S3900 Series
Configuration Guide

Models: S3900-24T4S/S3900-24F4S/S3900-48T4S

CONFIGURATION GUIDE

Contents

1. Physical Layer

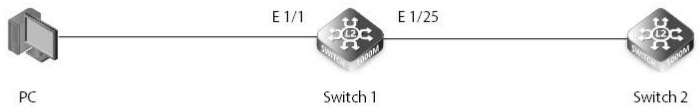
1.1 Auto-negotiation for Port Speed and Duplex Mode

1.1.1 Introduction

The Ethernet interface works at 10/100/1000Mbps, which can be full-duplex or half-duplex mode. Users can choose one of them according to the actual networking situation, but the two cannot work at the same time. In auto-negotiation mode, the interface speed and duplex mode are determined by the interfaces at both ends of the link through negotiation. Once the negotiation is passed, the devices at both ends of the link are locked in the same duplex mode and interface rate. The auto-negotiation function takes effect only when the devices at both ends of the link support it. If the peer device does not support the auto-negotiation function, or the peer device's auto-negotiation mode is inconsistent with the local device, the interface may be in the Down state.

1.1.2 Networking Ideas

Log in to the switch through a PC connection to test the rate and duplex mode.



1.1.3 Configuration

(1) Log in to the switch using the Console cable, SSH, or Telnet. Use #show interfaces brief to view the port status as shown below：

```
Switch 1#show interfaces brief
Interface Type          Admin   Link-Status   Negotiation   Speed/Duplex   Group
---------------------------------------------------------------------------- -----
Eth 1/ 1   1000BASE-T     Up      Up            Auto          1000full       None
Eth 1/ 2   1000BASE-T     Up      Up            Auto          1000full       None
Eth 1/ 3   1000BASE-T     Up      Down          Auto                         None
Eth 1/ 4   1000BASE-T     Up      Down          Auto                         None
Eth 1/ 5   1000BASE-T     Up      Down          Auto                         None
Eth 1/ 6   1000BASE-T     Up      Down          Auto                         None
Eth 1/ 7   1000BASE-T     Up      Down          Auto                         None
Eth 1/ 8   1000BASE-T     Up      Down          Auto                         None
Eth 1/ 9   1000BASE-T     Up      Down          Auto                         None
Eth 1/10   1000BASE-T     Up      Down          Auto                         None
Eth 1/11   1000BASE-T     Up      Down          Auto                         None
Eth 1/12   1000BASE-T     Up      Down          Auto                         None
Eth 1/13   1000BASE-T     Up      Down          Auto                         None
Eth 1/14   1000BASE-T     Up      Down          Auto                         None
Eth 1/15   1000BASE-T     Up      Down          Auto                         None
Eth 1/16   1000BASE-T     Up      Down          Auto                         None
Eth 1/17   1000BASE-T     Up      Down          Auto                         None
Eth 1/18   1000BASE-T     Up      Down          Auto                         None
Eth 1/19   1000BASE-T     Up      Down          Auto                         None
Eth 1/20   1000BASE-T     Up      Down          Auto                         None
Eth 1/21   1000BASE-T     Up      Down          Auto                         None
Eth 1/22   1000BASE-T     Up      Down          Auto                         None
Eth 1/23   1000BASE-T     Up      Down          Auto                         None
Eth 1/24   1000BASE-T     Up      Down          Auto                         None
Eth 1/25   10GBASE SFP+ Up        Up            Disable       10Gfull        None
Eth 1/26   10GBASE SFP+ Up        Up            Disable       10Gfull        None
Eth 1/27   10GBASE SFP+ Up        Down          Disable       10Gfull        None
Eth 1/28   10GBASE SFP+ Up        Down          Disable       10Gfull        None
```

(2) Gigabit electrical ports of FS S39 series switches support auto-negotiation mode, and support 100 / 1000Mbps in speed. The configuration is as follows：

```
Switch 1#configure terminal
Switch 1(config)#interface ethernet 1/1
Switch 1(config-if)#no shutdown
Switch 1(config-if)#no negotiation       //Need to turn off auto-negotiation mode to reduce speed
Switch 1(config-if)#speed 100full       //Optional 100 half
Switch 1(config-if)#exit
```

(3) The optical port supports 1/10G. The 10G speed is reduced to 1G, which needs to be manually configured. The command is as follows：

```
Switch 1#configure terminal
Switch 1(config)#interface ethernet 1/25
Switch 1(config-if)#no shutdown
Switch 1(config-if)#no negotiation        //Need to turn off auto-negotiation mode to reduce speed
Switch 1(config-if)#speed 1000full
Switch 1(config-if)#exit
```

1.1.4 Verification

After the configuration is complete, use #show interfaces brief to check the port status. The status is as follows:

```
Switch 1#show interfaces brief
Interface Type          Admin   Link-Status   Negotiation     Speed/Duplex    Group
-------------------------------------------------------------------------------- -----
Eth 1/ 1    1000BASE-T      Up        Up              Disable         100full        None
Eth 1/ 2    1000BASE-T      Up        Up              Disable         100half        None
Eth 1/ 3    1000BASE-T      Up        Down            Auto                           None
Eth 1/ 4    1000BASE-T      Up        Down            Auto                           None
Eth 1/ 5    1000BASE-T      Up        Down            Auto                           None
Eth 1/ 6    1000BASE-T      Up        Down            Auto                           None
Eth 1/ 7    1000BASE-T      Up        Down            Auto                           None
Eth 1/ 8    1000BASE-T      Up        Down            Auto                           None
Eth 1/ 9    1000BASE-T      Up        Down            Auto                           None
Eth 1/10    1000BASE-T      Up        Down            Auto                           None
Eth 1/11    1000BASE-T      Up        Down            Auto                           None
Eth 1/12    1000BASE-T      Up        Down            Auto                           None
Eth 1/13    1000BASE-T      Up        Down            Auto                           None
Eth 1/14    1000BASE-T      Up        Down            Auto                           None
Eth 1/15    1000BASE-T      Up        Down            Auto                           None
Eth 1/16    1000BASE-T      Up        Down            Auto                           None
Eth 1/17    1000BASE-T      Up        Down            Auto                           None
Eth 1/18    1000BASE-T      Up        Down            Auto                           None
Eth 1/19    1000BASE-T      Up        Down            Auto                           None
Eth 1/20    1000BASE-T      Up        Down            Auto                           None
Eth 1/21    1000BASE-T      Up        Down            Auto                           None
Eth 1/22    1000BASE-T      Up        Down            Auto                           None
Eth 1/23    1000BASE-T      Up        Down            Auto                           None
Eth 1/24    1000BASE-T      Up        Down            Auto                           None
Eth 1/25    10GBASE SFP+ Up        Up              Disable         1000full       None
Eth 1/26    10GBASE SFP+ Up        Up              Disable         10Gfull        None
Eth 1/27    10GBASE SFP+ Up        Down            Disable         10Gfull        None
Eth 1/28    10GBASE SFP+ Up        Down            Disable         10Gfull        None
```

2. Layer 2 Features

2.1 DHCP Client

2.1.1 Introduction

When the device functions as a DHCP client, the Option 60 field is filled with the configured content in the DHCP request packet sent from this interface.

2.1.2 Networking Ideas

Log in to the switch through a PC connection and start the DHCP client.

2.1.3 Configuration

(1) Log in to the switch using the Console cable, SSH, or Telnet.

(2) Configure client interface VLAN 1 with the following command:

```
Switch 1#ip dhcp restart client
Switch 1#configure terminal
Switch 1(config)#interface vlan 1
Switch 1(config-if)#ip add dhcp
Switch 1(config-if)#exit
```

2.1.4 Verification

Check with #show ip interface brief

```
Switch#show ip interface brief
VLAN 1 is Administrative Up - Link Up
   Address is 64-9D-99-10-06-60
   Index: 1001, MTU: 1500
   Address Mode is DHCP
   Proxy ARP is disabled
   DHCP Client Vendor Class ID (text): S3900-24T4S
   DHCP Relay Server:
```

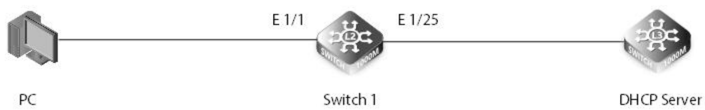
2.2 DHCP Relay

2.2.1 Introduction

The giaddr field information carried in the request message sent by the DHCP relay to the DHCP server is the IP address of the VLAN interface. When the DHCP server responds to the Response packet, it will judge the network segment where the DHCP client is based on the information in this field.

2.2.2 Networking Ideas

Verify that the S39 series switches support DHCP Relay. The configuration is not on the same network segment, deploy a distributed gateway, and connect the PC and the DHCP server. The DHCP relay function needs to be used on the distributed gateway that the user accesses, so that the user can obtain a dynamic IP address from the DHCP server through the DHCP protocol.



2.2.3 Configuration

Enable the DHCP relay function

```
Switch 1#configure terminal
Switch 1(config)#vlan database
Switch 1(config-vlan)#vlan 5
Switch 1(config-vlan)#exit
Switch 1(config)#interface ethernet 1/1
Switch 1(config-if)#switchport mode access
Switch 1(config-if)#switchport access vlan 5
Switch 1(config-if)#exit
Switch 1(config)#interface vlan 5
Switch 1(config-if)#ip add 5.5.5.2/24
Switch 1(config-if)#exit
Switch 1(config)#interface vlan 1
Switch 1(config-if)#ip add 10.100.1.254/24
Switch 1(config-if)#ip dhcp relay server 5.5.5.1
Switch 1(config-if)#exit
```

2.2.4 Verification

Check with #show ip interface brief

```
Switch 1#show ip interface brief
VLAN 1 is Administrative Up - Link Up
   Address is 64-9D-99-10-06-60
   Index: 1001, MTU: 1500
   Address Mode is Static
   IP Address: 10.100.1.254 Mask: 255.255.255.0
   Proxy ARP is disabled
   DHCP Client Vendor Class ID (text): S3900-24T4S
   DHCP Relay Server: 5.5.5.1
VLAN 5 is Administrative Up - Link Down
   Address is 64-9D-99-10-06-60
   Index: 1005, MTU: 1500
   Address Mode is Static
   IP Address: 5.5.5.2 Mask: 255.255.255.0
   Proxy ARP is disabled
   DHCP Client Vendor Class ID (text): S3900-24T4S
   DHCP Relay Server:
```

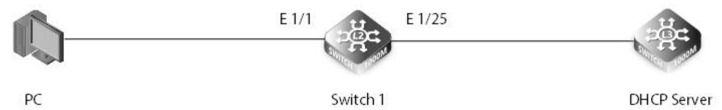
2.3 DHCP Option 82

2.3.1 Introduction

Option 82 (DHCP Relay Agent Information Option), which records the location information of the DHCP Client。The DHCP snooping device adds Option 82 to the DHCP request message to pass the location information of the DHCP client to the DHCP server, so that the DHCP server can assign a suitable IP address and other configuration information to the host and implement security control on the client.

2.3.2 Networking Ideas

The user obtains an IP address through DHCP. To distinguish different users in the same VLAN, the administrator can enable its Option 82 function after enabling DHCP snooping on the Switch. Then when the Switch receives the DHCP request message sent by the user's application for an IP address, it will insert Option 82 into the message to mark the user's precise location information, such as the MAC address, the VLAN to which it belongs, and the number of the connected interface. After receiving the DHCP request message with Option82 option, DHCP Server can know the exact physical location of the user through the content of Option82 option and then assign the appropriate IP address and other configuration information to the user according to the IP address allocation policy or other security policy deployed on it.



2.3.3 Configuration

Enable DHCP Option 82

```
Switch 1#ip dhcp restart client
Switch 1#configure terminal
Switch 1(config)#interface vlan 5
Switch 1(config-if)#ip add dhcp
Switch 1(config-if)#exit
Switch 1(config)#ip dhcp snooping
Switch 1(config)#ip dhcp snooping vlan 5//open DHCP Snooping
Switch 1(config)#ip dhcp snooping information option
```

2.3.4 Verification

Check with #show ip dhcp snooping

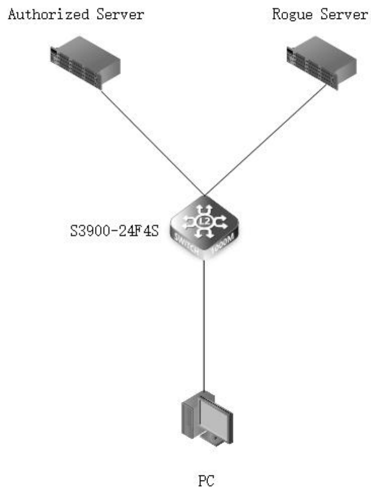
```
Switch 1#show ip dhcp snooping
Global DHCP Snooping Status: enabled
Option82 Status: enabled
Option82 Sub-option Format: extra subtype included
Option82 Remote ID: MAC Address (hex encoded)
Option82 Remote ID TR101 VLAN Field: enabled
Option82 TR101 Board ID: none
DHCP Snooping Information Policy: replace
DHCP Snooping is configured on the following VLANs:
    5
Verify Source MAC-Address: enabled
DHCP Snooping Rate Limit: unlimited
                                      Circuit-ID        Circuit-ID     Circuit-ID
Interface Trusted Max-Number    mode               Value          TR101 VLAN Field
--------- ------- ----------    ---------------    ------------    ----------------
Eth 1/1     No       16          VLAN-Unit-Port     ---             enabled
Eth 1/2     No       16          VLAN-Unit-Port     ---             enabled
```

2.4 DHCP Snooping

2.4.1 Introduction

In networking, DHCP Snooping is a security feature of the network switch to prevent unauthorized DHCP servers sending IP addresses to DHCP clients, or prohibit unrecognized devices sending port-related information to a DHCP server.

