L2T4 Industrial Managed Swith

User Manual

V5.6.0

Please read before using the device

TABLE OF CONTENTS

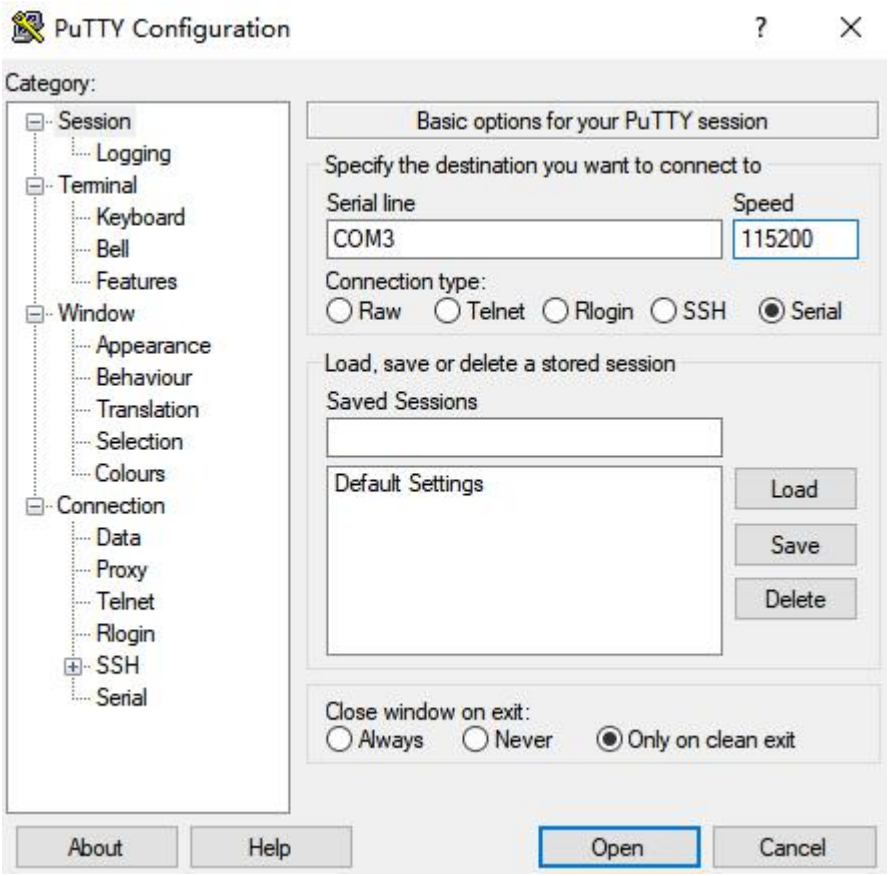
1. Login switch configuration

1.1. CLI

1.1.1 CLI enter by console

Step 1. Connect switch console port to PC

Step 2. Open the software support console port, "PuTTY" as example here



- Select the serial method
- Input the serial device using by PC Serial line
- Set baud rate at 115200 at "Speed"
- Enter the login screen.

  Notes: Make sure the serial port configuration is correct, baud rate 115200,

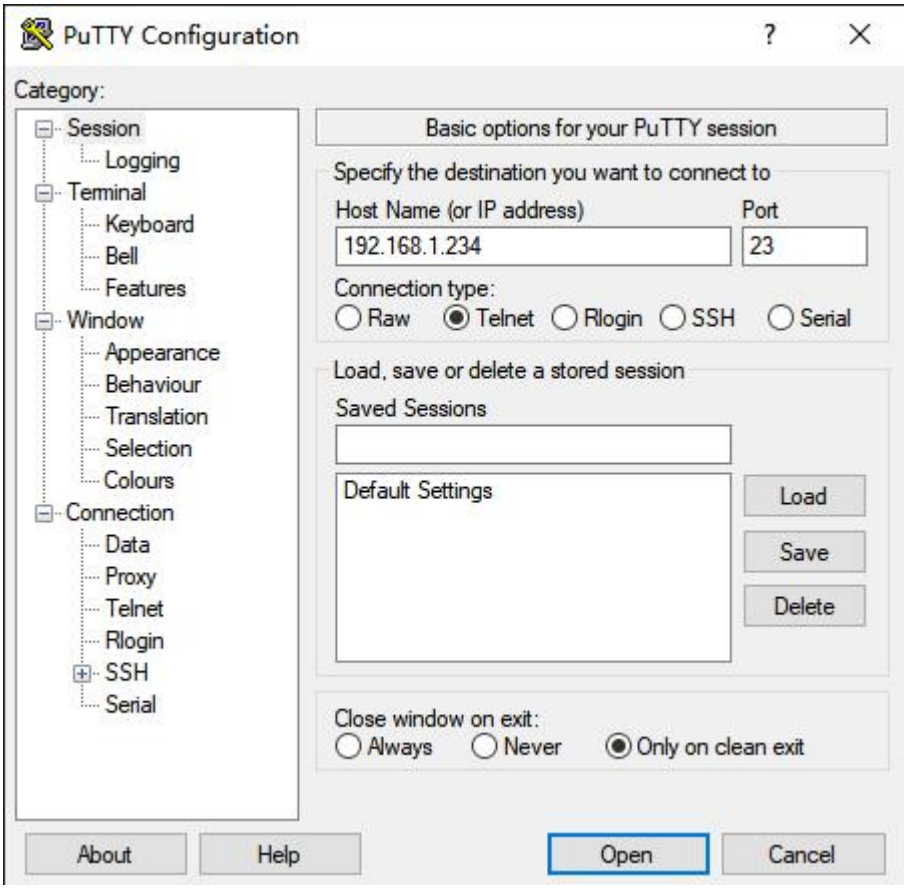
  Data digital is 8, parity check is none, end 1, flow control at none

- Login device, enter CLI mode after input user name and password;
  Notes: the default name/password: admin

1.1.2 CLI enter by Telnet

Step 1: Connect switch console port to PC

Step 2: Open the software support Telnet, "PuTTY" as example here



- Select Telnet
- Input the switch IP address into Host Name
- Enter the login screen, input username and password
  Notes: the default name/password: admin

Suggestion: it is suggested that the administrator should configure telnet service as soon as possible after logging in the switch for the first time, so that the device can be configured and managed through the remote terminal in the later stage.

Enter Configure mode

SWITCH# **configure terminal**

Enable Telnet server

SWITCH(config)**#telnet-server enable**

1.1.3 CLI command mode

CLI management screen has different command mode, the user in the command mode determines the commands can be used

Mode Name	Symbol	Mode Conversion	Description
User mode	SWITCH>	configure enable into Privilegaed Mode	Support device information display, debug command line, etc
Privileged mode	SWITCH#	configure terminal into Global mode configure disable into User mode	Support network test, Support function module information viewing, Support configuration save, clear and other operations
Global mode	SWITCH(config)#	Configure exit into Privileaged mode, configure interface into INTERFACE MODE	Support all command based on the Global mode
Interface mode	SWITCH(config-if)#	Configure exit into Full-mode Configure end into Privileged mode	Support configuration commands in interface mode, including physical interface, aggregation interface and SVI interface

1.1.4 CLI NO command

Most of the CLI configuration commands have corresponding the related NO commands, clear or restore the default configuration. Input "?" for command reference after no command operated

For example: add VLAN 100, clear VLAN 100

```
SWITCH(config)#vlan 100
SWITCH(config)#no vlan 100
```

1.1.5 Command Format Description

For the configuration commands in this document, keywords are in **bold font**. Parameters that are not keywords are indicated in *italics*.

In addition, the special symbols in the configuration commands are described as follows.

Sharp brackets < >: Indicates the configurable range of values.

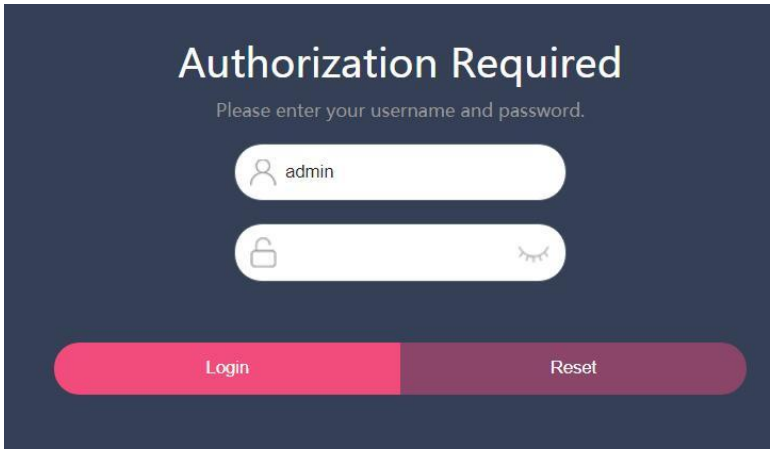
Middle brackets [ ]: Indicates that the command inside the brackets is optional.

Small brackets (|): where "|" is used to separate multiple commands, the last position can be empty, empty means optional, the same as the meaning of the middle brackets.

Curly brackets {|}: where "|" is used to separate multiple commands. The parentheses cannot be terminated by "|". Generally speaking, there must be at least two commands in curly brackets, which means at least one command is selected from two commands, and the order of the commands is irrelevant.

1.2. Web management

The web server has been enabled by default, server IP is 192.168.1.234.



All configuration operated by web management needs to be saved manually (in the upper right corner of web network management page), otherwise configuration will be lost after restart.

The CLI commands for configuring web services are as follows

Enter configuration mode

SWITCH# configure terminal

Enable web service

SWITCH(config)# web-server enable

2. System management

2.1. Configure save/clear

The Web management path:

Homepage -> Upper Right Corner -> Save,

Homepage -> System -> Configuration File management

Save command

SWITCH#**write**

Restore default configuration command

SWITCH#**copy default-config startup-config**

Restore the device to make the configuration effect.

2.2. Reboot

The Web management path: Homepage -> System -> Reboot

Reboot Command

SWITCH#**reload**

2.3. User login

The Web management path:

Homepage -> System -> User management;

Homepage -> System -> Telent Server

Add new user, change password

SWITCH(config)#**username** *NAME* **password** *LINE*

If the user NAME does not exist, add the user, if it exists, modify the user's password

The device has its own user "admin" and password "admin" by default, and it 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 adopts encryption method

Delete operation does not support delete operation user himself

To delete an online user, you need to kick the user offline before deleting

Kick online users offline

SWITCH#**clear line (vty | console)** *LINE*

vty Indicates remote login user

console Indicates serial port login user

LINE information can be viewed in the show users command

Do not support this operation on web management

Configure Enable web management

SWITCH(config)#**web-server enable**

Web management enable as default

Do not support this operation on web management

Configure Telnet Enable

SWITCH(config)#**telnet-server enable**

Telnet enable as default

Show online users

SWITCH#**show users**

```
SWITCH#show users
Type      Line   User            Host(s)    Idle       PID
con       0      admin           idle       00:00:03   1932
```

2.4. System name

The Web management path: Homepage -> Basic information -> Host Name

Configure system name

SWITCH(config)#**hostname** *WORD*

The name must consist of printable characters and cannot exceed 63 bytes in length

Configuration takes effect immediately

2.5. System upgrade

The Web management path:Homepage -> System -> System Upgrade

Configure system upgrade

SWITCH#**upgrade tftp tftp:**//*SERVER/FILENAME*

Firmware upgrade commandsneed to build a TFTP server on the terminal and ensure the two-way interconnection between the terminal and the device network

SERVER: TFTPTFTP server IP and the relative address of the server window and firmware upgrade file

FILENAME: Firmware upgrade file

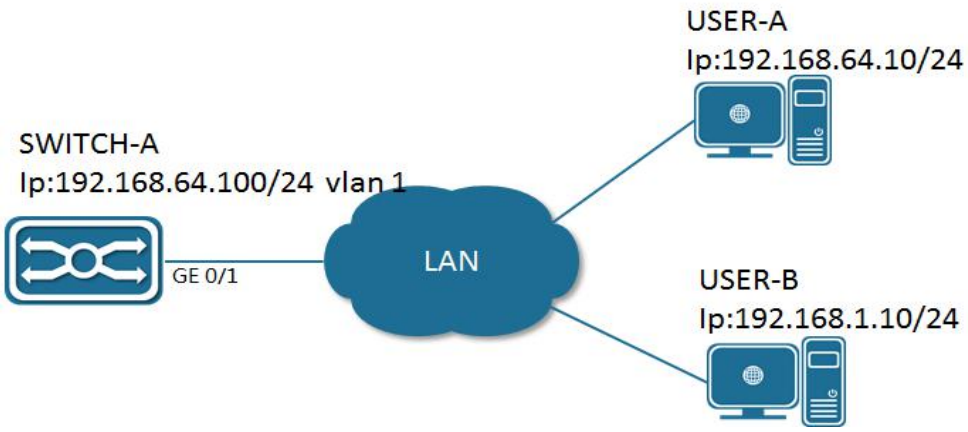
The firmware upgrade will take 5-6 minutes, restart the device to complete.

Make sure no power off during firmware upgrade.

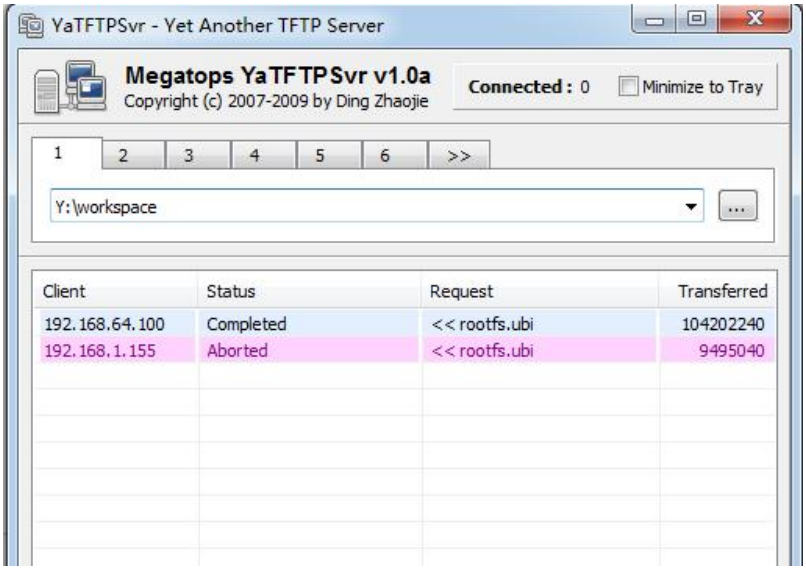
Configuration case

Remote telnet to complete the firmware upgrade

- Below diagram as example,SWITCH-A is the equipment to be upgraded, open telnet function, User-A is the Hosts on the same segment LAN network segment,USER-B is the management device in the LAN, both can telnet login to SWITCH-A



- Select USER-B for version upgrade operation,Open the TFTP server software on USER-B, and put the upgrade file firmware-release-5.1.0.bin in the Y:/workspace directory.



- USER-B telnet login SWITCH-A, execute upgrade commands in privileged mode

```
SWITCH#upgrade tftp tftp://192.168.5.101/firmware-release-5.1.0.bin
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
100 68.7M    0 68.7M    0     0   275k      0 --:--:--  0:04:15 --:--:-- 12324
100 68.7M    0 68.7M    0     0   275k      0 --:--:--  0:04:15 --:--:--  275k
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 @ 43e0000 -- 27 % complete flash_erase: Skipping bad block at 04400000
Erasing 128 Kibyte @ f5e0000 -- 100 % complete
Bad block at 4400000, 1 block(s) from 4400000 will be skipped
Reboot system to finish upgrade? (y/n):
```

- After the upgrade command is executed, select "y" to restart the device to complete the upgrade, select "n" to continue the operation, and the upgrade will be completed till the next restart

2.6. System time

The Web management path:Homepage -> System -> Date and Time

Manually configure the system time

SWITCH# **clock set** *HH:MM:SS DAY MON YEAR*

Set the system time

Configuration Case

Configure 2107-10-01 15H 30M 0sec

```
SWITCH# clock set 15:30:00 1 october 2017
```

Configure NTP Server

SWITCH(config)#**ntp server** *A.B.C.D*

Configure the IP address of the NTP server (domain name configuration is not supported). After the configuration is complete, if the device maintains network connectivity with the server, the device will automatically synchronize time information from the server. The first time synchronization will take about 4-8 minutes.

Configure System Time Zone

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

Configure the system time zone, the default is UTC, support standard time zone configuration, such as London time zone keyword "London", Hong Kong time zone keyword "Hong_Kong", etc.

