SAN Telequip (P) Ltd.,
504 & 505 Deron Heights, Baner Road, Pune
411045, India
Phone : +91-20-27293455, 8793779568
Email Id : info@santelequip.com

Connecting Converting Leading !

SAN TELEQUIP

USER MANUAL FOR

IESLMG 302-2S A

Managed Giga Industrial Ethernet Switch

SAN Telequip (P) Ltd.,
504 & 505 Deron Heights, Baner Road
Pune 411045, India
Phone : +91-20-27293455, 8793779568
email : info@santelequip.com

TABLE OF CONTENTS

Table of Contents

SAN Telequip (P) Ltd.,
504 & 505 Deron Heights, Baner Road
Pune 411045, India
Phone : +91-20-27293455, 8793779568
email : info@santelequip.com

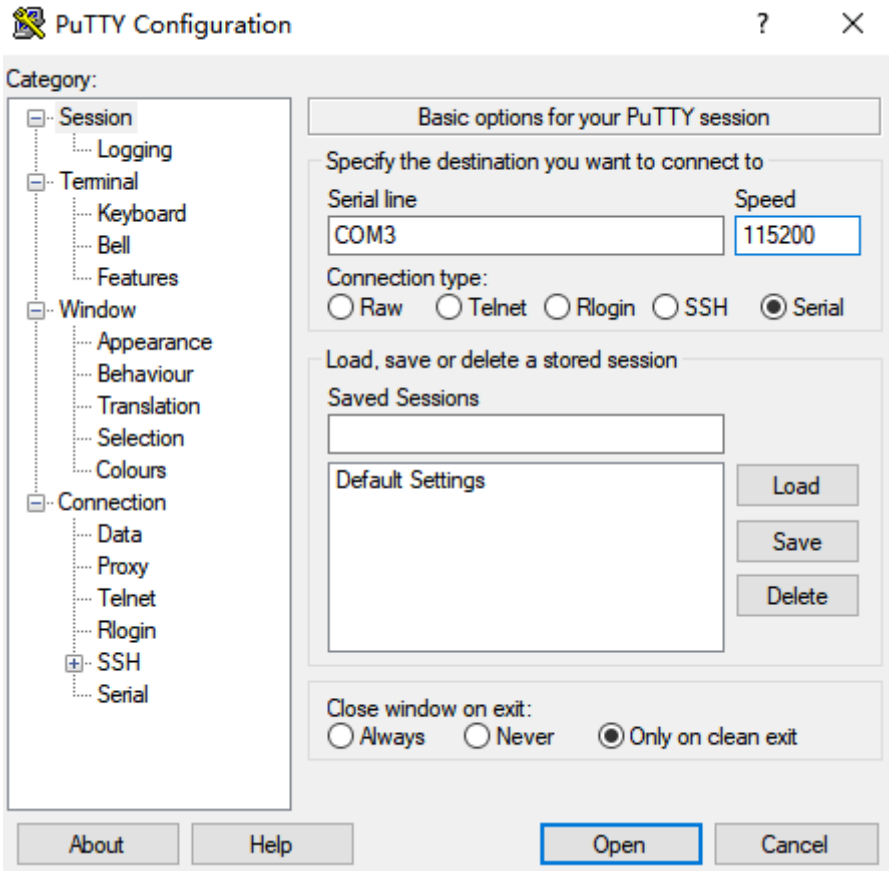
1. Login switch configuration

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

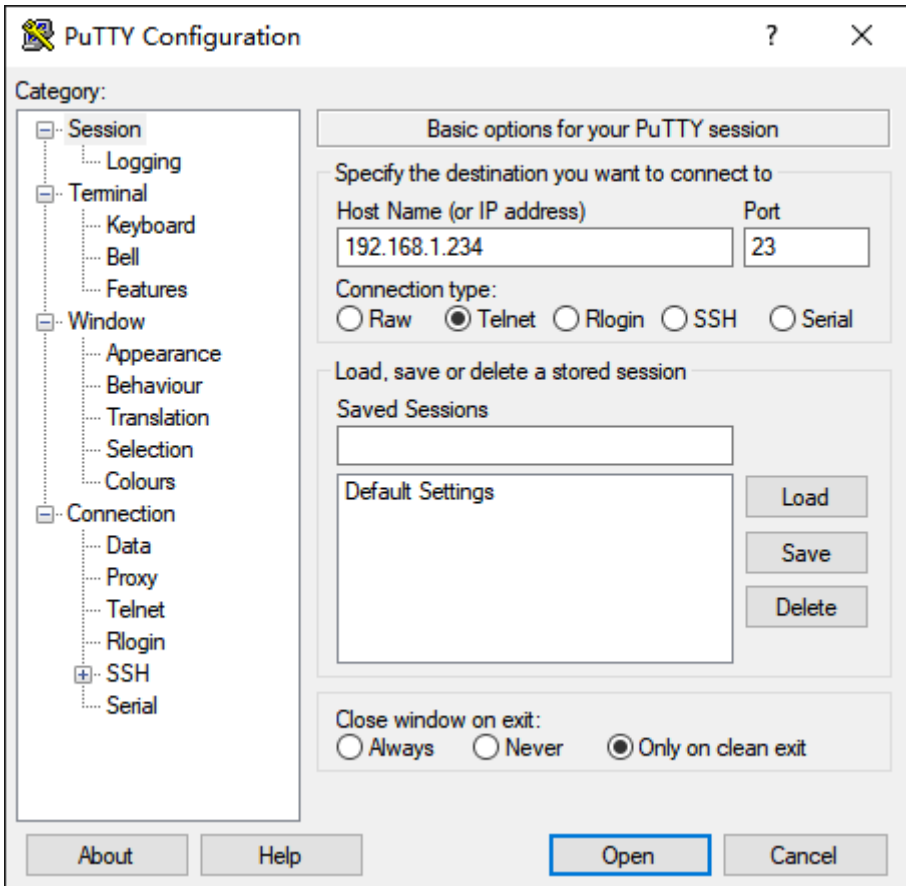


- Select the serial method
- Input the serial device using by PC Serial line
- Set baud rate at 115200 at “Speed”
- Enter the login screen.
  Notes: Make sure the serial port configuration is correct, baud rate 115200, Data digital is 8, parity check is none, end 1, flow control at none
- Login device, 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 the switch's console port to the PC using a network cable.