2.4.2 Topology



2.4.3 Configuration

(1) Enter global configuration mode by issuing the configure terminal command.

```
S3900-24F4S#configure terminal
```

(2) Create a VLAN.

```
S3900-24F4S(config)#vlan database
S3900-24F4S(config-vlan)#vlan 10
S3900-24F4S(config-vlan)#exit
```

(3) Set the port that connects to the client as the access interface and add it into the VLAN.

```
S3900-24F4S(config)#interface ethernet 1/23
S3900-24F4S(config-if)#switchport mode access
S3900-24F4S(config-if)#switchport access vlan 10
S3900-24F4S(config-if)#exit
```

(4) Set the port that connects to the DHCP server as the access interface and add it into the VLAN.

```
S3900-24F4S(config)#interface ethernet 1/24
S3900-24F4S(config-if)#switchport mode access
S3900-24F4S(config-if)#switchport access vlan 10
S3900-24F4S(config-if)#exit
```

(5) Enable DHCP Snooping on the VLAN.

```
S3900-24F4S(config)#ip dhcp snooping
S3900-24F4S(config)#ip dhcp snooping vlan 10
```

(6) Change the trust setting of the port that is connected to the DHCP server to trust at the interface configuration level.

```
S3900-24F4S(config)#interface ethernet 1/24
S3900-24F4S(config-if)#ip dhcp snooping trust
S3900-24F4S(config-if)#end
```

(7) Check whether the DHCP binding table is created to verify the configuration.

```
S3900-24F4S#show ip dhcp snooping binding
MAC Address         IP Address      Lease(sec)      Type            VLAN      Interface
64-9D-99-9d-ab-42   10.32.96.19     2673            dhq>-snooping   10        Eth 1/23
```

2.5 Static link aggregation & 802.3ad with LACP

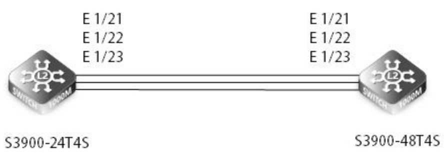
2.5.1 Introduction

In networking, the LACP (link aggregation control protocol) technology is used to increase the bandwidth of a single connection and provide redundancy in case one of the links fails. The LACP configuration can achieve two types of link aggregation groups (LAGs): dynamic LAGs and static LAGs.

NOTE:

- Theoretically, any LACP link group can be formed by links with different transmission media and data rate. But when links with different data rates have to be connected as one aggregation group, please remember to manually limit the higher data rate to the lowest one.
- FS S3900 series switches allow for the maximum of 26 aggregation link groups between two switches. As for a single LACP connection group, the S3900-48T4S switch type enables a maximum of 52 ports to be bundled together; while the S3900-24T4S and S3900-24T4S can accommodate no more than 28 ports together. Notably, every LACP link group of S3900 series switches can only have 8 active ports to work at the same time, while the remaining ports can only do back-up. Only if the active port fails down, can the back-up port join the active group to work.
- If you need to do LACP for S3900-series switches with other devices, please make sure the other devices also support LACP, otherwise the LACP link cannot be set up.

2.5.2 Topology



2.5.3 Configuration

Static Configuration Commands

(1) Create a port-channel and configure it to work in LACP mode to implement link aggregation. The configuration of S3900-24T4S is similar to that of S3900-48T4S and is not mentioned here.

```
S3900-48T4S(config)#interface port-channel 1
```

(2) Add member interfaces to the channel-group. The configuration of S3900-48T4S is similar to that of S3900-24T4S and is not mentioned here.

```
S3900-48T4S#configureterminal
S3900-48T4S (config)#interface ethernet 1/21
S3900-48T4S (config-if)#channel-group 1 mode on
S3900-48T4S (config-if)#exit
S3900-48T4S (config)#interface ethernet 1/22
S3900-48T4S (config-if)#channel-group 1 mode on
S3900-48T4S (config-if)#exit
```

(3) Create VLANs and add interfaces to the VLANs.

```
S3900-48T4S (config)#vlan database
S3900-48T4S (config-vlan)#vlan 10
S3900-48T4S (config-vlan)#exit
S3900-48T4S (config)#interface port-channel 1
S3900-48T4S (config-if)#switchport mode trunk
S3900-48T4S (config-if)#switchport trunk allowed vlan add 10
```

(4) Verify the configuration. Check information about the channel-group on each switch and check whether link negotiation is successful.

```
S3900-48T4S #show interfaces status port-channel 1
Group Type: Static
Port Type: 1000BASE-T
Link Status: Up
Speed-duplex Status: 1000full
Max Frame Size: 1518 bytes (1522 bytes for tagged frames)
MAC Learning Status: Enabled
Member Ports: Eth1/21, Eth1/22
Active Member Ports: Eth1/21, Eth1/22
```

Dynamic Configuration Commands

(1) Add member interfaces to the channel-group. The configuration of S3900-48T4S is similar to that of S3900-24T4S and is not mentioned here.

```
S3900-24T4S#configure terminal
S3900-24T4S (config)#interface ethernet 1/21
S3900-24T4S (config-if)#channel-group 1 mode auto
S3900-24T4S(config-if)#exit
S3900-24T4S (config)#interface ethernet 1/22
S3900-24T4S (config-if)#channel-group 1 mode auto
S3900-24T4S (config-if)#exit
S3900-24T4S (config)#interface ethernet 1/23
S3900-24T4S (config-if)#channel-group 1 mode auto
S3900-24T4S (config-if)#exit
```

(2) Set the LACP system priority and determine the Actor so that the Partner selects active interfaces based on the Actor interface priority. (Optional configuration)

```
S3900-24T4S (config)#interface port-channel 1
S3900-24T4S (config-if)#lacp system-priority 100
```

(3) Set the upper threshold for the number of active interfaces to improve reliability. (Optional configuration)

```
S3900-24T4S (config)#interface port-channel 1
S3900-24T4S (config-if)#lacp max-member-count 8
```

(4) Set LACP interface priorities and determine active interfaces so that interfaces with higher priorities are selected as active interfaces. (Optional configuration)

```
S3900-24T4S (config)#interface ethernet 1/21
S3900-24T4S (config-if)#lacp port-priority 100
S3900-24T4S(config-if)#exit
S3900-24T4S(config)#interface ethernet 1/22
S3900-24T4S (config-if)#lacp port-priority 100
```

(5) Create VLANs and add interfaces to the VLANs. (Optional configuration)

```
S3900-24T4S (config)#vlan database
S3900-24T4S (config-vlan)#vlan 10
S3900-24T4S (config-vlan)#exit
S3900-24T4S (config)#interface port-channel 1
S3900-24T4S (config-if)#switchport mode trunk
S3900-24T4S (config-if)#switchport trunk allowed vlan add 10
```

(6) Verify the configuration. Check information about the channel-group on each switch and check whether link negotiation is successful.

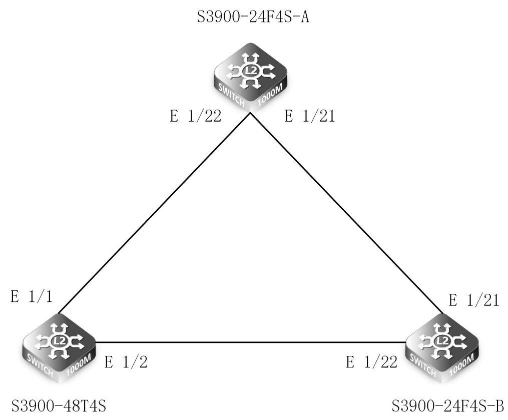
```
S3900-24T4S#show interfaces status port-channel 1
Group Type: LACP
Port Type: 1000BASE SFP
Link Status: Up
Speed-duplex Status: 1000full
Max Frame Size: 1518 bytes (1522 bytes for tagged frames)
MAC Learning Status: Enabled
Member Ports: Eth1/21, Eth1/22, Eth1/23
Active Member Ports: Eth1/21, Eth1/22,Eth1/23
S3900-48T4S#show interfaces status port-channel 1
Group Type: LACP
Port Type: 1000BASE SFP
Link Status: Up
Speed-duplex Status: 1000full
Max Frame Size: 1518 bytes (1522 bytes for tagged frames)
MAC Learning Status: Enabled
Member Ports: Eth1/21, Eth1/22, Eth1/23
Active Member Ports: Eth1/21, Eth1/22, Eth1/23
S3900-24T4S#show lacp
Port Channel: 1
Max Member Count: 8
Timeout: Long
State: Active
--------------------------------------------------------------
Member Port: Eth 1/21
System Priority: 100
Port Priority: 100
--------------------------------------------------------------
Member Port: Eth 1/22
System Priority: 100
Port Priority: 100
--------------------------------------------------------------
Member Port: Eth 1/23
System Priority: 100
Port Priority: 32768
S3900-48T4S#show lacp
Port Channel: 1
Max Member Count: 8
Timeout: Long
State: Active
--------------------------------------------------------------
Member Port: Eth 1/21
System Priority: 32768
Port Priority: 32768
--------------------------------------------------------------
Member Port: Eth 1/22
System Priority: 32768
Port Priority: 32768
--------------------------------------------------------------
Member Port: Eth 1/23
System Priority: 32768
Port Priority: 32768
```

2.6 STP

2.6.1 Introduction

STP (Spanning Tree Protocol) is a Layer 2 protocol that runs on network switches. The main purpose of STP is to prevent the loop caused by redundant paths, avoiding the broadcast storm and MAC address table unstable.

2.6.2 Topology



2.6.3 Configuration

(1) Configure S3900-24F4S-A first. Enable STP in a global schema, and set STP mode and priority, configuring it as the root bridge.

```
S3900-24F4S-A(config)#spanning-tree
S3900-24F4S-A(config)#spanning-tree mode stp
S3900-24F4S-A(config)#spanning-tree priority 0
```

(2) Configure S3900-24F4S-B. Enable STP in a global schema, and set STP mode.

```
S3900-24F4S-B(config)#spanning-tree
S3900-24F4S-B(config)#interface vlan 1
```

(3) Configure S3900-48T4S. Enable STP in a global schema, and set STP mode.

```
S3900-48T4S(config)#spanning-tree
S3900-48T4S(config)#spanning-tree mode stp
```

(4) Check information about STP state on each switch and verify whether STP configuration is successful.
Check S3900-24F4S-A state.

```
S3900-24F4S-A#show spanning-tree brief
Spanning Tree Mode: STP
Spanning Tree Enabled/Disabled: Enabled
Designated Root: 0.ECD68A369C78
Current Root Port: 0
Current Root Cost: 0
Interface   Role  Sts   Bridge ID    Port ID          Prio          Cost     STP
------------------------------------------------------------------------------------------------------------------------------------------------------------
Eth 1/1     DISB  BLK   0.ECD68A369C78    128.1    128          20000    EN
Eth 1/2     DISB  BLK   0.ECD68A369C78    128.2    128          20000    EN
Eth 1/3     DISB  BLK   0.ECD68A369C78    128.3     128         20000   EN
Eth 1/4     DISB  BLK   0.ECD68A369C78    128.4    128          20000    EN
Eth 1/5     DISB  BLK   0.ECD68A369C78    128.5    128          20000    EN
Eth 1/6     DISB  BLK   0.ECD68A369C78    128.6    128          20000    EN
Eth 1/7     DISB  BLK   0.ECD68A369C78    128.7    128          20000    EN
Eth 1/8     DISB  BLK   0.ECD68A369C78    128.8    128          20000    EN
Eth 1/9     DISB  BLK   0.ECD68A369C78    128.9    128          20000    EN
Eth 1/10    DISB  BLK   0.ECD68A369C78    128.10    128         20000    EN
Eth 1/11    DISB  BLK   0.ECD68A369C78    128.11    128       20000      EN
Eth 1/12    DISB  BLK   0.ECD68A369C78    128.12    128       20000      EN
Eth 1/13    DISB  BLK   0.ECD68A369C78    128.13    128       20000      EN
Eth 1/14    DISB  BLK   0.ECD68A369C78    128.14    128       20000      EN
Eth 1/15    DISB  BLK   0.ECD68A369C78    128.15    128       20000      EN
```

```
Eth 1/16    DISB  BLK   0.ECD68A369C78       128.16      128              20000       EN
Eth 1/17    DISB  BLK   0.ECD68A369C78       128.17      128              20000       EN
Eth 1/18    DISB  BLK   0.ECD68A369C78       128.18      128              20000       EN
Eth 1/19    DISB  BLK   0.ECD68A369C78       128.19      128              20000       EN
Eth 1/20    DISB  BLK   0.ECD68A369C78       128.20      128              20000       EN
Eth 1/21    DESG FWD         0.ECD68A369C78 128.21      128              20000       EN
Eth 1/22    DESG FWD         0.ECD68A369C78 128.22      128              20000       EN
```