View System Time

SWITCH#**show clock**

3. Configure interface

The Web management path:

Homepage -> Interface -> Port Management

Homepage -> Interface -> Port Statistics

Homepage –> Interface -> Port Isolation

3.1. Interface types overview

The interface of the network switch can be divided into Layer 2 interface and Layer 3 interface. This switch only supports Layer 2 interface.

L2 interface here including switch port and Port Channel.

The Switch Port is composed of a single physical port on the device and only has the Layer 2 switching function. The port can be an Access Port, Hybrid Port or Trunk Port. It can be configured a port as an Access Port, Hybrid Port or Trunk Port through the Switch Port interface configuration command.

Port Channel is abbreviated as PO, which is composed of multiple physical member ports. It can bundle multiple physical links together to form a simple logical link, which we call an aggregation port. For Layer 2 switching, the aggregation port is like a high-bandwidth Switch port, which can superimpose the bandwidth of multiple ports and expand the link bandwidth.

3.2. Configuration command

Configure Interface range

SWITCH(config)#**interface** *GigabitEthernet0/1-4,GigabitEthernet0/5-6*

When multiple range combinations, separate with ',' in the middle, without spaces

Max. Support 5 groups of range

When the configuration of a certain port in the middle fails, the configuration is returned and the subsequent port is not continued

Configure interface description

SWITCH(config-if)#**description**

The interface description is up to 80 characters

Configure interface shut down

SWITCH(config-if)#**shutdown**

Disable interface, enable default

Only supports physical port configuration

Configure port speed

SWITCH(config-if)#**speed** {**10 | 100 | 1000| 10000 | auto** }

When configured as auto or no speed, the port speed is auto-negotiation mode

Default auto-negotiation

Do not support configuration on aggregate member ports and SVI ports

Configure port duplex

SWITCH(config-if)# **duplex** {**auto | full | half** }

When configured as auto or no duplex, the port is auto-negotiation mode

Default duplex auto-negotiation

Do not support configuration on aggregate member ports and SVI ports

When speed and duplex exit the auto-negotiation mode, the port auto-negotiation is closed

Configure flow control

SWITCH(config-if)#**flowcontrol** {**on | off | auto** }

Default auto-negotiation

Do not support configuration on aggregate member ports and SVI ports

Configure MTU

SWITCH(config-if)# **mtu** LENGTH

The allowed setting range is 64~10240 bytes, the default is 1526 bytes

Do not support configuration on aggregate member ports and SVI ports

Configure SFP Port

SWITCH(config-if)# **port mode** {**1000base-x| 100base-fx}**

Default 1000Base-X

Only supports configuration on the physical port

Configure port isolation

SWITCH(config-if)#**switchport isolation**

Default Non-Isolation

Does not support isolation configuration on the aggregation port and vlan port

3.3. Configuration case

Configure the port of GigabitEthernet0/1,named it " TEST_A"

```
SWITCH(config)#interface GigabitEthernet0/1
SWITCH(config-if)#description TEST_A
```

Shut down the port of GigabitEthernet0/1

```
SWITCH(config)#interface GigabitEthernet0/1
SWITCH(config-if)#shutdown
```

Forced the speed at 100M, Full-duplex, enable flow control

```
SWITCH(config)#interface GigabitEthernet0/1
SWITCH(config-if)#speed 100
SWITCH(config-if)#duplex full
SWITCH(config-if)#flowcontrol on
```

Configure the port GigabitEthernet0/1, MTU at 1024,

```
SWITCH(config)#interface GigabitEthernet0/1
SWITCH(config-if)#mtu 1024
```

3.4. Show Command

Show interface brief

SWITCH#**show interface brief**

```
SWITCH#show interface brief
Codes: ETH - Ethernet, LB - Loopback , AGG - Aggregate , MLAG - MLAG Aggregate
       FR - Frame Relay, TUN -Tunnel, PBB - PBB Logical Port, VP - Virtual Port
       CVP - Channelised Virtual Port, METH - Management Ethernet, UNK- Unknown
       ED - ErrDisabled, PD - Protocol Down, AD - Admin Down , NA - Not Applicab
```

```
le
      NOM - No operational members , PVID - Port Vlan-id

--------------------------------------------------------------------------------

Ethernet              Type Status Reason Speed Duplex Flowcontrol Autoneg Port

Interface                                                          Ch #

--------------------------------------------------------------------------------

GigabitEthernet0/1    ETH  up     none   1000M  FULL   OFF         ON     --

GigabitEthernet0/2    ETH  down   PD     --     --     --          --     --

GigabitEthernet0/3    ETH  down   PD     --     --     --          --     --

GigabitEthernet0/4    ETH  down   PD     --     --     --          --     --
```

Show a single-port configuration and status information

SWITCH#**show interface** *IFNAME*

```
SWITCH#show interface GigabitEthernet0/1

Interface GigabitEthernet0/1

  Hardware is ETH  Current HW addr: 0022.3300.0a0a

  Logical:(not set)

  Port Mode is access

  Index 1 metric 0 mtu 1500

  Interface configure:

    Media type: RJ45 mtu: 1500 admin status: no shutdown

    Speed: auto Duplex: auto Flowcontrol: off

  Interface status:

    Link status: UP Bandwidth: 1g

    Speed: 1000M Duplex: full Flowcontrol: off

  input packets:

    Good Octets Rx          : 228042

    Good Packets Rx         : 1480

    Broadcast Packets Rx    : 109
```

```
  Multicast Packets Rx    : 979
 ouput packets:
  Good Octets Tx          : 243972
  Good Packets Tx         : 3811
  Broadcast Packet Tx     : 3419
  Multicast Packet Tx     : 1
 un-normal packets:
  Drop Events             : 0
  Undersized Pkts Recvd   : 0
  Oversized Pkts Recvd    : 0
  Bad CRC                 : 0
```

Show Port packets statistics

SWITCH#**show counters interface** IFNAME

```
SWITCH#show counters interface GigabitEthernet0/1
Interface GigabitEthernet0/1
 5 seconds input rate    : 192 bits/sec, 0 packets/sec
 5 seconds output rate   : 200 bits/sec, 0 packets/sec
 Rxload                  : 0.00%
 Txload                  : 0.00%
 Good Octets Tx          : 245572
 Good Octets Rx          : 230000
 Bad Octets Rx           : 0
 Mac Tx Err Pkts         : 0
 Good Packets Tx         : 3836
 Good Packets Rx         : 1491
 Bad Packets Rx          : 0
 Broadcast Packet Tx     : 3443
```

Broadcast Packets Rx : 110

Multicast Packet Tx : 1

Multicast Packets Rx : 988

pkts_64_octets Rx : 0

pkts_65_127_octets Rx : 0

pkts_128_255_octets Rx : 0

pkts_256_511_octets Rx : 0

pkts_512_1023_octets Rx : 0

pkts_1024_max_octets Rx : 0

pkts_64_octets : 4258

pkts_65_127_octets : 253

pkts_128_255_octets : 786

pkts_256_511_octets : 0

pkts_512_1023_octets : 30

pkts_1024_max_octets : 0

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
```

Show port isolation configuration information

SWITCH#**show switchport isolate**

```
SWITCH#show switchport isolate
interface                config
GigabitEthernet0/1       normal
GigabitEthernet0/2       normal
GigabitEthernet0/3       normal
GigabitEthernet0/4       normal
GigabitEthernet0/5       normal
GigabitEthernet0/6       normal
Port-Channel1            normal
```

4. MAC address management

The Web management path: Homepage -> L2 Switch -> MAC Management

4.1. MAC address overview

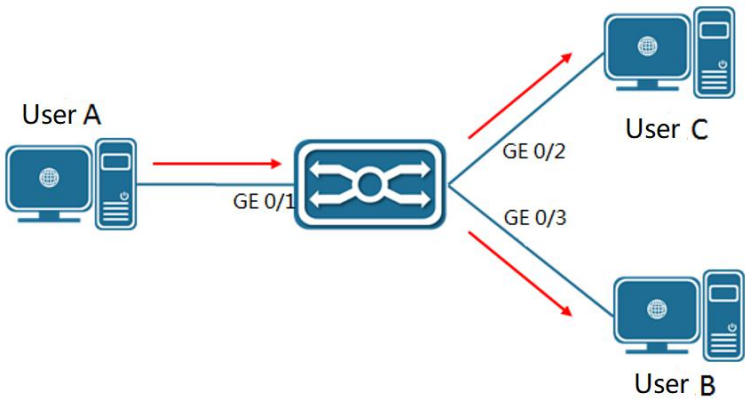
The MAC address table records the MAC address, interface, and VLAN ID information of the devices connected to the device. Based on the MAC address table lookup, the Ethernet switch decides whether to use the Known Unicast or Unnamed Broadcast forwarding method.

Known unicast: The Ethernet switch finds a table entry in the MAC address table that corresponds to the destination MAC address and VLAN ID of the message and the output port in the table entry is unique, and the message is output directly from the port corresponding to the table entry.

Unknown broadcast: The Ethernet switch does not find the table entry corresponding to the destination MAC address in the address table, and the message is sent to the output of all ports in the VLAN to which it belongs except for the message input port.

The MAC address of an Ethernet switch can be obtained dynamically or statically configured, and in general is obtained by dynamic acquisition. The working principle of dynamic MAC address learning is given below by analyzing the interaction process between user A and user C.

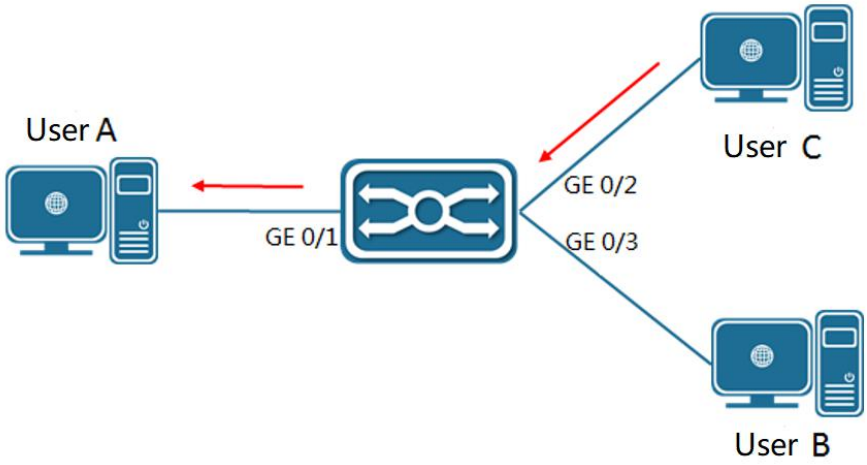
User A sends a message to port GigabitEthernet0/1 of the switch, and the Ethernet switch learns the MAC address of user A into the MAC address table. Since there is no source MAC address of user C in the address table, the Ethernet switch sends the message to all ports in the same VLAN1 except the GigabitEthernet0/1 connected to user A, including the ports of user B and user C. At this time, user B can receive the message sent by user A that does not belong to it.



Current dynamic MAC address table information:

User	VLAN	MAC address	Port
User A	1	000E.C6C1.C8AB	GigabitEthernet0/1

At this time, the MAC address of user A already exists in the MAC address table of the Ethernet switch, and the message is forwarded to GigabitEthernet0/1 port as a unicast, while the Ethernet switch will learn the MAC address of user C. Unlike the previous one, user B does not receive the message sent by user C to user A at this time.



Current dynamic MAC address table information:

User	VLAN	MAC address	port
User A	1	000E.C6C1.C8AB	GigabitEthernet0/1
User C	1	000E.C6C1.C8AD	GigabitEthernet0/2

After one interaction between user A and user C, the device learns the source MAC address of user A and user C. After that, the message interaction between user A and user C is forwarded in unicast mode, after which user B will not receive the interaction message between user A and user C.

4.2. Configuration command

Configure Dynamic MAC address aging time

SWITCH(config)#**mac-address-table aging-time** *<0-600>*

In the range of 0-600 seconds.

Default 300 seconds.

When configured as 0, MAC address aging function is disabled.

Configure static MAC address

SWITCH(config)#**mac-address-table static** *MAC_ADDR* **vlan** *VLANID* **interface** *IFNAME*

When the device receives a packet with MAC_ADDR as the destination address on the VLAN specified by VLANID, the packet will be forwarded to the interface specified by IFNAME

IFNAME support physical port and aggregation port

Configure MAC address filter

SWITCH(config)#**mac-address-table filter** *MAC_ADDR* **vlan** *VLANID*

When the device receives a packet with the address specified by MAC_ADDR as the source or destination address on the VLAN specified by the VLANID, it will be discarded

Clear dynamic MAC address

SWITCH#**clear mac-address-table dynamic**

SWITCH#**clear mac-address-table dynamic vlan** *VLANID*

SWITCH#**clear mac-address-table dynamic interface** *IFNAME*

Support all MAC address clear,including the MAC based-on VLAN and based-on port

4.3. Configuration case

Configure dynamic MAC address aging time to 60 seconds

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

Configure static MAC address, all destination MAC address 000E.C6D1.C8AB, and forward VLAN 1 packets from port Gigabit Ethernet 0 / 1

```
SWITCH(config)#mac-address-table static 000E.C6D1.C8AB vlan 1 interface GigabitEthernet0/1
```

Configure MAC address filtering and discard packets with VLAN 1 source or destination MAC address of 000E.C6C1.C8AB

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

Clear the dynamic MAC address of port gigabitethernet 0 / 1

```
SWITCH#clear mac-address-table dynamic interface GigabitEthernet0/1
```

4.4. Show Command

Show MAC address

SWITCH#**show mac-address-table**

```
SWITCH#show  mac-address-table
 VLAN     MAC Address     Type      Ports
 -----+---------------+---------+----------------------+
 20     0000.0000.0009   filter    drop
 20     0000.0000.000a   filter    drop
```

Show the statistics of the number of MAC addresses

SWITCH#**show mac-address-table count**

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

5. VLAN Configuration

The Web management path: Homepage -> L2 Switch -> VLAN

5.1. VLAN overview

VLAN is the abbreviation of Virtual Local Area Network, which is a logical network divided on a physical network. VLANs have the same properties as a normal physical network, except that they are not limited by physical location. Layer 2 unicast, broadcast, and multicast frames are forwarded and propagated within a VLAN without going directly into other VLANs.

Port-based VLAN is the simplest method of VLAN segmentation. Users can divide the ports on a device into different VLANs, so that messages received from a port will only be transmitted within the corresponding VLAN, thus enabling the isolation of broadcast domains and the division of virtual workgroups.

The port link types of Ethernet switches can be divided into three types: Access, Trunk, and Hybrid, which are handled differently when adding VLANs and forwarding messages.

- Access: the port can belong to only 1 VLAN; generally used for connections between the switch and end users.
- Trunk: the port can belong to multiple VLANs and can receive and send messages from multiple VLANs, but only Native VLANs can be used without VLAN tags; generally used for connections between switches.
- Hybrid: The port can belong to multiple VLANs, can receive and send messages from multiple VLANs, and can be configured with or without VLAN tagging for the relevant VLAN according to the user's needs; can be used for connection between switches or for connection to the user's computer.

5.2. Configuration command

Create VLAN

SWITCH(config)#**vlan** *VLAN_RANGE*

Configure Access Port

SWITCH(config)#**interface** GigabitEthernet0/1

SWITCH(config-if)#**switchport mode access**

Configure the port type as Access port (by default, the port is Access type)

Configure the VLAN to which the Access port belongs

SWITCH(config-if)#**switchport access vlan** *VLANID*

Add the current port to the specified VLAN (by default, all Access ports belong to and only belong to VLAN1), the no command restores the default

The above command can only be used after the interface has been configured as an access port, and the specified VLAN must have been created;When configured as non-VLAN 1, if the corresponding VLAN is deleted, it will automatically revert to VLAN 1

Trunk Configuration

SWITCH(config)#**interface** *GigabitEthernet0/1*

SWITCH(config-if)#**switchport mode trunk**

Configure the port type as Trunk port.

Trunk Port Allowed VLAN

SWITCH(config-if)#**switchport trunk allowed vlan** {**all** | *VLAN_LIST* | **none**}

Notes: the command available after trunk setting successfully

All: automatic mode, Automatically add all created VLANs including the subsequent creation

None: Clear the allowed VLAN, the port do not belong to any VLAN including native VLAN

VAN_LIST: Manual set the allowed VLAN, if setted at ALL (automatic mode), the allowed VLAN be cleared firstly, then add VLAN. VLAN LIST support standard Multi VLAN

When the "no" keyword is added in the front, the VLAN is deleted from the allowed VLAN list_ VLAN represented by list

When setting ALL, change the maintenance of allowed VLAN list to automatic mode,Other commands are changed to manual mode (By default, it is in automatic mode. When switching from other port mode to trunk port, it is in automatic mode)

Only the created VLANcan be added to the allowed VLAN list; When a VLAN is deleted, the corresponding VLAN in the allowed VLAN list will be deleted automatically.

Configure trunk port Native VLAN

SWITCH(config-if)#**switchport trunk native vlan** *VLANID*

Set native VLAN of trunk port. (by default, the native VLAN of trunk port is vlan1), and the no command returns to the default;

The above command can only be used when the interface has been configured as trunk port

The setting of native VLAN has nothing to do with whether the allowed VLAN contains this VLAN or even whether the VLAN is created, that is, native VLAN can be set as a VLAN that is not created

The native VLAN ID of the trunk port connected to the device must be consistent, otherwise the native VLAN packets will not be transmitted correctly

Configure hybrid port

SWITCH(config-if)#**switchport mode hybrid**

Configure hybrid port allowed VLAN list

SWITCH(config-if)#**switchport hybrid allowed vlan** {**all** | *VLAN_LIST* | **none**}

The above command can only be used when the interface has been configured as a hybrid port

All means automatic mode, which automatically joins all created VLANs (even if it is created later, it will automatically join);

None means clear the Allowed VLAN list, that is, the port does not belong to any VLAN (including Native Vlan);

VLAN_LIST means to manually set the Allowed VLAN list. If it was ALL (automatic mode) before, the Allowed VLAN list will be cleared first, and then the VLAN list will be added. VLAN_LIST supports standard multiple VLAN representation methods ("-" and "," and a combination of the two);

When the NO keyword is added in front, it means to delete the VLAN indicated by VLAN_LIST from the Allowed VLAN list;

When setting ALL, the maintenance of the Allowed VLAN list is changed to automatic mode, and other commands are changed to manual mode. (By default, it is automatic mode. When switching from other port mode to Hybrid port, it is automatic mode);

Only VLANs that have been created 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;

Configure the default VLAN of hybrid port

SWITCH(config-if)#**switchport hybrid vlan** *VLANID*

Set the default VLAN of the hybrid port (when the port receives the untagged packet, it defaults to the specified VLAN; when the port outputs, it carries the packet of the default VLAN and outputs untag), (by default, the default VLAN of the port is vlan1), and the no command returns to the default;

The above command can only be used when the interface has been configured as a hybrid port

The setting of the default VLAN has nothing to do with whether the allowed VLAN contains this VLAN or even whether the VLAN is created, that is, the default VLAN can be set as a VLAN that is not created

Configure the hybrid port untagged VLAN list

SWITCH(config-if)#**switchport hybrid untagged vlan** *VLAN_LIST*

Since the default VLAN must be untag output, it is not maintained by the untagged VLAN list

By default, the untagged VLAN list is empty (that is, except for the default VLAN, all other VLANs are tagged out);

The VLAN maintained by the untagged VLAN list must be in the allowed VLAN list of the hybrid 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, and the process is irreversible.

The default VLAN ID of the hybrid port connected to the device must be consistent, otherwise the packets of the default VLAN will not be transmitted correctly

5.3. Show Command

In privilege mode, you can view VLAN information. The information displayed includes VLAN ID, VLAN status, VLAN member port and VLAN configuration information

Show VLAN

SWITCH#**show vlan** *VLANID*

