 3 gateway, the Switch reduces the ARP burden for the real gateway.

- Configure PC:

Configure the IP addresses of PC1, PC2 and PC3 as shown in the figure, and specify the gateway at the same time. For example, the gateway of PC1 and P2 is 192.168.1.1.

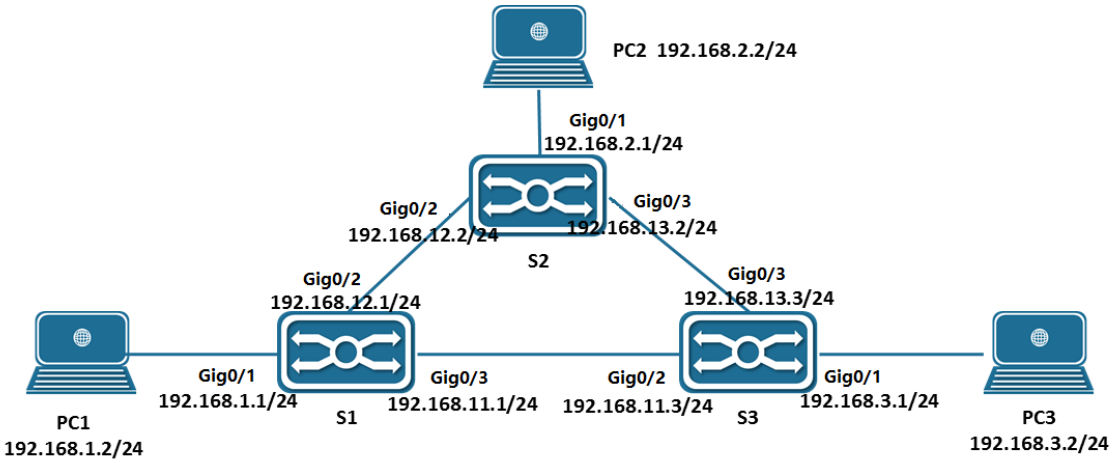
- Configure SWITCH:
  - Configure the Layer 3 port and IP address: (Assume that the interface connecting PC1-PC4 is gigabitEthernet0/1-4, and the uplink interface is gigabitEthernet0/17)

```
SWITCH(config)#vlan 2-3,100
SWITCH(config)#interface gigabitEthernet0/1-2
SWITCH(config-if)#switch access vlan 2
SWITCH(config)#interface gigabitEthernet0/3-4
SWITCH(config-if)#switch access vlan 3
SWITCH(config)#interface gigabitEthernet0/17
SWITCH(config-if)#switch access vlan 100
SWITCH(config)#int vlan2
SWITCH(config-if)#ip address 192.168.1.1/24
SWITCH(config)#int vlan3
SWITCH(config-if)#ip address 192.168.2.1/24
SWITCH(config)#int vlan100
SWITCH(config-if)#ip address 192.168.100.2/24
```

  - Configure a static route (default route):

```
SWITCH(config-if)ip route 0.0.0.0/0 192.168.100.1
```

Case 2: Intranet Layer 3 Interconnection



In the network environment shown above, PC1, PC2 and PC3 are interconnected through S1, S2 and S3 respectively.

- Configure PC

Configure the IP addresses of PC1, PC2 and PC3 as shown in the figure, and specify the gateway at the same time. For example, the gateway of PC1 is 192.168.1.1.

- Configure S1
  - Configure the Layer 3 port and IP address:

```
SWITCH(config)#vlan 2-4
SWITCH(config)#interface gigabitEthernet0/1
SWITCH(config-if)#switch access vlan 2
SWITCH(config)#interface gigabitEthernet0/2
SWITCH(config-if)#switch access vlan 3
SWITCH(config)#interface gigabitEthernet0/3
SWITCH(config-if)#switch access vlan 4
SWITCH(config)#int vlan2
SWITCH(config-if)#ip address 192.168.1.1/24
SWITCH(config)#int vlan3
SWITCH(config-if)#ip address 192.168.12.1/24
SWITCH(config)#int vlan4
SWITCH(config-if)#ip address 192.168.13.1/24
```

  - Configure a static route:

```
SWITCH(config)#ip route 192.168.2.0/24 192.168.12.2
SWITCH(config)#ip route 192.168.3.0/24 192.168.11.3
```

- S2 and S3 are configured similarly to S1.

12.4. Display Information

- Show L3 Interface

```
SWITCH#show ip interface brief
Interface          IP-Address       Admin-Status      Link-Status
GiE0/3             10.10.20.1       up                down
vlan10             192.168.65.166   up                up
```

```
SWITCH#show ipv6 interface brief
Interface              IPv6-Address              Admin-Status
vlan10                 2001:db8:0:f104::1        [up/up]
vlan1000               unassigned                [up/up]
```

- **Show ARP Entries**

```
SWITCH#show arp
Address                 HWaddress                 Interface       Type
192.168.1.238           00:00:00:00:04:86         vlan2           Static
192.168.2.46            00:00:00:00:05:45         vlan3           Static
192.168.3.110           00:00:00:00:08:59         vlan4           Static
192.168.0.12            00:00:00:00:00:09         vlan1           Static
192.168.0.1             00:0e:c6:d8:c7:f7         vlan1           Dynamic
10.100.2.2              00:01:a0:00:10:11         GiE0/2          Dynamic
```

- **Show Ipv6 Neighbor Entries**

```
SWITCH #show ipv6 neighbors
IPv6 Address                  MAC Address       Interface       Type
ff02::16                      3333.0000.0016    vlan10          dynamic
ff02::1:ff00:1                3333.ff00.0001    vlan10          dynamic
ff02::1:ff40:251a             3333.ff40.251a    vlan10          dynamic
```

- **Show Routing Table Entries**

```
SWITCH#show ip route
IP Route Table for VRF "default"
Gateway of last resort is 192.168.1.3 to network 0.0.0.0
S*      0.0.0.0/0 [1/0] via 192.168.1.3, vlan2
S       192.168.0.0/16 [1/0] via 192.168.0.10, vlan1
C       192.168.0.0/24 is directly connected, vlan1
C       192.168.1.0/24 is directly connected, vlan2
C       192.168.2.0/24 is directly connected, vlan3
C       192.168.3.0/24 is directly connected, vlan4
C       10.100.2.0/30 is directly connected, gigabitEthernet0/2
```

13. Configuring ACL

13.1. Overview of ACL

The ACL Implement packet filtering by configuring matching rules and processing operations for packets. The ACL can effectively prevent illegal users from accessing the network, and can also control traffic and save network resources.

Packet matching rules defined by ACL can also be referenced by other functions that need to differentiate traffic, such as the definition of traffic classification rules in QoS.

The ACL classifies packets through a series of matching conditions, which can be SMAC, DMAC, SIP, DIP, etc. According to the matching conditions, ACLs can be divided into the following types:

Standard IP-based ACL: Make rules based only on the source IP address of the packet.

Extended IP-based ACL: formulate rules based on the source IP address, destination IP address, ETYPE, and protocol of the data packet.

MAC-based ACL: formulate rules based on the source MAC address and destination MAC address of the data packet.

Named ACL: formulating rules is the same as IP-based standard ACL, extended ACL.

13.2. Configuring

- **Creating a IP-based Standard ACL**

Command	**SWITCH(config)#ip-access-list ACLID {permit | deny} {SIPADDR SIPADDRMASK | any}** **SWITCH(config)#no ip-access-list ACLID {permit | deny} {SIPADDR SIPADDRMASK | any}** **SWITCH(config)#no ip-access-list ACLID**
Description	**Define a standard IP-based ACL rule by using a source IPv4 address and wildcard.** **The ACLID is a decimal number from 1 to 99 or 1300 to 1999.** **Enter deny or permit to specify whether to deny or permit access if conditions are matched.** **The SIPADDR is the source IPv4 address of the network from which the packet is being sent.** **The SIPADDRMASK applies wildcard bits to the SIPADDR.** **The keyword any as an abbreviation for SIPADDR and SIPADDRMASK of 0.0.0.0 255.255.255.255. You do not need to enter a source-wildcard.**

- **Creating a IP-based Extended ACL**

Command	**SWITCH(config)# ip-access-list ACLID {permit | deny} {TYPE} {SIPADDR SIPADDRMASK | any} {DIPADDR DIPADDRMASK | any}** **SWITCH(config)#no ip-access-list ACLID {permit | deny} TYPE {SIPADDR SIPADDRMASK | any} {DIPADDR DIPADDRMASK | any}** **SWITCH(config)# no ip-access-list ACLID**
Description	**Define an extended IP-based ACL rule.** **The ACLID is a decimal number from 100 to 199 or 2000 to 2699.** **Enter deny or permit to specify whether to deny or permit the packet if conditions are matched.** **For TYPE, enter the name or number of an IP protocol: gre, igmp, opcomp, ip, rsvp, vrrp, pim, tcp, or udp, or an integer in the range 0 to 255 representing an IP protocol number. To match any Internet protocol, use the keyword any.** **The SIPADDR is the number of the network from which the packet is sent.**

	The SIPADDRMASK applies wildcard bits to the SIPADDR. **The DIPADDR is the network to which the packet is sent.** **The DIPADDRMASK applies wildcard bits to the DIPADDR.** **SIPADDR, SIPADDRMASK, DIPADDR, and DIPADDRMASK can be specified as any, The keyword for 0.0.0.0 255.255.255.255.**

- **Creating a MAC-based ACL**

Command	**SWITCH(config)#mac-access-list ACLID {permit | deny} {SMAC SMACMASK | any} {DMAC DMACMASK | any}** **SWITCH(config)#no mac-access-list ACLID {permit | deny} {SMAC SMACMASK | any} {DMAC DMACMASK | any}** **SWITCH(config)#no mac-access-list ACLID**
Description	**Define an MAC-based ACL rule, specify to permit or deny any source MAC address, a source MAC address with a mask, and any destination MAC address, destination MAC address with a mask.** **The ACLID is a decimal number from 100 to 199 or 2000 to 2699.** **SMAC, SMACMASK, DMAC, and DMACMASK can be specified as any, The keyword for 0000.0000.0000 ffff.ffff.ffff.** **Enter deny or permit to specify whether to deny or permit the packet if conditions are matched.**

- **Creating a Named IP-based Standard ACL**

Command	**SWITCH(config)#ip-access-list standard ACLNAME {permit | deny} {SIPADDR SIPADDRMASK | any}** **SWITCH(config)#no ip-access-list standard ACLNAME {permit | deny} {SIPADDR SIPADDRMASK | any}** **SWITCH(config)#no ip-access-list standard ACLNAME**
Description	**Define a standard ACL rule using the ACLNAME, specify one or more conditions denied or permitted to decide if the packet is forwarded or dropped.** **The SIPADDR is the source IPv4 address of the network from which the packet is being sent.** **The SIPADDRMASK applies wildcard bits to the SIPADDR.** **The keyword any as an abbreviation for SIPADDR and SIPADDRMASK of 0.0.0.0 255.255.255.255. You do not need to enter a source-wildcard.**

- **Creating a Named IP-based Extended ACL**

Command	**SWITCH(config)#ip-access-list extended ACLNAME {permit | deny} TYPE {SIPADDR SIPADDRMASK | any} {DIPADDR DIPADDRMASK | any}** **SWITCH(config)#no ip-access-list extended ACLNAME {permit | deny} TYPE {SIPADDR SIPADDRMASK | any} {DIPADDR DIPADDRMASK | any}** **SWITCH(config)#no ip-access-list extended ACLNAME**
Description	**Define a extended ACL rule using the ACLNAME, specify one or more conditions denied or permitted to decide if the packet is forwarded or dropped.** **For TYPE, enter the name or number of an IP protocol: gre, igmp, opcomp, ip, rsvp, vrrp, tcp, or udp, or an integer in the range 0 to 255 representing an IP protocol number. To match any Internet protocol, use the keyword any.**

	The SIPADDR is the number of the network from which the packet is sent. The SIPADDRMASK applies wildcard bits to the SIPADDR. The DIPADDR is the network to which the packet is sent. The DIPADDRMASK applies wildcard bits to the DIPADDR. SIPADDR, SIPADDRMASK, DIPADDR, and DIPADDRMASK can be specified as any, The keyword for 0.0.0.0 255.255.255.255.

Note

- Maximum of 128 rules can be configured under a ACL.
- The mask is inverted, For example, to match an IP address in the range of 192.168.1.0/24, configure 192.168.1.0 0.0.0.255.
- For the named ACL, the first character of ACLNAME cannot be a number.
- When creating an ACL, by default, the end of the ACL contains an implicit deny statement for all packets that it did not find a match for before reaching the end.

- Applying ACL to an Interface

Command	SWITCH(config-if)#access-group ACLNAME input SWITCH(config-if)#no access-group ACLNAME input
Description	Control access to the specified interface.

Note

- When an ACL has been applied to a interface, if you need to add or delete a rule, you need to un-apply it from the interface first.

13.3. Examples

Example 1: This example shows how to filter the ingress packets of port gigabitEthernet0/1, and allow the packets whose SIP is 192.168.1.0/24, and discard other packets.

Step 1: Entering ACL rules.

```
SWITCH(config)#ip-access-list 1   permit   192.168.1.0 0.0.0.255
SWITCH(config)#ip-access-list 1 deny any
```

Step 2: Applying ACL to the interface gigabitEthernet0/1.

```
SWITCH(config)#interface gigabitEthernet0/1
SWITCH(config-if)#access-group 1 in
```

13.4. Display Information

- Display ACL Information

```
SWITCH#show ip-access-list 1
  Standard IP access list: 1
    permit 1.1.1.1
    deny    any
```

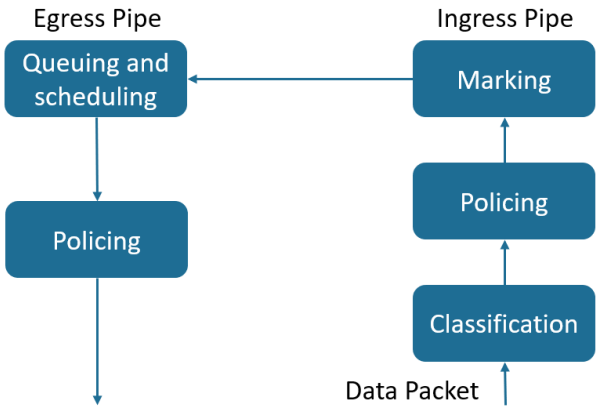
```
SWITCH#show mac-access-list 200
  Extended MAC-ACCESS-LIST: 200
    permit host 0001.0002.0003 any
deny    any any
```

14. Configuring QoS

14.1. Overview of QoS

Typically, networks operate on a best-effort delivery basis, which means that all traffic has equal priority and an equal chance of being delivered in a timely manner. When congestion occurs, all traffic has an equal chance of being dropped. When you configure the QoS feature, you can select specific network traffic, prioritize it according to its relative importance, and use congestion-management and congestion-avoidance techniques to provide preferential treatment. Implementing QoS in your network makes network performance more predictable and bandwidth utilization more effective.