Check S3900-24F4S-B state.

```
S3900-24F4S-B#show spanning-tree brief
Spanning Tree Mode: STP
Spanning Tree Enabled/Disabled: Enabled
Designated Root: 0.ECD68A369C78
Current Root Port (Eth): 1/21
Current Root Cost: 20000
Interface   Role   Sts    Bridge ID                    Port ID   Prio     Cost        STP
--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------
Eth 1/1     DISB BLK    32768.ECD68A369B13  128.1       128       20000       EN
Eth 1/2     DISB BLK    32768.ECD68A369B13  128.2       128       20000       EN
Eth 1/3     DISB BLK    32768.ECD68A369B13  128.3       128       20000       EN
Eth 1/4     DISB BLK    32768.ECD68A369B13  128.4       128       20000       EN
Eth 1/5     DISB BLK    32768.ECD68A369B13  128.5       128       20000       EN
Eth 1/6     DISB BLK    32768.ECD68A369B13  128.6       128       20000       EN
Eth 1/7     DISB BLK    32768.ECD68A369B13  128.7       128       20000       EN
Eth 1/8     DISB BLK    32768.ECD68A369B13  128.8       128       20000       EN
Eth 1/9     DISB BLK    32768.ECD68A369B13  128.9       128       20000       EN
Eth 1/10    DISB BLK    32768.ECD68A369B13  128.10      128       20000       EN
Eth 1/11    DISB BLK    32768.ECD68A369B13  128.11      128       20000       EN
Eth 1/12    DISB BLK    32768.ECD68A369B13  128.12        128       20000     EN
Eth 1/13    DISB BLK    32768.ECD68A369B13  128.13        128       20000     EN
Eth 1/14    DISB BLK    32768.ECD68A369B13  128.14          128       20000   EN
Eth 1/15    DISB BLK    32768.ECD68A369B13  128.15        128       20000     EN
Eth 1/16    DISB BLK    32768.ECD68A369B13  128.16        128       20000     EN
Eth 1/17    DISB BLK    32768.ECD68A369B13  128.17        128       20000     EN
Eth 1/18    DISB BLK    32768.ECD68A369B13  128.18        128       20000     EN
Eth 1/19    DISB BLK    32768.ECD68A369B13  128.19        128       20000     EN
Eth 1/20    DISB BLK    32768.ECD68A369B13  128.20        128       20000     EN
Eth 1/21    ROOTFWD  0.ECD68A369C78        128.21        128       20000     EN
Eth 1/22    ALTN BLK    32768.000000000202   128.2       128       20000       EN
```

Check S3900-48T4S state.

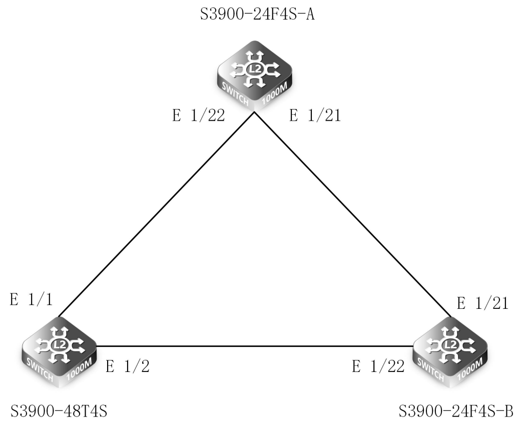
```
S3900-48T4S-A-3#show spanning-tree brief
Spanning Tree Mode: STP
Spanning Tree Enabled/Disabled: Enabled
Designated Root: 0.ECD68A369C78
Current Root Port (Eth): 1/1
Current Root Cost: 20000
Interface   Role         Sts    Bridge ID                      Port ID       Prio    Cost   STP
--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------
Eth 1/1     ROOT         FWD  0.ECD68A369C78          128.22        128    20000         EN
Eth 1/2     DESG         FWD  32768.000000000202   128.2          128    20000         EN
```

2.7 RSTP

2.7.1 Introduction

RSTP is the improvement of STP. Because the STP network convergence speed is slow, IEEE introduced RSTP to provide significant recovery in response to network changes or failures. RSTP is backward compatible with standard STP.

2.7.2 Topology



2.7.3 Configuration

(1) Configure S3900-24F4S-A first. Enable STP in a global schema, and set STP mode and priority, configuring it as the root bridge.

```
S3900-24F4S-A(config)#spanning-tree
S3900-24F4S-A(config)#spanning-tree priority 0
S3900-24F4S-A(config)#spanning-tree mode rstp
```

(2) Configure S3900-24F4S-B. Enable STP in a global schema, and set STP mode.

```
S3900-24F4S-B(config)#spanning-tree
S3900-24F4S-B(config)#spanning-tree mode rstp
```

(3) Configure S3900-48T4S. Enable STP in a global schema, and set STP mode.

```
S3900-48T4S(config)#spanning-tree
S3900-48T4S(config)#spanning-tree mode rstp
```

(4) Check information about RSTP state on each switch and verify whether RSTP configuration is successful.
Check S3900-24F4S-A state.

```
S3900-24F4S-A#show spanning-tree brief
Spanning Tree Mode: RSTP
Spanning Tree Enabled/Disabled: Enabled
Designated Root: 0.ECD68A369C78
Current Root Port: 0
Current Root Cost: 0
Interface  Role  Sts  Bridge ID       Port ID  Prio  Cost  STP
Eth 1/1    DISB  BLK  0.ECD68A369C78  128.1    128   20000  EN
Eth 1/2    DISB  BLK  0.ECD68A369C78  128.2    128   20000  EN
Eth 1/3    DISB  BLK  0.ECD68A369C78  128. 3   128   20000  EN
Eth 1/4    DISB  BLK  0.ECD68A369C78  128.4    128   20000  EN
Eth 1/5    DISB  BLK  0.ECD68A369C78  128. 5   128   20000  EN
Eth 1/6    DISB  BLK  0.ECD68A369C78  128.6    128   20000  EN
Eth 1/7    DISB  BLK  0.ECD68A369C78  128.7    128   20000  EN
Eth 1/8    DISB  BLK  0.ECD68A369C78  128.8    128   20000  EN
Eth 1/9    DISB  BLK  0.ECD68A369C78  128.9    128   20000  EN
Eth 1/10   DISB  BLK  0.ECD68A369C78  128.10   128   20000  EN
Eth 1/11   DISB  BLK  0.ECD68A369C78  128.11   128   20000  EN
Eth 1/12   DISB  BLK  0.ECD68A369C78  128.12   128   20000  EN
Eth 1/13   DISB  BLK  0.ECD68A369C78  128.13   128   20000  EN
Eth 1/14   DISB  BLK  0.ECD68A369C78  128.14   128   20000  EN
Eth 1/15   DISB  BLK  0.ECD68A369C78  128.15   128   20000  EN
Eth 1/16   DISB  BLK  0.ECD68A369C78  128.16   128   20000  EN
Eth 1/17   DISB  BLK  0.ECD68A369C78  128.17   128   20000  EN
Eth 1/18   DISB  BLK  0.ECD68A369C78  128.18   128   20000  EN
Eth 1/19   DISB BLK  0.ECD68A369C78 128.19    128   20000   EN
Eth 1/20   DISB BLK  0.ECD68A369C78 128.20    128   20000   EN
Eth 1/21   DESG FWD  0.ECD68A369C78 128.21    128   20000   EN
Eth 1/22   DESG FWD  0.ECD68A369C78 128.22    128   20000   EN
```

Check S3900-24F4S-B state.

```
S3900-24F4S-B#show spanning-tree brief
Spanning Tree Mode: RSTP
Spanning Tree Enabled/Disabled: Enabled
Designated Root: 0.ECD68A369C78
Current Root Port (Eth): 1/21
Current Root Cost: 20000
Interface   Role  Sts   Bridge ID    Port ID     Prio        Cost  STP
Eth 1/1     DISB  BLK   32768.ECD68A369B13  128.1     128   20000    EN
Eth 1/ 2    DISB  BLK   32768.ECD68A369B13  128.2     128   20000    EN
Eth 1/ 3    DISB  BLK   32768.ECD68A369B13  128.3     128   20000    EN
Eth 1/4     DISB  BLK   32768.ECD68A369B13  128.4     128   20000    EN
Eth 1/ 5    DISB  BLK   32768.ECD68A369B13  128.5     128   20000    EN
Eth 1/ 6    DISB  BLK   32768.ECD68A369B13  128.6     128   20000    EN
Eth 1/7     DISB  BLK   32768.ECD68A369B13  1287      128   20000    EN
Eth 1/ 8    DISB  BLK   32768.ECD68A369B13  128.8     128   20000    EN
Eth 1/ 9    DISB  BLK   32768.ECD68A369B13  128.9     128   20000    EN
Eth 1/10    DISB  BLK   32768.ECD68A369B13  128.10    128   20000    EN
Eth 1/11    DISB  BLK   32768.ECD68A369B13  128.11    128   20000    EN
Eth 1/12    DISB  BLK   32768.ECD68A369B13  128.12    128   20000    EN
Eth 1/13    DISB  BLK   32768.ECD68A369B13  128.13    128   20000    EN
Eth 1/14    DISB  BLK   32768.ECD68A369B13  128.14    128   20000    EN
Eth 1/15    DISB  BLK   32768.ECD68A369B13  128.15    128   20000    EN
Eth 1/16    DISB  BLK   32768.ECD68A369B13  128.16    128   20000    EN
Eth 1/17    DISB  BLK   32768.ECD68A369B13  128.17    128   20000    EN
Eth 1/18    DISB  BLK   32768.ECD68A369B13  128.18    128   20000    EN
Eth 1/19    DISB  BLK   32768.ECD68A369B13  128.19    128   20000    EN
Eth 1/20    DISB  BLK   32768.ECD68A369B13  128.20    128   20000    EN
Eth 1/21    ROOTFWD  0.ECD68A369C78         128.21    128   20000    EN
Eth 1/22    ALTN BLK   32768.000000000202   128.2     128   20000    EN
```

Check S3900-48T4S state.

```
S3900-48T4S#show spanning-tree brief
Spanning Tree Mode: RSTP
Spanning Tree Enabled/Disabled: Enabled
Designated Root: 0.ECD68A369C78
Current Root Port (Eth): 1/1
Current Root Cost: 20000
Interface   Role Sts   Bridge ID             Port ID    Prio        Cost      STP
Eth 1/1     ROOTFWD  0.ECD68A369C78       128.22     128         20000     EN
Eth 1/2     DESG FWD  32768.000000000202   128.2      128         20000     EN
```

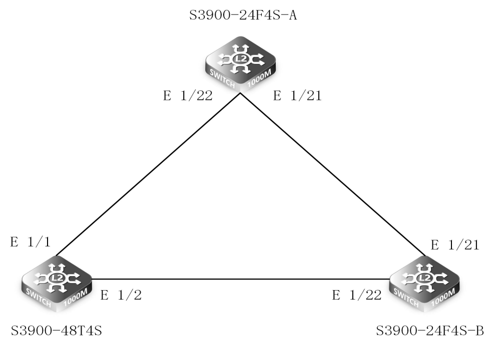
2.8 MSTP

2.8.1 Introduction

MSTP, a multiple spanning tree protocol, can divide a switching network into multiple domains, and multiple spanning trees are formed in each domain. The spanning trees are independent of each other to achieve the separation of different VLAN traffic and achieve the purpose of network load balancing.

2.8.2 Topology

Perform MSTP protocol calculation in process units. Ports that are not in the same process do not participate in MSTP protocol calculation in this process, so that the spanning tree calculations in each process are independent of each other and do not affect each other.



2.8.3 Configuration

(1) Create VLAN

```
S3900-24F4S-A#configure terminal
S3900-24F4S-A(config)#vlan database
S3900-24F4S-A(config-vlan)#vlan 7
S3900-24F4S-A(config-vlan)#vlan 8
S3900-24F4S-A(config-vlan)#exit
```

(2) Link mode is trunk and allows all VLANs to pass

```
S3900-24F4S-A#configure terminal
S3900-24F4S-A(config)#interface ethernet 1/20
S3900-24F4S-A(config-if)#switchport mode trunk
S3900-24F4S-A(config-if)#switch trunk allowed vlan all
S3900-24F4S-A(config-if)#interface ethernet 1/21
S3900-24F4S-A(config-if)#switchport mode trunk
S3900-24F4S-A(config-if)#switch trunk allowed vlan all
```

(3) Create MST domain

```
S3900-24F4S-A#configure terminal
S3900-24F4S-A(config)#spanning-tree mode mstp
S3900-24F4S-A(config)#spanning-tree mst configuration
S3900-24F4S-A(config-mstp)#mst 1 vlan 7
S3900-24F4S-A(config-mstp)#mst 2 vlan 8
S3900-24F4S-A(config-mstp)#revision 1
S3900-24F4S-A(config-mstp)#name fs
S3900-24F4S-A(config-mstp)#
```

(4) Configure priority for instance 1 and instance 2

```
S3900-24F4S-A#configure terminal
S3900-24F4S-A(config)#spanning-tree mst configuration
S3900-24F4S-A(config-mstp)#mst 1 priority 4096
S3900-24F4S-A(config-mstp)#mst 2 priority 8192
```

NOTE：Switch B and Switch C can be configured according to Switch A.