```
SWITCH#show vlan 2
Bridge  VLAN ID  Name    State H/W Status Member ports

                                (u)-Untagged, (t)-Tagged
======= ======= ============ ======= ====================
1       2       VLAN0002 ACTIVE  Up          GigabitEthernet0/1(u)GigabitEthernet0/2(t)
```

6. ERPS Configuration

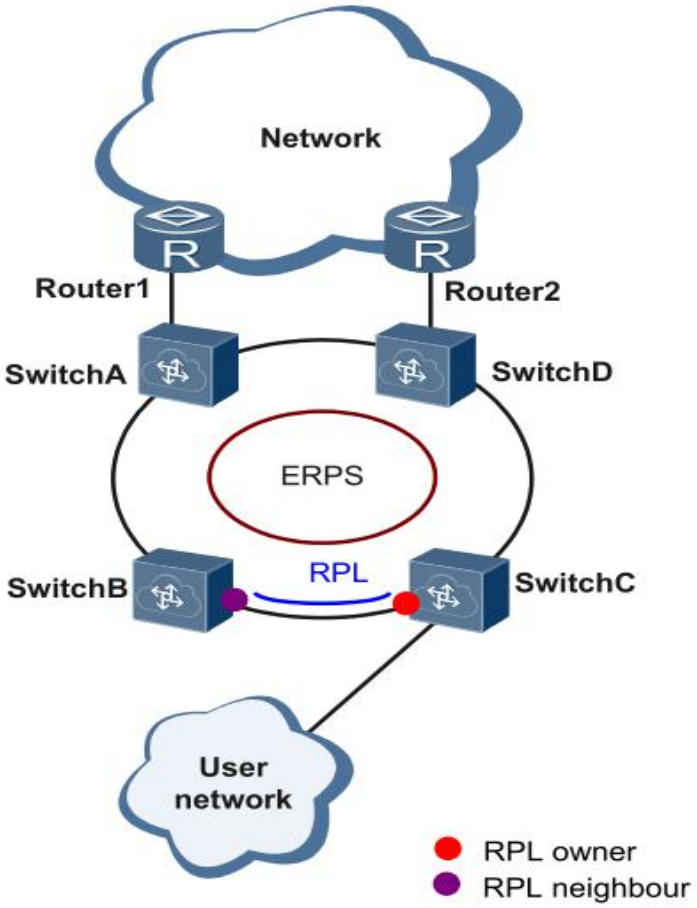
The Web management path: HomePage -> L2 Switch -> ERPS

6.1. ERPS Overview

ERPS (Ethernet Ring Protection Switching, Ethernet Ring Protection Switching Protocol) is a ring network protection protocol developed by the ITU, also known as G.8032. It is a link layer protocol specially applied to the Ethernet ring network. When the Ethernet ring network is complete, it can prevent broadcast storms caused by the data loop, and when a link on the Ethernet ring network is disconnected, it can quickly restore the communication between various nodes on the ring network.

At present, STP is another technology that solves the loop problem of the Layer 2 network. STP application is relatively mature, but its convergence time is relatively long (second level). ERPS is a link layer protocol specially applied to the Ethernet ring network. The layer 2 convergence performance is within 50ms, and it has a faster convergence speed than STP.

Typical ERPS networking:

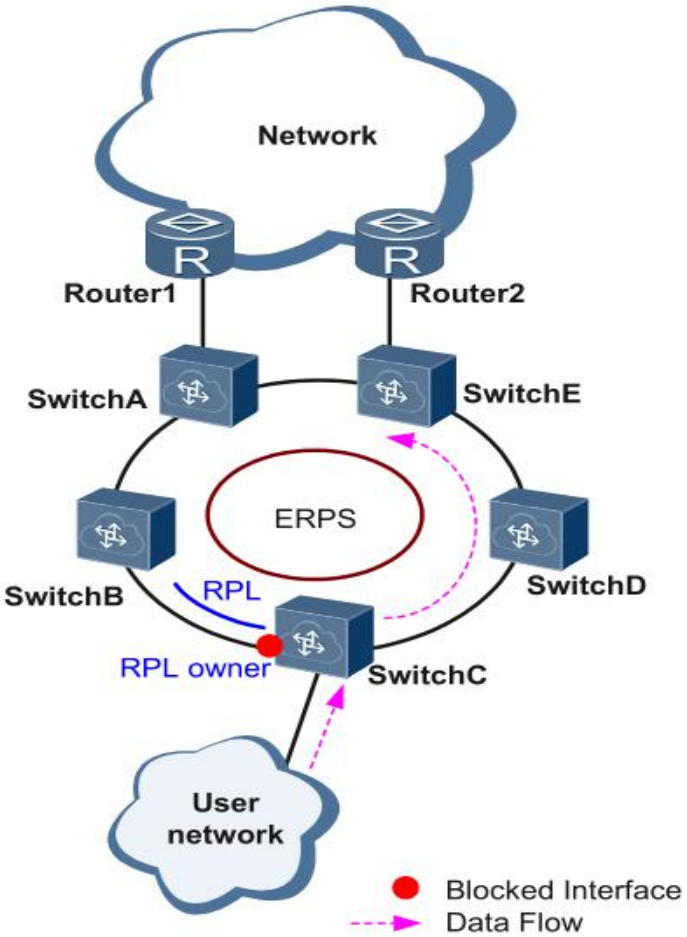


6.2. ERPS Principle Introduction

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 switching device can join the same ERPS ring. In an ERPS ring, in order to prevent loops, a loop-breaking mechanism can be activated to block the RPL owner port and eliminate loops. When a link failure occurs in the ring network, the equipment running the ERPS protocol can quickly release the blocked port, perform link protection switching, and restore the link communication between nodes on the ring network. This section mainly uses examples in the form of link normal -> link failure -> link recovery (including protection switching operations) to introduce the basic implementation principle of ERPS under single-ring networking.

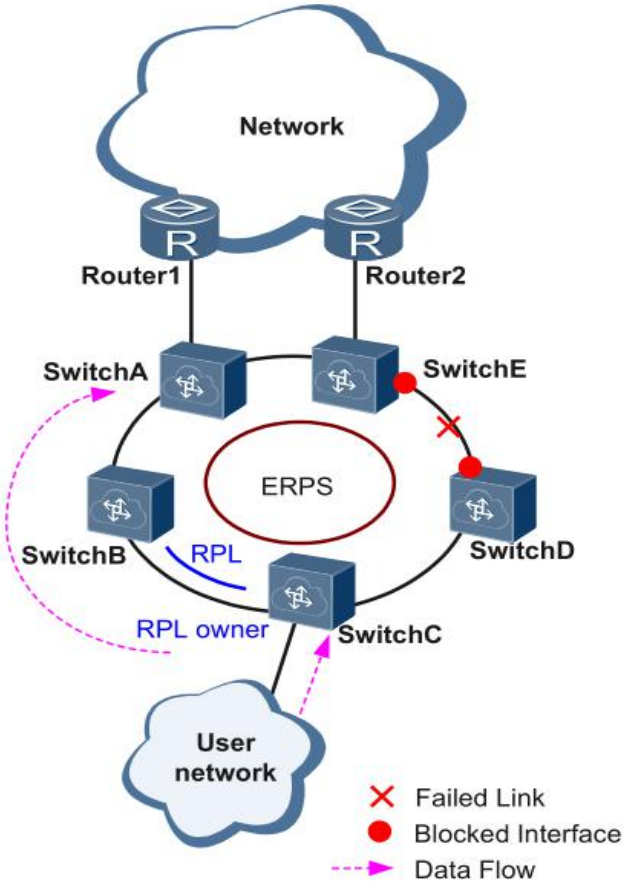
Link normal

As shown in the figure below, the devices on the loop composed of SwitchA to SwitchE communicate normally. To prevent loops, ERPS will first block the RPL owner port. If the RPL neighbour port is configured, this port will also be blocked, and other ports can forward business traffic normally.



Link failure

As shown in the figure, when the link between SwitchD and SwitchE fails, the ERPS protocol starts the protection switching mechanism to block the ports at both ends of the failed link, and then releases the RPL owner port. These two ports resume user traffic. Receiving and sending, thus ensuring uninterrupted traffic.



Link recovery

After the link is restored to normal, if the ERPS ring is configured in the failback mode, the device where the RPL owner port is located will block the traffic on the RPL link again, and the failed link will be used again to complete the transmission of user traffic.

6.3. Configuration command

Create ERPs ring

SWITCH(config)#**erps ring** *<1-255>* **east-interface** *IFNAME* **west-interface** *IFNAME*

ERPs ring is composed of a group of layer-2 switching devices with the same control VLAN and interconnection, which is the basic unit of ERPs protocol. Each device in the ring needs to be configured

Ring number is the unique identification of ERPs ring

Create ERPs instance

SWITCH(config)#**erps instance** *NAME*

At the same time, it will enter the instance configuration mode

For layer 2 devices running ERPs protocol, the VLAN that transmits ERPs protocol packets and data packets must be mapped to the protection instance, so that the ERPs protocol can forward or block these packets according to its blocking principle. Otherwise, VLAN packets may produce broadcast storm in the ring network, resulting in network unavailability

Associate ERPs instances and rings

SWITCH(config-erps-inst)#**ring** <*1-255*>

Configure the correspondence between ERPs instances and rings

Configure ERPs instance level

SWITCH(config-erps-inst)#**level** <*0-7*>

Configure ERPs instance level

Configure the configuration template used by the ERPs instance

SWITCH(config-erps-inst)#**profile** *NAME*

Configure ERPs configuration template name

Configuring RPL roles in ERPs instances

SWITCH(config-erps-inst)#**rpl-role** *XXX*

An ERPs ring has only one RPL owner port, which is determined by the user configuration. The RPL owner port is blocked to forward the user traffic to prevent the generation of loops in the ERPs ring

Configure management VLAN of ERPs instance

SWITCH(config-erps-inst)#**vlan** <2-4094> **raps-channel**

Configure / delete management VLAN of ERPs instance

Each ERPs ring must be configured with a management VLAN, and different ERPs rings must use different management VLANs

Configuration of intersecting sub ring resistor

SWITCH(config-erps-inst)#**sub-ring block** {**east-interface | west-interface**}

Configure ERPs instance as sub ring instance, and specify sub ring resistance

Configure the MST instance associated with the ERPs instance

SWITCH(config-erps-inst)#**id** <*0-255*>

The default MST instance ID is 0

Associate the VLAN indirectly by associating MST instance ID (see "configuring the corresponding relationship between MST VLAN and instance" in configuring STP spanning tree protocol for details)

Changing MST instances is not currently supported in intersecting rings

Configure virtual channel and non virtual channel of subring

SWITCH(config-erps-inst)#**virtual-channel attached-to-instance** *NAME*

SWITCH(config-erps-inst)# **non-virtual-channel**

Configure the type of ERPs intersecting subring: virtual channel, and associate the type of main ring or non virtual channel

The display position of this command in show running config must be after the display position of the associated instance. Generally, you only need to ensure that the ID and instance name of the subring are larger than those of the primary ring

Create ERPs configuration template

SWITCH(config)#**erps profile** *NAME*

Create ERPs configuration template and enter ERPs template configuration mode after successful creation

Configure the switchback mode of ERPs template

SWITCH(config-erps-prof)#**revertive**

Configure ERPs automatic Switchback

Configure timer parameters of ERPs template

SWITCH(config-erps-prof)#**timer** {**wait-to-restore** {*<1-12>* | **default**} | **hold-off** {*<0-100>* | **default**} | **guard-timer** {*<1-200>* | **default**}}

wait-to-restore: Unit minute; The failback time after recovery is 5 minutes by default

hold-off：The unit is 100 ms;The holding time before port forward is 0 by default, and direct forward is not delayed;

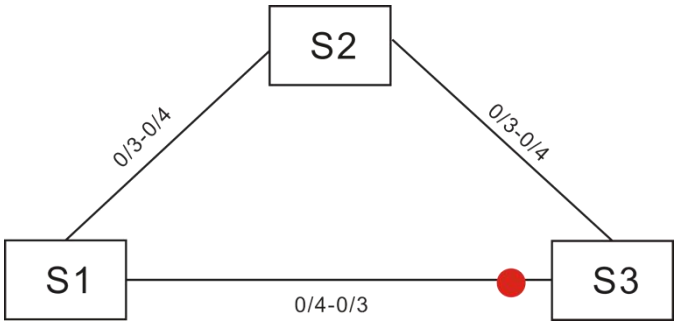
guard-timer：The unit is 10ms; the protection window when the state changes to avoid misjudgment caused by receiving the previous state message, the default value is 50:500ms

The guard timer parameter will limit the network scale to a certain extent. It is conservatively recommended that when there are more than 300 nodes in the ring network, the parameter should be directly set to the maximum value to avoid that the old packets can not be discarded normally due to the large network scale; no special configuration is required for nodes within 300;

6.4. Configuration case

Case : single ring

As shown in the topology in the figure below, the direct link of S1 and S2 is blocked by default, and the link is recovered in time in case of failure to ensure the availability of the network. The data VLANs are 1, 2 and 3.



Switch S1, S2 configuration

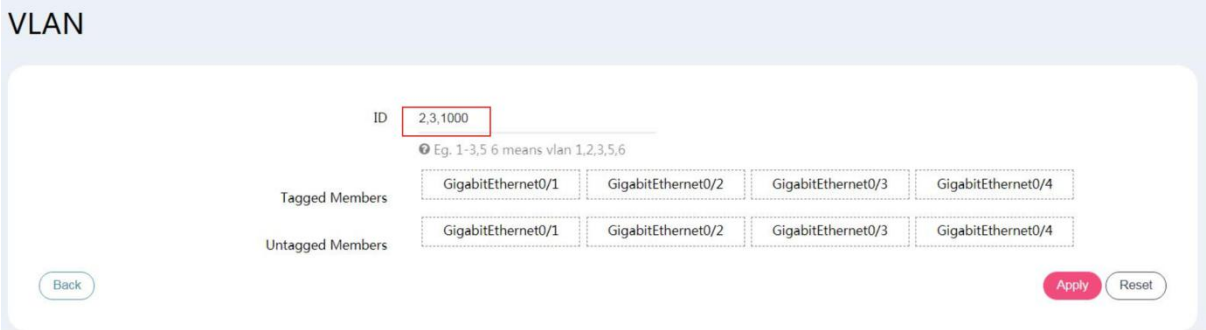
- CLI Reference configuration