The QoS implementation is based on the Differentiated Services (Diff-Serv) architecture, an emerging standard from the Internet Engineering Task Force (IETF). This architecture specifies that each packet is classified upon entry into the network. The following Figure shows the model of the QoS.



Classification

Classification is the process of distinguishing one kind of traffic from another by examining the fields in the packet. Classification is enabled only if QoS is globally enabled on the switch. By default, QoS is globally disabled, so no classification occurs.

During classification, the switch performs a lookup and assigns a QoS label to the packet. The QoS label identifies all QoS actions to be performed on the packet and from which queue the packet is sent.

The QoS label is based on the DSCP or the CoS value in the packet and decides the queueing and scheduling actions to perform on the packet. The label is mapped according to the trust setting and the packet type.

Trust CoS:

- **QoS with CoS label.**
- **For tagged packets, the CoS uses the CoS information in the tag.**
- **For packets without tags, the CoS adopts the default CoS value of the port.**

Trust DSCP:

- **For non-IP packets, the QoS is labeled with CoS; for packets with tags, CoS uses the CoS information in the tag; for packets without tags, the CoS uses the default CoS of the port.**
- **For IP packets, QoS has a DHCP label; select the DSCP value of the packet.**

No trust:

- **QoS with CoS label**
- **CoS adopts the default CoS value of the port.**

Policing(Ingress)

The ingress policer meters the given flow and classifies as either in-profile or out-of-profile. Out-of-profile packets may be discarded or have their QOS attributes remarked.

Marking

After a packet is classified and has a DSCP-based or CoS-based QoS label assigned to it, the marking process can begin.

For packets with CoS labels:

- **Use the configured CoS-to-DSCP mapping relationship to generate DSCP values for packets.**
- **Select the egress queue for the packet through the CoS-to-Queue mapping relationship.**

For packets with DSCP labels

- **Modify the DSCP value of the packet through the DSCP-to-DSCP mapping relationship.**
- **Generate a new CoS value for the packet through the DSCP-to-CoS mapping relationship.**
- **Select the egress queue for the packet through the DSCP-to-Queue mapping relationship.**

Queuing and scheduling

Generally, there are 8 queues for QoS exit, which map the 0-7 priority relationship of CoS. The packet enters the corresponding egress queue according to the final marked CoS and CoS-to-Queue relationship. For the priority of packet processing in the egress queue, there are the following algorithms:

- **WRR: The weight scheduling algorithm processes the packets in each queue in turn. The weight configuration can be used to change the number of queue packets processed in each cycle. The larger the weight, the higher the queue priority.**
- **SP: Strict scheduling algorithm, traverse queue 7 to queue 0 in each loop, when the initial processing of the packets in the high-priority queue ends, continue to process the low-priority queue.**
- **SP+WRR: The combination of WRR and SP, the global WRR mode, supports a specific queue configured as SP mode, and the queue configured as SP mode is a high-priority queue, which is processed first.**

Policing(Egress)

The egress policer meters the given flow and classifies as either in-profile or out-of-profile. Out-of-profile packets may be discarded.

14.2. Configuring

- **Enabling QoS Globally**

Command	**SWITCH(config)#mls qos enable** **SWITCH(config)#no mls qos**
Description	**Enabling QoS Globally.** **Default is disabled.**

- **Configuring Scheduling algorithm**

Command	**SWITCH(config)#mls qos algorithm {sp | wrr}**
Description	**Configuring the queue scheduling algorithm, support two modes: wrr and sp.**

- **Configuring Queue Wrr-weight**

Command	**SWITCH(config)#mls qos wrr-weight <0-7> <0-32>**
Description	**Configure the queue weight. The queue weight is only valid for wrr mode.** **The default weight of all queues is 1.** **When in wrr mode, configure the queue weight to 0, the queue will schedule in sp mode.**

- **Configuring Trust Mode on the Interface**

Command	SWITCH(config-if)#mls qos trust {cos | dscp} SWITCH(config-if)#no mls qos trust
Description	Configure the port trust mode, the default is not trust mode. When in no trust mode, the CoS field and DHCP field of the packet will be modified according to the default CoS of the port. When in trust cos mode, the same as the no trust mode for untagged packets, and for tagged packets, use the own CoS of the packet. When configuring trust dscp mode, for ip packets, select the packet with DSCP, and for non-ip packets, the same as trust cos mode.

- Configuring Default CoS on the interface

Command	SWITCH(config-if)#mls qos cos <0-7> SWITCH(config-if)#no mls qos cos
Description	Configure the default CoS of the port. The default CoS takes effect for the ingress packets without tags. The default port cos is 0.

- Configuring CoS-to-DSCP Mapping

Command	SWITCH(config)#mls qos cos-dscp <0-63> <0-63> <0-63> <0-63> <0-63> <0-63> <0-63> <0-63> SWITCH(config)#no mls qos cos-dscp
Description	Configure CoS-to-DSCP mapping. Default CoS-to-DSCP mapping: 0-0, 1-8, 2-16, 3-24, 4-32, 5-40, 6-48, 7-56.

- Configuring CoS-to-Queue Mapping

Command	SWITCH(config)#mls qos cos-queue <0-7> <0-7> SWITCH(config)#no mls qos cos-queue <0-7>
Description	Configure CoS-to-Queue mapping. Default CoS-to-Queue mapping: 0-0, 1-1, 2-2, 3-3, 4-4, 5-5, 6-6, 7-7.

Note

When the configured port is no trust, trust cos or trust dscp and the port is not ip: the cos-dscp configuration takes effect, modify the packet dscp according to the mapping relationship, and the cos-queue configuration takes effect, modify the packet export queue according to the mapping relationship.

- Configuring DSCP-to-CoS Mapping

Command	SWITCH(config)#mls qos dscp-cos <0-63> to <0-7> SWITCH(config)#no mls qos dscp-cos
Description	Configure DSCP-to-CoS mapping. Default DSCP-to-CoS mapping: <0-7>-0, <8-15>-1, <16-23>-2, <24-31>-3, <32-39>-4, <40-47>- 5, <48-55>-6, <56-63>-7.

- **Configuring DSCP-to-DSCP Mapping**

Command	**SWITCH(config)#mls qos dscp-mutation <0-63> to <0-63>** **SWITCH(config)#no mls qos dscp-mutation**
Description	**Configure DSCP-to-DSCP mapping.**

- **Configuring DSCP-to-Queue Mapping**

Command	**SWITCH(config)#mls qos dscp-queue <0-63> <0-7>** **SWITCH(config)#no mls qos dscp-queue <0-63>**
Description	**Configure DSCP-to-Queue mapping.** **Default DSCP-to-Queue mapping: <0-7>-0, <8-15>-1, <16-23>-2, <24-31>-3, <32-39>-4, <40-47>- 5, <48-55>-6, <56-63>-7.**

Note

When configuring the port as trust dscp and ip packets: the dscp-cos configuration takes effect, modify the packet dscp according to the mapping relationship, and the dscp-queue configuration takes effect, and modify the packet egress queue according to the mapping relationship. When a colleague configures dscp-dscp at the same time, first perform dscp-dscp conversion, and then perform dscp-cos mapping as a result.

- **Creating Class-map**

Command	**SWITCH(config)#class-map CNAME** **SWITCH(config-cmap)#** **SWITCH(config)#no class-map CNAME**
Description	**Create class-map.** **After creating a class-map, automatically enter the class-map mode.**

- **Configuring Class-map Maching Rule**

Command	**SWITCH(config-cmap)# match access-group ACLNAME** **SWITCH(config-cmap)#no match access-group ACLNAME**
Description	**Configure to match ACL entries for class-map.**

Command	**SWITCH(config-cmap)#match ip-dscp <0-63>** **SWITCH(config-cmap)#no match ip-dscp**
Description	**Configure to match the DHCP field in the IP packet, up to 64 different DHCP values can be configured.**

Command	**SWITCH(config-cmap)#match cos <0-7>** **SWITCH(config-cmap)#no match cos**

Description	**Configure to match the CoS field in the packet, up to 8 different CoS values can be configured.**

Command	**SWITCH(config-cmap)#match ethertype ETYPE** **SWITCH(config-cmap)#no match ethertype**
Description	**Configure to match the ethernet protocol type field of the packets.**

Command	**SWITCH(config-cmap)#match {vlan <1-4094> | vlan-range <1-4094> to <1-4094>}** **SWITCH(config-cmap)#no match {vlan | vlan-range}**
Description	**Configure to match vlan field in the packet, support range configuration.**

Command	**SWITCH(config-cmap)#match layer4 {tcp | udp} {source-port | destination-port} VALUE** **SWITCH(config-cmap)#no match layer4 {tcp | udp} {source-port | destination-port} VALUE**
Description	**Configure to match Layer 4 port fields of TCP and UDP packets.**

Command	**SWITCH(config-cmap)#match vlan-range <1-4094> to <1-4094> ethertype ETYPE** **SWITCH(config-cmap)#no match vlan-range**
Description	**Configure to match vlan and etype fields in the packets.**

- **Creating Policy-map**

Command	**SWITCH(config)#policy-map PNAME** **SWITCH(config-pmap)#** **SWITCH(config)#no policy-map PNAME**
Description	**Configure policy-map**

- **Attaching Policy-map to Class-map**

Command	**SWITCH(config-pmap)# class-map CNAME** **SWITCH(config-pmap-c)#** **SWITCH(config-pmap)#no class-map CNAME**
Description	**Attach class-map to policy-map.** **A policy-map can attach up to 8 class-maps.**

- **Configuring Action**

Command	**SWITCH(config-pmap-c)#set cos <0-7>** **SWITCH(config-pmap-c)#no set cos**
Description	**Configure policy action: modify the cos field of packets.**

Command	SWITCH(config-pmap-c)#set ip-dscp <0-63> SWITCH(config-pmap-c)#no set ip-dscp
Description	Configure policy action: modify the ip-dscp field of packets.

Command	SWITCH(config-pmap-c)#set vlan <1-4094> SWITCH(config-pmap-c)#no set vlan
Description	Configure policy action: modify packet vlan.

Command	SWITCH(config-pmap-c)#nest vlan <1-4094> SWITCH(config-pmap-c)#no nest vlan
Description	Configure policy action: add external tags to matching packets.

Command	SWITCH(config-pmap-c)#police cir <32-1000000> cbs <4-31250> exceed-action drop SWITCH(config-pmap-c)#no police
Description	Configure policy action: rate-limit. Cir is the speed limit water line, in kbps. Cbs is burst capacity, unit Kbyte.

Note

The value of cir is determinable. For example, if the speed limit is 1M, then the value of cir is 1024, but the value of cbs is taken from the empirical value. When the cbs value is set large, the flow peak is higher, and the speed limit is stable, but the average speed may be higher than the speed limit value; when the cbs value is set small, the flow peak is lower, the speed limit fluctuates greatly, and the average speed may be lower than the speed limit value. It is recommended that the cbs configuration take 4 times the value of cir.

- **Applying Policy-map on the Interface**

Command	SWITCH(config-if)#service-policy input PNAME SWITCH(config-if)#no service-policy input
Description	Apply the policy-map on the interface. Only one policy-map can be applied to an interface.

- **Configuring Ingress Rate-limit on the interface**

Command	SWITCH(config-if)#rate-limit input <64-1000000> <32-16384> SWITCH(config-if)#no rate-limit input
Description	Configure port ingress rate limit.

	The first parameter is limit level, in kbps. The second parameter is burst level, in Kbyte.

- Configuring Egress Rate-limit on the interface

Command	SWITCH(config-if)#rate-limit output <64-1000000> <32-16384> SWITCH(config-if)#no service-policy output
Description	Configure port egress rate limit. The first parameter is limit value, in kbps. The second parameter is burst value, in Kbyte.

Note

The limit value is determinable. For example, if the speed limit is 1M, then the limit value is 1024, but the burst value is taken from the experience value. When the burst value is large, the flow peak is higher, and the speed limit is stable, but the average rate may be higher than the speed limit value; when the burst value is small, the flow peak is lower, the speed limit fluctuates greatly, and the average rate may be lower than the speed limit value. . It is recommended that the burst configuration be 4 times the limit value.

14.3. Examples

Example 1: This example shows how to Configure ingress and egress rate-limit on the interface.

Step 1: Configuring Ingress rate-limit on interface gigabitEthernet0/1.

```
SWITCH(config-if)#rate-limit input 1024 4096
```

Step 2: Configuring Egress rate-limit on interface gigabitEthernet0/1.

```
SWITCH(config-if)#rate-limit output 1024 4096
```

Example 2: This example shows how to configure flow-based rate-limit.

Step 1: Enable QoS globally.

```
SWITCH(config)#mls qos enable
```

Step 2：Create ACL rule.

```
SWITCH(config)#ip-access-list 1 permit 192.168.64.1
```

Step 3：Create class-map, policy-map, attach ACL to the class-map, attach class-map to the policy-map, and configure the policy-map action.

```
SWITCH(config)#class-map c1
SWITCH(config-cmap)#match access-group 1
SWITCH(config-cmap)#exit
SWITCH(config)#policy-map p1
SWITCH(config-pmap)#class-map c1
SWITCH(config-pmap-c)#police cir 1024 cbs 4096 exceed-action drop
```

Step 4: Apply policy-map to the interface.

```
SWITCH(config)#interface gigabitEthernet0/1
SWITCH(config-if)#service-policy input p1
```

Example 3: This example shows how to configure port-based QoS service, to Implement preferential forwarding of specific port packets.