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

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 **full 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

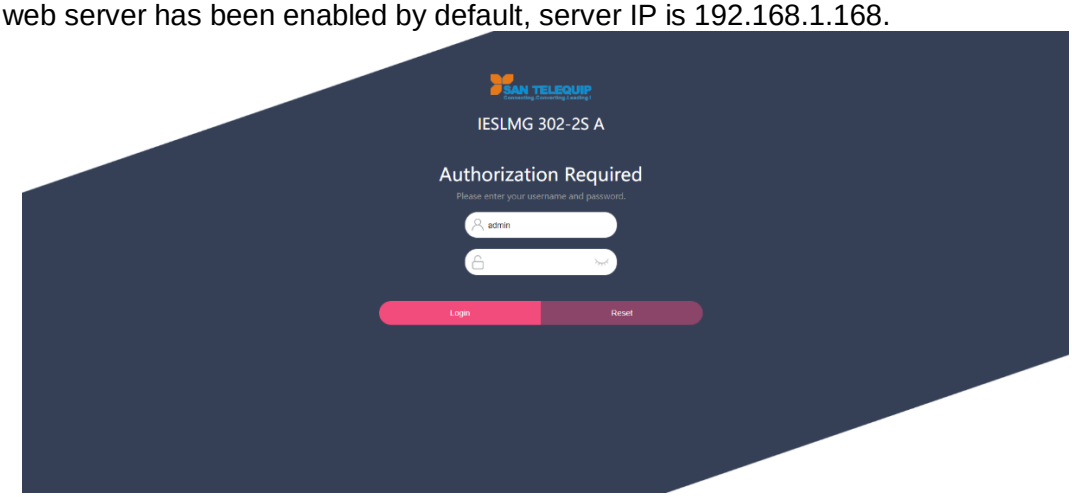
For example: add VLAN 100, clear VLAN 100

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

SAN Telequip (P) Ltd.,
504 & 505 Deron Heights, Baner Road
Pune 411045, India
Phone : +91-20-27293455, 8793779568
email : info@santelequip.com

1.2. Web management

The web server has been enabled by default, server IP is 192.168.1.168.



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

SAN Telequip (P) Ltd.,
504 & 505 Deron Heights, Baner Road
Pune 411045, India
Phone : +91-20-27293455, 8793779568
email : info@santelequip.com

2. System management

2.1. Configure save/clear

The corresponding path is:
Homepage -> Upper right corner -> Save
Homepage -> System -> Configuration file management

Save command
SWITCH#**write**
Restore default configuration command
SWITCH#**copy default-config startup-config**
Restart the device to make the configuration effect.

2.2. Reboot

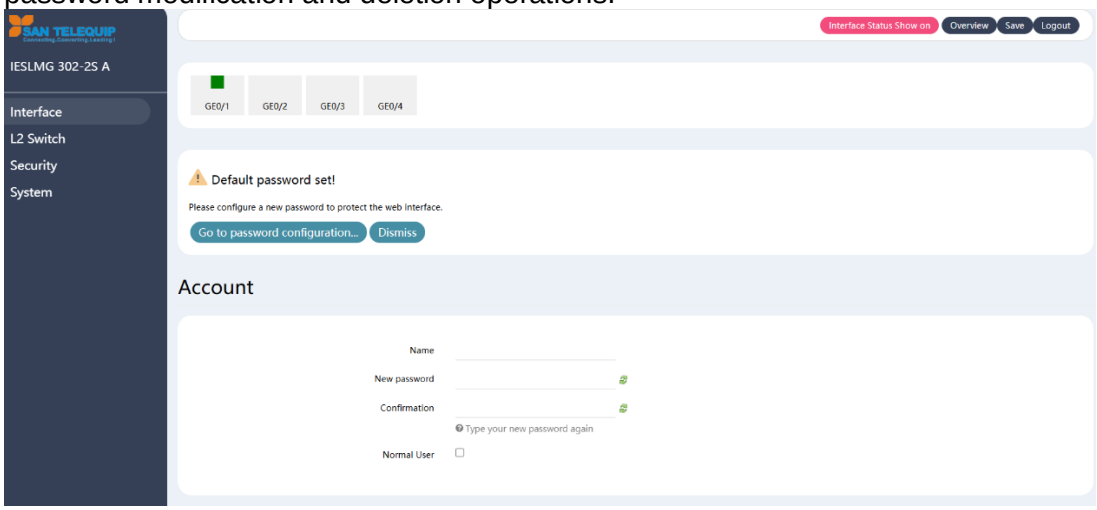
Path: Homepage -> System -> Reboot

Reboot Command
SWITCH#**reload**

2.3. User login

Path: Homepage -> System -> User management, 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

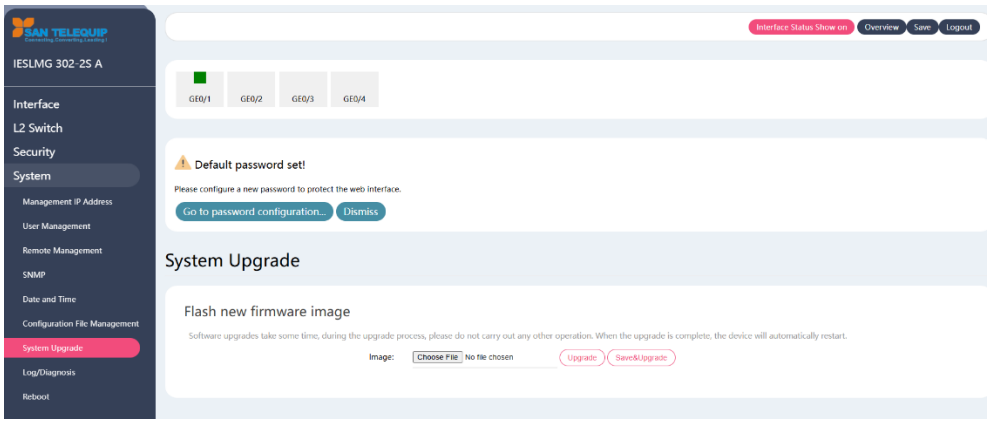
Path on Web: Homepage ->Basic information -> device name

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

Web Path: Homepage -> System -> System upgrade

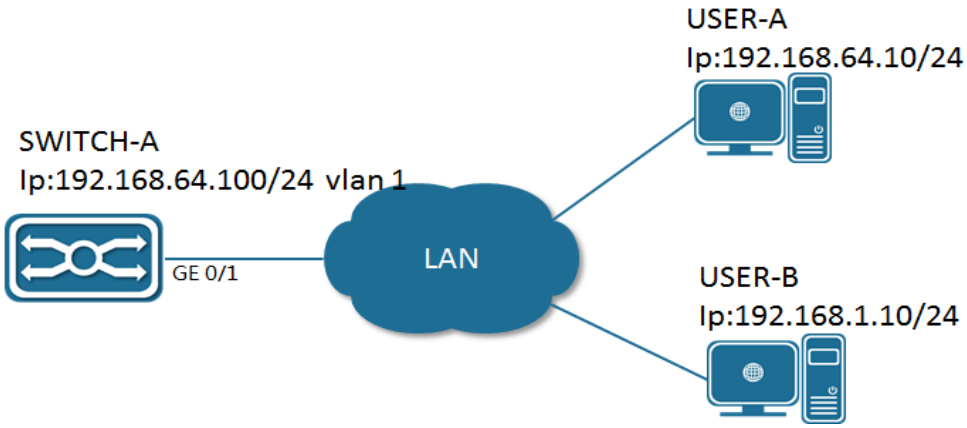
Configure system upgrade
SWITCH# **upgrade tftp tftp://**SERVER**/**FILENAME
Firmware upgrade commandsneed to build a TFTP server on the terminal and ensure the two-way interconnection between the terminal and the device network
SERVER: TFTPTFTP server IP and the relative address of the server window 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.