2.8.4 Verification

Check with #show spanning-tree mst number

```
S3900-24F4S-A#show spanning-tree mst 1
Spanning tree brief for instance 1
###### MST 1 Vlans Mapped                : 7
 Spanning Tree Enabled Mode MSTP
 Default port cost method                : Short
 Root ID        Priority      4096
                Address       64:9D:99:10:06:60
                Hello Time    2 sec    Max Age 20 sec    Forward Delay 15 sec
 Bridge ID      Priority      4096
                 Address       64:9D:99:10:06:60
                 Hello Time    2 sec    Max Age 20 sec    Forward Delay 15 sec
                 Max hops 20 Remaining Hops    20
 Number of topology changes 0 last change occurred 1887 ago
 Transmission Limit                : 3
 Flooding Behavior                 : filtering
Interface Role Sts    Bridge ID                    Port ID       Prio Cost        STP
--------- ---- ----- -------------------------- ----------    --- -------- ------
Eth 1/20    DISB BLK    4096.1.64:9D:99:10:06:60    128.20       128      20000 EN
Eth 1/21    DISB BLK    4096.1.64:9D:99:10:06:60    128.21       128      20000 EN

S3900-24F4S-A#show spanning-tree mst 2
Spanning tree brief for instance 2
###### MST 2 Vlans Mapped                : 8
 Spanning Tree Enabled Mode MSTP
 Default port cost method                : Short
 Root ID        Priority      8192
                 Address       64:9D:99:10:06:60
                 Hello Time    2 sec    Max Age 20 sec    Forward Delay 15 sec
```

```
 Bridge ID      Priority        8192
                    Address        64:9D:99:10:06:60
                    Hello Time    2 sec    Max Age 20 sec    Forward Delay 15 sec
                    Max hops 20 Remaining Hops    20
 Number of topology changes 0 last change occurred 1931 ago
 Transmission Limit                          : 3
 Flooding Behavior                           : filtering
Interface Role Sts      Bridge ID                        Port ID        Prio Cost         STP
--------- ---- ----- -------------------------- ----------     --- -------- ------
Eth 1/20      DISB BLK      8192.2.64:9D:99:10:06:60      128.20         128        20000 EN
Eth 1/21      DISB BLK      8192.2.64:9D:99:10:06:60      128.21         128        20000 EN
```

2.9 BPDU Guard/filtering

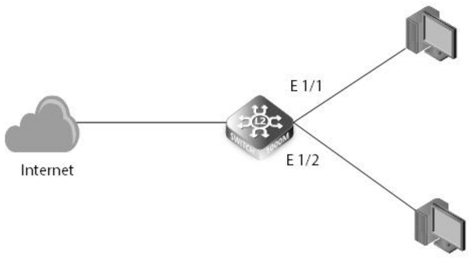
2.9.1 Introduction

On the switching device, usually the port directly connected to a non-switching device such as a user terminal (such as a PC) or a file server is configured as an edge port. Normally, edge ports will not receive RST BPDU. If someone forges the RST BPDU maliciously and attacks the switching device, when the edge port receives the RST BPDU, the switching device will automatically set the edge port as a non-edge port and re-calculate the spanning tree, causing network shock. After the BPDU protection function is enabled on the switching device, if an edge port receives a RST BPDU, the edge port will be blocked, but the attributes of the edge port will not change.

Introduction to edge ports and bpdu-filter

For a communication network running the spanning tree protocol, when the current port is configured as an edge port by using the command # spanning-tree portfast, the port no longer participates in spanning tree calculation, thereby helping to accelerate the convergence time of the network topology and enhance the stability of the network. However, the port still sends BPDU packets, which may cause BPDU packets to be sent to other networks, causing shocks on other networks. This problem can be solved by configuring the command #stp bpdu-filter enable on the port. Configure this command on a network edge device so that an edge port does not process or send BPDU packets. This port is the BPDU filter port.

2.9.2 Topology



(1) Switch enable stp
(2) The corresponding port of the switch is set as an edge port
(3) Switch corresponding edge port set the corresponding protection function

2.9.3 Configuration

(1) Enable rstp function

```
Switch#configure terminal
Switch(config)#spanning-tree
Switch(config)#spanning-tree mode rstp
```

(2) Switch ports set as edge ports

```
Switch(config)#interface ethernet 1/1
Switch(config-if)#spanning-tree portfast
Switch(config-if)#exit
Switch(config)#interface ethernet 1/2
Switch(config-if)#spanning-tree portfast
Switch(config-if)#exit
```

(3) Enable bpdu-guard on port 1/1, and enable bpdu-filter on port 1/2

```
Switch(config)#interface ethernet 1/1
Switch(config-if)#spanning-tree bpdu-guard
Switch(config-if)#exit
Switch(config)#interface ethernet 1/2
Switch(config-if)#spanning-tree bpdu-filter
Switch(config-if)#exit
```

2.9.4 Verification

Check with #show spanning-tree interface ethernet 1/1

```
Switch#show spanning-tree interface ethernet 1/1
Eth 1/ 1 Information
---------------------------------------------------------------
 Stp Status                            : Enabled
 Port Role/State                       : Disabled/Discarding
 Port Priority                         : 128
 Port Cost                             : Admin=0 Oper=20000
 Designated Root/Cost                  : 32768.64:9D:99:10:06:60/0
 Designated Bridge/Port                : 32768.64:9D:99:10:06:60/128.1
 Port Fast                             : Admin=Enabled Oper=Enabled
 Link Type                             : Admin=Auto Oper=Point-to-point
 Forward Transitions                   : 0
 Root Guard Status                     : Disabled
 BPDU Flooding                         : Enabled
 BPDU Guard Status/Recovery            : Enabled/No-auto(300 s)
 BPDU Filter Status                    : Disabled
 TC Prop Stop                          : Disabled
 Loopback Detection Status/Mode        : Enabled/Auto
 Loopback Detection Trap/Action        : Disabled/Shutdown
```

```
Switch#show spanning-tree interface ethernet 1/2
Eth 1/ 2 Information
---------------------------------------------------------------
 Stp Status                            : Enabled
 Port Role/State                       : Disabled/Discarding
 Port Priority                         : 128
 Port Cost                             : Admin=0 Oper=20000
 Designated Root/Cost                  : 32768.64:9D:99:10:06:60/0
 Designated Bridge/Port                : 32768.64:9D:99:10:06:60/128.2
 Port Fast                             : Admin=Enabled Oper=Enabled
 Link Type                             : Admin=Auto Oper=Point-to-point
 Forward Transitions                   : 0
 Root Guard Status                     : Disabled
 BPDU Flooding                         : Enabled
 BPDU Guard Status/Recovery            : Disabled/No-auto(300 s)
 BPDU Filter Status                    : Enabled
 TC Prop Stop                          : Disabled
 Loopback Detection Status/Mode        : Disabled/Auto
 Loopback Detection Trap/Action        : Disabled/Shutdown
```

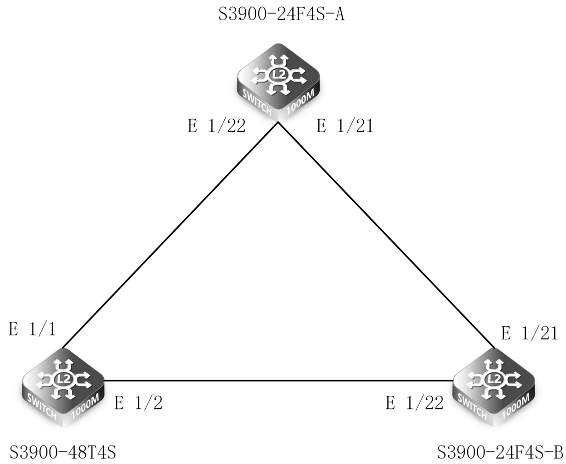
2.10 Root Guard

2.10.1 Introduction

Due to incorrect configuration of the maintenance personnel or malicious attacks on the network, the legal root bridge in the network may receive a higher priority RST BPDU, which will cause the legal root bridge to lose its root status and cause incorrect changes in the network topology.This illegal topology change will cause the traffic that should have passed through the high-speed link to be dragged to the low-speed link, causing network congestion.

For a designated port with the root protection function enabled, its port role can only remain as the designated port. Once a designated port with Root protection enabled receives a RST BPDU with a higher priority, the port state will enter the Discarding state and no longer forward packets. After a period of time (usually twice the Forward Delay), if the port does not receive any higher priority RST BPDUs, the port will automatically return to the normal Forwarding state.

2.10.2 Networking Ideas



2.10.3 Example Configuration Commands

```
S3900-24F4S-A(config)#interface ethernet 1/21
S3900-24F4S-A((config-if)#spanning-tree guard root
```

2.10.4 Verification

```
S3900-24F4S-A(#show spanning-tree interface ethernet 1/21
Eth 1/21 Information
-------------------------------------------------------------------
 Stp Status                              : Enabled
 Port Role/State                         : Designate/Forwarding
 Port Priority                           : 128
 Port Cost                               : Admin=0 Oper=20000
 Designated Root/Cost                    : 32768.64:9D:99:10:06:60/0
 Designated Bridge/Port                  : 32768.64:9D:99:10:06:60/128.12
 Port Fast                               : Admin=Auto Oper=Enabled
 Link Type                               : Admin=Auto Oper=Point-to-point
 Forward Transitions                     : 6
 Root Guard Status                       : Enabled
 BPDU Flooding                           : Enabled
 BPDU Guard Status/Recovery              : Disabled/No-auto(300 s)
 BPDU Filter Status                      : Disabled
 TC Prop Stop                            : Disabled
 Loopback Detection Status/Mode          : Disabled/Auto
 Loopback Detection Trap/Action          : Disabled/Shutdown
```

2.11 Supports Voice VLAN

2.11.1 Introduction

A voice VLAN is a VLAN (virtual local area network) that is specifically allocated for user's voice data streams. It ensures the quality of a voice service due to the priority of voice stream transmission when other services (video or data services) are transmitted simultaneously.

2.11.2 Topology

2.11.3 Configuration

Configuration on MAC Address-based Mode

(1) Create a VLAN

```
S3900-48T4S#configure terminal
S3900-48T4S (config)#vlan database
S3900-48T4S (config-vlan)#vlan 2
```

(2) Configure the VLAN to allow ethernet 1/1 and ethernet 1/2 interface to pass.

```
S3900-48T4S(config)#interface ethernet 1/1
S3900-48T4S(config-if)#switchport mode hybrid
S3900-48T4S(config-if)#switchport hybrid pvid 2
S3900-48T4S(config-if)#switchport hybrid allowed vlan add 2 untagged
S3900-48T4S(config)#interface ethernet 1/2
S3900-48T4S(config-if)#switchport mode trunk
S3900-48T4S(config-if)#switchport trunk allowed vlan add 2
```

(3) Configure the OUI to match the source MAC address (the MAC address of the IP phone, here is 64-9D-99-1F-02-02) of the received packet.

```
S3900-48T4S(config)#voice vlan 2
S3900-48T4S(config)#voice vlan mac-address 64-9D-99-00-00-00 mask ff-ff-ff-00-00-00 description voice
```

(4) Configure the voice VLAN function on the interface.

```
S3900-48T4S(config)#interface ethernet 1/1
S3900-48T4S(config-if)#switchport voice vlan auto
S3900-48T4S(config-if)#switchport voice vlan priority 6
S3900-48T4S(config-if)#switchport voice vlan rule oui
S3900-48T4S(config-if)#switchport voice vlan security
```

(5) Check the configuration results.

```
S3900-48T4S#show voice vlan status
Port         Mode       Security      Rule         Priority Remaining Age
                                                            (minutes)
-----------------------------------------------------------------------------------------------------------------------------------
Eth 1/1      Auto       Enabled       OUI                   6 NA
S3900-1#show voice vlan oui
OUI Address               Mask                   Description
-----------------------------------------------------------------------------------------------------------------------------------
64-9D-99-00-00-00    FF-FF-FF-00-00-00          voice
```

Configuration on VLAN-based Mode

(1) Create a VLAN

```
S3900-48T4S#configure terminal
S3900-48T4S (config)#vlan database
S3900-48T4S (config-vlan)#vlan 2
```

(2) Configure the VLAN to allow ethernet 1/1 and ethernet 1/2 interface to pass.

```
S3900-48T4S(config)#interface ethernet 1/1
S3900-48T4S(config-if)#switchport mode hybrid
S3900-48T4S(config-if)#switchport hybrid allowed vlan add 2 tagged
S3900-48T4S(config)#interface ethernet 1/2
S3900-48T4S(config-if)#switchport mode trunk
S3900-48T4S(config-if)#switchport trunk allowed vlan add 2
```

(3) Configure VLAN 2 as a voice VLAN and use a VLAN-based voice VLAN.

```
S3900-48T4S(config)#voice vlan 2
S3900-48T4S(config)#interface ethernet 1/1
S3900-48T4S(config-if)#switchport voice vlan auto
S3900-48T4S(config-if)#switchport voice vlan priority 6
```

(4) Check the configuration results.

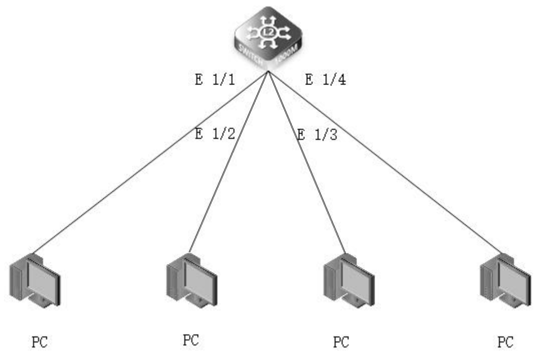
```
S3900-48T4S#show voice vlan status
Port      Mode         Security      Rule                       Priority Remaining Age
                                                                       (minutes)
-----------------------------------------------------------------------------------------------------------------------------------
Eth 1/1   Auto         Disabled      OUI                               6 NA
```

2.12 Port-based VLAN

2.12.1 Introduction

VLAN (Virtual Local Area Network) is a technology that divides a physical LAN into multiple broadcast domains to control the broadcast storm, enhance LAN security and simplify network management. The hosts in the VLAN can communicate with each other, but different VLANs cannot communicate with each other. Consequently, broadcast packets are confined to within a single VLAN.