Step 1: Enable QoS globally.

```
SWITCH(config)#mls qos enable
```

Step 2: Configure interface gigabitEthernet0/1 and gigabitEthernet0/2 trust cos. Set gigabitEthernet0/1 default CoS to 0. Set gigabitEthernet0/2 default CoS to 2.

```
SWITCH(config)#interface gigabitEthernet0/1
SWITCH(config-if)#mls qos trust cos
SWITCH(config-if)#mls qos cos 0
SWITCH(config-if)#exit
SWITCH(config)#interface gigabitEthernet0/2
SWITCH(config-if)#mls qos trust cos
SWITCH(config-if)#mls qos cos 2
```

Step 3: Configure CoS-to-Queue mapping.

```
SWITCH(config)#mls qos cos-queue 0 0
SWITCH(config)#mls qos cos-queue 2 2
```

Step 4: Configure scheduling algorithm wrr.

```
SWITCH(config)#mls qos algorithm wrr
```

Step 5: Configuring queue 2 weight 0.

```
SWITCH(config)#mls qos weight 2 0
```

14.4. Display Information

- **Display Scheduling Algorithm and Weight Information**

```
SWITCH#show mls qos algorithm
Mls qos algorithm is WRR.

Queue-id     0     1     2     3     4     5     6     7
Weight       1     1     1     1     1     1     1     1
```

- **Display CoS-to-DSCP and CoS-to-Queue Mapping Information**

```
SWITCH#show mls qos cos-maps
----------------------------
Cos         Dscp        Queue
----------------------------
0           0           0
1           8           1
2           16          2
3           24          3
4           32          4
5           40          5
6           48          6
7           56          7
```

- **Display DSCP-to-CoS, DSCP-to-DSCP and DSCP-to-Queue Mapping Information**

```
SWITCH#show mls qos dscp-maps
-------------------------------------------
Dscp        Cos        Mutation        Queue
-------------------------------------------
```

```
0       0       0       0
1       0       1       0
2       0       2       0
3       0       3       0
4       0       4       0
5       0       5       0
6       0       6       0
7       0       7       0
8       1       8       1
9       1       9       1
10      1       10      1
11      1       11      1
12      1       12      1
13      1       13      1
14      1       14      1
15      1       15      1
```

- Display QoS Configuration on the Interfaces

```
SWITCH#show mls qos interfaces
-------------------------------
Interface       Trust mode   Cos
-------------------------------
GiE0/1          Not          0
GiE0/2          Not          0
GiE0/3          Not          0
GiE0/4          Not          0
GiE0/5          Not          0
GiE0/6          Not          0
GiE0/7          Not          0
GiE0/8          Not          0
```

- Display Class-map Configuration

```
SWITCH#show class-map

    CLASS-MAP-NAME: c1
      Match Cos: 3
```

- Display Policy-map Configuration

```
SWITCH#show policy-map

  POLICY-MAP-NAME: p1
    State: detached

    CLASS-MAP-NAME: c1
      Match Cos: 3
      Police: Mode: SrTCM
```

```
        cir (1024 Kbps)
        cbs (4096 KBytes)
        exceed-action (drop)
```

- **Display Rate-limit Configuration on the Interfaces**

```
SWITCH#show rate-limit
------------------------------------------------------------
Interface       In limit   In burst   Out limit   Out burst
------------------------------------------------------------
GiE0/1          --         --         --          --
GiE0/2          --         --         --          --
GiE0/3          1024       4096       --          --
GiE0/4          --         --         --          --
GiE0/5          --         --         --          --
GiE0/6          --         --         --          --
GiE0/7          --         --         --          --
GiE0/8          --         --         --          --
GiE0/9          --         --         --          --
GiE0/10         --         -          1024        4096
```

15. Configuring DHCP Snooping

15.1. Overview of DHCP Snooping

DHCP snooping (Dynamic Host Configuration Protocol) is a security feature that acts like a firewall between untrusted hosts and trusted DHCP servers. When DHCP snooping is enabled on a VLAN, the system examines DHCP messages sent from untrusted hosts associated with the VLAN and extracts their IP addresses and lease information. This information is used to build and maintain the DHCP snooping database.

DHCP snooping is enabled on a per-VLAN basis. By default, the feature is inactive on all VLANs. You can enable the feature on a single VLAN or a range of VLANs.

Trusted Sources

The DHCP snooping feature determines whether traffic sources are trusted or untrusted. DHCP snooping acts as a guardian of network security by keeping track of valid IP addresses assigned to downstream network devices by a trusted DHCP server. The default trust state of all interfaces is untrusted.

DHCP Snooping Limit Rate

Configure the number of DHCP packets per second that an interface can receive, to reduce or eliminate the impact of DHCP packet attack from this interface.

MAC Address Verification

With DHCP snooping MAC address verification enabled, DHCP snooping verifies that the source MAC address and the client hardware address match in DHCP packets that are received on untrusted ports. The source MAC address is a Layer 2 field associated with the packet, and the client hardware address is a Layer 3 field in the DHCP packet.

Option-82 Insertion

DHCP Option82 option is also called DHCP relay agent information option, one of many dhcp options. The Option82 option is a DHCP option proposed to enhance the security of the DHCP server and improve the IP address allocation strategy. The addition and stripping of options are implemented by the relay component.

DHCP Database

The DHCP snooping feature dynamically builds and maintains the database using information extracted from intercepted DHCP messages. The database contains an entry for each untrusted host with a leased IP address if the host is associated with a VLAN that has DHCP snooping enabled. The database does not contain entries for hosts connected through trusted interfaces. When the ip verify source function is enabled on the interface, database entrys act as valid users on the interface.

15.2. Configuring

- **Enable DHCP Snooping Globally**

Command	**SWITCH(config)#ip dhcp snooping** **SWITCH(config)#no ip dhcp snooping**
Description	**Enables DHCP snooping globally.**

- **Enable DHCP Snooping on Vlans**

Command	**SWITCH(config)#ip dhcp snooping vlan VID** **SWITCH(config)#no ip dhcp snooping vlan VIID**
Description	**Enables DHCP snooping on a VLAN or VLAN range, For example:**

	Ip dhcp snooping vlan 3-10. **By default, DHCP Snooping is enabled on all VLANs.**

- **Configuring Trust Resources**

Command	**SWITCH (config-if)#ip dhcp snooping trust** **SWITCH (config-if)#no ip dhcp snooping trust**
Description	**Configures the interface as trusted.** **By default, All interfaces are untrusted.**

- **Enabling Mac Address Verification**

Command	**SWITCH (config)#ip dhcp snooping verify mac-address** **SWITCH (config)#no ip dhcp snooping verify mac-address**
Description	**Enables DHCP snooping MAC address verification.** **By default is disabled.**

- **Configuring Rate Limit on Interface**

Command	**SWITCH (config-if)#ip dhcp snooping rate-limit PPS** **SWITCH (config-if)#no ip dhcp snooping rate-limit**
Description	**Configures DHCP packet rate limiting.** **PPS range from 0 to 128.** **If PPS is set to 0, this interface will drop all Incoming DHCP packets.**

Note

✦ Due to hardware limitations, for DHCP rate limit, when the limit value is not 0, the software rate limit is used, and when the limit value is 0, the hardware rate limit is used. Software rate limit will consumes CPU resources.

- **Enabling Option-82 Data Insertion**

Command	**SWITCH (config)#ip dhcp snooping information option-82** **SWITCH (config-if)#no ip dhcp snooping information option-82**
Description	**Enables DHCP option-82 data insertion.**

- **Configuring DHCP Snooping Database Write-delay Time**

Command	**SWITCH (config)#ip dhcp snooping database write-delay SECONDS** **SWITCH (config-if)#no ip dhcp snooping database write-delay**
Description	**Configuring DHCP Snooping data to be written to flash at regular intervals** **SECONDS range from 600 to 86400 by unit second.**

- **Trigger DHCP Snooping Database Write-flash**

Command	**SWITCH (config)#ip dhcp snooping database write-flash**

Description	**Trigger DHCP Snooping database write-flash.**

- **Trigger DHCP Snooping Database renew from flash**

Command	**SWITCH(config)#ip dhcp snooping database renew**
Description	**Trigger DHCP Snooping database renew from flash.**

- **Clear DHCP Snooping Database**

Command	**SWITCH#clear ip dhcp snooping database (vlan VLANID | interface IFNAME | mac-address XXXX.XXXX.XXXX | ip-address A.B.C.D | flash)**
Description	**Clear DHCP Snooping database based on port, vlan, MAC address, or IP address.** **Support to clear database in flash.**

15.3. Examples

Example 1: This is an example of DHCP Snooping typical application. The interface of gigabitEthernet0/8 is connected to DHCP server; USER-A obtains IP address by dynamic; There are other DHCP servers in the LAN, which will affect the IP address assignment of USER-A. Diagram as show in the Figure 1-1 below.

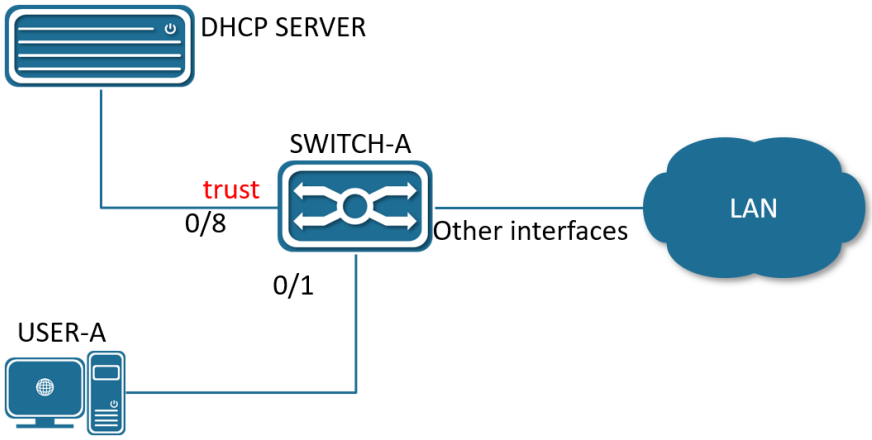


Figure 1-1 Typical application of DHCP Snooping Diagram

- **Enable DHCP Snooping Globally.**

```
SWITCH#configure terminal
SWITCH(config)#ip dhcp snooping
```

- **Configuring gigabitEthernet0/8 as Trusted Resource.**

```
SWITCH(config)#interface gigabitEthernet0/8
SWITCH(config-if)#ip dhcp snooping trust
```

15.4. Display Information

- **Display DHCP Snooping Information**

```
SWITCH#show ip dhcp snooping
Ip dhcp snooping                    : Enabled
No ip dhcp snooping vlan            : 2-5
```

```
Verify mac-address                    : Disabled
Information option-82                 : No
database write-delay                  : 0 seconds

Interface              Trusted        Rate limit (pps)
-----------------------------------------------------------
gigabitEthernet0/16    yes            unlimited
```

16. Configuring 802.1X Authentication

16.1. Overview of 802.1X Authentication

The IEEE802 LAN/WAN committee proposed the 802.1X protocol to solve the problem of wireless LAN network security.Later, the 802.1X protocol was widely used in Ethernet as a common access control mechanism for LAN ports, mainly to solve the problems of authentication and security in Ethernet.

The 802.1X protocol is a port based network access control protocol."Port-based network access control" means that, at the port level of the LAN access device, the access to the network resources is controlled through authentication for the connected user equipment.

16.1.1. 802.1X Architecture

The 802.1X system is a typical Client/Server structure, as shown in Figure 3, including three entities: Client, Device and Authentication server.

Figure 3 802.1X Authentication System Architecture

- **A client is an entity on a local area network that is authenticated by the device on the other end of the link.The client is generally a user terminal device, and the user can initiate 802.1X authentication by starting the client software.The client must support EAPOL (Extensible Authentication Protocol over LAN).**
- **The device side is another entity on the local area network that authenticates connected clients.The device side is usually a network device that supports the 802.1X protocol. It provides the client with a port to access the LAN. The port can be a physical port or a logical port.**
- **The authentication server is an entity that provides authentication services for the device.The authentication server is used for user authentication, authorization and accounting, usually a RADIUS (Remote Authentication Dial-In User Service) server.**

16.1.2. 802.1X Authentication Method

The 802.1X authentication system uses EAP (Extensible Authentication Protocol) to realize the exchange of authentication information between the client, the device and the authentication server.

- **Between the client and the device, the EAP protocol packets use the EAPOL encapsulation format and are directly carried in the LAN environment.**
- **There are two ways to exchange information between the device and the RADIUS server.One is that the EAP protocol packet is relayed by the device, and is carried in the RADIUS protocol using the EAPOR (EAP over RADIUS) encapsulation format; the other is that the EAP protocol packet is terminated by the device. Packets with the PAP (Password**

Authentication Protocol) or CHAP (Challenge Handshake Authentication Protocol) attribute attribute interact with the RADIUS server for authentication.

16.1.3. 802.1X Basic Concepts

16.1.3.1. Controlled/Uncontrolled Port

The device side provides a port for the client to access the LAN. This port is divided into two logical ports: a controlled port and an uncontrolled port.Any frame arriving at this port is visible on both controlled and uncontrolled ports.