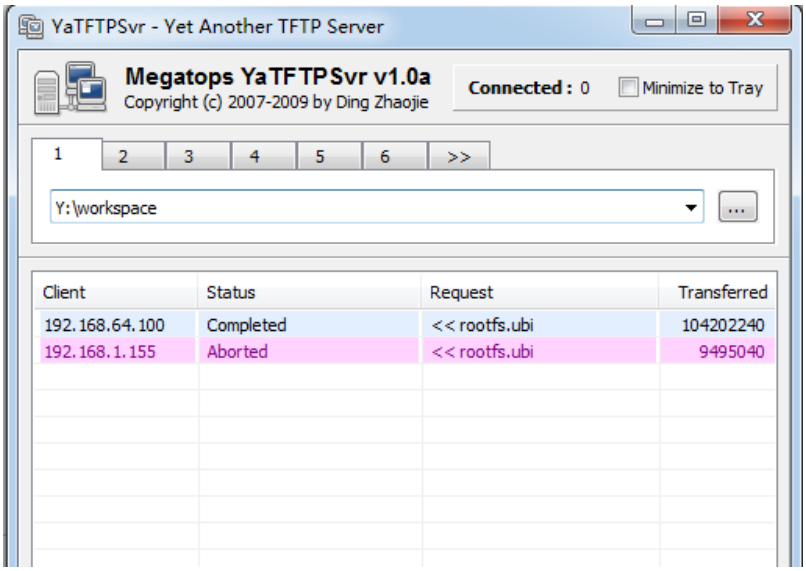
Configuration case

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

Web Path: Homepage -> System -> Time and date

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

Web Path: Homepage -> interface -> Port management, port statistics, 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,

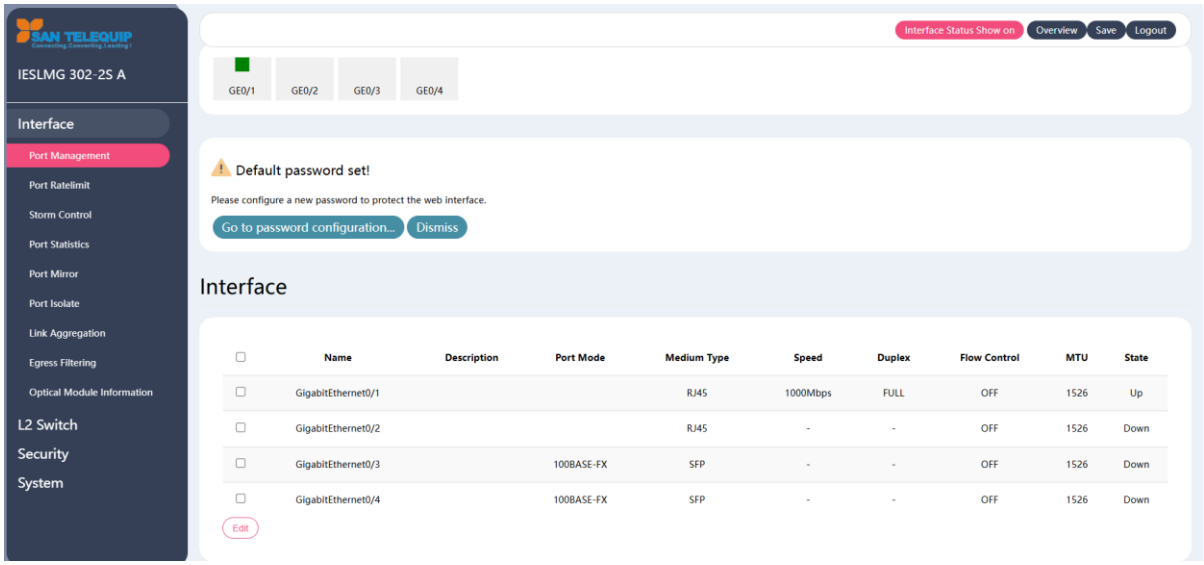
```
SWITCH(config)#interface GigabitEthernet0/1
SWITCH(config-if)#mtu 1024
```

SAN Telequip (P) Ltd.,
504 & 505 Deron Heights, Baner Road
Pune 411045, India
Phone : +91-20-27293455, 8793779568
email : info@santelequip.com

3.4. Display Command

Show interface brief

SWITCH# **show interface brief**

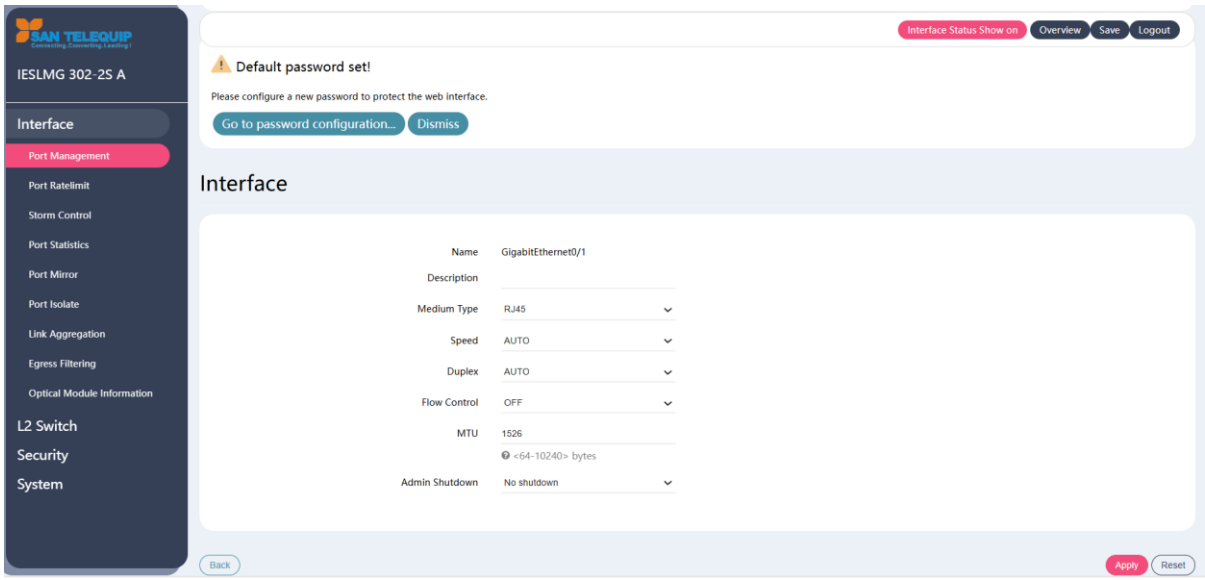



```
SWITCH#show interface brief
Codes: ETH - Ethernet, LB - Loopback , AGG - Aggregate , MLAG - MLAG Aggregate
       FR - Frame Relay, TUN -Tunnel, PBB - PBB Logical Port, VP - Virtual Port
       CVP - Channelised Virtual Port, METH - Management Ethernet, UNK- Unknown
       ED - ErrDisabled, PD - 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     --     --     --          --     --
```

Display a single-port configuration and status information

SWITCH# **show interface** IFNAME

SAN Telequip (P) Ltd.,
504 & 505 Deron Heights, Baner Road
Pune 411045, India
Phone : +91-20-27293455, 8793779568
email : info@santelequip.com




```
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
```

Display Port message statistics

SWITCH#**show counters interface** IFNAME

```
SWITCH#show counters interface GigabitEthernet0/1
Interface GigabitEthernet0/1
```

SAN Telequip (P) Ltd.,
504 & 505 Deron Heights, Baner Road
Pune 411045, India
Phone : +91-20-27293455, 8793779568
email : info@santelequip.com

```
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
```