2.12.2 Topology



2.12.3 Configuration

Configure VLAN for the Access Interface

(1) Login to the S3900-24F4S switch and enter into the CLI interface.

(2) Create VLAN 10 and VLAN 20 in the S3900-24F4S switch 1.

```
S3900-24F4S#configure terminal
S3900-24F4S(config)#vlan database
S3900-24F4S(config-vlan)#vlan 10,20
```

(3) Configure the 1/1 port as the access interface and add it into VLAN 10

```
S3900-24F4S(config)#interface ethernet 1/1
S3900-24F4S(config-if)#switchport mode access
S3900-24F4S(config-if)#switchport access vlan 10
```

(4) Configure the 1/2 port as the access interface and add it into VLAN 20

```
S3900-24F4S(config)#interface ethernet 1/2
S3900-24F4S(config-if)#switchport mode access
S3900-24F4S(config-if)#switchport access vlan 20
```

(5) Configure the 1/3 port as the access interface and add it into VLAN 10

```
S3900-24F4S(config)#interface ethernet 1/3
S3900-24F4S(config-if)#switchport mode access
S3900-24F4S(config-if)#switchport access vlan 10
```

(6) Configure the 1/4 port as the access interface and add it into VLAN 20

```
S3900-24F4S(config)#interface ethernet 1/4
S3900-24F4S(config-if)#switchport mode access
S3900-24F4S(config-if)#switchport access vlan 20
```

(7) After the configuration is successful, PC1 and PC3 are in the same VLAN 10 and can communicate with each other. PC2 and PC4 can communicate with each other and cannot communicate with PC1 and PC3.

Configure VLAN for the Trunk Interface

(1) Login to the S3900-24F4S switch and enter into the CLI interface.

(2) Create VLAN 10 and VLAN 20 in the S3900-24F4S switch 1.

```
S3900-24F4S#configure terminal
S3900-24F4S(config)#vlan database
S3900-24F4S(config-vlan)#vlan 10,20
```

(3) Configure the 1/1 port as the access interface and add it into VLAN 10.

```
S3900-24F4S(config)#interface ethernet 1/1
S3900-24F4S(config-if)#switchport mode access
S3900-24F4S(config-if)#switchport access vlan 10
```

(4) Configure the 1/2 port as the access interface and add it into VLAN 20.

```
S3900-24F4S(config)#interface ethernet 1/2
S3900-24F4S(config-if)#switchport mode access
S3900-24F4S(config-if)#switchport access vlan 20
```

(5) Configure the 1/3 port as the trunk interface and allow all VLANs to get through.

```
S3900-24F4S(config)#interface ethernet 1/3
S3900-24F4S(config-if)#switchport mode trunk
S3900-24F4S(config-if)#switchport trunk allowed vlan all
```

(6) Do the same configuration on S3900-24F4S switch 2 like the switch 1 above, and then connect the two trunk ports together.

(7) After the configuration is successful, PC1 and PC3 can communicate with each other and PC2 and PC4 can also communicate with each other.

Configure VLAN for the Hybrid Interface

(1) Login to the S3900-24F4S switch and enter into the CLI interface.

(2) Configure VLAN 10, VLAN 20, and VLAN 30 on the S3900-24F4S switch 1.

```
S3900-24F4S#configure terminal
S3900-24F4S(config)#vlan database
S3900-24F4S(config-vlan)#vlan 10,20,30
```

(3) Configure the 1/1 port as the hybrid interface, default VLAN as 10 and allow untagged VLAN 10, 30 to get through.

```
S3900-24F4S(config)#interface ethernet 1/1
S3900-24F4S(config-if)#switchport mode hybrid
S3900-24F4S(config-if)#switchport hybrid pvid 10
S3900-24F4S(config-if)#switchport hybrid allowed vlan add 10,30 untagged
```

(4) Configure the 1/2 port as the hybrid interface, default VLAN as 20 and allow untagged VLAN 20, 30 to get through.

```
S3900-24F4S(config)#interface ethernet 1/2
S3900-24F4S(config-if)#switchport mode hybrid
S3900-24F4S(config-if)#switchport hybrid pvid 20
S3900-24F4S(config-if)#switchport hybrid allowed vlan add 20,30 untagged
```

(5) Configure the 1/3 port as the hybrid interface and allow tagged VLAN 10, 20, 30 to get through.

```
S3900-24F4S(config)#interface ethernet 1/3
S3900-24F4S(config-if)#switchport mode hybrid
S3900-24F4S(config-if)#switchport hybrid allowed vlan add 10,20,30 tagged
```

(6) Create VLAN 10, 20, 30 in the S3900-24F4S switch 2.

```
S3900-24F4S#configure terminal
S3900-24F4S(config)#vlan database
S3900-24F4S(config-vlan)#vlan 10,20,30
```

(7) Configure the 1/1 port as the hybrid interface, default VLAN as 30 and allow untagged VLAN 10, 20, 30 to get through.

```
S3900-24F4S(config)#interface ethernet 1/1
S3900-24F4S(config-if)#switchport mode hybrid
S3900-24F4S(config-if)#switchport hybrid pvid 30
S3900-24F4S(config-if)#switchport hybrid allowed vlan add 10,20,30 untagged
```

(8) Configure the 1/3 port as the hybrid interface and allow tagged VLAN 10, 20, 30 to get through.

```
S3900-24F4S(config)#interface ethernet 1/3
S3900-24F4S(config-if)#switchport mode hybrid
S3900-24F4S(config-if)#switchport hybrid allowed vlan add 10,20,30 tagged
```

(9) After the configuration is successful, PC1 and PC2 can communicate with PC3 and PC1 cannot communicate with PC2.

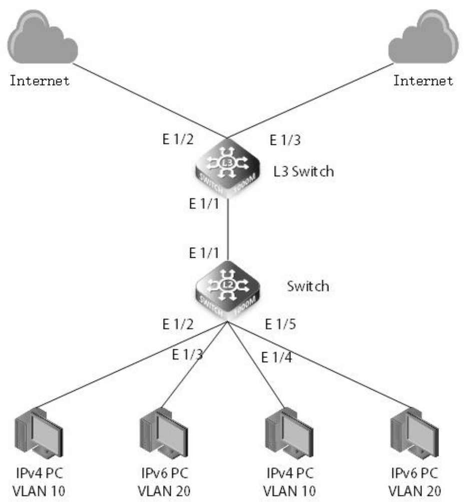
2.13 IEEE 802.1v Protocol-based VLAN

2.13.1 Introduction

There are usually multiple services such as IPTV, VoIP, and Internet access using different protocols in the LAN network. To facilitate network management, services using the same protocol are classified into the same VLAN for management. Thus there will be multiple protocol-based VLANs in one network. Processing data frames based on protocols such as IP, IPX, AT, etc, protocol-based VLAN is a VLAN that can only be configured in the hybrid interface to define filtering criteria for untagged packets.

NOTE:
- When receiving an untagged frame from a port, the switch will identify the protocol profile of the frame and then determine the VLAN that the frame belongs to.
- If protocol-based VLANs are configured on the interface and the protocol profile of the frame matches a protocol-based VLAN, the switch adds the VLAN tag to the frame.
- If protocol-based VLANs are configured on the interface and the protocol profile of the frame matches no protocol-based VLAN, the switch adds the PVID(Port VLAN ID) of the interface to the frame.

2.13.2 Topology



2.13.3 Configuration

(1) Configure the IPv4 address for the PC1 and PC3; configure the IPv6 address for the PC2 and PC4.

```
IPv4: 192.168.10.2
IPv4:192.168.10.3
IPv6: 2001::1:2
IPv6: 2001::1:3
```

(2) Create VLAN 10 and VLAN 20 on the Switch switch.

```
Switch(config)#vlan database
Switch(config-vlan)#vlan 10
Switch(config-vlan)#vlan 20
Switch(config-vlan)#exit
```

(3) Configure the network protocol to associate with the corresponding VLAN.

```
Switch(config)#protocol-vlan protocol-group 1 add frame-type ethernet protocol-type ip
Switch(config)#protocol-vlan protocol-group 2 add frame-type ethernet protocol-type ipv6
Switch(config)#protocol-vlan protocol-group 3 add frame-type ethernet protocol-type arp
Switch(config)#interface ethernet 1/2
Switch(config-if)#protocol-vlan protocol-group 1 vlan 10
Switch(config-if)#protocol-vlan protocol-group 3 vlan 10
Switch(config-if)#exit
Switch(config)#interface ethernet 1/3
Switch(config-if)#protocol-vlan protocol-group 2 vlan 20
Switch(config-if)#exit
Switch(config)#interface ethernet 1/4
Switch(config-if)#protocol-vlan protocol-group 1 vlan 10
```

```
Switch(config-if)#exit
Switch(config)#interface ethernet 1/5
Switch(config-if)#protocol-vlan protocol-group 2 vlan 20
Switch(config-if)#exit
```

(4) Configure the eth1/2-5 port of Switch switch as the hybrid interface and remove the corresponding VLAN tags.

```
Switch(config)#int ethernet 1/2
Switch(config-if)#switchport mode hybrid
Switch(config-if)#switchport hybrid allowed vlan add 10 untagged
Switch(config)#int ethernet 1/3
Switch(config-if)#switchport mode hybrid
Switch(config-if)#switchport hybrid allowed vlan add 20 untagged
Switch(config)#int ethernet 1/4
Switch(config-if)#switchport mode hybrid
Switch(config-if)#switchport hybrid allowed vlan add 10 untagged
Switch(config)#int ethernet 1/5
Switch(config-if)#switchport mode hybrid
Switch(config-if)#switchport hybrid allowed vlan add 20 untagged
```

(5) Configure the eth1/1 port of Switch switch as the trunk interface and allow all VLANs to get through.

```
Switch(config)#int ethernet 1/1
Switch(config-if)#switchport mode trunk
Switch(config-if)#switchport trunk allowed vlan all
```

(6) Verify your configuration.

```
Switch# show protocol-vlan protocol-group
Protocol Group ID    Frame                 Type Protocol Type
---------------------------------------------------------------------------------------------------------------------------------------------------------------
1                    Ethernet               08 00
2                    Ethernet               86 DD
Switch# show int protocol-vlan protocol-group
Port                 Protocol Group ID              VLAN ID
Eth 1/2                    1                          10
Eth 1/3                    2                          20
```

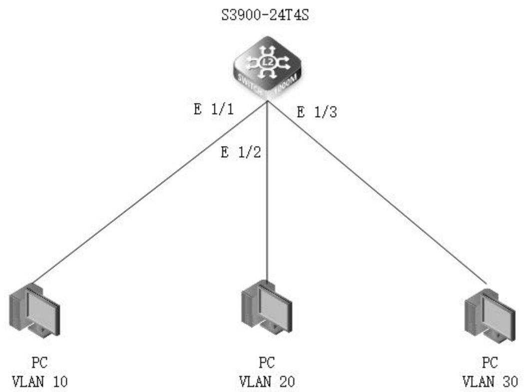
2.14 IP Subnet-based VLAN

2.14.1 Introduction

A VLAN(virtual LAN) is any broadcast domain that is partitioned and isolated in a computer network at the data link layer which groups devices from different physical LANs into a single logical network, improving simplicity, security, traffic management, or economy.

NOTE:
- The IP subnet-based VLAN Configurations are only applicable on hybrid ports.
- The IP subnet-based VLAN Configurations are only applied to untagged packets.

2.14.2 Topology



2.14.3 Configuration

(1) Create IP subnet-based VLANs on S3900-24T4S switch.

```
S3900-24T4S#configure terminal
S3900-24T4S(config)#subnet-vlan subnet 10.1.1.0 255.255.255.0 vlan 10
S3900-24T4S(config)#subnet-vlan subnet 10.1.2.0 255.255.255.0 vlan 20
S3900-24T4S(config)#subnet-vlan subnet 10.1.3.0 255.255.255.0 vlan 30
S3900-24T4S(config)#exit
```

(2) Verify IP subnet-based VLAN configuration.

```
S3900-24T4S#show subnet-vlan
IP Address  Mask           VLAN ID  Priority
10.1.1.0    255.255.255.0    10     0
10.1.2.0    255.255.255.0    20     0
10.1.3.0    255.255.255.0    30     0
```

(3) Create VLAN 10, VLAN 20 and VLAN 30 on the switch.

```
S3900-24T4S#configure terminal
S3900-24T4S(config)#vlan database
S3900-24T4S(config-vlan)#vlan 10
S3900-24T4S(config-vlan)#vlan 20
S3900-24T4S(config-vlan)#vlan 30
S3900-24T4S(config-if)#exit
```

(4) Configure IP address on the switch.

```
S3900-24T4S(config)#interface vlan 10
S3900-24T4S(config-if)#ip add 10.1.1.1/24
S3900-24T4S(config-if)#exit
S3900-24T4S(config)#int vlan 20
S3900-24T4S(config-if)#ip add 10.1.2.1/24
S3900-24T4S(config-if)#exit
S3900-24T4S(config)#interface vlan 30
S3900-24T4S(config-if)#ip add 10.1.3.1/24
S3900-24T4S(config-if)#exit
```