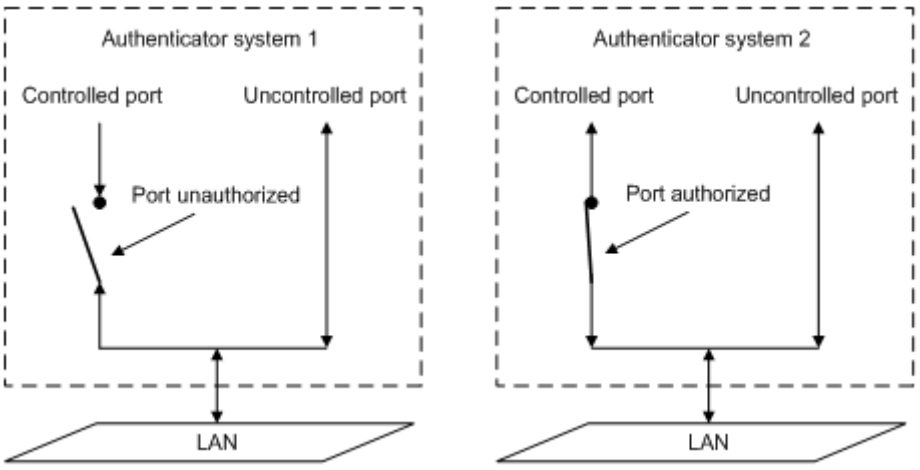
- **The uncontrolled port is always in a two-way connection state and is mainly used to transmit EAPOL protocol frames to ensure that the client can always send or receive authentication packets.**
- **The controlled port is in a bidirectional connection state in the authorized state and is used to transmit service packets; in the unauthorized state, it is forbidden to receive any packets from the client.**

16.1.3.2. Authorized/Unauthorized Status

The device uses the authentication server to authenticate the client that needs to access the LAN, and controls the authorization/unauthorized status of the controlled port according to the authentication result (Accept or Reject).

Figure 4 Shows the effect of different authorization states on the controlled port on packets passing through this port. The figure compares the port status of two 802.1X authentication systems. The controlled port of system 1 is in an unauthorized state (equivalent to opening the port switch), and the controlled port of system 2 is in an authorized state (equivalent to closing the port switch).

Figure 4 Effects of Authorization Status on Controlled Ports



The user can control the authorization status of the port through the access control mode configured under the port.The port supports the following three access control modes:

- **Forced authorization mode (authorized-force): indicates that the port is always in an authorized state, allowing users to access network resources without authorization.**
- **Force unauthorized mode unauthorized-force): Indicates that the port is always in an unauthorized state and does not allow users to authenticate.The device does not provide authentication services for clients accessing through this port.**

- **Auto-identification mode (auto): indicates that the initial state of the port is an unauthorized state, only EAPOL packets are allowed to send and receive, and users are not allowed to access network resources; If the authentication is passed, the port switches to the authorized state, allowing the user to access network resources.This is also the most common case.**

16.1.3.3. Controlled Direction

In the unauthorized state, the controlled port can be set as one-way controlled and two-way controlled.

- **When two-way control is implemented, the transmission and reception of frames are prohibited;**
- **When unidirectional control is implemented, receiving frames from the client is prohibited, but sending frames to the client is allowed.**

16.1.4. Authentication process for 802.1X

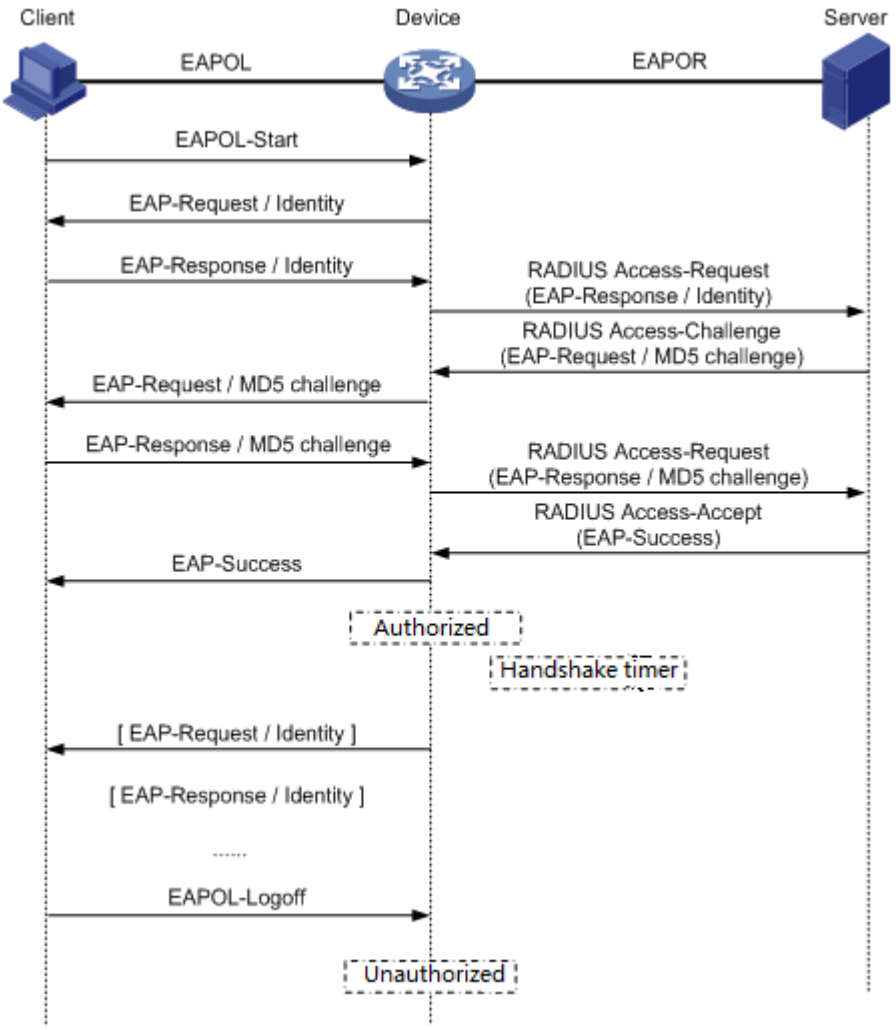
The 802.1X system supports EAP relay mode and EAP termination mode to interact with the remote RADIUS server to complete authentication.The following descriptions of the two authentication methods take the client's initiative to initiate authentication as an example.

16.1.4.1. EAP Relay Mode

This method is specified by the IEEE 802.1X standard, and EAP (Extensible Authentication Protocol) is carried in other high-level protocols, such as EAP over RADIUS, so that the extensible authentication protocol packets can reach the authentication server through complex networks. Generally speaking, the EAP relay mode requires the RADIUS server to support EAP attributes: EAP-Message and Message-Authenticator, which are used to encapsulate EAP packets and protect RADIUS packets carrying EAP-Message respectively.

The following takes EAP-MD5 as an example to introduce the basic business process, as shown in Figure5

Figure5 IEEE 802.1X EAP relay business process of authentication system



The authentication process is as follows:

1) When the user needs to access the network, open the 802.1X client program, enter the username and password that have been applied and registered, and initiate a connection request (EAPOL-Start message).At this point, the client program will send a message requesting authentication to the device to start an authentication process.

2) After receiving the data frame requesting authentication, the device will send a request frame (EAP-Request/Identity message) to request the user's client program to send the entered username.

3) The client program responds to the request from the device and sends the username information to the device through a data frame (EAP-Response/Identity message).The device sends the data frame sent by the client through packet processing (RADIUS Access-Request message) to the authentication server for processing.

4) After receiving the username information forwarded by the device, the RADIUS server compares the information with the username table in the database, finds the password information corresponding to the username, and encrypts it with a randomly generated encrypted word. , and also send this encrypted word to the device through the RADIUS Access-Challenge message, and the device forwards it to the client program.

5) After receiving the encrypted word (EAP-Request/MD5 Challenge message) from the device, the client program uses the encrypted word to encrypt the password part (this encryption algorithm is usually irreversible) , generate an EAP-Response/MD5 Challenge packet, and send it to the authentication server through the device.

6) The RADIUS server compares the received encrypted password information (RADIUS Access-Request message) with the local encrypted password information. If they are the same, the user is considered to be a legitimate user, and the authentication is passed. messages (RADIUS Access-Accept packets and EAP-Success packets).

7) After receiving the authentication message, the device changes the port to the authorized state, allowing users to access the network through the port.During this period, the device will monitor the user's online status by periodically sending handshake messages to the client.By default, if the two handshake request packets are not answered by the client, the device will log the user offline, preventing the user from going offline due to abnormal reasons and the device cannot sense it.

8) The client can also send an EAPOL-Logoff message to the device to actively request to log off.The device changes the port status from authorized to unauthorized, and sends an EAP-Failure packet to the client.

16.2. Configuring

- Enabling/disabling 802.1X Authentication Globally

Command	SWITCH(config)# dot1x enable SWITCH(config)#no dot1x enable
Description	Enable and disable the 802.1X function globally.

- Enabling/disabling 802.1X authentication on the Interface

Command	SWITCH(config-if)# dot1x port-control auto SWITCH(config-if)#no dot1x port-control auto
Description	The port enables or disables the 802.1X function.

- Configuring RADIUS Server

Command	SWITCH(config)# radius-server host A.B.C.D auth-port <0-65535> acct-port <0-65535> key WORD SWITCH(config)#no radius-server host A.B.C.D
Description	Configure authentication server information. The default authentication port is 1812 and the accounting port is 1813. Please ensure that the RADIUS server and the device management address communicate with each other.

- Configuring EAPOL Protocol Version Number

Command	SWITCH(config-if)# dot1x protocol-version <1-2> SWITCH(config-if)#no dot1x protocol-version
Description	Configure the version number of the EAPOL protocol on the specified port.

	Optional configuration, default is 2.

- Configuring Authentication Silent Time

Command	SWITCH(config-if)# dot1x quiet-period <1-65535> SWITCH(config-if)#no dot1x quiet-period
Description	Configure the hold time of the HELD state. Optional configuration, the unit is seconds, the default is 60.

- Configuring the Re-authentication Function

Command	SWITCH(config-if)# dot1x reauthentication SWITCH(config-if)#no dot1x reauthentication
Description	The re-authentication function is enabled on the configuration port. Optional configuration, disabled by default.

- Configuring the Maximum Number of Re-authentications

Command	SWITCH(config-if)# dot1x reauthMax <1-10> SWITCH(config-if)#no dot1x reauthMax
Description	Configure the maximum number of times for port re-authentication. If the number of re-authentication requests exceeds the limit and there is no response, the port becomes unauthorized. Optional configuration, default 2 times.

- Configuring to Enable key Transfer Capability

Command	SWITCH(config-if)# dot1x keytxenabled { disable | enable}
Description	Configure the port key transfer function. Optional, disabled by default.

- Configuring Timer Timeout

Command	SWITCH(config-if)# dot1x timeout {re-authperiod <1-4294967295> | server-timeout <1-65535> | supp-timeout <1-65535> | tx-period <1-65535>} SWITCH(config-if)#no dot1x timeout {re-authperiod | server-timeout | supp-timeout | tx-period}
Description	Configure the port timer time. Optional configuration, the default re-authentication period is 3600 seconds, the server timeout is 30 seconds, the client authentication timeout is 30 seconds, and the client request timeout is 30 seconds.

- **Enabling/disabling MAC Authentication Globally**

Command	**SWITCH(config)# mac-auth enable** **SWITCH(config)#no mac-auth enable**
Description	**Enable or disable the MAC authentication function globally.**

- **Enabling/disabling MAC Authentication on the Interface**

Command	**SWITCH(config-if)# mac-auth {enable | disable}**
Description	**The port enables or disables the MAC authentication function.**

- **Enabling/disabling MAC Authentication Dynamic VLAN Delivery on the Interface**

Command	**SWITCH(config-if)# mac-auth dynamic-vlan-creation {enable | disable}**
Description	**The port enables or disables dynamic VLAN delivery of MAC authentication.** **The current version is not supported.**

- **Configuring MAC Authentication Failure Handling**

Command	**SWITCH(config-if)# mac-auth auth-fail-action {drop-traffic | restrict-vlan <2-4094>}**
Description	**Configure the behavior of MAC authentication failure.** **Optional configuration, default is drop-traffic: drop traffic.** **The current version is not supported.**

- **Configuring RADIUS Server Death Time**

Command	**SWITCH(config)# radius-server deadtime <0-1440>** **SWITCH(config)# no radius-server deadtime**
Description	**Configure the RADIUS server death time.During the authentication process, the dead server will be automatically skipped, and the non-dead server will be selected for authentication.** **Optional configuration, the default is 0 minutes.**

- **Configuring RADIUS Server Default Key**

Command	**SWITCH(config)# radius-server key STRING** **SWITCH(config)# no radius-server key**
Description	**Configure the RADIUS server default key.** **Optional configuration.**

- **Configuring RADIUS Server Retransmission Times**

Command	**SWITCH(config)# radius-server retransmit <1-100>** **SWITCH(config)# no radius-server retransmit**
Description	**Configure the RADIUS server retransmission times.** **Optional configuration, the default is 3 times.**

- **Configuring RADIUS Server Timeout**

Command	**SWITCH(config)# radius-server timeout <1- 60>** **SWITCH(config)# no radius-server timeout**
Description	**Configure the RADIUS server timeout period.** **Optional configuration, the default is 5 seconds.**

16.3. Examples

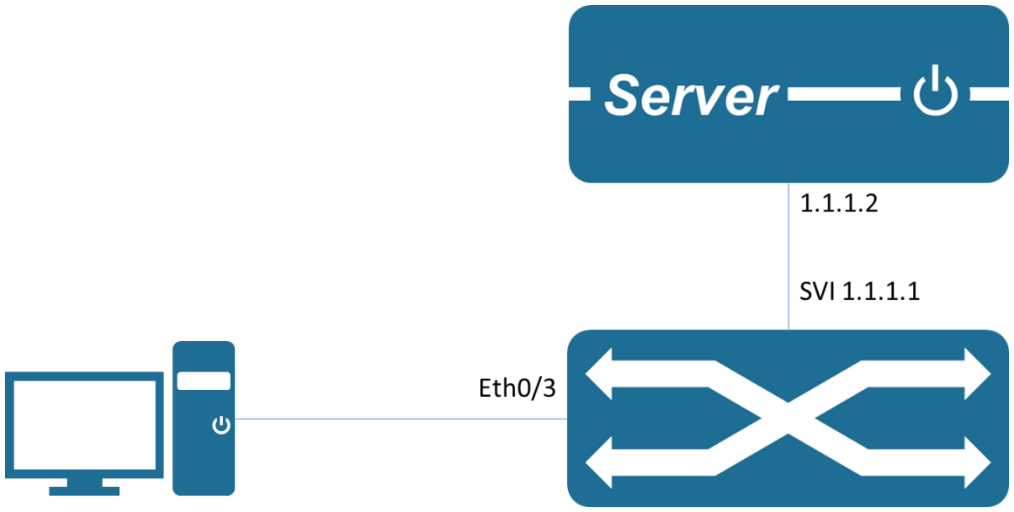
16.3.1. 802.1X Port Authentication Scenario

1) Requirement

- **Requires authentication of access users on port GigabitEthernet0/3 to control their access to the Internet.**
- **RADIUS server group IP address 1.1.1.2.**
- **Set the shared key to be used when the system exchanges packets with the RADIUS server as name.**

2) Network Diagram

Figure 6 802.1X Typical network diagram for 802.1x authentication



3) Typical configuration example

Device side:

```
SWITCH(config)#dot1x enable
SWITCH(config)#interface gigabitEthernet0/3
SWITCH(config-if)#dot1x port-control auto
```

```
SWITCH(config-if)#exit
SWITCH(config)#radius-server host 1.1.1.2 key name
```

Server:

Configure NAS authentication device 1.1.1.1 and communication key name.