```
SWITCH(config)#vlan 2,3,1000

SWITCH(config)#interface GigabitEthernet0/3-4

SWITCH(config-if)#switchport mode trunk

SWITCH(config)#erps ring 1 east-interface GigabitEthernet0/3 west-interface
      GigabitEthernet0/4

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
```

- Web reference configuration

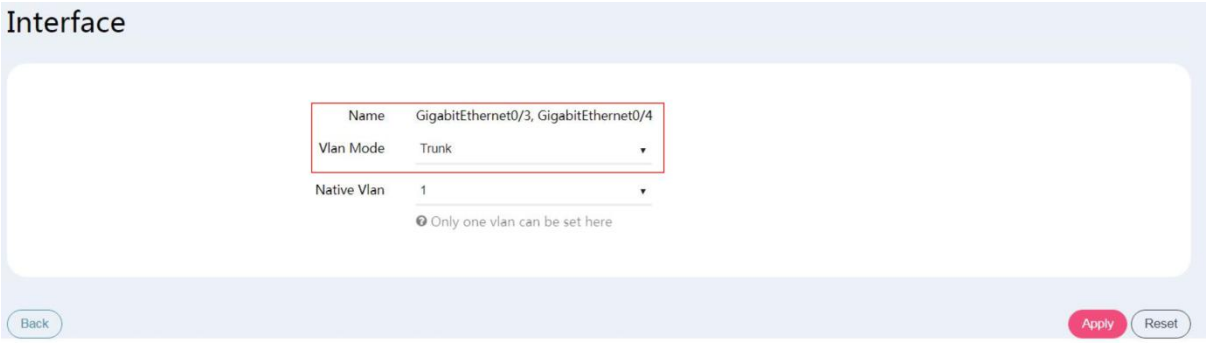
1) Add VLAN 2, 3, 1000

Add VLAN in Homepage -> L2 Switch -> VLAN, and then click apply



2) Gigabit Ethernet 0 /3-4 is configured as trunk port

Select the port to be configured in Homepage -> L2 Switch -> VLAN, click Edit, modify port VLAN mode, and then click apply.

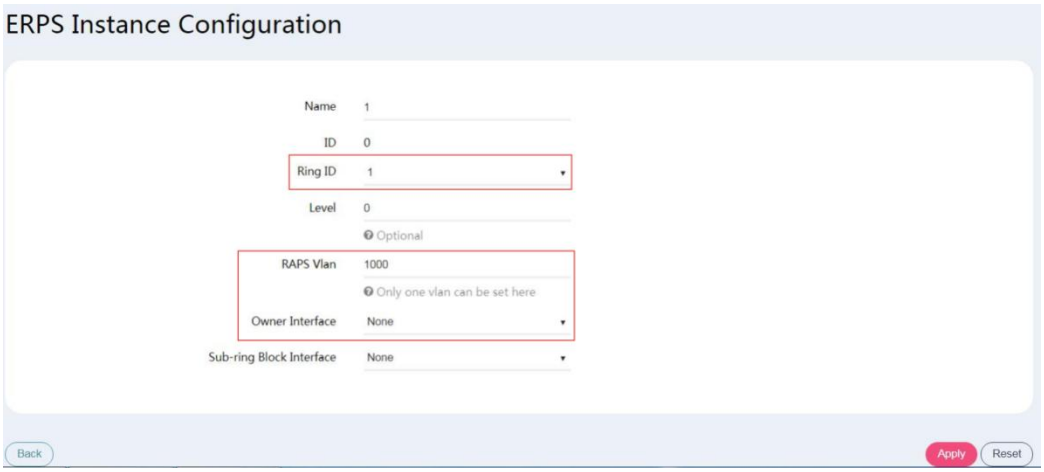


3) Add ERPs ring 1

Add the ERPs ring configuration in Homepage -> L2 Switch -> ERPS, select the corresponding port, and then click apply

4) Add ERPs instance 1

Add ERPs instance configuration in Homepage -> L2 Switch -> ERPS, select the corresponding ring number, manage VLAN and whether the owner interface, and then click apply



Switch S3 reference configuration

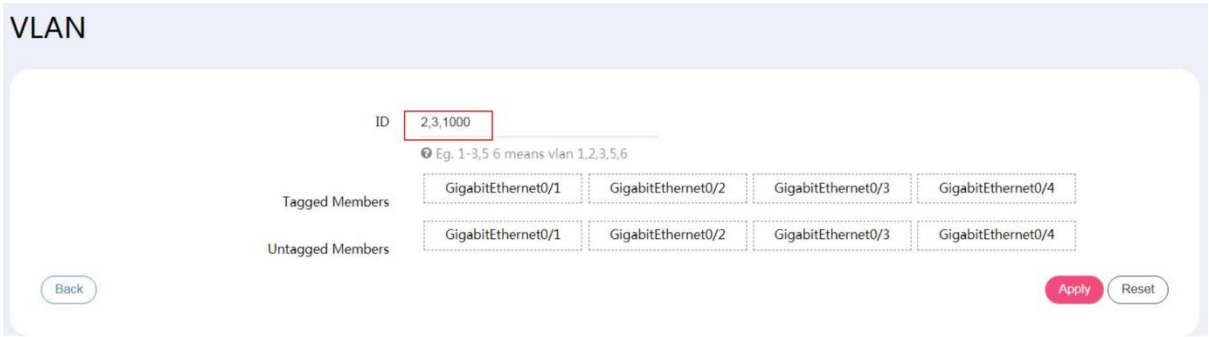
- CLI Reference configuration

```
SWITCH(config)#vlan 2,3,1000

SWITCH(config)#interface GigabitEthernet0/3-4

SWITCH(config-if)#switchport mode trunk

SWITCH(config)#erps ring 1 east-interface GigabitEthernet0/3 west-interface
      GigabitEthernet0/4

SWITCH(config)#erps instance 1

SWITCH(config-erps-inst)#ring 1

SWITCH(config-erps-inst)#rpl-role owner east-interface

SWITCH(config-erps-inst)#vlan 1000 raps-channel
```

- Web reference configuration

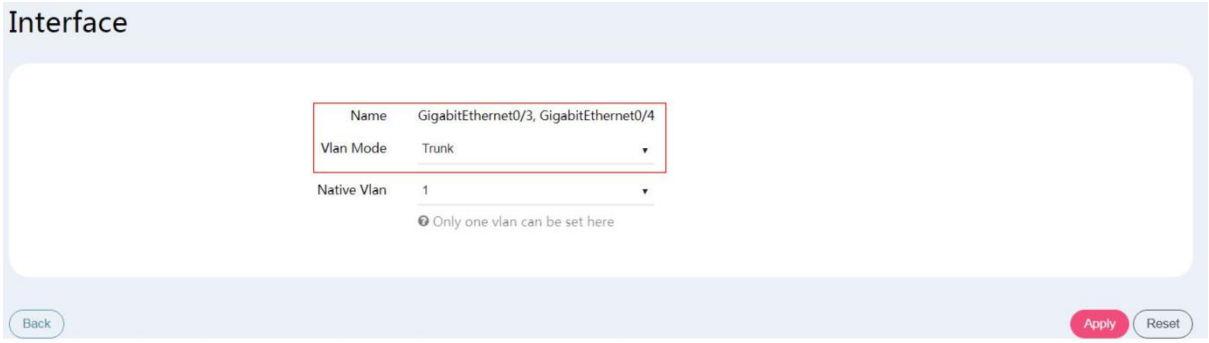
1) Add VLAN 2,3,1000

Add VLAN in Homepage -> L2 Switch -> VLAN, and then click apply



2) Gigabit Ethernet 0 / 3-4 is configured as trunk port

Select the port to be configured in Homepage -> L2 Switch -> VLAN, click Edit, modify port VLAN mode, and then click apply.

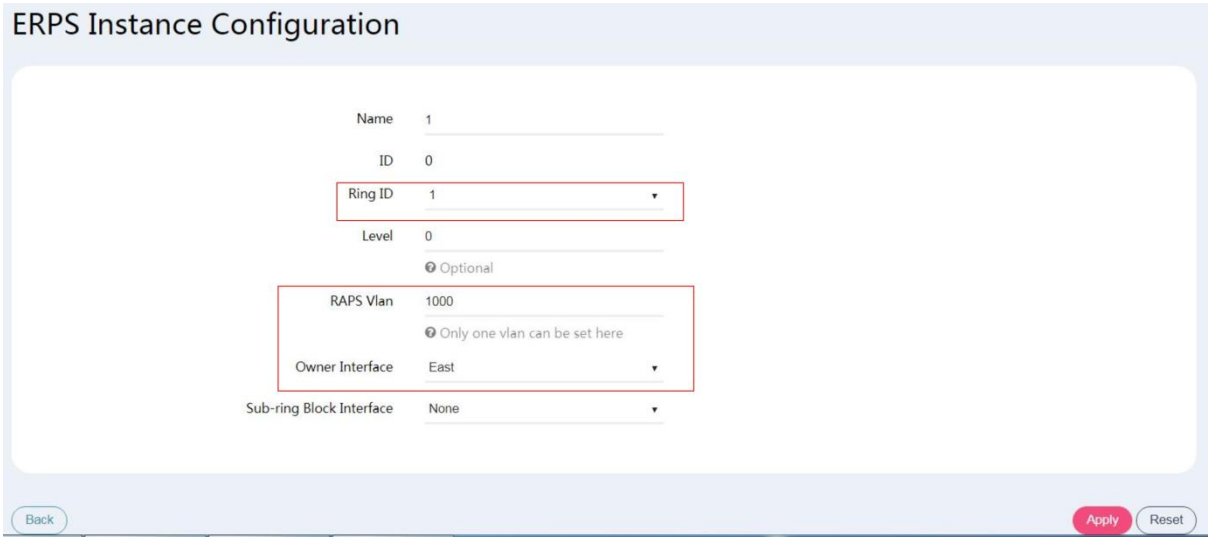


3) Add ERPs ring 1

Add the ERPs ring configuration in Homepage -> L2 Switch -> ERPS, select the corresponding port, and then click apply

4) Add ERPs instance 1

Add ERPs instance configuration in Homepage > L2 Switch > ERPS, select the corresponding ring number, manage VLAN and whether the owner interface, and then click apply.



6.5. Show command

Show ERPS Ring

SWITCH#**show erps ring** *<1-255>*

```
SWITCH#show erps ring 1


Ring     : 1
==========
Bridge   : 1
East     : GigabitEthernet0/9
West     : GigabitEthernet0/10
ERP Inst :1,
```

Show ERPS instance

SWITCH#**show erps instance** *NAME*

```
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)
West 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 Configuration template

SWITCH#**show erps profile** *NAME*

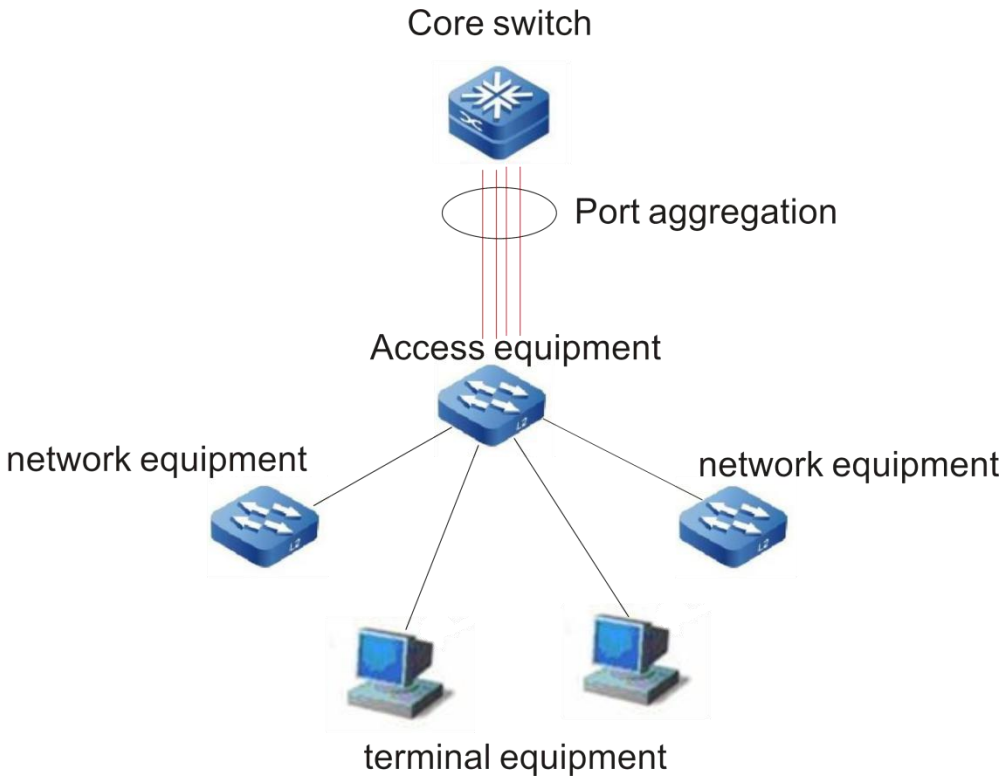
```
SWITCH#show erps profile 1


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

7. Port aggregation

The Web management path: Homepage -> Interface -> Port Aggregation

7.1. Port aggregation overview

Multiple physical links are bundled together to establish a logical link. This logical link is called port channel port, and this function is called port aggregation function. The function of aggregation port conforms to IEEE802.3ad standard. It can be used to expand link bandwidth and provide higher connection reliability. It is often used to connect ports, as shown in the figure below



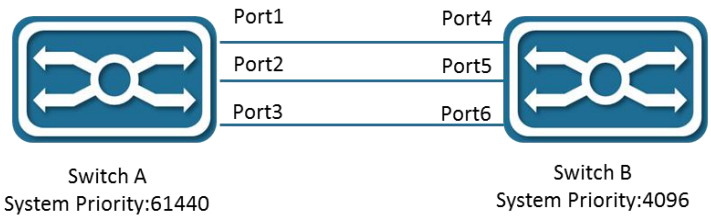
The aggregation port has the following characteristics: high bandwidth, the total bandwidth of the aggregation port is the sum of the bandwidth of the physical member ports; it supports a traffic balancing strategy, which can allocate traffic to each member link according to the strategy; supports link backup, when one of the aggregation ports When a member link is disconnected, the system will automatically distribute the traffic of the member link to other valid member links in the aggregation port.

7.2. LACP overview

LACP (Link Aggregation Control Protocol) based on the IEEE802.3ad standard is a protocol for dynamic link aggregation. If the port is enabled with LACP protocol, the port will send

LACPDU to announce its own system priority, system MAC, port priority, port number, operation key, etc. After the connected device receives the LACP packet from the opposite end, it compares the system priorities of both ends according to the system ID in the packet. At the end with the higher system ID priority, the ports in the aggregation group will be set in the aggregation state according to the port ID priority from high to low, and updated LACP packets will be sent. After the peer device receives the packets, The corresponding port will also be set to the aggregation state, so that the two parties can reach the same when the port leaves or joins the aggregation group. Only after the ports of both parties complete the dynamic aggregation and binding operation, the physical link can forward data packets.

After LACP member port links are bound, periodic LACP packets interaction will be performed. When the LACP packet is not received for a period of time, the packet is considered to be timed out, the member port link is unbound, and the port is not forwardable again. status. There are two modes of timeout here: long timeout mode and short timeout mode. In long timeout mode, the port sends a packet every 30 seconds. If the peer packet is not received in 90 seconds, it is in 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 opposite end in 3 seconds, it is in a packet receiving timeout.



As shown in the figure above, switch A and switch B are connected together through 3 ports. Set the system priority of switch A to 61440, and set the system priority of switch B to 4096. Open LACP link aggregation on the three directly connected ports of switches A and B, set the aggregation mode of the three ports to active mode, and set the port priority of the three ports to the default priority of 32768.

After receiving the LACP packet from the opposite end, switch B finds that its system ID priority is higher (the system priority of switch B is higher than that of switch A), so it follows the order of port ID priority (in the case of the same port priority) , According to the port number from small to large) set ports 4, 5, and 6 to be in aggregation state. After switch A receives the updated LACP packet from switch B, it finds that the system ID of the opposite end has a higher priority and sets the port to the aggregation state, and also sets the ports 1, 2, and 3 to the aggregation state.

7.3. Configuration command

Port join static aggregation port

SWITCH(config-if)#**channel-group** *ID* (**mode manual)**

Port join dynamic aggregation port

SWITCH(config-if)#**channel-group** *ID* **mode** {**active** | **passive**}

Support 12 aggregation ports <1-12>;

An aggregate port is either static or dynamic, which is determined by the joining mode of the first member port

Active aggregation mode means that the port will initiate LACP aggregation operation actively; passive aggregation mode means that the port will not initiate LACP aggregation operation actively, but will participate in LACP calculation passively after receiving LACP packets from neighbors

When the port channel port is not created and the first port is added to the aggregate port, the port channel port is created actively, and the default attribute of the port channel port is the port attribute;

The premise of port joining aggregation port is the same as the following basic properties of aggregation port

- VLAN attribute configuration of port
- Port isolation configuration

Configure LACP system priority

SWITCH(config)#**lacp system-priority** *system-priority*

The system priority range is < 1-65535 >, and the default 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;

Configure LACP port priority

SWITCH(config-if)#**lacp port-priority** *port-priority*

Port priority is configured in interface mode, only physical port configuration is supported

The system priority range is < 1-65535 >, and the default is 32768

Configure LACP port timeout mode

SWITCH(config-if)#**lacp timeout** {**long | short**}

The port timeout mode is configured in the interface mode and only supports physical port configuration

The default mode is long mode, LACP packets sending interval is 30s, 90s timeout; short mode, LACP packets sending interval is 1s, 3S timeout

7.4. Configuration case

Configure Gigabit Ethernet 0 / 5 and Gigabit Ethernet 0 / 6 ports to join port-channel1