(5) Configure Ethernet 1/1, Ethernet 1/2, and Ethernet 1/3 as hybrid interfaces and permit packets of VLAN 10, 20, and 30 to pass through in an untagged mode.

```
S3900-24T4S(config)#interface ethernet 1/1
S3900-24T4S(config-if)#switchport mode hybrid
S3900-24T4S(config-if)#switchport hybrid allowed vlan add 10 untagged
S3900-24T4S(config-if)#switchport hybrid allowed vlan add 20 untagged
S3900-24T4S(config-if)#switchport hybrid allowed vlan add 30 untagged
S3900-24T4S(config-if)#exit
S3900-24T4S(config)#int ethernet 1/2
S3900-24T4S(config-if)#switchport mode hybrid
S3900-24T4S(config-if)#switchport hybrid allowed vlan add 30 untagged
S3900-24T4S(config-if)#switchport hybrid allowed vlan add 20 untagged
S3900-24T4S(config-if)#switchport hybrid allowed vlan add 10 untagged
S3900-24T4S(config-if)#exit
S3900-24T4S(config)#int ethernet 1/3
S3900-24T4S(config-if)#switchport mode hybrid
S3900-24T4S(config-if)#switchport hybrid allowed vlan add 10 untagged
S3900-24T4S(config-if)#switchport hybrid allowed vlan add 20 untagged
S3900-24T4S(config-if)#switchport hybrid allowed vlan add 30 untagged
S3900-24T4S(config-if)#exit
```

(6) Check the VLAN interface on S3900-24T4S switch.

```
S3900-24T4S#show vlan all
VLAN ID : 1
Name : DefaultVlan
Type : Static
Members : Eth1/ 1(S) Eth1/ 2(S)Eth1/ 3(S) Eth1/ 4(S) Eth1/ 5(S)
Eth1/ 6(S) Eth1/ 7(S) Eth1/ 8(S) Eth1/ 9(S) Eth1/10(S)
Eth1/11(S)Eth1/12(S)Eth1/13(S) Eth1/14(S) Eth1/15(S)
Eth1/16(S) Eth1/17(S) Eth1/18(S) Eth1/19(S) Eth1/20(S)
```

```
Eth1/21(S) Eth1/22(S) Eth1/23(S) Eth1/24(S) Eth1/25(S)
Eth1/26(S) Eth1/27(S) Eth1/28(S) Eth1/29(S) Eth1/30(S)
Eth1/31(S) Eth1/32(S) Eth1/33(S) Eth1/34(S) Eth1/35(S)
Eth1/36(S) Eth1/37(S) Eth1/38(S) Eth1/39(S) Eth1/40(S)
Eth1/41(S) Eth1/42(S) Eth1/43(S) Eth1/44(S) Eth1/45(S)
Eth1/46(S) Eth1/47(S) Eth1/48(S) Eth1/49(S) Eth1/50(S)
Eth1/51(S) Eth1/52(S)
VLAN ID : 10
Name :
Type : Static
Members : Eth1/ 1(S) Eth1/ 2(S) Eth1/ 3(S)
VLAN ID : 20
Name :
Type : Static
Members : Eth1/ 1(S) Eth1/ 2(S) Eth1/ 3(S)
VLAN ID : 30
Name :
Type : Static
Members : Eth1/ 1(S) Eth1/ 2(S) Eth1/ 3(S)
```

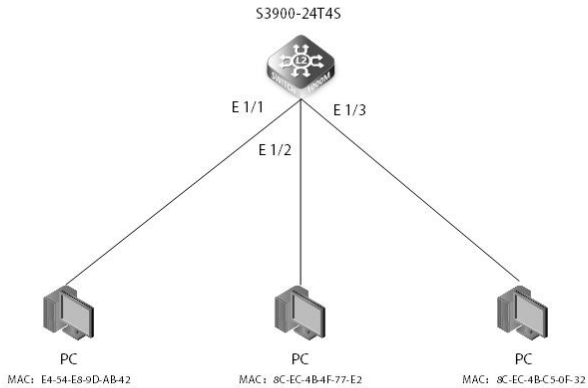
2.15 MAC-based VLAN

2.15.1 Introduction

MAC address-based VLAN is a method to allow incoming untagged packets to be assigned to a VLAN based on the source MAC address of the packet. Even if the users frequently change their physical locations, the network administration won't need to reconfigure VLANs which improves security and access flexibility on a network.

NOTE:
- When configuring the static MAC manually, you need to enter the right MAC address of the PC.
- If a MAC address is associated with the MAC VLAN, you can't use the MAC address to configure other MAC VLANs.
- In the access and trunk interface, only if the MAC address-based VLAN is the same as the PVID (Port VLAN ID) can the feature be applied normally. Therefore, MAC address-based VLAN must be configured in the hybrid interface.

2.15.2 Topology



2.15.3 Configuration

(1) Check the MAC addresses of the PC1/ PC2 (PC1: 64-9D-99-9D-AB-42; PC2: 64-9D-99-4F-77-E2).

(2) Create VLAN 10 on the S3900-24T4S switch 1 and set the IP address.

```
S3900-24T4S#configure terminal
S3900-24T4S(config)#vlan database
S3900-24T4S(config-vlan)#vlan 10
S3900-24T4S(config-vlan)#exit
S3900-24T4S(config)#int vlan 10
S3900-24T4S(config-if)#ip add 192.168.20.1/24
```

(3) Configure the eth1/1 of the S3900-24T4S switch 1 as hybrid port and remove the tags of VLAN 10.

```
S3900-24T4S(config)#int ethernet 1/1
S3900-24T4S(config-if)#switchport mode hybrid
S3900-24T4S(config-if)#switchport hybrid allowed vlan add 10 untagged
```

(4) Configure the MAC addresses of the PC1 and PC2 and associate them with VLAN 10 (support priority setting and generally the default VLAN is 0).

```
S3900-24T4S(config)# mac-vlan mac-address 64-9D-99-9D-AB-42 vlan 10
S3900-24T4S(config)# mac-vlan mac-address 64-9D-99-4F-77-E2 vlan 10
```

(5) Verify the configuration. Use ping commands to inquiry the IP address of VLAN 10 on the PC1.

```
C:UsersDell>ping 192.168.20.1
Pinging 192.168.20.1 with 32 bytes of data:
Reply from 192.168.20.1: bytes=32 time=11ms TTL=64
Reply from 192.168.20.1: bytes=32 time=2ms TTL=64
Reply from 192.168.20.1: bytes=32 time=2ms TTL=64
Reply from 192.168.20.1: bytes=32 time=2ms TTL=64

Ping statistics for 192.168.20.1:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 2ms, Maximum = 11ms, Average = 4ms
```

(6) Use ping commands to inquiry the IP address of VLAN 10 on the PC2.

```
C:UsersDell>ping 192.168.20.1
Pinging 192.168.20.1 with 32 bytes of data:
Reply from 192.168.20.1: bytes=32 time=11ms TTL=64
Reply from 192.168.20.1: bytes=32 time=2ms TTL=64
Reply from 192.168.20.1: bytes=32 time=2ms TTL=64
Reply from 192.168.20.1: bytes=32 time=2ms TTL=64

Ping statistics for 192.168.20.1:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 2ms, Maximum = 11ms, Average = 4ms
```

(7) Connect the PC2 with the S3900-24T4S switch 2 (the MAC address of the PC2 is not associated with VLAN 10) and use the ping commands to inquiry the IP address of VLAN 10 of S3900-24T4S switch 1.

```
C:UsersDell>ping 192.168.20.1
Pinging 192.168.20.1 with 32 bytes of data:
Request timed out
Request timed out
Request timed out
Request timed out

Ping statistics for 192.168.20.1:
Packets: Sent = 4, Received = 0, Lost = 4 (100% loss)
```

2.16 VLAN translation

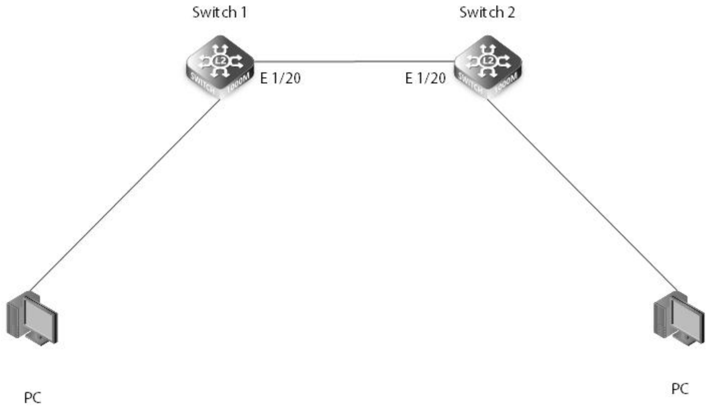
2.16.1 Introduction

Service providers' business customers often have specific VLAN ID requirements. The VLANs required by different customers of the same network service provider may overlap, and user traffic through the service provider equipment may also be mixed. By assigning different VLAN IDs to each customer to map its own VLAN ID, it is possible to separate the communication of customers of different applications.
With VLAN translation, service providers can use a range of VLANs to serve customers with their own VLAN ID. The customer VLAN ID is translated, and the traffic from customers of different applications is separated on the service provider's device, even when they appear in the same VLAN.

QinQ technology effectively expands the number of VLANs by stacking two 802.1Q headers in an Ethernet frame, making the number of VLANs up to 4096 × 4096. At the same time, multiple VLANs can be multiplexed into a core VLAN. ISPs usually establish a VLAN model for each customer, and use the General Attribute Registration Protocol / General VLAN Registration Protocol (GARP / GVRP) to automatically monitor the VLANs of the entire backbone network and extend the spanning tree protocol (STP) to speed up network convergence, thereby Provide resilience to the network. QinQ technology is good as an initial solution, but as the number of users increases, the SVLAN model also brings scalability issues. Because some users may wish to carry their own VLAN ID when transmitting data between branches, this makes MSPs using QinQ technology face the following two problems: First, the VLAN identification of the first customer may conflict with other customers; Second, service providers will be severely limited by the number of identifications available to customers. If users are allowed to use their own VLAN ID space in their own way, the core network still has a limit of 4096 VLANs.

2.16.2 Topology

Configure different VLANIFaddresses on the two switches, configure VLAN translation, and use a PC at both ends to perform a PING test to see if different VLANs can translate and communicate.



2.16.3 Configuration

Switch1 configuration

Switch 1 creates vlan 30 and 40, configures ip for vlan30, and allows all vlans on port e 1/20 to pass, and converts vlan40 to vlan30.

```
switch1#config t
switch1 (config)#vlan database
switch1 (config-vlan)#vlan 30,40
switch1 (config)#interface vlan 30
switch1 (config-if)#ip add 192.168.20.1 255.255.255.0
switch1 (config)#interface ethernet 1/20
switch1 (config-if)#switchport mode trunk
switch1 (config-if)#switchport trunk allowed vlan all
switch1 (config-if)#switchport vlan-translation 40 30
```

Switch 2 creates vlan 40, configures ip for vlan40, and allows port e 1/20 to allow vlan40 to pass

Switch2 configuration

```
switch2#config t
switch2(config)#vlan database
switch2 (config-vlan)#vlan 40
switch2 (config)#interface vlan 40
switch2 (config-if)#ip add 192.168.20.2 255.255.255.0
switch2 (config)#interface ethernet 1/20
switch2 (config-if)#switchport mode trunk
switch2 (config-if)#switchport trunk allowed vlan add 40
```

2.16.4 Verification

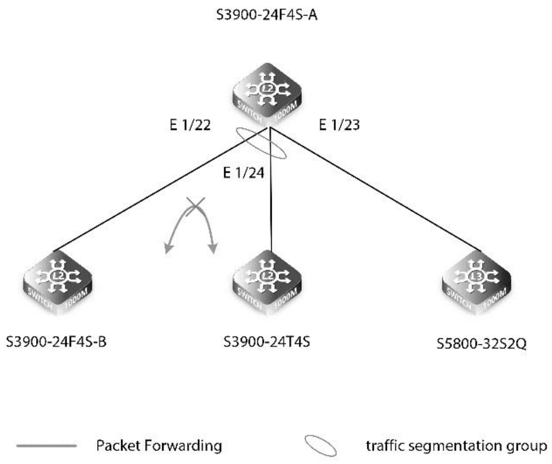
```
Switch1#show vlan-translation

Interface Old VID New VID
--------- ------- -------
Eth 1/20         40       30


Switch2#show vlan-translation

Interface Old VID New VID
--------- ------- -------
Eth 1/20         30       40
```

2.17 Traffic Segmentation

2.17.1 Introduction

Traffic segmentation, also known as port isolation or private VLAN, is a technique used to provide more secure and flexible networking solutions via isolating switch ports in the same VLAN of Layer 2. FS S3900 series switches, with abundant Layer 2 and Layer 2+ features, also support traffic segmentation.

2.17.2 topology



2.17.3 Configuration

(1) Configure vlan 2 and IP address for S3900-24F4S-A, and set its eth 1/22, eth 1/23, eth 1/24 port as trunk mode and allow vlan add 2.

```
S3900-24F4S-A#configure terminal
S3900-24F4S-A(config)#interface vlan 2
S3900-24F4S-A(config-if)#ip add 10.1.1.1/24
S3900-24F4S-A(config-if)#exit
S3900-24F4S-A(config)#interface ethernet 1/22
S3900-24F4S-A(config-if)#switchport mode trunk
S3900-24F4S-A(config-if)#switchport trunk allowed vlan add 2
S3900-24F4S-A(config-if)#exit
S3900-24F4S-A(config)#interface ethernet 1/23
S3900-24F4S-A(config-if)#switchport mode trunk
S3900-24F4S-A(config-if)#switchport trunk allowed vlan add 2
S3900-24F4S-A(config-if)#exit
S3900-24F4S-A(config)#interface ethernet 1/24
S3900-24F4S-A(config-if)#switchport mode trunk
S3900-24F4S-A(config-if)#switchport trunk allowed vlan add 2
S3900-24F4S-A(config-if)#exit
```

(2) Configure traffic segmentation for S3900-24F4S-A.

```
S3900-24F4S-A(config)#traffic-segmentation
S3900-24F4S-A(config)#traffic-segmentation downlink ethernet 1/22
S3900-24F4S-A(config)#traffic-segmentation downlink ethernet 1/23
S3900-24F4S-A(config)#traffic-segmentation uplink ethernet 1/24
```

(3) Verify the configuration. Check the status of traffic segmentation on S3900-24F4S-A and check whether the downlink ports are set successful.