Display 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

Web Path: Homepage -> Switch -> Mac management

4.1. 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

4.2. 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 message 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
```

SAN Telequip (P) Ltd.,
504 & 505 Deron Heights, Baner Road
Pune 411045, India
Phone : +91-20-27293455, 8793779568
email : info@santelequip.com

4.3. Display Command

Display MAC address

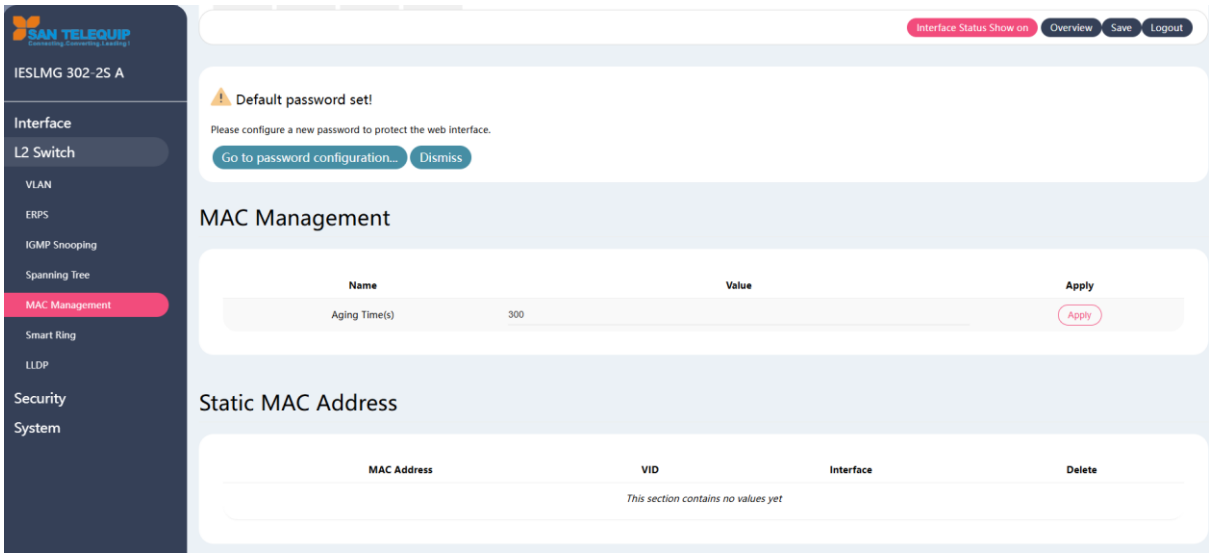
SWITCH#**show mac-address-table**

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

Display 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

Web Path: Homepage -> Switch -> VLAN

5.1. 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 message 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 ALLl, 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 message, it defaults to the specified VLAN; when the port outputs, it carries the message 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 message of the default VLAN will not be transmitted correctly

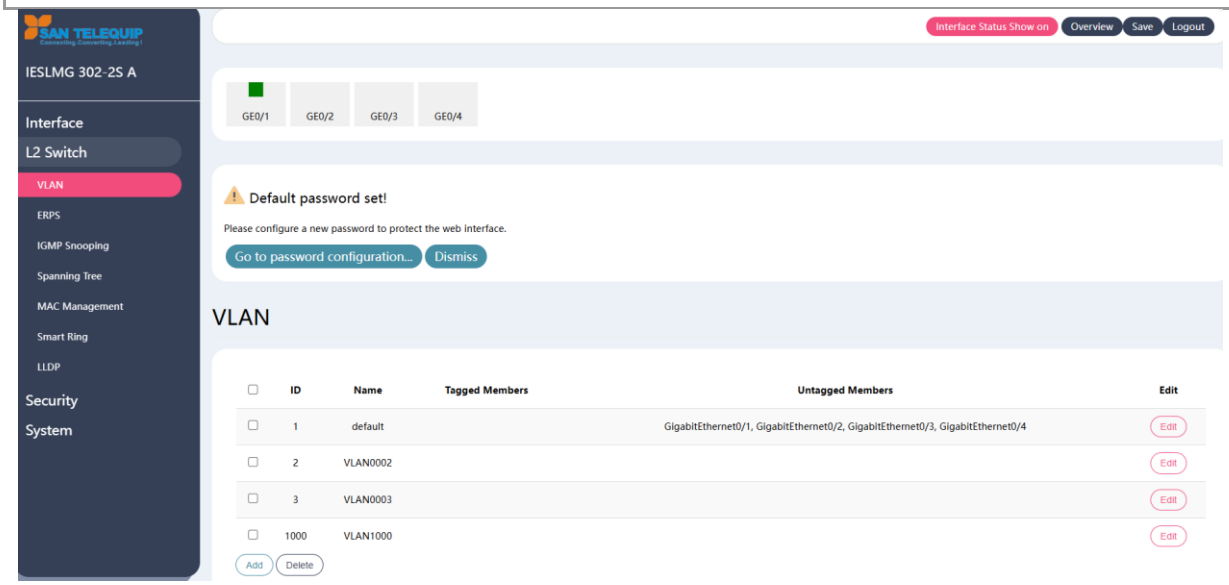
5.2. Display Command

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

Display 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

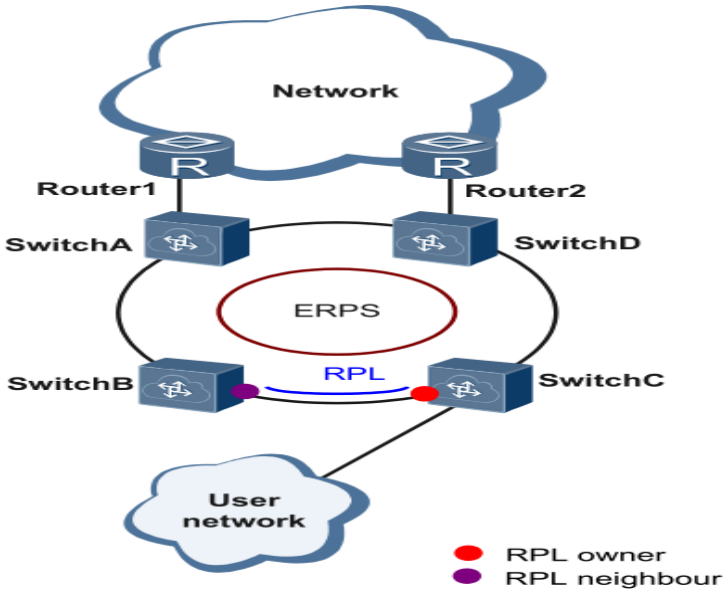
The corresponding Web Path: Home Page > exchange > ERPS

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.

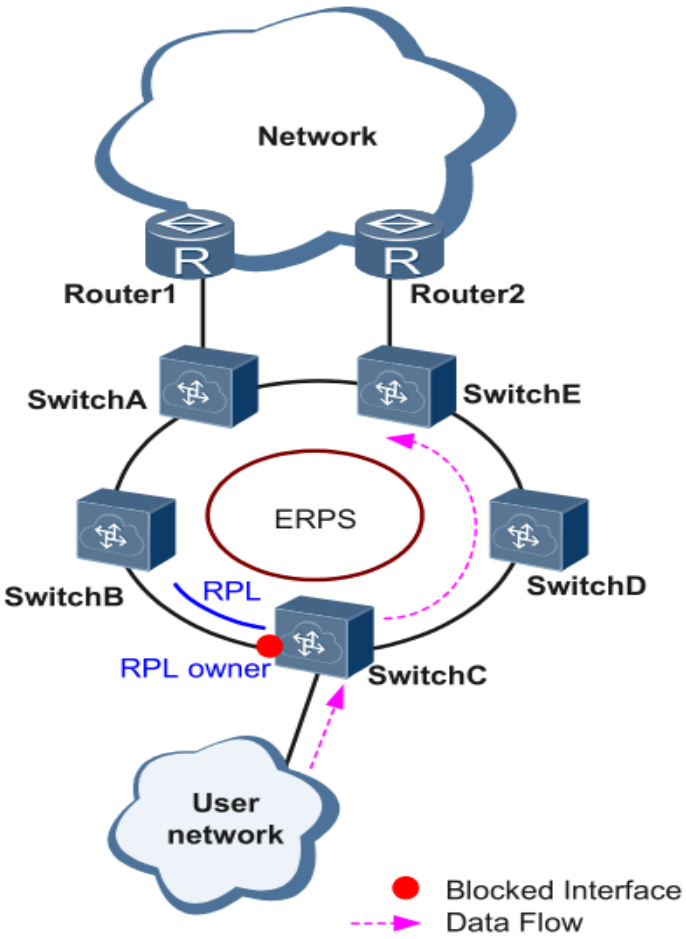
Typical ERPS networking:



6.2. ERPS Principle Introduction

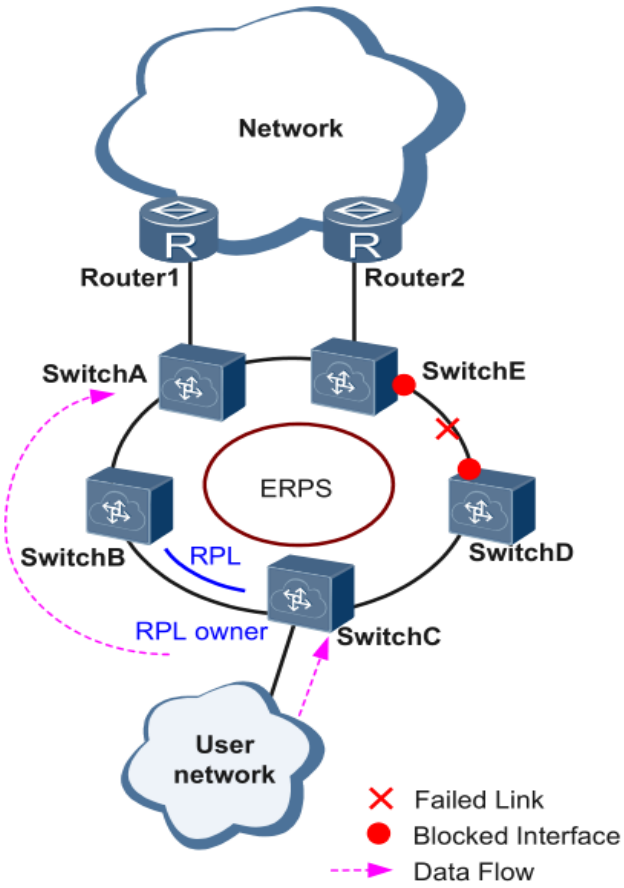
ERPS is a standard ring network protocol dedicated to the Ethernet link layer, with the ERPS ring as the basic unit. Only two ports on each layer 2 switching device can join the same ERPS ring. In an ERPS ring, in order to prevent loops, a loop-breaking mechanism can be activated to block the RPL owner 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 messages and data messages must be mapped to the protection instance, so that the ERPs protocol can forward or block these messages 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