```
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
```

7.5. Show command

Show aggregation port configuration and status information

SWITCH#**show port-channel**

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

Interface Port-Channel3
  Type: static
  Member:
    GigabitEthernet0/5     link down     Disable

Interface Port-Channel8
  Type: LACP
  Member:
    GigabitEthernet0/7     link up       Enable
    GigabitEthernet0/8     link up       Enable
```

Show aggregate port load balancing mode

This switch does not support port load balancing mode configuration and can only use source destination MAC address mode

SWITCH#**show port-channel load-balance**

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

Show LACP brief information

SWITCH#**show lacp summary**

```
SWITCH#show lacp summary
% Aggregator Port-Channel8 1008
% Aggregator Type: Layer2
% Admin Key: 0008 - Oper Key 0008
%   Link: GigabitEthernet0/7 (7) sync: 1 status: Bundled
%   Link: GigabitEthernet0/8 (8) sync: 1 status: Bundled
```

Show LACP details

SWITCH#**show lacp detail**

```
SWITCH#show lacp detail
% Aggregator Port-Channel 8 1008
% Aggregator Type: Layer2
%  Mac address: 00:02:04:ee:25:46
%  Admin Key: 0008 - Oper Key 0008
%  Actor LAG ID- 0x8000,00-02-04-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: GigabitEthernet0/7 (7) sync: 1 status: Bundled
%   Link: GigabitEthernet0/8 (8) sync: 1 status: Bundled
```

Show LACP packets statistics

SWITCH#**show lacp counter**

```
SWITCH#show lacp counter
```

```
% Traffic statistics
  Port        LACPDUs        Marker       Marker-Rsp       Pckt err
              Sent   Recv    Sent   Recv   Sent   Recv     Sent   Recv
% Aggregator Port-Channel8 1008
GigabitEthernet0/7   23     13     0      0      0      0        0      0
GigabitEthernet0/8   25     15     0      0      0      0        0      0
```

Show LACP system ID

SWITCH#**show lacp sys-id**

```
SWITCH#show lacp sys-id
% System 8000,00-02-04-ee-25-46
```

Show LACP port information

SWITCH#**show lacp** *ID*

```
SWITCH#show lacp 8
% Aggregator Port-Channel8 1008 Admin Key: 0008 - Oper Key 0008
% Partner LAG ID: 0x8000,00-01-a0-00-10-10,0x0032
% Partner Oper Key 0050
```

Show LACP member port information

SWITCH#**show lacpport** *IFNAME*

```
SWITCH#show lacp port GigabitEthernet0/19
% LACP link info: GigabitEthernet0/19 - 19
% LAG ID: 0x8000,00-02-04-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

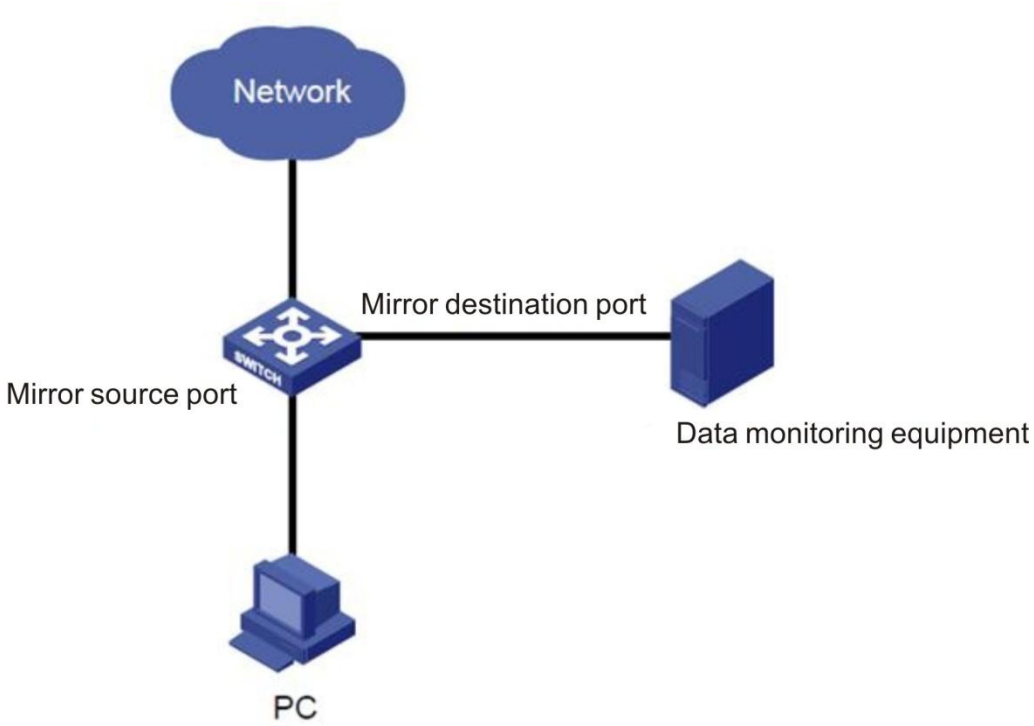
% Aggregator ID: 1008

8. Configure SPAN

The Web management path: Homepage –> Interface -> Port Mirror

8.1. SPAN Overview

SPAN (local Switched Port Analyzer) is a local mirror function. The span function copies the packets from the specified port to the destination port. Generally, the span destination port will access data detection devices. Users can use these devices to analyze the packets received by the destination port for network monitoring and troubleshooting.



SPAN does not affect the packet switch between the source port and the destination port, but copies all ingress and egress packets from the source port to the destination port. When the mirror traffic of the source port exceeds the bandwidth of the destination port, for example, if the 100 Mbps destination port monitors the traffic of the 1000 Mbps source port, the packet may be discarded.

Based on session management, the source port and destination port of span are configured in the session. In a session, there can only be one destination port, but multiple source ports can be configured at the same time.

8.2. Configuration command

Create session

SWITCH(config)#**monitor session** *ID*

Create a session and enter session mode at the same time

7 sessions are supported

Configure session description

SWITCH(config-monitor)#**description** *DESCRIPTION*

Configure session source port

SWITCH(config-monitor)#**source interface** *IFNAME* {**both | rx | tx**}

Configure session destination port

SWITCH(config-monitor)#**destination interface** *IFNAME*

8.3. Configuration case

The port of GigabitEthernet 0/8 is used to monitor the ingress packets of GigabitEthernet 0/1 and the ingress and egress packets of GigabitEthernet 0/2. The monitoring session is described as "traffic"_ MONITOR"

```
SWITCH#configure terminal
SWITCH(config)#monitor session 1
SWITCH(config-monitor)#
SWITCH(config-monitor)#description TRAFFIC_MONITOR
SWITCH(config-monitor)#source interface GigabitEthernet0/1 rx
SWITCH(config-monitor)#source interface GigabitEthernet0/2 both
SWITCH(config-monitor)#destination interface GigabitEthernet0/8
```

8.4. Show command

Show specific sessions

SWITCH#**show monitor session** *ID*

```
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
```

9. Storm control

The Web management path: HomePage -> Interface -> Storm Control

9.1. Storm control overview

When there is too much broadcast, multicast or unknown unicast data flow in LAN, it will lead to network performance degradation and even network paralysis, which is called broadcast storm. Storm control limits the speed of broadcast, multicast and unknown unicast data streams. When the rate of broadcast, unknown name multicast or unknown unicast data stream received by the switch port exceeds the set bandwidth, the device will only allow the data stream through the set bandwidth, and the data stream beyond the bandwidth will be discarded, so as to avoid excessive flooding data stream into the LAN to form a storm

9.2. Configuration command

Configure interface storm control strategy

SWITCH(config-if)#**storm-control** {**broadcast | multicast | unicast | all | unicast-broadcast | multicast-broadcast**} **level** *LEVEL*

It supports the selection of configuration in broadcast / multicast / unicast / all / unicast broadcast / multicast broadcast, which cannot coexist

Where multicast is unknown multicast packet and unicast is unknown list broadcast packet. The level value is the percentage of port bandwidth, which supports adaptive port rate change

9.3. Configuration Case

Configure port Gigabitethernet 0/1, speed limit of unknown multicast is 10% of total bandwidth

```
SWITCH#configure terminal
SWITCH(config)#interface GigabitEthernet0/1
SWITCH(config-if)#storm-control multicast level 10
```

9.4. Show command

Shows all port storm control configurations

SWITCH#**show storm-control**