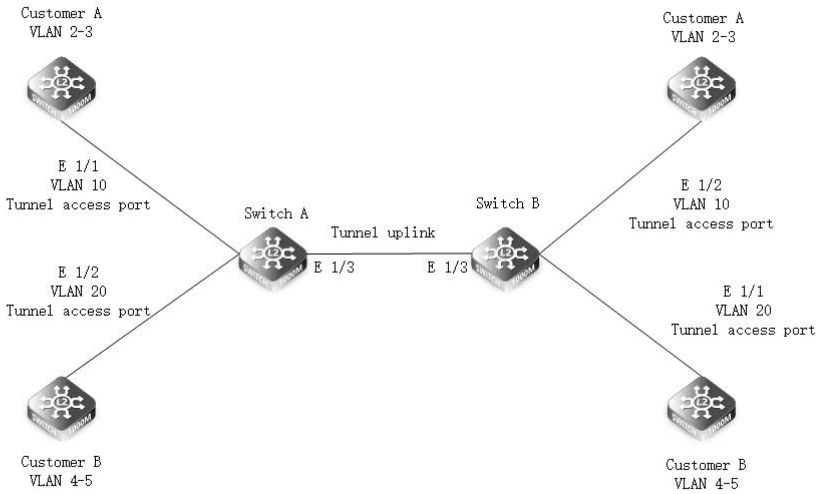
```
S3900-24F4S-A#show traffic-segmentation
Traffic Segmentation Status: Enabled
Traffic pass through uplink ports: No
Session                 Uplink Ports            Downlink Ports
----------------------------------------------------------------------------------------------------------------------------------------------------------------
1                       Ethernet 1/24           Ethernet 1/22 Ethernet 1/23
```

2.18 IEEE 802.1ad QinQ

2.18.1 Introduction

Using 802.1Q tunneling, the client's VLAN tag is encapsulated in the public VLAN tag and packets with two tags will traverse on backbone network. The client's VLAN tag will be shield and only the public VLAN tag will be used to transmit. By separating data stream, the 44 client's VLAN tag is transmitted transparently and different VLAN tags can be used repeatedly. Therefore, using 802.1Q tunneling expands the available VLAN tags.

2.18.2 topology



2.18.3 Configuration

SwitchA:

(1) Create vlan

```
SwitchA(config)#vlan database
SwitchA(config-vlan)#vlan 2-5,10,20
```

(2) Enable qinq function and develop access and uplink interfaces

```
SwitchA(config)#dot1q-tunnel system-tunnel-control
SwitchA(config)#interface ethernet 1/1
SwitchA(config-if)# switchport dot1q-tunnel mode access
SwitchA(config-if)#exit
SwitchA(config)#interface ethernet 1/2
SwitchA(config-if)# switchport dot1q-tunnel mode access
SwitchA(config-if)#exit
SwitchA(config)#interface ethernet 1/3
SwitchA(config-if)#switchport dot1q-tunnel mode uplink
SwitchA(config-if)#exit
```

(3) Configure CVLAN and SVLAN on the interface.

```
SwitchA(config)#interface ethernet 1/1
SwitchA(config-if)# switchport hybrid allowed vlan add 10 untagged
SwitchA(config-if)# switchport dot1q-tunnel service 10 match cvid 2
SwitchA(config-if)# switchport dot1q-tunnel service 10 match cvid 3
SwitchA(config-if)#exit
SwitchA(config)#interface ethernet 1/2
SwitchA(config-if)# switchport hybrid allowed vlan add 20 untagged
SwitchA(config-if)# switchport dot1q-tunnel service 20 match cvid 4
SwitchA(config-if)# switchport dot1q-tunnel service 20 match cvid 5
SwitchA(config-if)#exit
SwitchA(config)#interface ethernet 1/3
SwitchA(config-if)#switchport mode trunk
SwitchA(config-if)#switchport trunk allowed vlan add 10,20
```

(4) The configuration of SwitchB is the same as that of SwitchA. It is not repeated here.

Verify configuration

```
SwitchA#show dot1q-tunnel service
 Port        C-VID     S-VID
 -------- ------- -------
 Eth 1/ 1         2           10
 Eth 1/ 1         3           10
 Eth 1/ 2         4           20
 Eth 1/ 2         5           20
```

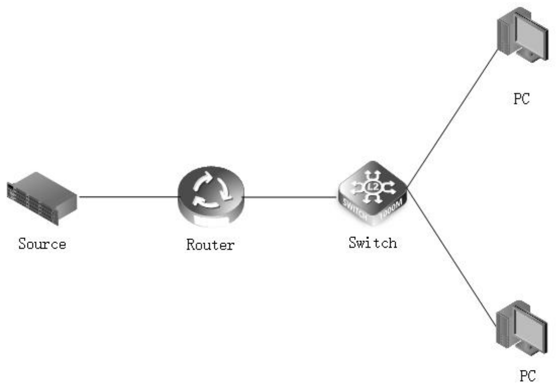
2.19 IGMP Snooping

2.19.1 Introduction

IGMP Snooping (Internet Group Management Protocol Snooping) is an IPv4 Layer 2 multicast protocol. It listens to the multicast protocol packets sent between the Layer 3 multicast device and the user host to maintain the outbound interface information of the multicast packets. In order to manage and control the forwarding of multicast data packets at the data link layer.

Purpose
In many cases, multicast packets inevitably pass through some Layer 2 switching equipment, especially in LAN environments. As shown in Figure 1, between the multicast user and the Layer 3 multicast device Router, multicast packets must pass through the Layer 2 switch Switch.

Figure 1 Networking diagram of IGMP Snooping

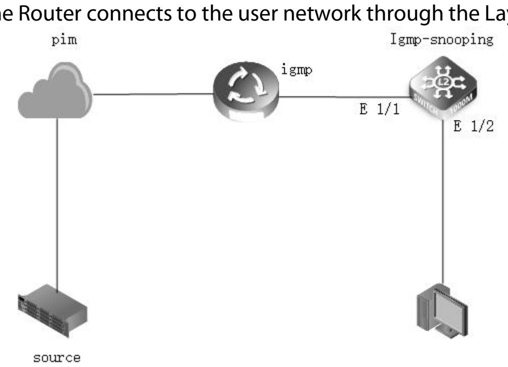


After the Router forwards the multicast packets to the Switch, the Switch forwards the multicast packets to the multicast users. Because the destination address of a multicast packet is a multicast group address, this type of MAC entry cannot be learned on a Layer 2 device. Therefore, the multicast packet will be broadcast on all interfaces and be in the same broadcast domain as it. Of multicast members and non-multicast members can receive multicast messages. This not only wastes network bandwidth, but also affects network information security.

IGMP Snooping effectively solves this problem. After IGMP Snooping is configured, a Layer 2 multicast device can listen and analyze IGMP messages between the multicast user and the upstream router. Based on this information, it can establish Layer 2 multicast forwarding entries to control the forwarding of multicast data packets. This prevents the broadcast of multicast data in the Layer 2 network.

2.19.2 Topology

In the multicast network shown below, the Router connects to the user network through the Layer 2 Switch.



(1) Create a VLAN on the Switch and add the interface to the VLAN.
(2) Enable global and VLAN IGMP Snooping.

2.19.3 Configuration

(1) Create a vlan and add the corresponding interfaces to the corresponding vlan.

```
Switch#configure terminal
Switch(config)#vlan database
Switch(config-vlan)#vlan 10
Switch(config-vlan)#exit
Switch(config)#interface ethernet 1/1
Switch(config-if)#switchport mode trunk
Switch(config-if)#switchport trunk allowed vlan add 10
Switch(config-if)#exit
Switch(config)#interface ethernet 1/2
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access vlan 10
Switch(config-if)#exit
```

(2) Enable IGMP Snooping

```
Switch(config)#ip igmp snooping          //Enable global IGMP Snooping
Switch(config)#ip igmp snooping vlan 10        // Enable IGMP Snooping in VLAN 10
```

(3) If no other switch is in the igmp-snooping network, it is recommended to enable the querier function.

```
Switch(config)#ip igmp snooping querier
```

2.19.4 Verification

```
Switch#show ip igmp snooping
  IGMP Snooping                          : Enabled
  Router Port Expire Time                : 300 s
  Router Alert Check                     : Disabled
  Router Port Mode                       : Forward
  TCN Flood                              : Disabled
  TCN Query Solicit                      : Disabled
  Unregistered Data Flood                : Disabled
  802.1p Forwarding Priority             : Disabled
  Unsolicited Report Interval            : 400 s
  Version Exclusive                      : Disabled
  Version                                : 2
  Proxy Reporting                        : Disabled
  Querier                                : Enabled

VLAN 10:
  --------
  IGMP Snooping                          : Enabled
  IGMP Snooping Running Status           : Active
  Version                                : Using global Version (2)
  Version Exclusive                      : Using global status (Disabled)
  Immediate Leave                        : Disabled
  Last Member Query Interval             : 10 (unit: 1/10s)
  Last Member Query Count                : 2
  General Query Suppression              : Disabled
  Query Interval                         : 125
  Query Response Interval                : 100 (unit: 1/10s)
  Proxy Query Address                    : 0.0.0.0
  Proxy Reporting                        : Using global status (Disabled)
  Multicast Router Discovery             : Disabled
```

2.20 Broadcast/Multicast/ Unknown Unicast Storm Control

2.20.1 Introduction

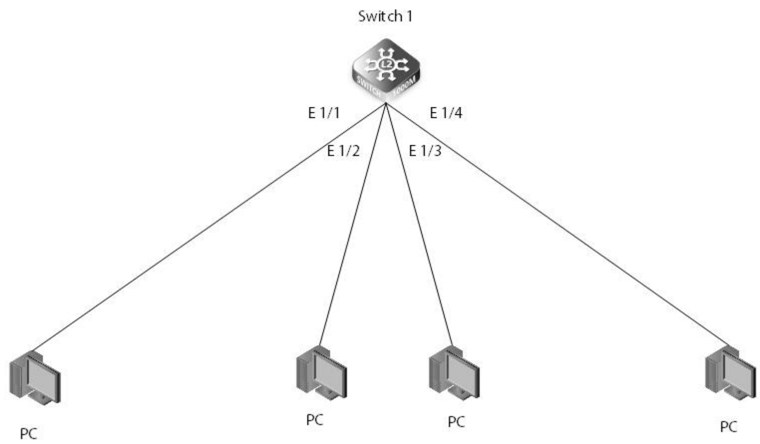
When the traffic exceeds the threshold specified by broadcast or multicast or unknown unicast traffic, packets exceeding this threshold will be dropped until the rate drops below the threshold. Using both rate limiting and storm control on the same interface may cause unexpected results. For example, suppose the broadcast storm control is set to 500 Kbps by the command "switchport broadcast packet-rate 500" on the Fast Ethernet port, and the rate limit is set to 20000 Kbps by the command "rate-limit input 20000". 20000 Kbps is 1/5 of the line speed (100 Mbps), the receiving rate is actually 100 Kbps, or 1/5 of the 500 Kbps limit set by the storm control command, so it is not recommended to use these two commands at the same time on the same interface.

Parameter Description:

Parameter	Parameter Description	Value
broadcast	Configures broadcast storm control	500-14880000
multicast	Configures multicast storm control	500-14880000
unicast	Configures unicast storm control	500-14880000

2.20.2 Topology

After configuring Storm Control, send broadcast, multicast, and unicast packets through a PC like a switch, and see if port traffic is restricted.



2.20.3 Configuration

Switch Configuration

Set the eth1/2 interface to drop broadcast packets that exceed 600 packets per second.

```
switch(config)#interface ethernet 1/2
switch(config-if)#switchport broadcast packet-rate 600
```

2.20.4 Verification

```
Switch#show interfaces counters ethernet 1/1
Ethernet 1/ 1

     Item                                                  Counters
---------------------------------------                  --------------------
Octets Input                                              193267
Octets Output                                             108450
Unicast Input Pkts                                        856
Unicast Output Pkts                                       538
Multi-cast Input Pkts                                     1079
Multi-cast Output Pkts                                    665
Broadcast Input Pkts                                      208
Broadcast Output Pkts                                     78
Discard Input Pkts                                        248
Discard Output Pkts                                       39
Alignment Errors                                          0
FCS Errors                                                0
Single Collision Frames                                   0
Multiple Collision Frames                                 0
Deferred Transmissions                                    0
Late Collisions                                           0
Excessive Collisions                                      0
Internal Mac Transmit Errors                              0
```

```
Internal Mac Receive Errors                    0
Frames Too Long                                 0
Carrier Sense Errors                            0
Symbol Errors                                    0
Pause Frames Input                              0
Pause Frames Output                            0
```

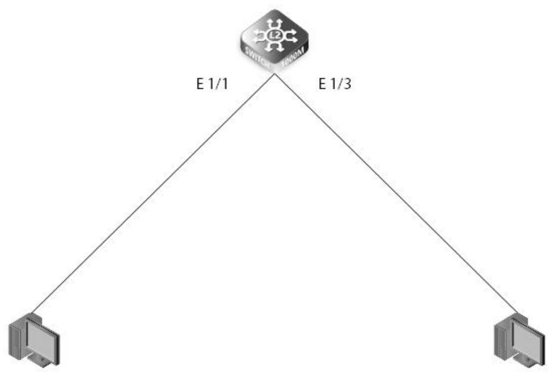
2.21 Jumbo frames

2.21.1 Introduction

Jumbo frames are Ethernet frames with a frame length greater than 1522 bytes. This is a vendor-standard extra-long frame format designed for Gigabit Ethernet. The use of jumbo frames can make full use of Gigabit Ethernet performance and improve data transmission efficiency by 50% to 100%. In the network storage application environment, jumbo frames have more extraordinary significance.