Add user account test password test.

The corresponding authentication method needs to be supported, such as EAP-MSCHAPv2

Client:

Enable 802.1X authentication client and log in with account test.

The corresponding authentication method needs to be supported, such as the EAP-MSCHAPv2 method.

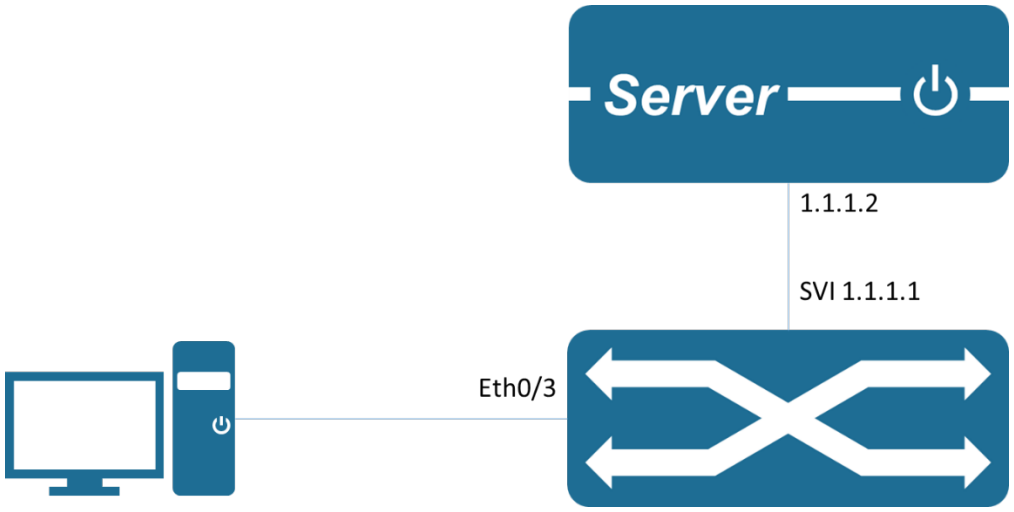
16.3.2. MAC Authentication Scenario

1) Requirement

- **Requires authentication of access users on port GigabitEthernet0/3 to control their access to the Internet.**
- **RADIUS server group IP address 1.1.1.2.**
- **Set the shared key when the system and the RADIUS server exchange messages as name.**

2) Network Diagram

Figure 7 Typical network diagram for MAC authentication



3) Typical configuration example

Device side:

```
SWITCH(config)# mac-auth enable
SWITCH(config)#interface gigabitEthernet0/3
SWITCH(config-if)#mac-auth enable
SWITCH(config-if)#exit
SWITCH(config)#radius-server host 1.1.1.2 key name
```

Server:

Configure NAS authentication device 1.1.1.1 and communication key name.

Add the client MAC address as the user account and password to the user database.

Client:

Enable the 802.1X authentication client and log in with any account.

16.4. Display Information

- **Show 802.1X Port Authentication Information**

```
SWITCH#show dot1x all
802.1X Port-Based Authentication Enabled
RADIUS server address: 1.1.1.2:1812
Next radius message id: 0
RADIUS client address: not configured

802.1X info for interface gigabitEthernet0/6
portEnabled: true - portControl: Auto
 portStatus: Unauthorized - currentId: 1
protocol version: 2
reAuthenticate: disabled
reAuthPeriod: 3600
 abort:F fail:F start:F timeout:F success:F
 PAE: state: Connecting - portMode: Auto
 PAE: reAuthCount: 1 - rxRespId: 0
 PAE: quietPeriod: 60 - reauthMax: 2 - txPeriod: 30
BE: state: Idle - reqCount: 0 - idFromServer: 0
BE: suppTimeout: 30 - serverTimeout: 30
 CD: adminControlledDirections: in - operControlledDirections: in
CD: bridgeDetected: false
KR: rxKey: false
KT: keyAvailable: false - keyTxEnabled: false
```

- **Display MAC Authentication Information**

```
SWITCH#show bridge
 Bridge CVLAN SVLAN BVLAN Port MAC Address FWD Time-out
 ---------+------+------+------+-----------+-- ---------------+-----+---------+
```

17. Configuring Port Security

17.1. Overview of Port Security

You can use port security to block input to an Fast Ethernet, or Gigabit Ethernet port when the MAC address of the station attempting to access the port is different from any of the MAC addresses that are specified for that port. Alternatively, you can use port security to filter traffic that is destined to or received from a specific host that is based on the host MAC address.

The maximum number of MAC addresses that you can allocate for each port depends on your network configuration. After you allocate the maximum number of MAC addresses on a port, you can either specify the secure MAC address for the port manually or have the port dynamically configure the MAC address of the connected devices.

When a secure port receives a packet, the source MAC address of the packet is compared to the list of secure source addresses that were manually configured or autoconfigured (learned) on the port. If a MAC address of a device that is attached to the port differs from the list of secure addresses, A violation occurs. Users can set a port to the following two modes to handle a security violation:

Restrict: Drops all packets from insecure hosts, but remains enabled, until the MAC of the host aged out dynamic. You can manually shutdown and no-shutdown the interface to recover from violation.

Shutdown: The shutdown mode option allows you to specify whether the port is to be permanently disabled or disabled for only a specified time. The default is for the port to shut down permanently. You can manually shutdown and no-shutdown the interface to recover from violation.

If you want to convert dynamic security users to static security users, you can enable the sticky function on the port. If the sticky function is enabled, the dynamic users learned on the port will exist as static users. If the configuration is saved, it will still exist after the device restarts.

Note

- ✧ **Only support L2 port for port security, such as physical port and L2 AP port.**
- ✧ **Only supports configuring port security function in access mode.**
- ✧ **Do not support AP member port configuration port security function.**
- ✧ **The destination port of the SPAN does not support the port security function.**
- ✧ **Does not support the port security function on ports that have been configured with static MAC addresses.**

17.2. Configuring

- **Enable Port Security**

Command	**SWITCH(config-if)#switchport port-security** **SWITCH(config-if)#no switchport port-security**
Description	**Enable Port Security on the interface.**

- **Setting the Max Number of Security Mac-address**

Command	**SWITCH(config-if)#switchport port-security maximum VALUE** **SWITCH(config-if)#no switchport port-security maximum**
Description	**The default maximum number of secure addresses is 1**

	VALUE range from 1 to 1024.

- Entering a Serurity Mac-address

Command	SWITCH(config-if)#switchport port-security mac-address MAC_ADDR SWITCH(config-if)#no switchport port-security mac-address MAC_ADDR
Description	Enters a secure MAC address for the interface. If you configure fewer secure MAC addresses than the maximum, the remaining MAC addresses will be dynamically learned.

- Enable sticky

Command	SWITCH(config-if)# switchport port-security mac-address sticky SWITCH(config-if)#no switchport port-security mac-address sticky
Description	Enable sticky learning on the interface.

- Configuring Port Security Aging

Command	SWITCH(config-if)#switchport port-security aging time MINUTES SWITCH(config-if)#no switchport port-security aging time
Description	Sets the aging time for the secure port. Valid range for aging_time is from 0 to 1440 minutes. If the time is equal to 0, aging is disabled for this port.

- Enable Port Security Aging Static Mac-address

Command	SWITCH(config-if)# switchport port-security aging static SWITCH(config-if)#no switchport port-security aging static
Description	enables aging for statically configured secure addresses on this port.

- Setting the Violation Mode

Command	SWITCH(config-if)# switchport port-security violation { strict | shutdown } SWITCH(config-if)#no switchport port-security violation
Description	Sets the violation mode, the action to be taken when a security violation is detected, as one of these: Restric: A port security violation restricts data and causes the SecurityViolation counter to increment and send an SNMP trap notification. Shutdown: The interface is error-disabled when a security violation occurs. You can manually reenable the by entering the shutdown and no shut down commands. When a secure port is in the error-disabled state, it will recover after errdisable recovery time.

17.3. Examples

Example 1：This is an example of Port Security typical application. Port Security is enabled on the interface gigabitEthernet0/1, the MAX secure Mac-address of the interface gigabitEthernet0/1 is 3, and we enter 3 secure Mac-address on the interface. When the interface gigabitEthernet0/1 receives a packet, If the SRC MAC-address of the packet differs from the list of secure Mac-addresses, the packet will be dropped.

```
SWITCH(config-if)#switchport port-security
SWITCH(config-if)#switchport port-security maximum 3
SWITCH(config-if)#switchport port-security mac-address 0001.0001.0001
SWITCH(config-if)#switchport port-security mac-address 0001.0001.0002
SWITCH(config-if)#switchport port-security mac-address 0001.0001.0003
```

17.4. Display Information

- Display Interfaces Port Security Brief

```
SWITCH#show port-security brief
interface    mac-address       mac-address       violation      violation
             maxinum             count             count        action
-------------------------------------------------------------------------------------------------
GiE0/1       10                  3                 0              shutdown
GiE0/2       1                   0                 0              restrict
GiE0/3       1                   0                 0              restrict
GiE0/4       1                   0                 0              restrict
GiE0/5       1                   0                 0              restrict
GiE0/6       1                   0                 0              restrict
GiE0/7       1                   0                 0              restrict
GiE0/8       1                   0                 0              restrict
```

- Display an Interface Port Security Information

```
SWITCH#show port-security interface gigabitEthernet0/1
Port Security                  : Enabled
Maimum MAC Addresses       : 10
Violation Mode                : Shutdown
Aging Time(mins)              : 10
Aging static                   : Enabled
Total MAC Addresses          : 3
Configured MAC Addresses    : 2
Security Violation Count       : 0
Last Violate Address           : --
```

- Display Secure Mac-address

```
SWITCH#show port-security Mac-address
interface    vlan      mac-address           type          left-time(min)
-------------------------------------------------------------------------------
GiE0/1       1         0001.0002.0004        static        10
GiE0/1       1         0001.0002.0003        static        10
GiE0/1       1         000e.c6c1.3a03        dynamic       10
```

- Display an Interface Secure Mac-address

```
SWITCH#show port-security mac-address interface gigabitEthernet0/1
interface    vlan      mac-address           type          left-time(min)
-------------------------------------------------------------------------------
GiE0/1       1         0001.0002.0004        static        10
```

GiE0/1	1	0001.0002.0003	static	10
GiE0/1	1	000e.c6c1.3a03	dynamic	10

18. Configuring Ip Source Guard

18.1. Overview of Ip Source Guard

IP Source Guard is a per-interface traffic filter that permits IP traffic only when the IP address and MAC address of each packet matches one of two sources of IP and MAC address bindings: Entries in the Dynamic Host Configuration Protocol (DHCP) snooping binding table; Static IP source entries that you configure.

Filtering on trusted IP and MAC address bindings helps prevent spoofing attacks, in which an attacker uses the IP address of a valid host to gain unauthorized network access.

Note

- ✧ **Only support L2 port for port security, such as physical port and L2 AP port.**
- ✧ **Do not support AP member port configuration port security function.**

18.2. Configuring

- **Enabling Ip Source Guard**

Command	**SWITCH(config-if)#ip verify source** **SWITCH(config-if)#no ip verify source**
Description	**Enables IP Source Guard on the interface.**

- **Configuring Static Ip Source Binding Entry**

Command	**SWITCH(config)# ip source binding XXXX.XXXX.XXXX vlan VALUE A.B.C.D interface IFNAME** **SWITCH(config)#no ip source binding XXXX.XXXX.XXXX vlan VALUE A.B.C.D interface IFNAME**
Description	**Creates a static IP source binding entry for the current interface.** **Example:** **SWITCH(config)# ip source binding 0001.0001.0001 vlan 1 1.1.1.10 interface gigabitEthernet0/1** **A single port can be configured with a maximum of 128 entries.**

18.3. Examples

Example 1: This is an example of Ip Source Guard typical application. Ip Source Guard is enabled on the interface gigabitEthernet0/1, and we enter 3 static binding entrys on the interface.

When the interface gigabitEthernet0/1 receives a packet, If the IP address and the MAC address of the packet differs from the list of static entrys, the packet will be dropped.

```
SWITCH(config)#interface gigabitEthernet0/1
SWITCH(config-if)#ip verify source
SWITCH(config)#ip source binding 0001.0001.0001 vlan 1 1.1.1.10 interface gigabitEthernet0/1
SWITCH(config)#ip source binding 0001.0001.0002 vlan 1 1.1.1.11 interface gigabitEthernet0/1
SWITCH(config)#ip source binding 0001.0001.0003 vlan 1 1.1.1.12 interface gigabitEthernet0/1
```

18.4. Display Information

- **Display Ip Verify Source Binding Rules**

```
SWITCH#show ip verify source
interface   Filter-type   Filter       IP-address       Mac-address    vlan
------------------------------------------------------------------------
GiE0/1      Ip            Permit     1.1.1.1          0001.0001.0001 1
GiE0/1      Ip            Deny       All              All            All
GiE0/2      Ip            Deny       All              All            All
```

- **Display Ip Verify Source Binding Entrys on the Interface**

```
SWITCH#show ip verify source interface gigabitEthernet0/1
interface   Filter-type   Filter       IP-address       Mac-address    vlan
-----------------------------------------------------------------------------------------------
GiE0/1      Ip            Permit     1.1.1.1          0001.0001.0001 1
GiE0/1      Ip            Deny       All              All            All
```

- **Display Ip Source Binding Entrys**

```
SWITCH#show ip source binding
interface   vlan   IP-address       Mac-address      Lease      Type
-----------------------------------------------------------------------------------------------
GiE0/1      1      1.1.1.1          0001.0001.0001 infinite     static
GiE0/2      1      1.1.2.1          0001.0002.0001 infinite     static
```

- **Display Ip Source Binding Entrys on the Interface**

```
SWITCH#show ip source binding interface gigabitEthernet0/1
interface   vlan   IP-address       Mac-address      Lease      Type
-----------------------------------------------------------------------------------------------
GiE0/1      1      1.1.1.1          0001.0001.0001 infinite     static
```

19. Configuring Arp-check

19.1. Overview of Arp-check

Arp-check is a per-interface traffic filter that permits ARP traffic only when the IP address and MAC address of each packet matches one of two sources of IP and MAC address bindings: Entries in the Dynamic Host Configuration Protocol (DHCP) snooping binding table; Static IP source entries that you configure.