```
SWITCH#show storm-control
Port                BcastLevel    McastLevel    Unicastlevel
GigabitEthernet0/1      100.00%       100.00%       100.00%
GigabitEthernet0/2      100.00%       100.00%        50.00%
GigabitEthernet0/3       80.00%       100.00%       100.00%
GigabitEthernet0/4      100.00%       100.00%       100.00%
GigabitEthernet0/5      100.00%       100.00%       100.00%
GigabitEthernet0/6      100.00%       100.00%       100.00%
```

10. Configuration SNMP

The Web management path: HomePage -> System -> SNMP

The current Web mangament only supports V2C.

10.1. SNMP overview

SNMP is an acronym for Simple Network Management Protocol, which became a network management standard in August 1988, RFC 1157, and is now the de facto network management standard for interconnected multi-vendor systems due to the support of many manufacturers.

The SNMP protocol allows network administrators to query information, network configuration, fault location, capacity planning, and network monitoring and management of nodes on the network, which are the basic functions of SNMP.

The following versions of SNMP currently 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 : Provides the following security features by authenticating and encrypting data.

    1) Ensures that data is not tampered with during transmission.

    2) Ensures that data is sent from a legitimate data source.

    3) Encrypts messages to ensure data confidentiality.

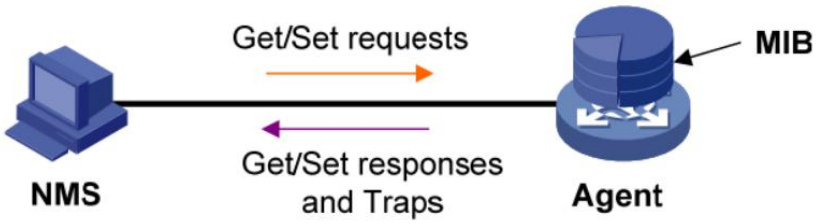
SNMP networks contain two elements, NMS and Agent.

- The NMS (Network Management System) is the manager of the SNMP network and provides a friendly human-machine interface that allows network administrators to perform most network management tasks.

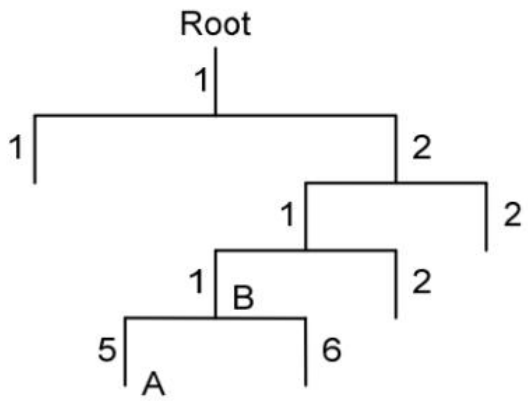
- The Agent is the manager of the SNMP network and is responsible for receiving and processing request messages from the NMS. In some emergency situations, such as interface status changes, the Agent will actively send alarm messages to the NMS.

When the NMS manages the device, it usually pays more attention to some parameters, such as interface status, CPU utilization, etc. The collection of these parameters is called MIB (Management Information Base). These parameters are called nodes in the MIB, and the MIB defines a hierarchical relationship between nodes and a set of properties of the objects, such as their names, access rights, and data types. Each Agent has its own MIB, and each managed device has its own MIB file, which is compiled on the NMS to generate the MIB for that device. the NMS performs read/write operations on the MIB nodes according

to the access rights to manage the Agent. the relationship between the NMS, Agent, and MIB is as follows.



The MIB is organized in a tree structure, which consists of many nodes, each of which represents a managed object that can be uniquely identified by a string of numbers representing a path starting from the root, called an OID (Object Identifier). As shown in the following figure.



Managed object B can be uniquely identified by a string of numbers {.1.2.1.1}, which is the OID of managed object B.

SNMP provides three basic operations to enable the interaction between the NMS and the Agent.

- GET operation: The NMS uses this operation to query the value of one or more nodes in the Agent MIB.
- SET operation: The NMS uses this operation to set the value of one or more nodes in the Agent MIB.
- Trap operation: The Agent uses this operation to send a Trap message to the NMS; the Agent does not require the NMS to send a response message. The NMS does not respond to the Trap message either.

The SNMP Agent currently supports SNMPv1, SNMPv2c, and SNMPv3 versions.

- SNMPv1 uses the Community Name authentication mechanism. The Community Name is similar to a password and is used to restrict communication between the NMS and the Agent. If the group name set by the NMS is different from the group name set on the managed device, the NMS and the Agent cannot establish an SNMP connection, thus

the NMS cannot access the Agent, and the alert messages sent by the Agent will be discarded by the NMS.

- SNMPv2c also adopts the group name authentication mechanism. SNMPv2c extends the functions of SNMPv1: it provides more operation types, supports more data types, and provides richer error codes to distinguish errors more carefully.
- SNMPv3 uses the USM (User-Based Security Model) authentication mechanism. Network administrators can set up authentication and encryption functions. Authentication is used to verify the legitimacy of the message sender to avoid access by illegal users; encryption is used to encrypt the transmission messages between NMS and Agent to avoid eavesdropping. With authentication and encryption, the communication between NMS and Agent can be more secure.

SNMPv1 and SNMPv2c versions use group names to identify whether or not they are authorized to use MIB objects. In order to be able to manage the device, the authentication name of the Network Management System (NMS) must match one of the group names defined in the device. A group name can have the following attributes.

- Read-only (Read-only): Provides authorized management workstations with read access to all MIB variables. A prerequisite for a successful connection between the NMS and the Agent is that the NMS and the Agent use the same version of SNMP.
- Read-write: Provides read and write access to all MIB variables for authorized management workstations.

Based on SNMPv2, SNMPv3 uses a security model to determine which security mechanism to use for data processing; there are three categories of security models available: noauth, auth, and priv.

- noauth: no security authentication is required; this security model is used by both SNNMPv1 and SNMPv2c.
- auth: security authentication is required, but the transmitted message PDUs are not encrypted.
- priv: Both security authentication and encryption of the transmitted message PDUs are required.

The details are shown in the following table.

Version	Security Model	Identification	Encryption	Description
v1	noauth	Community	None	Confirmation of data legitimacy by community name
v2c	noauth	Community	None	Confirmation of data legitimacy by community name
v3	noauth	User	None	Confirmation of data legitimacy by user name
v3	auth	MD5 or SHA	None	Provide MD5 or SHA based authentication mechanism for username and password.

v3	priv	MD5 or SHA	AES or DES	Provide MD5 or SHA based authentication mechanism for user name and password, and AES or DES based data encryption mechanism.

10.2. Configuration command

Configure SNMP View

SWITCH(config)# **snmp-server view** *WORD OID-TREE* **(include | exclude)**

An SNMP view can define several Oid-trees, and an Oid-tree is composed of two parts: oid and include. For example, ".1.3.6.1.2.1.1" include means that all MIB nodes under the "system" node belong to this view; ".1.3.6.1.2.1. 1" exclude means all the MIB nodes under the "system" node belong to this view except for the MIB nodes under the "system" node.

The length of view name ranges from 1 to 31, and the length of OID-TREE string ranges from 2 to 63. ".1" exclude means match all MIB nodes, and if Group does not specify view, it will match all MIB nodes by default.

To delete a view, use the command "no snmp-server view WORD (OID-TREE (include | exclude) |)" to delete only one of the Oid-trees or the whole view.

The view defines the range of MIB nodes that can be accessed. However, for a view to take effect, it must be associated by a valid group.

Configure SNMP Group

SWITCH(config)# **snmp-server group** *WORD* **(v3 (auth | noauth | priv) |) (read (null |** *READ-VIEW*) **|) (write (null |** *WRITE-VIEW*) **|)**

The SNMP group distinguishes between v3 and non-v3 versions (i.e., v1 and v2c). If it is a v3 version, define the security model for the group. group name length ranges from 1-31.

Optionally, configure the read view and write view of the group, that is, the range of MIB nodes that the group can read and the range of MIB nodes that can write. If view is not specified, it means that the MIB node range is all. If the keyword null is specified, it means that the corresponding operations on all MIB nodes are prohibited. read null means that read operations are prohibited; write null means that write operations are prohibited.

The view associated with the group must exist, otherwise the group will not be created successfully. Similarly, if the view associated with the group is deleted, the group will also be deleted automatically.

To delete a group, use the command "no snmp-server group WORD".

For a group to take effect, it must be associated by community (non-v3 version) or by user (v3 version).

Configure SNMP Community

SWITCH(config)# **snmp-server community** *WORD* **(group** *WORD* **| (ro |) |)**

Community length range is 1-31. community is used for SNMPv1 and SNMPv2c versions.

If the community is not associated with a group, you can specify that the community has read-only access to all MIB nodes with the ro keyword, or that the community has read-write access to all MIB nodes without any parameters.

The community must be associated with an existing non-v3 group; if the group does not exist or the version does not match, the community will not be created. Similarly, if the group associated with a community is deleted, the community will be automatically deleted.

After a community is associated with a group, the range of read and write MIB nodes will be determined by the range defined by the group (actually, it is determined by the view associated with the group).

To delete a community, use the command "no snmp-server community WORD".

Configure SNMP User

SWITCH(config)# **snmp-server user** *WORD* **(group** *WORD* **|) (((encrypted|) auth (md5 | sha)** *AUTH-PASSWORD*) **((priv (des | aes)** *PRIV-PASSWORD*) **|) |)**

user (user name) length range is 1-31. user is used for SNMPv3 version.

user can be associated with no group, when the access range is readable and writable to all MIB nodes.

The encrypted keyword is used to refresh the configuration and is not used during the configuration.

The auth and priv parameters are optional. The auth parameter is used to configure the algorithm for secure authentication, MD5 or SHA, and the password for secure authentication; the priv parameter is used to configure the algorithm for encrypting messages, AES and DES, and the password for encryption. The length of the authentication and encryption passwords ranges from 8 to 31.

The security model of user is determined by the auth and priv parameters. If no auth and priv parameters are configured, the security model is noauth; if auth parameters are configured without priv parameters, the security model is auth; if both auth and priv parameters are configured, the security model is priv.

If user configures the associated group, user must be associated with a group that exists and the version is v3. If the group does not exist or the version does not match, then user will not be created successfully. Similarly, if the group associated with user is deleted, the user will be deleted automatically.

After a user is associated with a group, the range of read and write MIB nodes will be determined by the range defined by the group (actually, it is determined by the view associated with the group).

Since both user and its associated group have defined security models, the available security models when accessing the SNMP agent are shown in the following table.

User security model	Group security model	Available security model
noauth	noauth	noauth
noauth	auth	none
noauth	priv	none
auth	noauth	noauth, auth
auth	auth	auth
auth	priv	none
priv	noauth	noauth, auth, priv
priv	auth	auth,priv
priv	priv	priv

The security model of user cannot be configured lower than group. For example, if the security model of group is auth and the security model of user is noauth, then the actual required security model is auth, but at this time user is not configured with auth parameters, therefore, the user cannot access any MIB node.

To delete user, use the command "no snmp-server user WORD".

Configure SNMP Host

SWITCH(config)# **snmp-server host (***A.B.C.D* | *X:X::X:X***) (traps | informs) (v1 | v2c | v3 (auth | noauth | priv))** *WORD* **(udp-port** *<1-1024>* **|)**

The host refers to the server receiving the SNMP trap, and can be represented by either an ipv4 address or an ipv6 address.

The message sent can be of either trap or inform type.

The parameter (v1 | v2c | v3 (auth | noauth | priv)) is used to determine the SNMP version and security model for the sent message.

The WORD parameter indicates the group name (community) or user name (user) of the sending message, corresponding to v1 and v2c versions using community and corresponding to v3 versions using user.

The optional parameter udp-port indicates that a non-default udp port number is used to send the message. The default udp port number is 162.

Multiple hosts can be configured at the same time, and the key of host is ip address, message type (traps or informs) and corresponding SNMP version. That is, multiple hosts can be configured simultaneously with the same ip address, different message types or corresponding SNMP versions.

A host can be configured with only one community or user, indicating which community or user is used to send messages.

To delete a host, use the command "no snmp-server host (A.B.C.D | X:X::X:X) (traps | informs) (v1 | v2c | v3)".

Configure SNMP TCP session

SWITCH(config)# **snmp-server tcp-session**

SNMP is based on UDP protocol by default, but can be configured based on TCP protocol.

To restore the UDP protocol, use the command "no snmp-server tcp-session".

Disable SNMP Trap

SWITCH(config)# **no snmp-server trap enable**

SNMP trap is enabled by default, but you can turn off trap (including inform) for the corresponding agent with the above command.

To turn trap back on, use the command "snmp-server trap enable".

Configure SNMP agent contact

SWITCH(config)#**snmp-server contact** *EMAIL*

This attribute corresponds to the MIB node ".1.3.6.1.2.1.1.4.0".

Configure SNMP agent location

SWITCH(config)#**snmp-server location** *LOCATION*

This attribute corresponds to the MIB node ".1.3.6.1.2.1.1.5.0".

10.3. Configuration case

Configure SNMP Agent：

- SNMPv2c, configure read-only community as ro-com; configure read-write community as com-mib for OID-Tree of .1.3.6.1.2.1.
- SNMPv3, configure user user-root (noauth) who can read and write all MIBs; configure user user-ro (noauth) who can read all MIBs; configure user user-1 (noauth) who can read and write with an OID-Tree of .1.3.6.1.2; configure user user-root who can read all MIBs, user-2 (auth) who can write all MIBs except those with an OID-Tree of .1.3.6.1.2.1.2, and user-3 (priv).

Configure the SNMP Trap host：

- Configure IPv4 host 192.168.1.100 traps, corresponding to user-2, and host 192.168.2.100 informs, corresponding to community com-mib.
- Configure the IPv6 host [2060::5] informs, corresponding to user-3.

The configurations corresponding to the above configuration requirements are as follows.

SWITCH#configure terminal	SWITCH#confi

```
SWITCH(config)# snmp-server view mib2 .1.3.6.1.2.1 include
SWITCH(config)# snmp-server view except-if .1.3.6.1.2.1.2 exclude
SWITCH(config)# snmp-server group v2c-g-mibs read mib2 write mib2
SWITCH(config)# snmp-server group v3-ro-g v3 noauth write null
SWITCH(config)# snmp-server group v3-g-mibs v3 noauth read mib2 write mib2
SWITCH(config)# snmp-server group v3-g-w-except-if v3 noauth write except-if
SWITCH(config)# snmp-server community ro-com ro
SWITCH(config)# snmp-server community com-mib group v2c-g-mibs
SWITCH(config)# snmp-server user user-root
SWITCH(config)# snmp-server user user-ro group v3-ro-g
SWITCH(config)# snmp-server user user-1 group v3-g-mibs
SWITCH(config)# snmp-server user user-2 group v3-g-w-except-if auth sha test-passwd
SWITCH(config)# snmp-server user user-3 group v3-g-w-except-if auth md5 test-passwd
priv des test-passwd
SWITCH(config)# snmp-server host 192.168.1.100 traps v3 auth user-2
SWITCH(config)# snmp-server host 192.168.2.100 informs v2c com-mib
SWITCH(config)# snmp-server host 2060::5 informs v3 priv user-3
```

10.4. Show command

show snmp-server (user | community | group | view | host |)

If you bring user, or community, or group, or view, or host, only the configuration information of the corresponding item is viewed, if you do not bring any parameters, then all configuration information is viewed.

```
SWITCH#show snmp-server
SNMP TCP Session: Disable
SNMP Trap: Enable
SNMP server view configuration
------------------------------------------------------------
View                OID                             Type
------------------+-------------------------------+---------
mib2                .1.3.6.1.2.1                    include
except-if           .1.3.6.1.2.1.2                  exclude

SNMP server group configuration
```

```
-------------------------------------------------------------------
Group                Ver   Sec mod RView               WView
-------------------+-----+-------+------------------+-------------------
v2c-g-mibs           v2c   noauth  mib2               mib2
v3-ro-g              v3    noauth                     null
v3-g-mibs            v3    noauth  mib2               mib2
v3-g-w-except-if     v3    noauth                     except-if

SNMP server community configuration
-------------------------------------------------------------------
Community            Group
-------------------+-------------------
ro-com               [def]:ro
com-mib              v2c-g-mibs

SNMP server user configuration
-------------------------------------------------------------------
User                 Auth    Priv    Group
-------------------+-------+-------+-------------------
user-root                            [def]:noauth
user-ro                              v3-ro-g
user-1                               v3-g-mibs
user-2               sha             v3-g-w-except-if
user-3               md5     des     v3-g-w-except-if

SNMP trap/inform host configuration
-------------------------------------------------------------------
Host Ipaddr                         Type    Ver + Secm  User/Community
---------------------------------+-------+-----------+-------------------
192.168.1.100                       trap    v3 auth     user-2
192.168.2.100                       inform  v2c         com-mib
2060::5                             inform  v3 priv     user-3
```

11. Configure RMON

11.1. RMON overview

SNMP is the most widely used network management protocol in the Internet. The agent software embedded in the device can collect and count the network communication information. The management software sends the query signal to the MIB of the agent through polling to get the information, and realizes the management of the network through the obtained information. Although the MIB counter records the sum of statistics, it can't analyze the history of daily communication. In order to comprehensively view the traffic and traffic changes in a day, the network management software needs continuous polling to analyze the network status through the information obtained.

Using SNMP for polling has two obvious disadvantages

- It takes up a lot of network resources. In large-scale network, a large number of network communication packets will be generated by polling, which will lead to network congestion and even network congestion. Therefore, SNMP is not suitable for managing large-scale network and recovering a large amount of data, such as routing table information.

- The task of collecting data in SNMP polling is completed by the network manager through the network management software. If the network manager monitors more than three network segments, the network manager may be unable to complete the task due to the heavy burden.

In order to improve the availability of management information, reduce the burden of management station, 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, mainly to monitor the data flow of a network segment and even the whole network. Here are the features of RMON:

- SNMP is the foundation of RMON, and RMON is the enhancement of SNMP

RMON is implemented based on SNMP architecture and compatible with the existing SNMP framework. It is still composed of NMS of network management workstation and agent running on various network devices. Because RMON does not use another set of mechanism, NMS and SNMP share the same network management workstation, network managers do not need to carry out additional learning, so the implementation is relatively simple

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

RMON protocol stipulates that the managed device can automatically send trap information when it reaches the alarm threshold, so the management device does not need to obtain the value of MIB variable through polling for comparison, so it can reduce the communication flow between the management device and the managed device, and achieve the purpose of simple and effective management of large-scale interconnection network

RMON allows multiple monitors to collect data in two ways

- Through the special RMON probe, NMS can directly obtain the management information and control the network resources from RMON probe, which can obtain all the information of RMON MIB

- The RMON agent is directly embedded in the network devices, making them network devices with the function of RMON probe. NMS uses SNMP to exchange data information and collect network management information. Due to the limitation of equipment resources, this method can not obtain all the data of RMON MIB, and basically only collects the information of four groups (alarm, event, history and Statistics)

Our equipment adopts the second method to realize the function of RMON agent. Through this function, the management device can obtain the overall traffic, error statistics and performance statistics of the network segment connected with the managed network device interface, and then realize the monitoring of the network.

11.2. RMON related concepts

Before configuring RMON, we need to understand the basic concepts of statistics, history, alarm and event groups defined by RMON specification.

Characteristics of RMON

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

The statistical function of RMON can be realized by RMON statistical group or RMON history group, which is divided into Ethernet statistical function and history statistical function

- Ethernet statistical function (corresponding to the statistical group in RMON MIB): the system counts the basic statistical information of each monitored network. 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 and collision times of various types. The statistical objects include the number of network conflicts, the number of CRC error packets, the number of too small (or too large) packets, the number of broadcast and multicast packets, the number of received bytes, the number of received packets, etc

- History statistics function (corresponding to the history group in RMON MIB): the system regularly collects and stores network status statistics for subsequent processing. The system will count all kinds of traffic information regularly according to the cycle, and the statistical data includes the bandwidth utilization, the number of wrong packets and the total number of packets.

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

- Event definition function (corresponding to event group in RMON MIB): event group controls events and prompts from devices, and provides information about all events generated by RMON agent. When an event occurs, log can be recorded or trap can be sent to the network management station

- Alarm threshold setting function (corresponding to the alarm group in RMON MIB): the system monitors the specified alarm variable (OID corresponding to any alarm object). After the user defines a set of thresholds and sampling time of the specified alarm in advance, the system will

obtain the value of the specified alarm variable according to the defined time cycle. When the value of the alarm variable is greater than or equal to the upper threshold, an upper limit alarm event is triggered; when the value of the alarm variable is less than or equal to the lower threshold, a lower limit alarm event is triggered. RMON agent will record the monitored status as log or send trap to network management station

- Error report notes

The RMON specification (rfc2819) defines multiple RMON groups, and the device implements four groups of statistics, history, alarm and event supported by the public MIB. The following is an introduction to these groups

- Statistics group

The statistics group stipulates that the system will continuously count all kinds of traffic information of the Ethernet interface, and store the statistical results in the Ethernet stats table, so that the management equipment can view them at any time. The statistical information includes the number of network conflicts, CRC error packets, too small (or too large) packets, broadcast, multicast packets, received bytes, received packets, etc.

After the statistics table entry is successfully created under the specified interface, the statistics group will count the number of packets of the current interface, and the result of statistics is a continuous cumulative value

- History group

The history group regularly collects and stores the statistical information of network status for subsequent processing

The history group contains two tables

- It is mainly used to set the sampling interval and other control information
- It is mainly used to store the history group, collect the network status statistics regularly, and provide the network administrator with the historical data of segment traffic, error packets, broadcast packets, utilization rate, collision times and other statistical information

- Event group

The event defined by event group is used in alarm group configuration item and 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 in the specified row of the event table and define the event processing method

- log：Send logs only
- trap：Send trap messages to NMS only
- log-trap：Send both log and trap message to NMS
- none：Do nothing

- Alarm group

The alarm group allows to define a set of thresholds in advance for monitoring the alarm variables (which can be any object of the local MIB). After the user defines the alarm table item, 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 threshold, an upper limit alarm event will be triggered; when the value of the alarm variable is less than or equal to the lower threshold, a lower limit alarm event will be triggered, and the alarm management will carry out corresponding operations according to the event definition handle

11.3. Configuration command

Configure RMON statistics group

SWITCH(config)#**rmon statistics** *<1-65535>* **interface** *IFNAME* {**owner** *OWNERNAME* **|**}

statistics <1-65535>: Statistics group index

owner OWNERNAME: Owner information

Configure RMON history group

SWITCH(config)# **rmon history** *<1-65535>* **interface** *IFNAME* **buckets** *<1-65535>* **interval** *<1-3600>* {**owner** *OWNERNAME* **|**}

histroy <1-65535>: History group index;

buckets <1-65535>: History bucket size;

interval <1-3600>: Recording period in seconds;

owner OWNERNAME: Owner information

Configure RMON event groups

SWITCH(config)#**rmon event** *<1-65535>* **(description** *DESCRIPTION***|) (log | trap** *COMMUNITY* **| log-trap** *COMMUNITY* **| none)** {**owner** *OWNERNAME* **|**}

event <1-65535>: Event group index

description DESCRIPTION: Event description

trap COMMUNITY: Trap community word, Only Trap

log-trapCOMMUNITY: Trap community word, log and trap generated at the same time

owner OWNERNAME: Owner information

Configure alarm group

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* **|**}

alarm <1-65535>: Alarm group index

object 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 cycle, The unit is seconds

absolute | delta: Sampling type, absolute value or difference value

rising-threshold <1-2147483645>: Rise threshold;

<1-65535>: Index of ascending events; index in corresponding event group;

falling-threshold <1-2147483645>: Descent threshold;

<1-65535>: Index of descending events; index in corresponding event group;

owner OWNERNAME: Owner information

Configure log entry upper limit

SWITCH(config)#**rmon max-log** *<1-65535>*

max-log <1-65535>: Upper limit of log 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 generated logs exceeds the limited number of entries, the old logs will be deleted according to the generation time to maintain the upper limit

11.4. Configuration case

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

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

The network management server needs to monitor the input traffic of port 1 of the device through RMON, with a cycle of 10 seconds. Once the number of bytes of the input traffic changes more than 1MB (1000000b), the alarm will be triggered and the log will be recorded