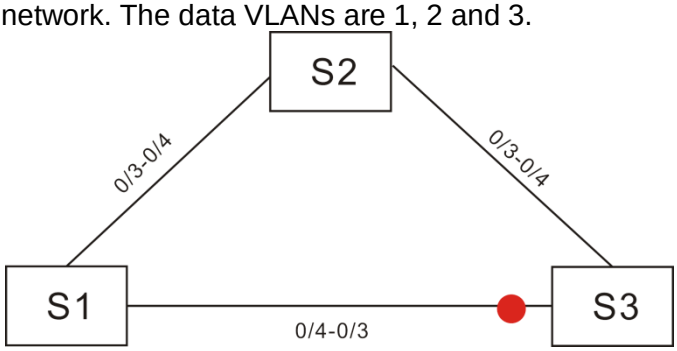
SWITCH(config-erps-prof)#**revertive**
Configure ERPs automatic Switchback
Configure timer parameters of ERPs template
SWITCH(config-erps-prof)#**timer** {**wait-to-restore** {<1-12> | **default**} | **hold-off** {<0-100> | **default**} | **guard-timer** {<1-200> | **default**}}
wait-to-restore: Unit 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 1: 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

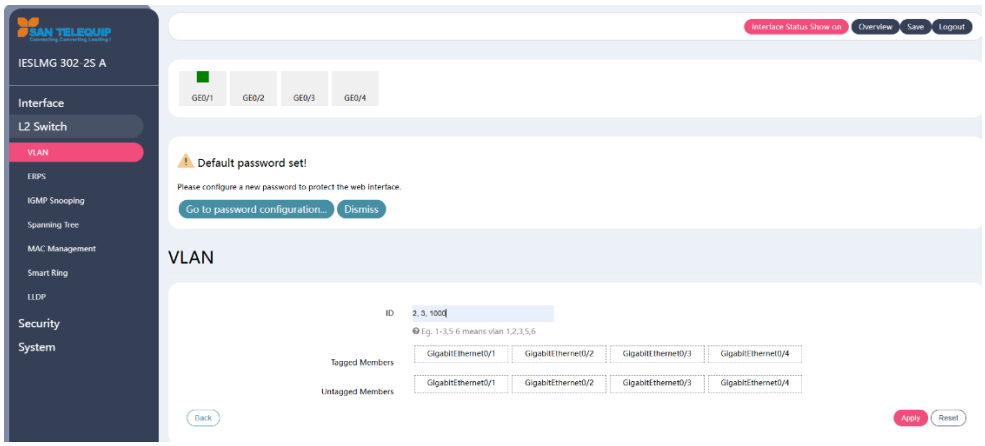
```
SWITCH(config)#vlan 2,3,1000
SWITCH(config)#interface GigabitEthernet0/3-4
SWITCH(config-if)#switchport mode trunk
SWITCH(config)#erps ring 1 east-interface GigabitEthernet0/3 west-interface
        GigabitEthernet0/4
SWITCH(config)#erps instance 1
SWITCH(config-erps-inst)#ring 1
SWITCH(config-erps-inst)#rpl-role non-owner
SWITCH(config-erps-inst)#vlan 1000 raps-channel
```

- Web reference configuration

1) Add VLAN 2, 3, 1000

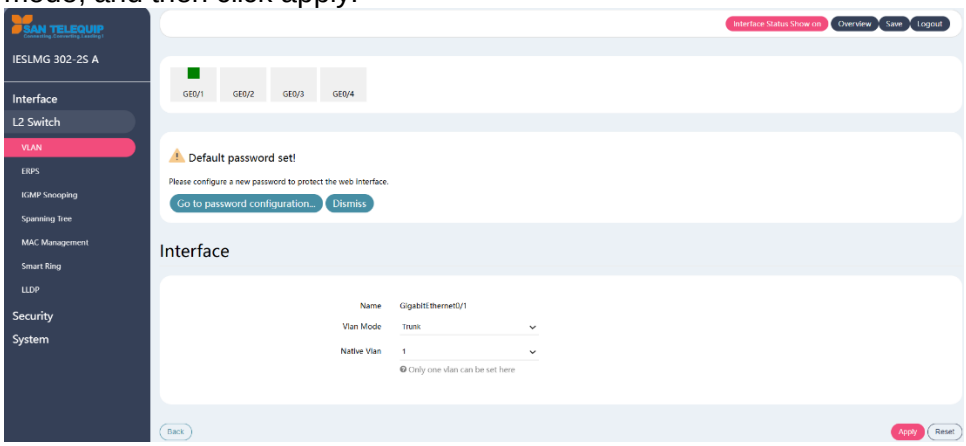
Add VLAN in home page > exchange > VLAN, and then click apply

SAN Telequip (P) Ltd.,
504 & 505 Deron Heights, Baner Road
Pune 411045, India
Phone : +91-20-27293455, 8793779568
email : info@santelequip.com



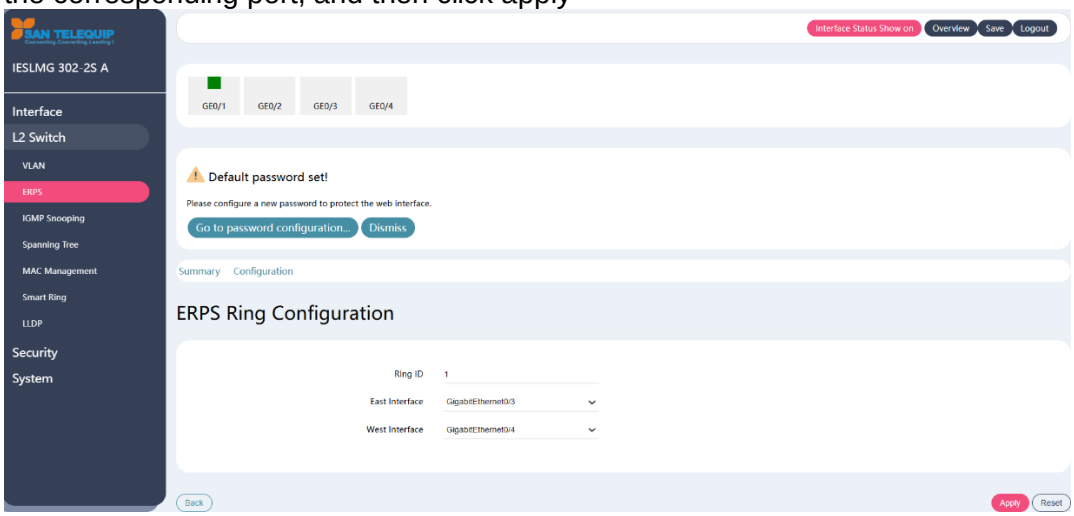
2) Gigabit Ethernet 0 /3-4 is configured as trunk port

Select the port to be configured in home page > Switch > VLAN, click Edit, modify port VLAN mode, and then click apply.



3) Add ERPs ring 1

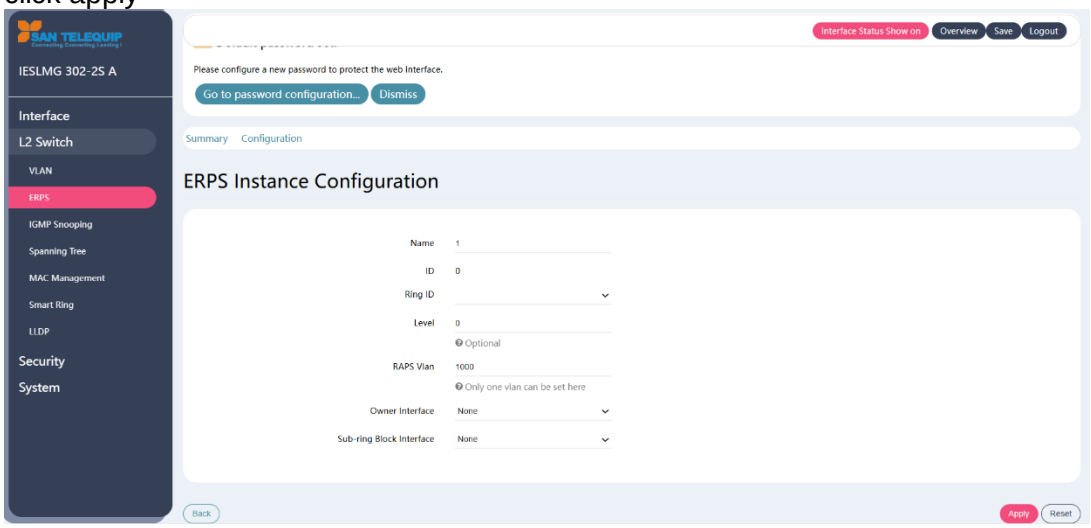
Add the ERPs ring configuration in home page > exchange > ERPs > configuration, select the corresponding port, and then click apply



4) Add ERPs instance 1

SAN Telequip (P) Ltd.,
504 & 505 Deron Heights, Baner Road
Pune 411045, India
Phone : +91-20-27293455, 8793779568
email : info@santelequip.com

Add ERPs instance configuration in home page > exchange > ERPs > configuration, select the corresponding ring number, manage VLAN and whether the owner interface, and then click apply



6.5. Display command

Display 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,
```