Filtering on trusted IP and MAC address bindings helps prevent spoofing attacks, in which an attacker uses the IP address of a valid host to gain unauthorized network access.

Note

- ✧ **Only support L2 port for port security, such as physical port and L2 AP port.**
- ✧ **Do not support AP member port configuration port security function.**

19.2. Configuring

- **Enabling Arp-check on the Interface**

Command	**SWITCH(config-if)#arp-check** **SWITCH(config-if)#no arp-check**
Description	**Enables Arp-check on the interface.**

19.3. Examples

Example 1：This is an example of Arp-check typical application. Arp-check is enabled on the interface gigabitEthernet0/1, and we enter 3 static binding entrys on the interface.

When the interface gigabitEthernet0/1 receives a ARP packet, If the IP address and the MAC address of the packet differs from the list of static entrys, the packet will be dropped.

```
SWITCH(config)#interface gigabitEthernet0/1
SWITCH(config-if)#ip verify source
SWITCH(config-if)#arp-check
SWITCH(config)#ip source binding 0001.0001.0001 vlan 1 1.1.1.10 interface gigabitEthernet0/1
SWITCH(config)#ip source binding 0001.0001.0002 vlan 1 1.1.1.11 interface gigabitEthernet0/1
SWITCH(config)#ip source binding 0001.0001.0003 vlan 1 1.1.1.12 interface gigabitEthernet0/1
```

20. Configuring SNMP Network Management

20.1. Overview of SNMP Network Management

SNMP is the abbreviation of Simple Network Management Protocol, which became a network management standard RFC1157 in August 1988.Up to now, due to the support of this protocol by many manufacturers, SNMP has become the de facto network management standard and is suitable for use in the interconnected environment of multi-manufacturer systems.

Using the SNMP protocol, network administrators can perform information query, network configuration, fault location, and capacity planning for nodes on the network. Network monitoring and management are the basic functions of SNMP.

Currently the following versions of SNMP exist:

SNMPv1: The first official version of the Simple Network Management Protocol, defined in RFC1157.

SNMPv2C: Community-Based SNMPv2 Management Architecture, defined in RFC1901.

SNMPv3: By authenticating and encrypting data, it provides the following security features:

- **Make sure that data is not tampered with during transmission.**
- **Make sure the data is sent from a legitimate data source.**
- **Encrypt messages to ensure data confidentiality.**

20.2. Configuring

- **Configuring Communication Community Words**

Command	**SWITCH(config)# snmp-server community COMMUNITY { ro | }** **SWITCH(config)# no snmp -server community COMMUNITY**
Description	**Configure/delete SNMP communication community word.** **ro : read-only identifier, configure the community word as a community word with only read permission; the default configuration is a community word with both read and write permissions.** **Supports configuring multiple community characters at the same time.**

- **Configuring SNMPv3 Views**

Command	**SWITCH(config)# snmp -server view NAME {include | exclude} OID** **SWITCH(config)# no snmp -server view name**
Description	**Configure/delete SNMPv3 views;** **Supports configuring multiple views at the same time, and supports configuring multiple rules for a single view;** **The system has all and none views by default and cannot be modified**

- **Configuring SNMP Groups**

Command	**SWITCH(config)# snmp -server group NAME {v3 | } { noAuthNoPriv | authNoPriv | authPriv } read RVIEW write WVIEW** **SWITCH(config)# snmp -server group NAME {v1 | v2c} read RVIEW write WVIEW** **SWITCH(config)# no snmp -server group name**

Description	**configure/delete SNMP groups;** **Support to configure multiple groups at the same time;** **create group information in order to be compatible with the old configuration when configuring the community , usually without additional attention**

- **Configuring SNMPv3 Users**

Command	**SWITCH(config)# snmp -server user NAME group GROUPNAME auth {md5 | sha} {AUTHPASS} priv { aes | des} PRIVPASS** **SWITCH(config)# no snmp -server user name**
Description	**configure/delete SNMP users;** **Support to configure multiple users at the same time;**

- **Configuring SNMP Host Notification Server**

Command	**SWITCH(config)# snmp -server host IPADDR {informs | traps} {v3 |} { noAuthNoPriv | authNoPriv | authPriv } user NAME** **SWITCH(config)# snmp -server host IPADDR {informs | traps} {v1 | v2c} community NAME** **SWITCH(config)# no snmp -server hostname _**
Description	**configure/delete SNMP server;** **Support to configure multiple servers at the same time;**

20.3. Examples

Requirements: The IP address of the SNMP network management server is 2.2.2.2, and the read-write communication group word is unified as public.

- **Enter the global configuration mode configuration:**

```
SWITCH#
SWITCH#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
SWITCH( config)#snmp-server community public
SWITCH( config)#snmp-server 2.2.2.2 community public
SWITCH( config)#
```

Case requirements: The IP address of the SNMP network management server is 2.2.2.2, SNMPv3 is used, the user test password is 12345678, the encryption key is 87654321; the authentication algorithm MD5, the encryption algorithm DES

```
SWITCH#
SWITCH#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
SWITCH( config)# snmp -server group test v3 authPriv read all write all
SWITCH( config)# snmp -server user test group test auth MD5 12345678 priv DES 87654321
SWITCH( config)# snmp -server host 2.2.2.2 informs v3 authPriv user test
```

21. Configuring RMON

21.1. Overview of RMON

SNMP is the most widely used network management protocol in the Internet. The collection and statistics of network communication information are realized through the agent software embedded in the device. The management software obtains the information by sending query signals to the MIB of the agent through polling, and realizes the management of the network through the obtained information. The management software sends queries to the proxy MIB by means of a query to obtain this information and manages the network through the information obtained. Although the MIB counter records the sum of the statistics, it does not allow historical analysis of the day-to-day communication situation. In order to provide a comprehensive view of the flow and traffic changes over the day, web hosting software requires continuous poll to analyze the status of the network through the information available.

Polling with SNMP has two distinct disadvantages:

- **Occupies a lot of network resources. In a large-scale network, a large number of network communication packets will be generated by polling, which will cause network congestion and even cause network congestion. Therefore, SNMP is not suitable for managing large-scale networks. , not suitable for recycling large amounts of data, such as routing table information.**
- **The task of collecting data in SNMP polling is done by the network administrator through the network management software. If the network administrator monitors more than 3 network segments, it may occur that the network is overloaded due to the heavy burden. A situation in which a manager is unable to complete a task.**

In order to improve the availability of management information, reduce the burden of management stations, and meet the needs of network administrators to monitor the performance of multiple network segments, IETF developed RMON to solve the limitations of SNMP in the expanding distributed interconnection. The monitoring function of the data traffic of the network segment and even the entire network. The following are the features of RMON:

- **SNMP is the basis for the realization of RMON, and RMON is the enhancement of SNMP functions.**

  RMON is implemented based on the SNMP architecture and is compatible with the existing SNMP framework. It is still composed of the network management workstation NMS and the agent running on each network device. Since RMON does not use another set of mechanisms, which are shared between NMS and SNMP, network managers do not need additional learning and are therefore simpler to achieve.

- **RMON enables SNMP to monitor remote network devices more effectively and proactively, and provides an efficient means for monitoring the operation of the network.**

  The RMON protocol stipulates that the managed device can automatically send Trap information when the alarm threshold is reached, so the management device does not need to obtain the value of the MIB variable through polling multiple times for comparison. The purpose of efficiently managing large interconnected networks.

RMON allows multiple monitors, and monitors can collect data in the following two ways:

- **Through a dedicated RMON Probe (detector), the NMS directly obtains management information from the RMON Probe and controls network resources. In this way, all the information of the RMON MIB can be obtained.**
- **Embed RMON Agent directly into network devices, making them network devices with RMON Probe function. The NMS uses SNMP to exchange data information with it and collect network management information. This method is limited by device resources and generally cannot obtain all the data of the RMON MIB. Basically, only four groups (alarms, events, history, and statistics) are collected.**

Our equipment adopts the second method and implements the RMON Agent function on the equipment. Through this function, the management device can obtain information such as overall traffic, error statistics, and performance statistics on the network segment connected to the managed network device interface, thereby realizing network monitoring.

21.2. Rationale

Before configuring RMON, you need to understand the basic concepts of the four groups of statistics, history, alarms, and events defined by the RMON specification.

RMON features

RMON mainly implements statistics and alarm functions, and is used for remote monitoring and management of managed devices by management devices in the network.

The RMON statistics function can be implemented through the RMON statistics group or the RMON history group, which are divided into Ethernet statistics functions and historical statistics functions.

- **Historical statistics function (corresponding to the historical group in the RMON MIB): The system periodically samples and collects network status statistics and stores them for subsequent processing. The system will periodically collect statistics on various traffic information, including bandwidth utilization, number of error packets and total number of packets.**
- **Ethernet statistics function (corresponding to the statistics group in the RMON MIB): The system collects basic statistics about each network being monitored. The system will continuously count the traffic of a certain network segment and the distribution of various types of packets, or the number of error frames of various types, the number of collisions, etc. The system will keep track of all traffic information on a regular basis, including bandwidth utilization, erroneous packages and total packages.**

The RMON alarm function includes the event definition function and the alarm threshold setting function. The RMON alarm function is realized by the combination of these two sub-functions.

- **Event definition function (corresponding to the event group in the RMON MIB): The event group controls the events and prompts from the device, and provides all events generated by the RMON Agent. When an event occurs, it can record logs or send Trap to the network management station.**
- **Set the alarm threshold function (corresponding to the alarm group in the RMON MIB): The system monitors the specified alarm variable (the OID corresponding to any alarm object). After the user pre-defines a set of thresholds and sampling time for the specified alarm, the system will obtain the value of the specified alarm variable according to the defined time period. When the value of the alarm variable is greater than or equal to the upper threshold, an upper alarm event will**

be triggered; When the value of the variable is less than or equal to the lower limit threshold, a lower limit alarm event is triggered. RMON Agent will record the above monitored status as a log or send Trap to the network management station.

Multiple RMON groups are defined in the RMON specification (RFC2819), and the device implements four groups of statistics, history, alarm, and events supported in the public MIB. These groups are introduced separately below.

- Statistics group

The statistics group specifies that the system will continuously collect statistics on various traffic information of the Ethernet interface, and store the statistical results in the Ethernet statistics table (etherStatsTable) for the management device to view at any time. Statistics include the number of network collisions, the number of CRC check error packets, the number of data packets that are too small (or too large), the number of broadcast and multicast packets, the number of bytes received, and the number of received packets.

After the statistics entry is successfully created on the specified interface, the statistics group collects statistics on the number of packets on the current interface, and the statistics result is a continuous accumulated value.

- History group

The history group periodically collects network status statistics and stores them for subsequent processing.

The history group contains two tables:

  - historyControlTable: It is mainly used to set control information such as sampling interval time.
  - etherHistoryTable: It is mainly used to store the historical data collected by the historical group on a regular basis for network status statistics, and to provide network administrators with historical data on network segment traffic, error packets, broadcast packets, utilization, and collision times and other statistical information.

- Event group

The event defined by the event group is used in the alarm group configuration item and the extended alarm group configuration item. When the monitoring object reaches the alarm condition, the event will be triggered. RMON event management is to add events to the specified row of the event table and define how the events are handled:

  - log: only send logs
  - trap: only send trap messages to NMS
  - log-trap: send both logs and trap messages to NMS
  - none: do nothing

- Alarm group

Alarm groups allow monitoring of a predefined set of thresholds for alarm variables (which can be arbitrary objects in the local MIB). After the user defines the alarm table item (alarmTable), the system will obtain the value of the monitored alarm variable according to the defined time period. When the value of the alarm variable is greater than or equal to the upper limit threshold, an upper limit alarm event will be triggered; If the value is less than or equal to the lower limit threshold, a lower limit alarm event is triggered, and the alarm management will perform corresponding processing according to the definition of the event.

21.3. Configuring

- Configuring Statistics Group

Command	**SWITCH(config)# rmon statistics <1-65535> interface IFNAME {owner OWNERNAME |}** **SWITCH(config-if)# no rmon statistics <1-65535>**
Description	**configure/delete statistics group.** **<1-65535>: Group index.** **IFNAME *:* interface name.** **OWNERNAME *:* owner information.**

- **Configuring History Group**

Command	**SWITCH(config)# rmon history <1-65535> interface IFNAME buckets <1-65535> interval <1-3600> {owner OWNERNAME |}** **SWITCH(config-if)# no rmon history <1-65535>**
Description	**configure/delete history group.** **<1-65535>: Group index.** **IFNAME *:* interface name.** **<1-65535>: History bucket size.** **<1-3600>: Recording period; the unit is seconds.** **OWNERNAME *:* owner information.**

- **Configuring Event Groups**

Command	**SWITCH(config)# rmon event <1-65535> {description DESCRIPTION |} {log | trap COMMUNITY | log-trap COMMUNITY | none} {owner OWNERNAME |}** **SWITCH(config-if)# no rmon event <1-65535>**
Description	**configure/delete event groups.** **<1-65535>: Group index.** **DESCRIPTION: Event description.** **COMMUNITY: Trap communication group word.** **OWNERNAME: owner information.**

- **Configuring an Alarm Group**

Command	**SWITCH(config)# rmon alarm <1-65535> object STRING <1-65535> {absolute | delta} rising-threshold <1-2147483645> <1-65535> falling-threshold <1-2147483645> <1-65535> {owner OWNERNAME |}** **SWITCH(config-if)# no rmon alarm <1-65535>**
Description	**Configure/delete alarm groups.** **<1-65535>: Group index.** **STRING: OID of alarm monitoring; for example, 1.3.6.1.2.1.2.2.1.10.1 indicates the number of bytes received by monitoring interface 1.** **<1-65535>: Monitoring period; the unit is seconds.** **<1-2147483645>: Rising Threshold.** **<1-65535>: Rising event index; corresponds to the index in the event group.** **<1-2147483645>: Falling Threshold.** **<1-65535>: Fall event index; corresponds to the index in the event group.**

	OWNERNAME: owner information.