```
SWITCH#configure terminal
SWITCH(config)#snmp-server community public
SWITCH(config)#snmp-server 2.2.2.2 community public
```

```
SWITCH(config)# rmon statistics 1 interface GigabitEthernet0/1 owner abc

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
```

11.5. Show command

Show event group log

SWITCH#**show rmon log**

12. IGMP Snooping

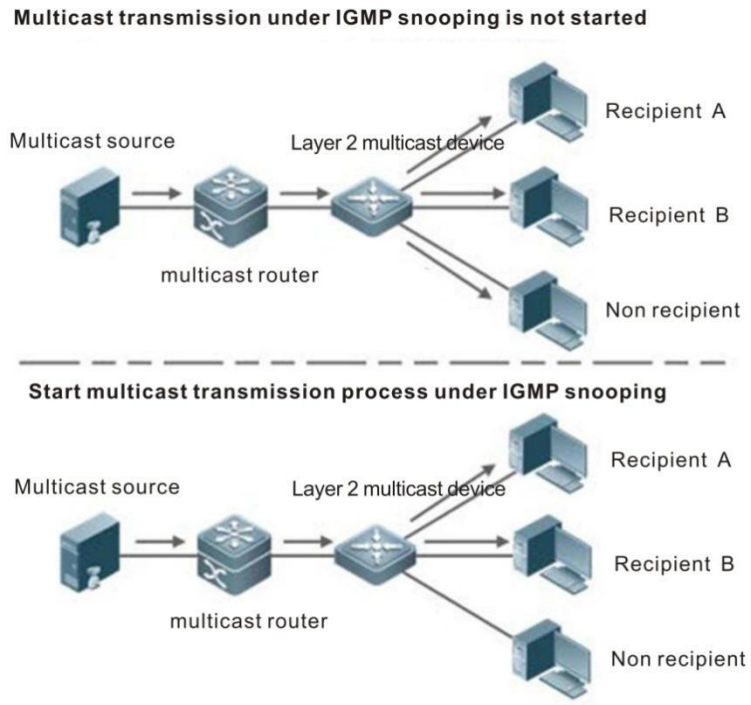
The Web management path: HomePage -> L2 Switch -> IGMP Snooping

12.1. IGMP snooping overview

IGMP snooping is the abbreviation of Internet Group Management Protocol Snooping (Internet Group Management Protocol Snooping). It is a multicast constraint mechanism running on layer 2 devices, which is used to manage and control multicast groups.

By analyzing the received IGMP packets, the layer 2 device running IGMP snooping establishes the mapping relationship between the port and the MAC multicast address, and forwards the multicast data according to the mapping relationship. When IGMP snooping is not running on the layer 2 device, the multicast data is broadcasted on the layer 2 device; when IGMP snooping is running on the layer 2 device, the multicast data of the known multicast group will not be broadcasted on the layer 2 device, but will be broadcasted to the designated receiver on the layer 2 device.

As shown in the figure below, when the layer 2 multicast device is not running IGMP snooping, the IP multicast packets is broadcast in the VLAN; when the layer 2 multicast device is running IGMP snooping, the IP multicast packets is only sent to the group member receiver



12.2. Configuration command

IGMP Snooping Port enabled

SWITCH(config-if)#**igmp snooping**

Off by default;

Only SVI interface configuration is supported

Configure IGMP snooping uplink

SWITCH(config-if)#**igmp snooping mrouter interface** *IFNAME*

Configuration is only supported on SVI interface

The uplink port is a physical port;

Configuring IGMP snooping static groups

SWITCH(config-if)#**igmp snooping static-group** *IPADDR* **source** *IPADDR* **interface** IFNAME

Configuration is only supported on SVI interface

Static group associated interface is physical port

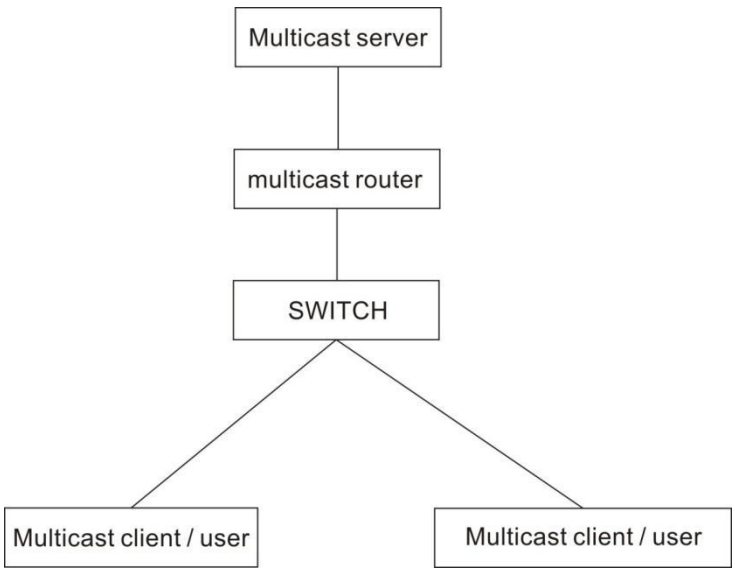
Configure IGMP snooping to fast leave

SWITCH(config-if)#**igmp snooping fast-leave**

Configuration is only supported on SVI interface；

12.3. Configuration case

Simplify the topology:



Basic configuration / role: (from top to down)

Server configuration

It is necessary to enable multicast service. VLC is used as multicast server to provide multicast service udp://225.0.0.1:1234, server IP 3.3.3.10

Router configuration

Run multicast routing protocol and enable IGMP, test with layer 3 switch to simulate, the main configuration is as follows

ip multicast-routing // Enable multicast routing

interface GigabitEthernet 0/23 // On the chain, connect to the server

no switchport

no ip proxy-arp

ip pim dense-mode // This is a simple choice of PIM intensive mode. It is recommended to use sparse mode when the actual network scale is large and multicast usage is small. For specific configuration, please refer to the configuration document of the corresponding device

ip address 3.3.3.3 255.255.255.0

interface Vlan1 // Chain down

no ip proxy-arp

ip pim dense-mode // This is a simple choice of PIM intensive mode. It is recommended to use sparse mode when the actual network scale is large and multicast usage is small. For specific configuration, please refer to the configuration document of the corresponding device

ip address 2.2.2.1 255.255.255.0

Switch configuration

Enable multicast

```
SWITCH(config-if)#igmp snooping
```

Client configuration

adopt udp://225.0.0.1 : 1234 to watch server multicast video, IP 2.2.2.10

12.4. Show command

Show IGMP snooping multicast group

SWITCH#**show igmp snooping groups**

Show IGMP snooping interface information

SWITCH#**show igmp snooping interface** *IFNAME*

```
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
```

Show IGMP snooping routing port information

SWITCH#**show igmp snooping mrouter** *SVINAME*

```
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)        --            --
```

Show IGMP snooping packets statistics

SWITCH#**show igmp snooping statistics interface** *SVINAME*

```
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

13. STP Spanning Tree

The Web management path: HomePage -> L2 Switch -> Spanning Tree

13.1. STP Overview

Spanning tree protocol is a layer-2 management protocol. It can eliminate layer-2 loops by selectively blocking redundant links in the network. At the same time, it also has the function of link backup.

Like the development process of many protocols, spanning tree protocol is constantly updated with the development of 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 there will be a broadcast storm. However, in order to enhance the reliability of a LAN, it is necessary to establish redundant links, some of which must be in the backup state. If the network fails and another link fails, the redundant link must be promoted to the active state. Manual control of such a process is obviously a very hard work, STP protocol will automatically complete this work. It can make the devices in a LAN play the following roles:

Find and start an optimal tree topology of LAN.

In order to select the best possible tree structure at any time, the network topology is automatically updated.

13.2. Configuration command

Configure STP mode

SWITCH(config)#**spanning-tree mode {stp | rstp | mstp}**

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 mode switching, the spanning tree protocol is turned off by default and needs to be re enabled

Enable STP

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

Off by default;

Configure STP priority

SWITCH(config)#**spanning-tree priority** *<0-61440>*

Default priority: 32768;

Priority of instance 0 in MSTP mode

Configure MST instance priority

SWITCH(config)#**spanning-tree instance** *<1-63>* **priority** *<0-61440>*

Default priority: 32768

Valid only in MSTP mode

Configure STP BPDU packet sending cycle

SWITCH(config)#**spanning-tree hello-time** *<1-10>*

The unit is seconds; the default is 2S

Configure STP port forwarding state delay time

SWITCH(config)#**spanning-tree forward-time** *<4-30>*

The unit is seconds; the default is 15S

Configure STP BPDU packet life cycle

SWITCH(config)#**spanning-tree max-age** *<6-40>*

The unit is seconds; the default is 20S

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 topological instability

Configure the maximum hops of STP BPDU packet

SWITCH(config)#**spanning-tree max-hops** *<1-40>*

The default is 20

Configure the maximum number of BPDU packets sent per second

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

The default is 6

Configure BPDU Guard

SWITCH(config)#**spanning-tree portfast bpdu-guard**

Global opening of BPDU guard is only effective for STP ports with fast forwarding enabled

Off by default;

Configure BPDU Filter

SWITCH(config)#**spanning-tree portfast bpdu-filter**

Turn on the BPDU filter globally, only for the ports with STP port fast forwarding enabled

Off by default;

Configure error port timeout recovery function

SWITCH(config)#**spanning-tree errdisable-timeout enable**

It is closed by default; that is to say, the error port will never time out and will be recovered automatically. It must be recovered manually

Configure error port timeout recovery interval

SWITCH(config)#**spanning-tree errdisable-timeout interval** *<10-1000000>*

Time interval: unit second, 300s by default

Enter MST mode

SWITCH(config)#**spanning-tree mst configuration**

Configure the corresponding relationship between MST VLAN and instance

SWITCH(config-mst)#**instance** *<1-63>* **vlan** {*VLANID*}

The first configured instance ID will be created at the same time

Configure MST zone name

SWITCH(config-mst)#**region** *NAME*

Configure MST version number

SWITCH(config-mst)#**revision** *<0-65535>*

Default is 0

Enable port STP

SWITCH(config-if)#**spanning-tree enable**

Default is on

Configure the relationship between port and MST instance

SWITCH(config-if)# **spanning-tree instance** *<1-63>*

By default, when configuring the relationship between instance and VLAN, the system will automatically generate the relationship data of port and instance according to the relationship between VLAN and port, without manual configuration

After the instance configuration is ready, if the relationship between port and VLAN is modified manually, for example, all VLANs of an instance join / leave ports, you need to maintain the relationship between port and instance manually through this command

After the instance configuration is ready, if the relationship between port and VLAN is modified manually, for example, all VLANs of an instance join / leave ports, you need to maintain the relationship between port and instance manually through this command

Configure port STP priority

SWITCH(config-if)#**spanning-tree priority** *<0-240>*

Priority must be configured as a multiple of 16

Default Priority :128

Priority of instance 0 in MSTP mode

Configure port MST instance priority

SWITCH(config-if)#**spanning-tree instance** *<1-63>* **priority** *<0-240>*

Default Priority :128

Priority must be configured as a multiple of 16

Valid only in MSTP mode

Configure port STP path expense

SWITCH(config-if)#**spanning-tree path-cost** *<1-200000000>*

Configure port STP link type

SWITCH(config-if)#**spanning-tree link-type** {**auto | point-to-point | shared**}

Auto: Duplex capability automatic setting mode based on link negotiation, full duplex is point-to-point connection

point-to-point: Enable fast forwarding

Shared: prohibitfast forwarding

Default is auto

Configure port STP port fast forwarding

SWITCH(config-if)#**spanning-tree portfast**

Indicates that the port directly connected device is not a bridge device and can forward quickly

Default is off

The configuration port is STP edge port

SWITCH(config-if)#**spanning-tree edgeport**

The command effect is equivalent to spanning tree portfast

Configure port STP edge port detection

SWITCH(config-if)#**spanning-tree autoedge**

Indicates that the port automatically identifies whether it is an edge port according to BPDU

Configure port STP root guard

SWITCH(config-if)#**spanning-tree guard root**

Configure port STP BPDU guard

SWITCH(config-if)#**spanning-tree bpdu-guard enable**

After opening the BPDU guard, if a BPDU is received on the port, it will enter the error disabled (blocked) state

It is only effective when STP port is enabled for fast forwarding at the same time

Configurable status: enable, disable, default

The default mode is default, which is determined by the global BPDU guard configuration status

Once enable or disable is configured, the current state configuration of the port shall prevail (i.e. global failure)

Configure port STP BPDU filter

SWITCH(config-if)#**spanning-tree bpdu-filter enable**

After opening BPDU filter, the port neither sends BPDU nor receives BPDU packet

It is only effective when STP port is enabled for fast forwarding at the same time

Configurable state: enable, disable, default;

The default mode is default, which is determined by the global BPDU filter configuration status.

Once enable or disable is configured, the current state configuration of the port shall prevail (i.e. global failure);

Configure port STP topology change notification limit

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

After the STP topology change notification limit is enabled, the port does not forward TC BPDU or refresh the address table

Priority of instance 0 in MSTP mode

Configure port MST instance topology change notification limit

SWITCH(config-if)#**spanning-tree instance** <*1-63*> **restricted-tcn**

After the STP topology change notification limit is enabled, the port does not forward TC BPDU or refresh the address table

Valid only in MSTP mode

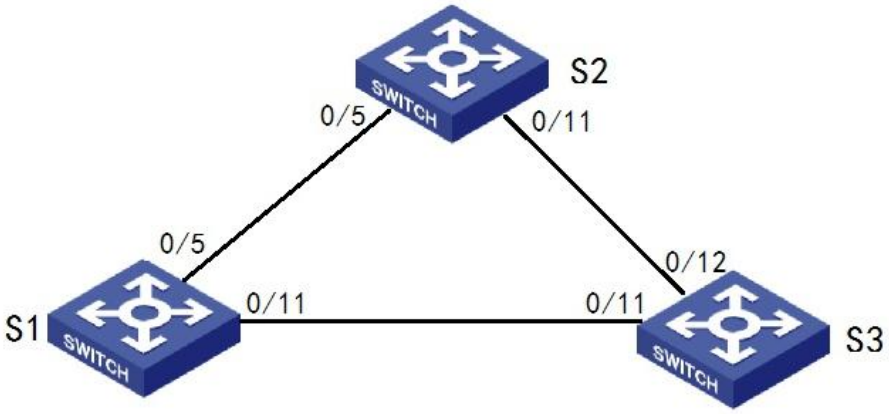
Mandatory STP version check on all ports

SWITCH#**clear spanning-tree detected protocols**

13.3. Configuration case

Case 1: implementation of link redundancy by RSTP ring protection

Simplified topology

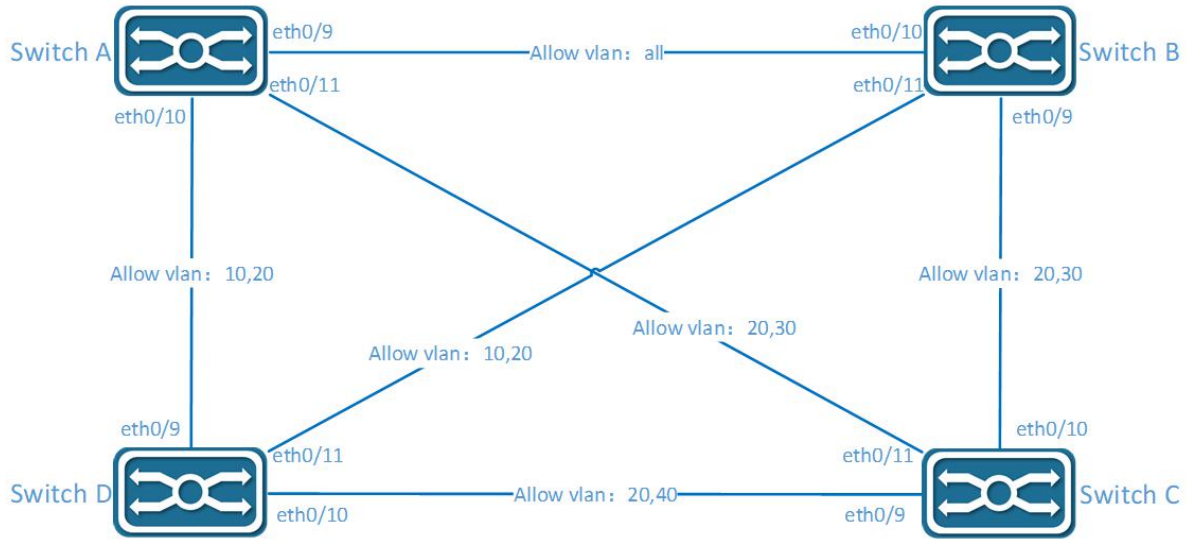


Switch S1, S2, S3 reference configuration

SWITCH(config)#spanning-tree mode rstp SWITCH(config)#spanning-tree enable

Case 2: MSTP realizes anti ring and link redundancy based on domain and instance

Simplified topology



Configuration planning

The device belongs to the same domain. The default domain is used here without additional configuration

VLAN 20 is a common VLAN, which is directly included in CST

Instance	VLAN
0	20
1	10
3	30
4	40

Switch A reference configuration

```
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

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

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

Switch B reference configuration

```
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

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
```

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

Switch C reference configuration

```
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

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

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

Switch D reference configuration

```
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


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
```

13.4. Show command

Show STP status

SWITCH#**show spanning-tree**

Show MSTP instance status

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

14. Configure POE

The Web management path: HomePage -> Interface -> Poe Management

14.1. POE Overview

PoE distributes both data and power over the same cable, This eliminates the need for having one set of cables and outlets for data, and another set for power. Also, because the voltage and power requirements are much lower than for mains powered devices, the cabling and installation costs are significantly reduced.