Display 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
================================================================
```

Display ERPS Configuration template

SWITCH#**show erps profile** NAME

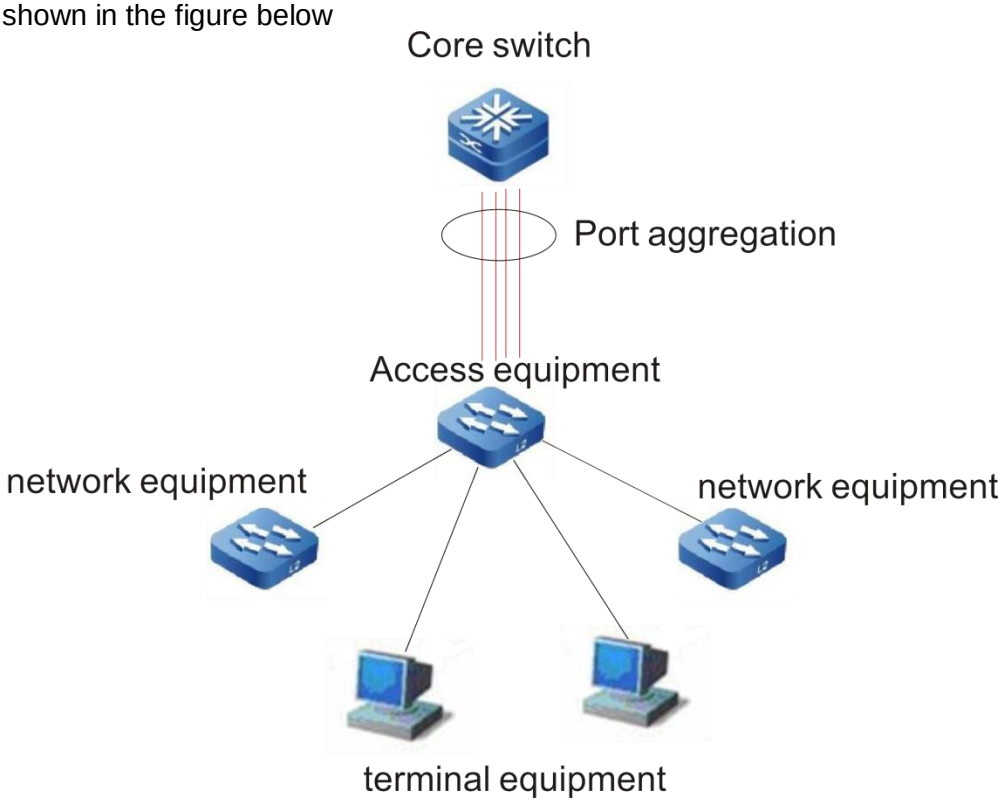
```
SWITCH#show erps profile 1