- **Configuring the Upper Limit of Log Entries**

Command	**SWITCH(config)# rmon max-log <1-65535>** **SWITCH(config-if)# no rmon max-log**
Description	**Configure/reset the upper limit of log entries.** **<1-65535>: Number of entries.** **The log here refers to the log generated by the event group, not the system log.** **The default upper limit is 100; when the number of logs generated exceeds the limit of entries, the old logs will be deleted according to the generation time to maintain the upper limit.**

21.4. Examples

Requirements

The IP address of the SNMP network management server is 2.2.2.2, and the community word for read and write communication is public.

The network management server needs to query the traffic of port 1 of the device through rmon

The network management server needs to monitor the input traffic of port 1 of the device through rmon. The cycle is 10 seconds.

Once the number of input bytes changes by more than 1MB (1000000B), an alarm is triggered and a log is recorded.

Configuration steps

Initialize the network management configuration

```
SWITCH#
SWITCH#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
SWITCH(config)#snmp-server community public
SWITCH(config)#snmp-server 2.2.2.2 community public
SWITCH(config)#
```

Configure the rmon statistics group (the following rmon configurations can be configured on the NMS through the MIB)

SWITCH(config)# rmon statistics 1 interface gigabitEthernet0/1 owner abc

Configure rmon events and alarm groups (the following rmon configurations can be configured on the NMS through MIB)

```
SWITCH(config)# rmon event 1 log-trap public owner abc
SWITCH(config)# rmon alarm 1 object 1.3.6.1.2.1.2.2.1.10.1 10 delta rising-threshold 1000000 1
falling-threshold 1000000 1
```

21.5. Display Information

- **Show Event Group LSog**

```
SWITCH#show rmon log
event 1 log 226 time 2304 desc
event 1 log 227 time 2314 desc
event 1 log 228 time 2324 desc
```

```
event 1 log 229 time 2334 desc
event 1 log 230 time 2344 desc
event 1 log 231 time 2354 desc
event 1 log 232 time 2364 desc
event 1 log 233 time 2374 desc
......
```

22. Configuring AAA

22.1. Overview of AAA

AAA is the abbreviation of Authentication Authorization and Accounting, which provides for authentication, authorization and accounting function into the configuration of the consistency framework.

AAA provides the following services in a modular fashion:

- **Authentication: Verify whether the user can obtain access rights. Optionally use RADIUS protocol, TACACS+ protocol or Local (local) and so on. Identity authentication is a method of identifying a user's identity before allowing access to the network and network services.**
- **Authorization: Which services are available to authorized users. AAA authorization is achieved by defining a series of attribute pairs, these attribute pairs describe the operations that the user is authorized to perform. These attribute pairs can be stored on a network device or remotely on a secure server.**
- **Accounting: record the user's use of network resources. When AAA accounting is enabled, the network device starts to send user usage of network resources. Each accounting record is composed of attribute pairs and stored on a secure server. These records can be read and analyzed by special software, so as to realize accounting, statistics and tracking of users' use of network resources.**

Using AAA has the following advantages:

- **Flexibility and controllability.**
- **Scalability.**
- **Standardized Certification.**
- **Multiple backup systems.**

AAA has the following relevant standards:

RFC2865 Remote Authentication Dial In User Service (RADIUS). C. Rigney, S. Willens, A. Rubens, W. Simpson. June 2000. (Format: TXT, HTML).

RFC2866 RADIUS Accounting. C. Rigney. June 2000. (Format: TXT, HTML).

RFC8907 The Terminal Access Controller Access-Control System Plus (TACACS+) Protocol. T. Dahm, A. Ota, DC Medway Gash, D. Carrel, L. Grant. September 2020.

22.2. Configuring

- **Enabling/disabling AAA Function Globally**

Command	**SWITCH(config)# aaa new-model** **SWITCH(config)# no aaa new-model**
Description	**Globally enable or disable the AAA function.**

- **Configuring AAA Server Group**

Command	**SWITCH(config)# aaa group server (radius) (default| NAME)** **SWITCH(config) # aaa group server (tacacs +) (default| NAME)** **SWITCH(config)# no aaa group server (radius|tacacs +) (default| NAME)**
Description	**Server group configuration.** **Optional.** **By default there is no server group configuration and no server method is used.**

- **Configuring AAA Server**

Command	**SWITCH(config-gs-rad)# server ABCD (auth-port <1-65535> |) (acct-port <1-65535> |) (key STRING)** **SWITCH(config-gs-tac)# server ABCD (port <1-65535> |) (key STRING)** **SWITCH(config-gs-rad)# no server ABCD** **SWITCH(config-gs-tac)# no server ABCD**
Description	**server group mode .** **Configure RADIUS, TACACS + server information, including basic IP address, port information, shared key** **Optional.** **Note: Due to implementation restrictions, the current radius accounting port number is always the authentication port number + 1, and the configuration is invalid.**

- **Configuring Server Group Timeout**

Command	**SWITCH(config-gs-rad)# timeout <1-120>** **SWITCH(config-gs-tac)# timeout <1-120>** **SWITCH(config-gs-rad)# no timeout** **SWITCH(config-gs-tac)# no timeout**
Description	**server group mode .** **Configure the timeout period for servers in the group.** **Optional.**

- **Configuring Group Service Information Fields**

Command	**SWITCH(config-gs-tac)# service NAME** **SWITCH(config-gs-tac)# no service**
Description	**TACACS+ server group mode .** **Configure the service information in the group.** **Optional.**

- **Configuring AAA Method Information**

Command	**SWITCH(config)# aaa (authentication|authorization|accounting) (login|ssh|web|dot1x|command) default {group (radius|tacacs+|NAME)|local|none}** **SWITCH(config)#no aaa (authentication|authorization|accounting) (login|ssh|web|dot1x|command) default**
Description	**Global configuration mode.** **Configure AAA method information.** **Optional.Local authentication is used by default.** **Note: The username (such as admin) that exists on the machine also needs to be provided during the none authentication, otherwise an error may occur.**

- **Configuring Remote User Information**

Command	**SWITCH(config)# username NAME remote** **SWITCH(config)#no username NAME**
Description	**Global configuration mode.** **Configure remote user information.** **Optional.** **Note: If the login authentication of the remote method is configured, but the remote user information is not configured on the device side, it may cause the user to pass the authentication and be unable to use it normally due to the lack of the local environment!**

22.3. Examples

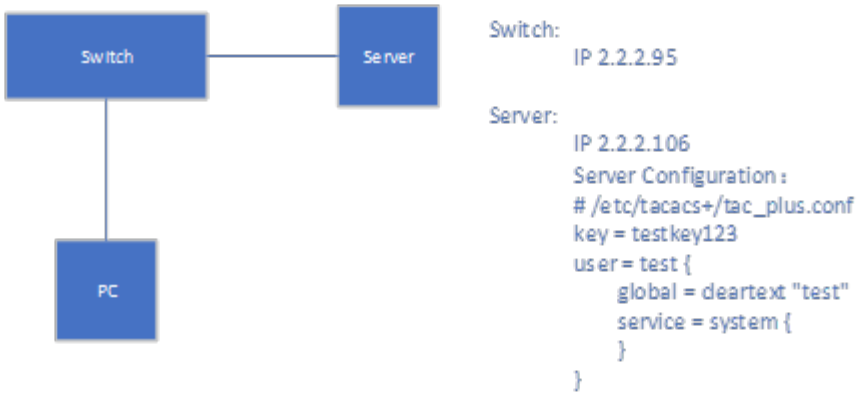
22.3.1. SSH Login Authentication Using Tacacs+ Method

1) Requirements

- **See the description of the network diagram**

4) Network diagram

Figure 8 Typical networking diagram for SSH through tacacs+ server authentication and accounting



Description: none

5) Typical configuration example

Switch:

```
SWITCH(config)# aaa new-model
SWITCH(config)# aaa group server tacacs+ default
SWITCH(config-gs-tac)# server 2.2.2.106 key testkey123
SWITCH(config-gs-tac)# exit
SWITCH(config)# aaa authentication ssh default group tacacs+
SWITCH(config)# aaa accounting ssh default group tacacs+
SWITCH(config)# username test remote
```

Device IP configuration and ssh configuration refer to the corresponding chapters in the configuration documentation, which are omitted here.

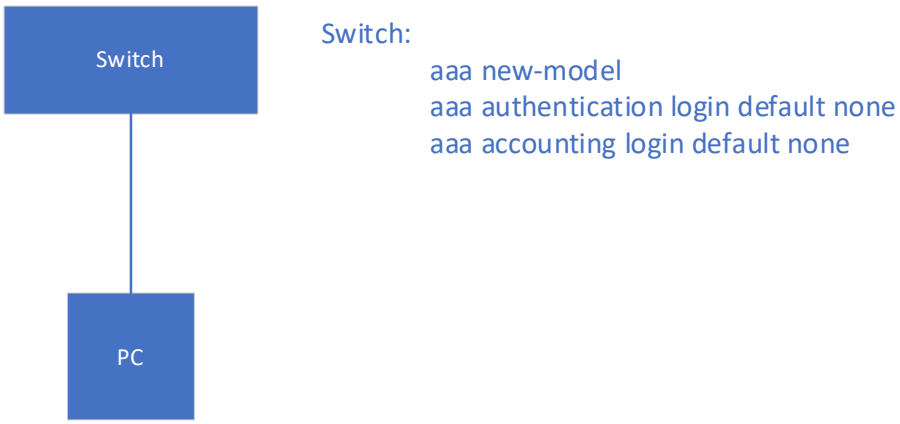
22.3.2. Use the None Method to Perform Serial Port Login

2) Requirements

- **See the description of the network diagram**

3) Network diagram

Figure9 Typical network diagram of serial port using none authentication and accounting



4) Typical configuration example

Refer to the network diagram

22.4. Display Information

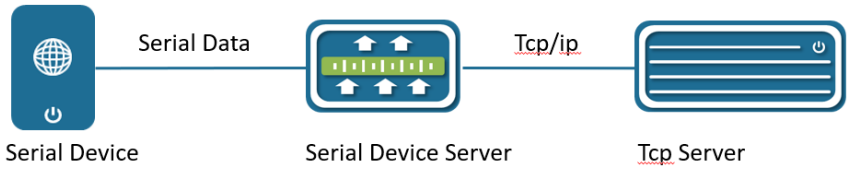
- **None**

23. Configuring Serial Device Server

23.1. Overview of Serial Device Server

The serial device server is used to connect serial devices to the Ethernet. The serial device server supports bidirectional conversion and transmission of network data and serial data.

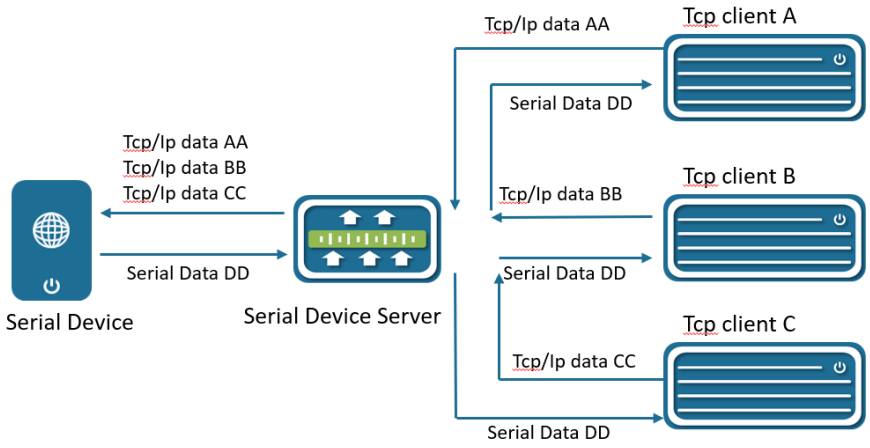
Serial device server work in tcp-client mode, as shown in figure below.



Serial device server work in tcp-client mode

Serial device server in tcp-client mode provides client connections for TCP network servers. it actively initiate a connection and connect to the server to realize the interaction between serial device and tcp server. The Tcp/Ip and serial data are transparently transmitted in both directions. The serial device server supports to establish multiple TCP Clients to connect to different Tcp Server.

Serial device server work in tcp-server mode, as show in figure below.



Serial device server work in tcp-server mode

In TCP Server mode, the module monitors the local port, accepts and establishes a connection for data communication when a connection request is sent. Used for communication with TCP clients within a local area network. It is suitable for scenarios where there is no server in the LAN and there are multiple computers or mobile phones requesting data from the module.