14.2. Configuration command

Configure Poe external power supply

SWITCH(config)#**poe powersupply** POWER

If the configured power is less than the power consumed by the current device, the PD device with the low priority port will be powered down, and the port priority is the higher priority with the smaller port ID;

Configure Poe port power supply enable

SWITCH (config-if)#**poe enable**

Configure Poe port power supply

Default is ON

14.3. Configuration case

Configure port GigabitEthernet 0/1 power supply enable

```
SWITCH(config)#interface GigabitEthernet0/1
SWITCH(config-if)#poe enable
```

14.4. Show Command

Show power supply information of Poe system

SWITCH#**show poe powersupply**

```
SWITCH#show poe powersupply
  Power supply              : 150W
  Power consume             : 44.1W
  Power management          : energy-saving
  Disconnect mode           : DC
  Powered ports             : 2
```

Show Poe port power supply information

SWITCH#**show poe interfaces**

```
SWITCH#show poe interfaces
Interface              enable  status  reason      class  icut(mA) power(W)
-------------------------------------------------------------------------
GigabitEthernet0/1     YES     OFF     short       4      --       --
GigabitEthernet0/2     YES     OFF     --          -      --       --
GigabitEthernet0/3     YES     OFF     --          4      270.2    14.0
GigabitEthernet0/4     YES     OFF     --          -      --       --
```

15. Configure 802.1X

The Web management path:

HomePage -> Security -> 802.1X Authentication

HomePage -> Security -> MAC Authentication

HomePage -> Security -> RADIUS

15.1. 802.1X overview

IEEE802 LAN/WAN committee proposed 802.1X protocol to solve the problem of wireless LAN network security. Later, 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 within Ethernet.

802.1X protocol is a port based network access control protocol. The term "port-based network access control" refers to the control of access to network resources through authentication of user devices at the port level of the LAN access device.

Architecture of 802.1X

The 802.1X system is a typical Client/Server architecture, as shown in the figure below, consisting of three entities: Client, Device, and Server.

- The client is an entity located at one end of a LAN segment that is authenticated by the device end at the other end of that link. The client is usually a user terminal device, and the user can initiate 802.1X authentication by launching the client software. The client must support EAPOL (Extensible Authentication Protocol over LAN).
- The device side is another entity located at one end of the LAN segment that authenticates the connected clients. The device side is usually a network device that supports 802.1X protocol, and it provides the client with a port to access the LAN, which can be either a physical port or a logical port.
- The Authentication server is the entity that provides authentication services for the device side. The authentication server is used to implement authentication, authorization and billing for users, usually a RADIUS (Remote Authentication Dial-In User Service) server.

802.1X Authentication Method

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

- Between the client and the device side, EAP protocol messages are directly carried in the LAN environment using the EAPOL encapsulation format.
- Between the device side and the RADIUS server, two ways can be used to exchange information. One is that EAP protocol messages are relayed from the device side and carried in the RADIUS protocol using the EAPOR (EAP over RADIUS) encapsulation format; the other is that EAP protocol messages are terminated from the device side and used to contain PAP (Password Authentication Protocol) or CHAP (Challenge Handshake Authentication Prot. Challenge Handshake Authentication Protocal) attributes to interact with the RADIUS server for authentication.

Basic concepts of 802.1X

Controlled/Uncontrolled port

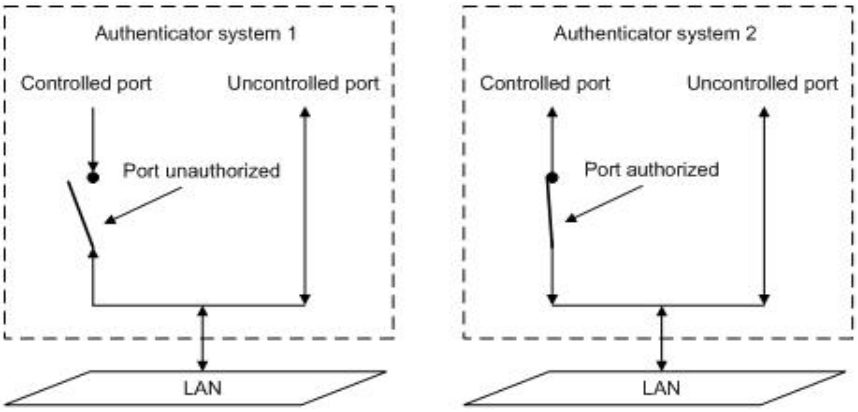
The device side provides clients with access to the LAN on a port that is divided into two logical ports: a controlled port and an uncontrolled port. Any frame arriving at this port is visible on both the controlled and uncontrolled ports.

- The uncontrolled port is always connected in both directions and is mainly used to deliver EAPOL protocol frames to ensure that clients can always send or receive authentication messages.
- The controlled ports are in a bi-directional connectivity state in the authorized state and are used to deliver service messages; receiving any messages from the client is prohibited in the unauthorized state.

Authorized/Unauthorized state

The device uses the authentication server to authenticate the clients that need to access the LAN and controls the authorized/unauthorized state of the controlled port accordingly according to the authentication result (Accept or Reject).

The following figure shows the effect of different authorization states on the controlled port on the messages passing through the port. The figure compares the port states of two 802.1X authentication systems. System 1's controlled port is in the unauthorized state (equivalent to the port switch being open), and System 2's controlled port is in the authorized state (equivalent to the port switch being closed).



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

- Forced-authorized mode (authorized-force): indicates that the port is always in the authorized state, allowing users to access network resources without authentication authorization.
- Forced unauthorized mode (unauthorized-force): the port is always in the unauthorized state and does not allow users to be authenticated. The device side does not provide authentication services to the clients accessing through the port.
- Automatic identification mode (auto): indicates that the initial state of the port is non-authorized, allowing only EAPOL messages to be sent and received, and not allowing users to access network resources; if the authentication is passed, the port switches to the authorized state and allows users to access network resources. This is also the most common case.

Controlled Direction

In the unauthorized state, the controlled port can be set to unidirectional controlled and bidirectional controlled.

- When bidirectional controlled is in effect, the sending and receiving of frames is prohibited.
- When unidirectional controlled is in effect, receiving frames from the client is prohibited, but sending frames to the client is allowed.

Currently, only unidirectional controlled is supported.

15.2. Configure command

Enable 802.1X authentication globally

SWITCH(config)# **dot1x enable**

Enable 802.1X authentication based port

SWITCH(config-if)# **dot1x port-control auto**

Configure RADIUS Server

SWITCH(config)# **radius-server host** *A.B.C.D* **[auth-port** *<0-65535>***] [acct-port** *<0-65535>***] [key** *WORD***]**

The default authentication port is 1812 and the accounting port is 1813.

Make sure that the RADIUS server and the device management address are Communicable.

Configure EAPOL Version

SWITCH(config-if)# **dot1x protocol-version** *<1-2>*

The default version is 2.

Configure authentication silence time

SWITCH(config-if)# **dot1x quiet-period** *<1-65535>*

in seconds, with a default silence time of 60 seconds.

Configure re-authentication

SWITCH(config-if)# **dot1x reauthentication**

Default off

Configure the maximum number of re-authentications

SWITCH(config-if)# **dot1x reauthMax** *<1-10>*

Configure the maximum number of port re-authentication, and if the re-authentication request exceeds the limit and there is no response, the port becomes unauthorized.

The default maximum number of times is 2.

Configuring enable key transfer capability

SWITCH(config-if)# **dot1x keytxenabled (disable | enable)**

Default off.

Configure 802.1X timer

SWITCH(config-if)# **dot1x timeout (re-authperiod** *<1-4294967295>* **| server-timeout** *<1-65535>* **| supp-timeout** *<1-65535>* **| tx-period** *<1-65535>***)**

In seconds.

The default re-authentication period of 3600 seconds.

The default server timeout of 30 seconds.

The default client authentication timeout of 30 seconds.

The default client request timeout of 30 seconds.

Enable MAC Authentication globally

SWITCH(config)# **mac-auth enable**

Enable/Disable MAC Authentication based-port

SWITCH(config-if)# **mac-auth (enable | disable)**

Configure RADIUS server deadtime

SWITCH(config)# **radius-server deadtime** *<0-1440>*

Configure the RADIUS server death time. The dead server is automatically skipped during the authentication process and the non-dead server is selected for authentication.

In minutes, default is 0 minutes.

Configure RADIUS server key

SWITCH(config)# **radius-server key** *STRING*

Configure the number of RADIUS server retransmissions

SWITCH(config)# **radius-server retransmit** *<1-100>*

The default value is 3.

Configure RADIUS server timeout time

SWITCH(config)# **radius-server timeout** *<1-60>*

In senconds，the default value is 5.

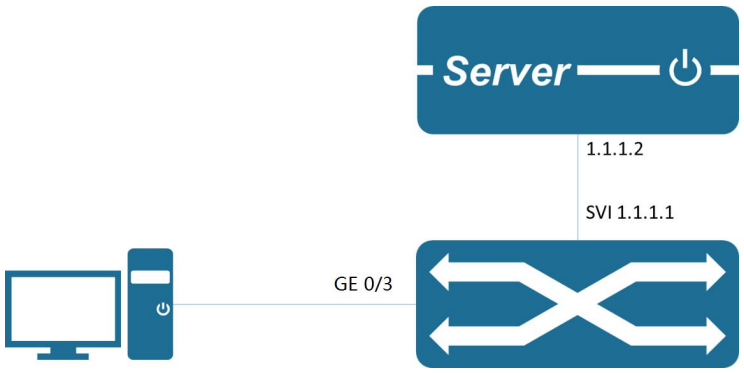
15.3. Configure case

802.1X port authentication scenarios

1) Requirements

- Authentication is required on port GigabitEthernet0/3 for access users to control their access to the Internet.
- RADIUS server IP address 1.1.1.2.
- Set the shared key to name when the system interacts with the RADIUS server.

2) Network diagram



3) Typical Configuration Examples

Switch Reference Configuration

```
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 Reference Configuration

Configure NAS authentication device 1.1.1.1 and communication key name.

Add user account test password test.

Need to support the corresponding authentication method, such as EAP-MSCHAPv2

Client reference configuration

Enable 802.1X authentication client and use account test to log in.

Need to support the corresponding authentication method, such as EAP-MSCHAPv2 method.

MAC authentication scenario

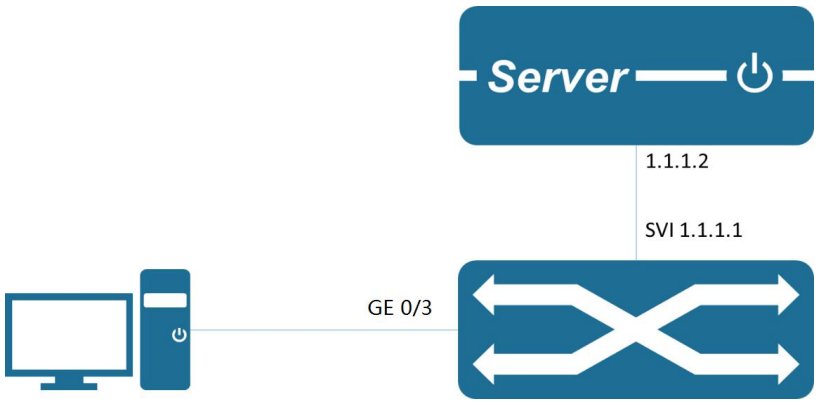
1) Requirement

It is required to authenticate access users on port GigabitEthernet0/3 to control their access to the Internet.

RADIUS server IP address 1.1.1.2.

Set the shared key to name when the system interacts with the RADIUS server for messages.

2) Network diagram



3) Typical Configuration Examples

Switch Reference Configuration

```
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 Reference Configuration

Configure NAS authentication device 1.1.1.1 and communication key name.

Configure the corresponding authentication method as EAP-MD5.

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

Client reference configuration

No action is required on the client.

15.4. Show command

Show 802.1X authentication information

SWITCH#**show dot1x all**

```
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
```

Show MAC Authentication information

显示 MAC 认证信息

SWITCH#**show bridge**

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

16. Configure Egress filtering

The Web management path: HomePage -> Interface -> Egress Filtering

16.1. Egress Filtering overview

The unknown unicast and group broadcast packets in the network will flood in the device. This function can be used to filter and protect the port and prevent the flood packets from being output from the specified port. Export filtering supports filtering unicast and multicast packets.

16.2. Configuration command

Configure egress unicast filtering

SWITCH(config-if)#**switchport block unicast**

Configuration on physical ports is only supported

Configure egress multicast filtering

SWITCH(config-if)#**switchport block multicast**

Configuration on physical ports is only supported

17. Configure IP

The Web management path: Homepage -> System -> Management IP Address

17.1. Management IP overview

The device supports various management and diagnostic functions based on IPv4 protocol and IPv6 protocol, such as ping, tracert, telnet, tftp upgrade, etc. It supports both local network (through IP addresses in the same segment) and cross-network (done by configuring the default gateway).

The default configuration of the device uses IPv4 protocol with IP address 192.168.1.234/24 and default gateway 192.168.1.1 on VLAN 1. All the above three parameters (VLAN, IP address, default gateway) can be modified.

The device can be configured with one IPv4 management address and one IPv6 management address respectively. The two management addresses are relatively independent, but the management VLAN must be the same.

When deleting IPs, the IPv4 management address and the IPv6 management address can be deleted separately or together.

17.2. Configuration command

IPv4 Configuration

SWITCH(config)#**management vlan** *VLAN_ID* **ip address** *A.B.C.D/M* **gateway** *A.B.C.D*

When configuring in global mode, the device can only support one management IPv4 address. When configuring a different management IPv4 address, the previous configuration will be automatically deleted.

IPv6 Configuration

SWITCH(config)#**management vlan** *VLAN_ID* **ipv6 address** *X.X::X.X/M* **gateway** *X.X::X.X*

When configuring in global mode, the device can only support one management IPv6 address. When configuring a different management IPv6 address, the previous configuration will be automatically deleted.

Delete IP address

SWITCH(config)#**no management vlan** *VLAN_ID* (**ip | ipv6** |)

When configuration deletion is performed in global mode without carrying the ip or ipv6 parameter, it means that both IPv4 management address and IPv6 management address are deleted.