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. Link aggregation

The corresponding configuration path of web network management is: home page, interface, port aggregation

7.1. Link 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

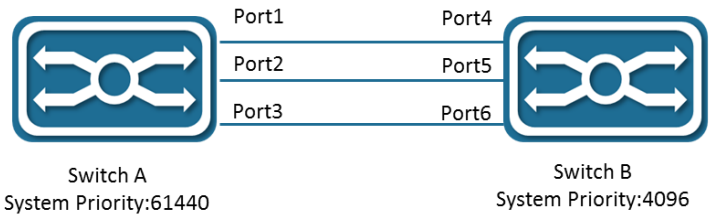


The aggregation port has the following characteristics: high bandwidth, the total bandwidth of the aggregation port is the sum of the bandwidth of the physical member ports; it supports a traffic balancing strategy, which can allocate traffic to each member link according to the strategy; supports link 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

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 exits 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 message interaction will be performed. When the LACP message 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 message every 30 seconds. If the peer message is not received in 90 seconds, it is in packet receiving timeout; In the short timeout mode, the port sends a message every 1 second. If it does not receive a message 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 message 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 messages 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 message sending interval is 30s, 90s timeout; short mode, LACP message 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. Display command

Display 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
```

Display 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
```

Display 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
```

Display LACP message statistics

SWITCH#**show lacpcounter**

```
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
```

Display LACP system ID

SWITCH#**show lacpsys-id**

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

Display LACP port information

SWITCH#**show lacp** ID

```
SWITCH#show lacp 8
```

SAN Telequip (P) Ltd.,
504 & 505 Deron Heights, Baner Road
Pune 411045, India
Phone : +91-20-27293455, 8793779568
email : info@santelequip.com

```
% 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
```

Display 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. Storm control

The corresponding configuration path of web network management is: Home Page > interface > storm control

8.1. 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

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

8.3. 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
```

8.4. Display 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%
```

SAN Telequip (P) Ltd.,
504 & 505 Deron Heights, Baner Road
Pune 411045, India
Phone : +91-20-27293455, 8793779568
email : info@santelequip.com

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%

9. Configuration SNMP

The corresponding web network management configuration path is: Home Page > system > SNMP

9.1. SNMP overview

SNMP is the abbreviation of simple network management protocol. It became a network management standard rfc1157 in August 1988. Up to now, due to the support of many manufacturers, SNMP has become the de facto network management standard, which is suitable for the interconnection environment of multi manufacturer systems
Using SNMP protocol, network administrator can query information, configure network, locate fault and plan capacity of nodes on the network. Network monitoring and management are the basic functions of SNMP
Currently, the following versions of SNMP exist
SNMPv1: The first official version of the Simple Network Management Protocol, defined in RFC1157.
SNMPv2C: Community-Based SNMPv2C management architecture, defined in RFC1901.
SNMPv3: By authenticating and encrypting data, the following security features are provided:

1) Ensure that the data is not tampered with during transmission.

2) 2) Ensure that the data is sent from a legal data source.

3) 3) Encrypt messages to ensure data confidentiality.

The current device only supports SNMPv1 and SNMPv2C versions.

9.2. Configuration command

Configure SNMP communication community word
SWITCH(config)#**snmp-server community** WORD [**ro**]
ro: Read only flag, which configures the group word as read-only permission; by default, it is configured as a group word with read-write permission at the same time,Support to configure multiple group words at the same time
Configure SNMP notification receiving server
SWITCH(config)#**snmp-server**IPADDR**community** WORD
Multiple servers can be configured at the same time

9.3. Configuration case

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

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

SAN Telequip (P) Ltd.,
504 & 505 Deron Heights, Baner Road
Pune 411045, India
Phone : +91-20-27293455, 8793779568
email : info@santelequip.com

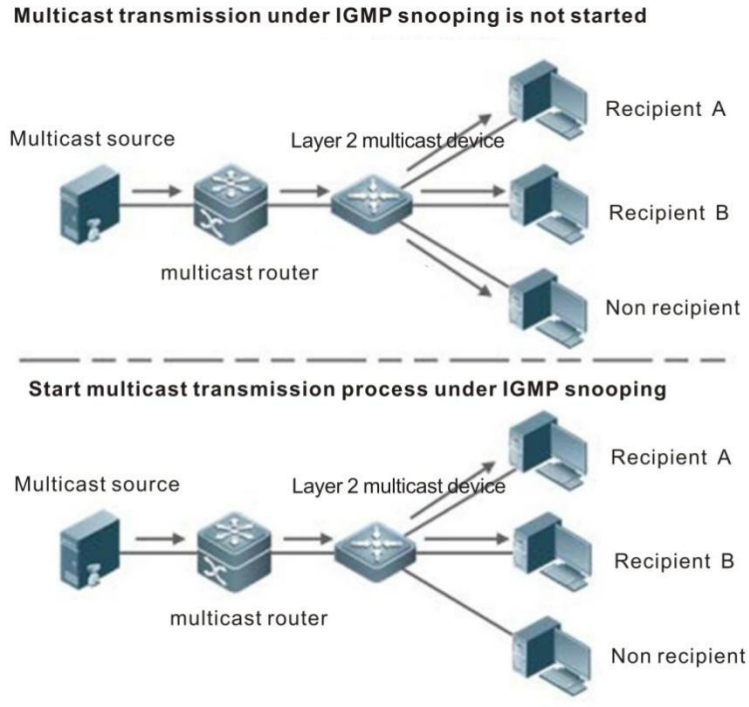
```
SWITCH(config)#snmp-server 2.2.2.2 community public
```

10. IGMP Snooping

The corresponding configuration path of web network management is: Home Page > exchange > IGMP snooping

10.1. 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 message, 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 message is broadcast in the VLAN; when the layer 2 multicast device is running IGMP snooping, the IP multicast message is only sent to the group member receiver



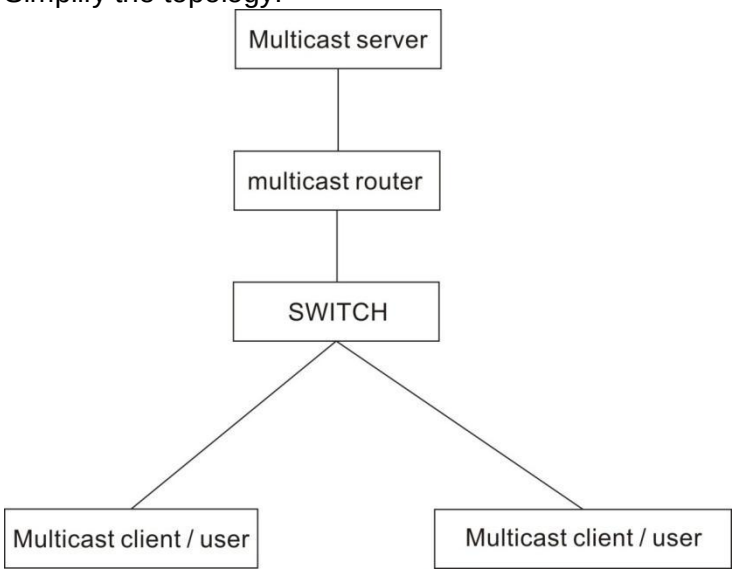
10.2. Configuration command

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；

10.3. 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

10.4. Display command

View IGMP snooping multicast group
SWITCH#**show igmp snooping groups**
View 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
```