23.2. Configuring

- **Entering Serial Port Config Mode**

Command	**SWITCH(config)#serial port NPORT**
Description	**NPORT: serial port server port number, which can be viewed through show serial port all summary.**

- **Clearing all Config on a Serial Port**

Command	**SWITCH(config)#no serial port NPORT**
Description	**NPORT: serial port server port number, which can be viewed through show serial port all summary.**

- **Configuring Operation Mode**

Command	**SWITCH(config-serial-port)#operation mode (tcp-client | tcp-server)**
Description	**Tcp-client: tcp client operation mode.** **Tcp-server: tcp server operation mode.** **Support no operation mode command, return to disabled state.**

- **Configuring Tcp-client**

Command	**SWITCH(config-serial-port)# tcp-client CLIENTID remote-address A.B.C.D remote-port L4-PORT (| local-port L4-PORT)**
Description	**CLIENTID: <1 4>, support to create 4 clients.** **A.B.C.D: IPv4 addresses** **L4-PORT: Layer 4 port number** **Local-port is an optional configuration, the default system automatically assigns.**

- **Configuring Tcp-server**

Command	**SWITCH(config-serial-port)# tcp-server local-port L4-PORT**
Description	**L4-PORT: Layer 4 port number** **To configure tcp-server mode, the local-port parameter must be configured.**

- **Configuring Tcp-server Max Connection**

Command	**SWITCH(config-serial-port)# tcp-server connection max CMAX**
Description	**CMAX: The maximum number of connections in tcp-server mode, the default is 1.**

- **Configuring Tcp Alive-check Time**

Command	**SWITCH(config-serial-port)# tcp alive-check time SECONDS**
Description	**SECONDS: If there is no data interaction during this time period, start alive detection** **Range: <10-300>, in seconds** **This parameter is supported in both Tcp-client and tcp-server modes.**

- **Configuring Rtu Baud-rate**

Command	**SWITCH(config-serial-port)# serial baud-rate (300 | 1200 | 9600 | 19200 | 38400 | 57600 | 115200)**
Description	**Default baud rate is 115200.**

- **Configuring Rtu Data-bits**

Command	SWITCH(config-serial-port)# serial data-bits (7 | 8)
Description	Default data is bit 8.

- **Configuring Rtu Parity**

Command	SWITCH(config-serial-port)# serial parity (none | odd | even | mark | space)
Description	Default check digit none.

- **Configuring Rtu Stop-bits**

Command	SWITCH(config-serial-port)# serial stop-bits (1 | 2)
Description	Default stop bit is 1.

- **Configuring Packet Length Max**

Command	SWITCH(config-serial-port)# serial packet length LENGTH
Description	The length of the serial data packet. If the length exceeds the LENGTH value, it will be packetized and forwarded to the network. LENGTH: range from 0 to 1460, default value is 1460.

- **Configuring Packet Interval**

Command	SWITCH(config-serial-port)# serial packet interval MILLISECONDS
Description	If the interval between bytes before and after the serial port data exceeds MILLISECONDS, the last byte of data is regarded as the new header byte. MILLISECONDS: range from 1 to 1000, default value is 10, in milliseconds.

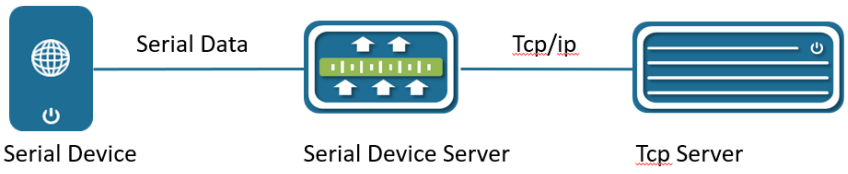
- **Configuring Fifo**

Command	SWITCH(config-serial-port)# serial fifo length LENGTH
Description	Serial data bits are transmitted at low speed, and data is transferred from the network end to the serial port to increase the fifo to improve the forwarding capability LENGTH: range from 0 to 128, default value is 64.

23.3. Examples

23.3.1. Example for Tcp-client

The following examples shows how to configure the serial device server work in tcp-client mode, As show in Figure below.



Serial device server work in tcp-client mode

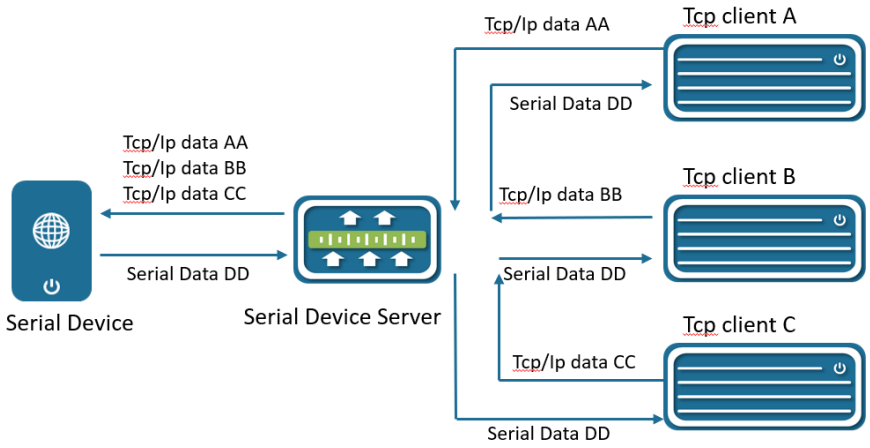
In this case, IP address of TCP Server is 192.168.64.1, local port number is 2000. We need to configure the serial port server to work in tcp-clent mode, configure tcp-client 1 to connect to the target TCP Server, and the local port is dynamically generated by the system.

The serial parameters are all in default.

```
SWITCH(config)#serial port 1
SWITCH(config-serial-port)#operation mode tcp-client
SWITCH(config-serial-port)#tcp-client 1 remote-address 192.168.64.1 remote-port 2000
SWITCH(config-serial-port)#tcp-client 2 remote-address 192.168.64.2 remote-port 2001
```

23.3.2. **Example for Tcp-server**

The following examples shows how to configure the serial device server work in tcp-server mode, As show in Figure below.



Serial device server work in tcp-server mode

In this case, we need to configure the serial device server to work in tcp-server mode, configure the local port number 2000, configure the maximum number of connections to 3.

TCP Client A/B/C access to server.

The serial parameters are all in default.

```
SWITCH(config)#serial port 1
SWITCH(config-serial-port)#operation mode tcp-server
SWITCH(config-serial-port)#tcp-server local-port 2000
SWITCH(config-serial-port)#tcp-server connection max 3
```

TCP Client A/B/C transmits data stream to serial device, and will not forward it between clients. when serial device transmits, the data stream will broadcast a copy on each client.

23.4. Display Information

- **Display serial port summary**

```
SWITCH#show serial port 1 summary
    Operation mode          :    tcp-client
    Tcp client 1            :    192.168.64.1:2000
    Tcp client 2            :    --
    Tcp client 3            :    --
    Tcp client 4            :    --
    Tcp server local port   :    --
```

```
Tcp server connection max   :     1
Tcp alive-check time        :     30
Serial baud-rate            :     115200
Serial data-bits            :     8
Serial parity               :     none
Serial stop-bits            :     1
Serial packet length        :     1460
Serial packet interval      :     10
Serial fifo length          :     64
```

- Display serial port status

```
SWITCH#show serial port 1 status
Port entity          Status   Remote                  Local
-----------------------------------------------------------------
1     tcp client 1   link     192.168.64.1:1024       192.168.64.100:47188
```

- Display serial port statistic

```
SWITCH#show serial port 1 statistic
    Net Octets Rx                 :   5824
      Net Packets Rx              :   728
      Net Octets Tx               :   5120
      Net Packets Tx              :   834
      Serial Octets Rx            :   5120
      Serial Packets Rx           :   834
      Serial Octets Tx            :   5824
      Serial Packets Tx           :   728
    Net Connect Up/Down times     :   1
    Serial Overload Drop Packets  :   0
```

24. Fault Diagnosis

24.1. Ping/tracerout

- **ping**

Command	**SWITCH#ping {ip IPADDR | ipv6 IPV6ADDR}**
Description	**Ping a remote host through IP.**

- **traceroute**

Command	**SWITCH# traceroute {ip IPADDR | ipv6 IPV6ADDR }**
Description	**Trace the path that packets take through the network.**

24.2. Display Port Optical Module DDM Information

- **Show interface opticatl-transceiver information**

Display the information of the optical/copper module inserted in the optical port.

Command	**SWITCH#show interface {IFNAME |} optical-transceiver {info |}**
Description	**If no interface-id is specified, the module information of all ports will be displayed.** **If info is not specified, the DDM information of the port module will be displayed, and if specified, the complete module information (basic information, alarm information, manufacturer information) will be displayed.**

DDM information display elements are as follows:

Key Word	Description
Temp	**The temperature of the module, in °C, accurate to 1°C.**
Voltage	**The voltage of the module, the unit is V, accurate to 0.01V.**
Bias	**The current of the module, in mA, accurate to 0.01mA.**
RX power	**The received optical power of the module, in dBm, accurate to 0.01dBM.**
TX power	**The transmit optical power of the module, in dBm, accurate to 0.01dBM.**
OK	**normal, no intervention required.**
WARN	**Alarm, indicating that the allowable range of the device is exceeded, and attention should be paid to.**
ALARM	**Abnormal, indicating that the device's allowable state is seriously exceeded and immediate intervention is required.**
ABSENT	**Absent.**
NA	**Port not supported/module not supported.**

TIMEOUT	Time out.
ERR	Mistake.

Display all port module DDM information

```
SWITCH#show interface optical-transceiver
  Port       Temp        Voltage       Bias          RX power      TX power
             [C]         [V]           [mA]          [dBm]         [dBm]
-------  ----------  -------------  -------------  -------------  -------------
GiE0/9    42(OK)      3.20(OK)      32.34(OK)     -3.98(OK)      1.64(OK)
GiE0/10   ABSENT      ABSENT        ABSENT        ABSENT         ABSENT
GiE0/11   ABSENT      ABSENT        ABSENT        ABSENT         ABSENT
GiE0/12   ABSENT      ABSENT        ABSENT        ABSENT         ABSENT
```

- Display the overall information of the port optical module/copper module

Error message:

Key Word	Description
Transceiver absent!	Failed to get information, maybe the module is not in place.
Get transceiver info timeout!	Timeout to get information, need to get it again.
Port doesn't support get module info!	The port does not support getting module information.

Basic Information

Key Word	Description
Transceiver Type	module type.
Connector Type	Interface Type.
Wavelength(nm)	Wavelength.
Link Length	Supported link lengths.
Digital Diagnostic Monitoring	Whether to support DDM function.
Vendor Serial Number	Module serial number.

Warning Information

Key Word	Description

RX Channel loss of signal	**Received signal loss.**
RX Channel power high	**High received optical power alarm.**
RX Channel power low	**Low received optical power alarm.**
TX Channel fault	**Send Error.**
TX Channel bias high	**Bias current high alarm.**
TX Channel bias low	**Bias current low alarm.**
TX Channel power high	**Sending high optical power alarm.**
TX Channel power low	**Sending low optical power alarm.**
Temperature high	**High temperature alarm.**
Temperature low	**Low temperature alarm.**
Voltage high	**High voltage alarm.**
Voltage low	**Low voltage alarm.**
None	**no alarm.**
This module doesn't support getting alarm!	**The module does not support getting alarm information.**

Manufacturer information

Key Word	Description
Vendor Name	**Manufacturer Names.**
Vendor OUI	**Manufacturer OUI.**
Vendor Part Number	**Manufacturer part number.**
Vendor Revision	**Manufacturer version number.**
Manufacturing Date	**Production Date.**
Encoding	**encoding type.**

Displays overall information about a single port module

```
SWITCH#show interface gigabitEthernet0/9 optical-transceiver info
#####################################################
                        gigabitEthernet0/9
+-----------------------------------------------+
|Transceiver base information:                  |
+-----------------------------------------------+
|Transceiver Type     :   1000BASE-ZX-SFP       |
|Connector Type       :   LC                    |
|Wavelength(nm)       :   1550                  |
|Link Length      :                             |
|     SMF fiber                                 |
|          -- 80km                              |
|Digital Diagnostic Monitoring   : YES          |
|Vendor Serial Number            : WT1703230031 |
+-----------------------------------------------+
|Transceiver current alarm information:         |
+-----------------------------------------------+
|None                                           |
+-----------------------------------------------+
|Transceiver vendor information:                |
+-----------------------------------------------+
|Vendor Name          : OEM                     |
|Vendor OUI           : 000000                  |
|Vendor Part Number   : SFP-GE-ZX-SM1550        |
|Vendor Revision      : V2                      |
|Manufacturing Date   : 2017-03-25              |
|Encoding             : 8B10B                   |
+-----------------------------------------------+
SWITCH#
```

Displays overall information for all port blocks

```
SWITCH#show interface optical-transceiver info
#####################################################
                        gigabitEthernet0/9
+-----------------------------------------------+
|Transceiver base information:                  |
+-----------------------------------------------+
|Transceiver Type     :   1000BASE-ZX-SFP       |
|Connector Type       :   LC                    |
|Wavelength(nm)       :   1550                  |
|Link Length      :                             |
|     SMF fiber                                 |
|          -- 80km                              |
|Digital Diagnostic Monitoring   : YES          |
```

```
|Vendor Serial Number                : WT1703230031      |
+-------------------------------------------------+
|Transceiver current alarm information:               |
+-------------------------------------------------+
|None                                                 |
+-------------------------------------------------+
|Transceiver vendor information:                      |
+-------------------------------------------------+
|Vendor Name             : OEM                        |
|Vendor OUI              : 000000                      |
|Vendor Part Number   : SFP-GE-ZX-SM1550               |
|Vendor Revision       : V2                           |
|Manufacturing Date   : 2017-03-25                     |
|Encoding                : 8B10B                       |
+-------------------------------------------------+
##################################################
                        gigabitEthernet0/10
+-------------------------------------------------+
|Transceiver base information:                        |
+-------------------------------------------------+
|Transceiver Type      :   1000BASE-GT-SFP             |
|Connector Type        :   Unknown or unspecified      |
|Wavelength(nm)        :   16652                       |
|Link Length       :                                  |
|      Cable Assembly copper                           |
|           -- 100m                                    |
|Digital Diagnostic Monitoring   : NO                  |
|Vendor Serial Number              : MTC100046         |
+-------------------------------------------------+
|Transceiver current alarm information:               |
+-------------------------------------------------+
This module doesn't support getting alarm!
|This module doesn't support getting alarm!           |
+-------------------------------------------------+
|Transceiver vendor information:                      |
+-------------------------------------------------+
|Vendor Name             : OEM                        |
|Vendor OUI              : 000000                      |
|Vendor Part Number   : SFP-T-CBTX                     |
|Vendor Revision       : F                            |
|Manufacturing Date   : 2014-10-01                     |
|Encoding                : 8B10B                       |
+-------------------------------------------------+
##################################################
```

```
                        gigabitEthernet0/11
 Get result error(Maybe Transceiver absent)!
 ####################################################
                        gigabitEthernet0/12
 Get result error(Maybe Transceiver absent)!
SWITCH#
```