View IGMP snooping routing port information
SWITCH#**show igmp snooping** mrouter SVI

```
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)         --            --
```

View IGMP snooping message statistics
SWITCH#**show igmp snooping statistics interface** SVI

```
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
```

SAN Telequip (P) Ltd.,
504 & 505 Deron Heights, Baner Road
Pune 411045, India
Phone : +91-20-27293455, 8793779568
email : info@santelequip.com

IGMPv2 query warnings : 456
IGMPv3 query warnings : 0

11. STP Spanning Tree

The corresponding configuration path of web network management is: Home Page > exchange > spanning tree

11.1. 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.

11.2. 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 message 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 message 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 message
SWITCH(config)#**spanning-tree max-hops** <1-40>
The default is 20
Configure the maximum number of BPDU messages 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 / exit 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 / exit 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 message

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

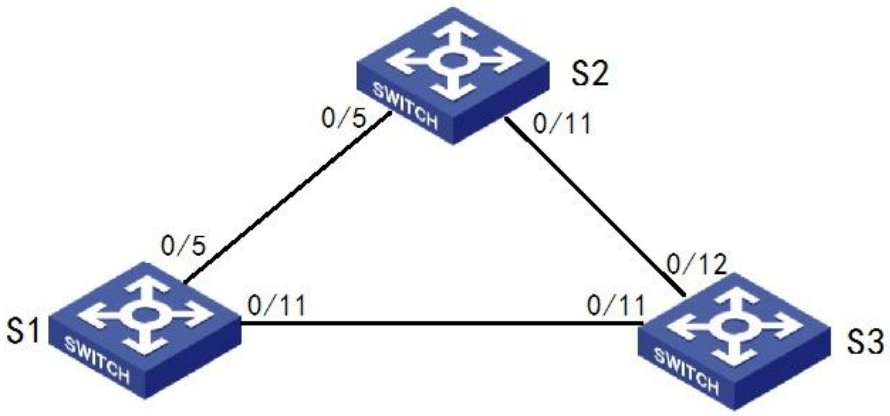
Mandatory STP version check on all ports

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

11.3. Configuration case

Case 1: implementation of link redundancy by RSTP ring protection

Simplified topology

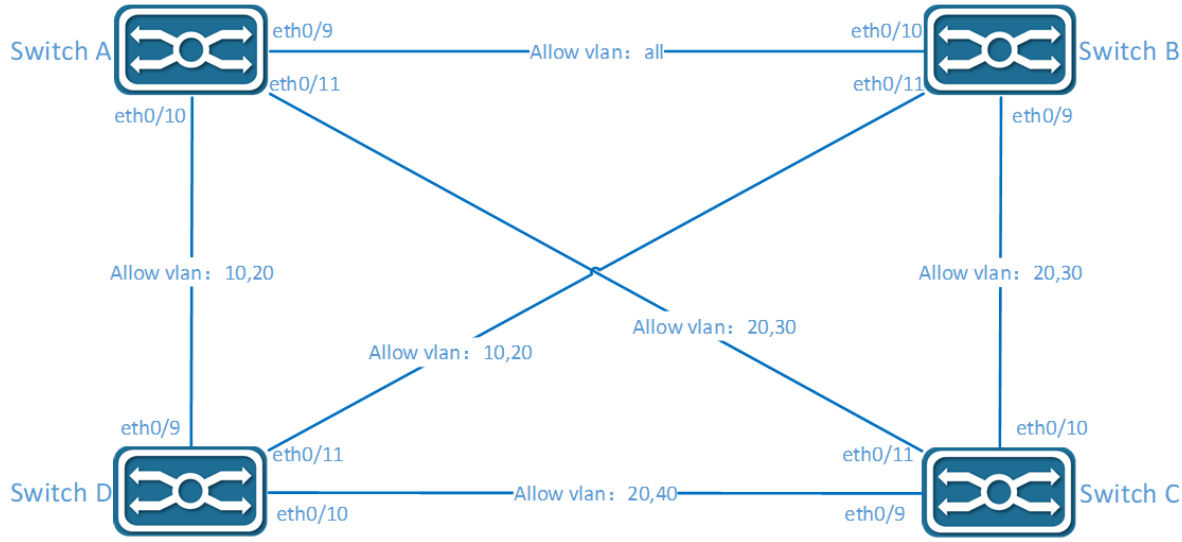


Switch S1, S2, S3 reference configuration

```
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
# 启用 MSTPEnable MSTP
SWITCH(config)#spanning-tree enable
```

11.4. Display command

View STP status
SWITCH#**show spanning-tree**
View MSTP instance status
SWITCH#**show spanning-tree mst instance**<1-63>

12. Configure POE

The corresponding configuration path of web network management is: Home Page > interface > Poe management

12.1. POE Overview

PoE distributes both data and power over the same cabling. 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.

12.2. 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

12.3. Configuration case

Configure port GigabitEthernet 0 / 1 power supply enable

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

12.4. Display Command

Display 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
```

Display Poe port power supply information
SWITCH#show poe interfaces

```
SWITCH#show poe interfaces
```

SAN Telequip (P) Ltd.,
504 & 505 Deron Heights, Baner Road
Pune 411045, India
Phone : +91-20-27293455, 8793779568
email : info@santelequip.com

```
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     --         -      --       --
```

SAN Telequip (P) Ltd.,
504 & 505 Deron Heights, Baner Road
Pune 411045, India
Phone : +91-20-27293455, 8793779568
email : info@santelequip.com

13. Configure Engress Filtering

The corresponding web network management configuration path is: Home Page > interface > Engress filtering

13.1. Engress filtering overview

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

13.2. Configuration command

Configure outlet unicast filtering
SWITCH(config-if)# **Unicast Egress Filtering**
Configuration on physical ports is only supported
Configure exit multicast filtering
SWITCH(config-if)# **Multicast Egress Filtering**
Configuration on physical ports is only supported

14. Configure IP

14.1. IP management overview

The device supports various management and diagnosis functions based on IP protocol, such as Ping, tracert, Telnet, TFTP upgrade, etc. It supports not only the interworking of this network segment (through the IP address in the same network segment), but also the interworking of cross network segments (by configuring the default gateway). The default management IP of the device is configured on VLAN 1, with the IP address of 192.168.1.158/24 and the default gateway of 192.168.1.1. The above three parameters (VLAN, IP address and default gateway) can be modified.

14.2. Configuration command

IP management 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 IP configuration. When configuring a different management IP, the previous configuration will be automatically deleted.