2.21.2 Topology

After the network card of PC and switch port both open the huge frame, use the PC to send 9200-byte frames to the switch to see if the switch can receive.



2.21.3 Configuration

Switch configuration

Enable jumbo frames globally and set the mtu value to 9216 on interface e 1/2

```
Switch(config)#jumbo frame
Switch(config)#interface ethernet 1/2
Switch(config-if)#switchport mtu 9216
```

2.21.4 Verification

```
Switch#show interfaces status ethernet 1/2
 Port Type                 : 1000BASE-T
 Link Status               : Down
 Speed-duplex Status       : 1000full
 Max Frame Size            : 9216 bytes (9220 bytes for tagged frames)
 MAC Learning Status       : Enabled
```

2.22 Port mirroring

2.22.1 Introduction

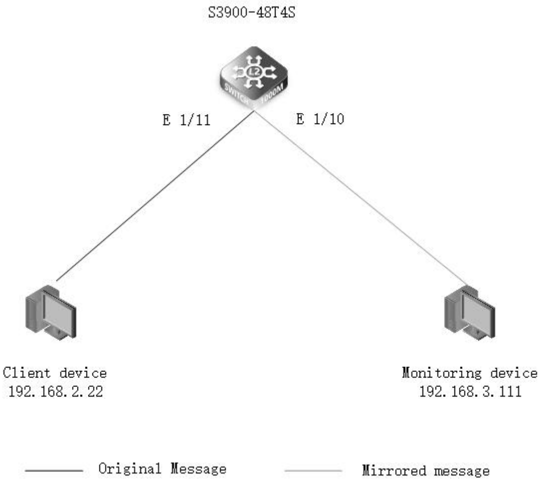
Port mirroring is used on a network switch or router to send copies of packets on the specified ports (source ports) to other specified ports (destination ports). FS S3900 series switches are the ideal Gigabit access and aggregation switches for SMB, enterprise and campus networks. They support port mirroring to help users monitor and analyze network traffic, and debug data or diagnose errors on a network.

2.22.2 Topology

Port mirroring includes local port mirroring and remote port mirroring based on the working range of mirroring.

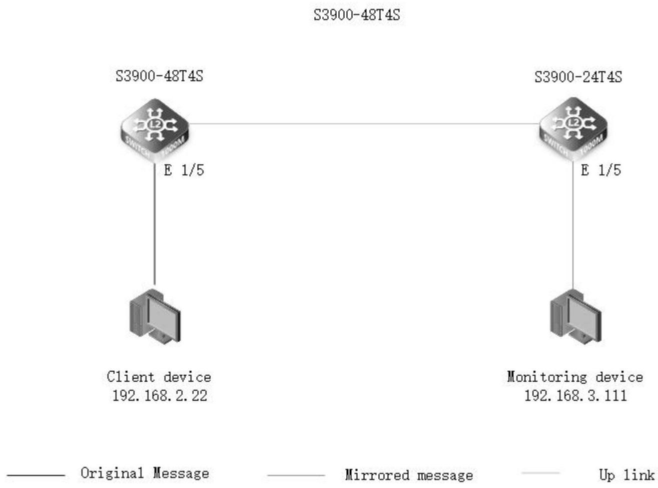
(1) Local Port Mirroring Application

Choose local mirroring mode when source ports and destination ports are on one S3900 switch. Take S3900-48T4S port mirroring application as an example. Once port mirroring is set, the source port (11) will copy the packet to the destination port (10), then users can use the monitoring device to monitor and analyze data from the client device.



(2) Remote Port Mirroring Application

In remote mirroring, source ports and destination ports do not belong to one S3900 switch. Destination port on one switch can monitor the source port on another switch via the connection between the two different switches. Take remote port mirroring application of S3900-48T4S and S3900-24T4S as an example. Set S3900-48T4S port (5) as the source port, and set S3900-24T4S port (5) as the destination port. And make an uplink connection between the two switches via the ports (10) on two sides. Thus, users can use the monitoring device connected to S3900-24T4S to monitor and analyze the data from the client device connected to S3900-48T4S switch.



2.22.3 Configuration

S3900 Series Switches Local Port Mirroring Configuration via CLI

(1) Create VLAN 10 on S3900-48T4S. Set the port (10) mode as Access and add the port to VLAN 10.

```
S3900-48T4S#configure terminal
S3900-48T4S(config)#vlan database
S3900-48T4S(config-vlan)#vlan 10
S3900-48T4S(config)#interface ethernet 1/10
S3900-48T4S(config-if)#switchport mode access
S3900-48T4S(config-if)#switchport access vlan 10
```

(2) Create VLAN 11. Set the port (11) mode as Access and add the port to the VLAN 11.

```
S3900-48T4S(config)#vlan database
S3900-48T4S(config-vlan)#vlan 11
S3900-48T4S(config)#interface ethernet 1/11
S3900-48T4S(config-if)#switchport mode access
S3900-48T4S(config-if)#switchport access vlan 11
```

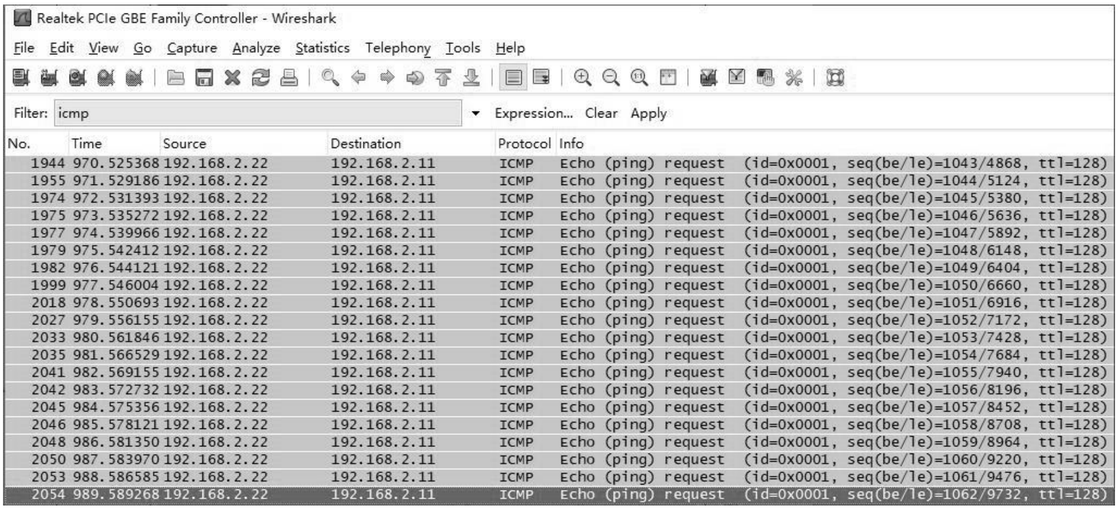
(3) Configure IP address of VLAN 10 and VLAN 11.

```
S3900-48T4S(config)#interface vlan 10
S3900-48T4S(config-if)#ip add 192.168.3.11 255.255.255.0
S3900-48T4S(config)#interface vlan 11
S3900-48T4S(config-if)#ip add 192.168.2.11 255.255.255.0
```

(4) Configure port mirroring on the destination port (10).

```
S3900-48T4S(config)#interface ethernet 1/10
S3900-48T4S(config-if)#port monitor ethernet 1/11 both
```

(5) Verify the results by the software of capturing packet Wireshark. Users can use the destination port (10) to capture the packet from the source port (11). This means port mirroring is successfully configured.



S3900 Series Switches Remote Port Mirroring Configuration via CLI

(1) Set S3900-48T4S port (5) as the source port.

```
S3900-48T4S#configure terminal
S3900-48T4S(config)#vlan database
S3900-48T4S(config-vlan)#vlan 200 media ethernet rspan
S3900-48T4S(config-vlan)#exit
S3900-48T4S(config)#rspan session 1 source interface e 1/5
```

(2) Configure S3900-48T4S port (10) as the uplink port.

```
S3900-48T4S(config)#rspan session 1 remote vlan 200 source uplink e 1/10
```

(3) Set S3900-24T4S port (5) as the destination port.

```
S3900-24T4S#configure terminal
S3900-24T4S(config)#vlan database
S3900-24T4S(config-vlan)#vlan 200 media ethernet rspan
S3900-48T4S(config-vlan)#exit
S3900-24T4S(config)#rspan session 1 destination interface e 1/5
```

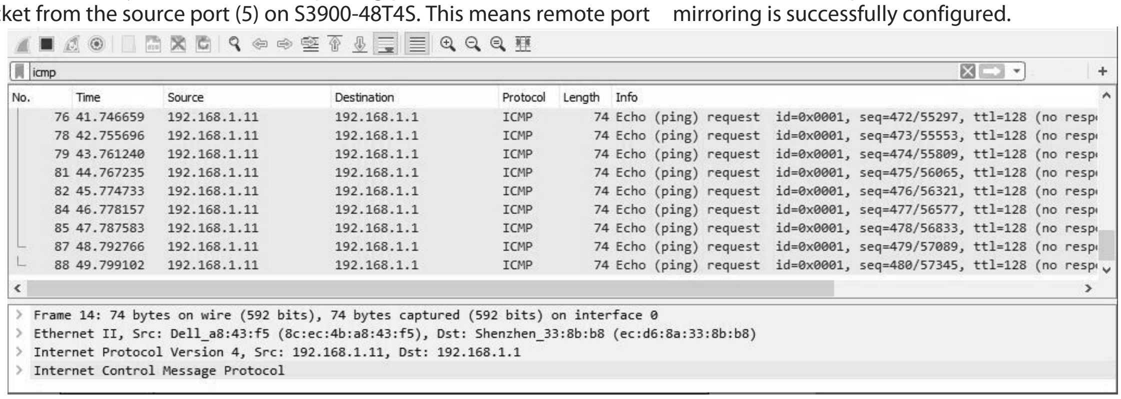
(4) Configure S3900-24T4S port (10) as the uplink port.

```
S3900-24T4S(config)#rspan session 1 remote vlan 200 destination uplink e 1/10
```

(5) View the configuration

```
S3900-48T4S#show rspan session
RSPAN Session ID : 1
Source Ports (mirrored ports)
RX Only : None
TX Only : None
BOTH : Eth 1/5
Destination Port (monitor port) : None
Destination Tagged Mode : None
Switch Role : Source
RSPAN VLAN : 200
RSPAN Uplink Ports : Eth 1/10
Operation Status : Up
```

(6) Verify the results by the software of capturing packet Wireshark. Users can use the destination port (5) on S3900-24T4S to capture the ICMP packet from the source port (5) on S3900-48T4S. This means remote port mirroring is successfully configured.

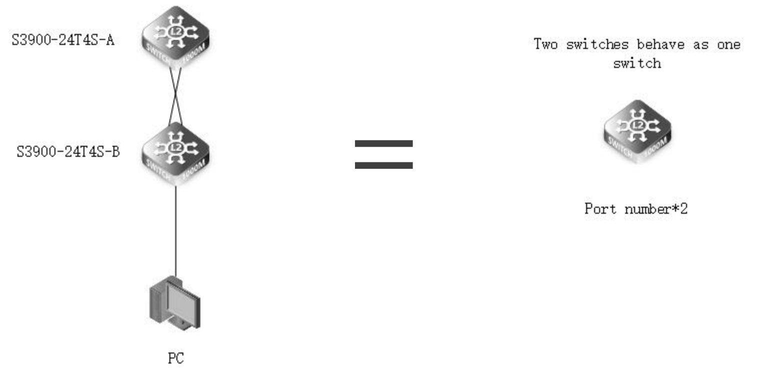


2.23 Stacking Links

2.23.1 Introduction

Switch stacking technology is a network solution that enables network switches to be connected together as a single unit with the same IP address. Set up as a single entity, stackable switches have not only optimized scalability and flexibility but also simplified network configuration and administration. FS S3900 series stackable switches, which are designed for the campus network, SMB, and home network, have the ability to stack as well.

2.23.2 Topology



2.23.3 Configuration

(1) Turn on the stacking function of two S3900-24T4S switches.

```
S3900-24T4S-A(config)#stacking enable 1
S3900-24T4S-B(config)#stacking enable 1
```

(2) Save configuration and then restart the two switches.

```
S3900-24T4S-A#copy running-config startup-config
S3900-24T4S-A#restart
S3900-24T4S-B#copy running-config startup-config
S3900-24T4S-B#restart
```

(3) Check the status of the master switch. S3900-24T4S-A is the master switch and S3900-24T4S-B is the slave switch. Users cannot log in to the slave switch when the master switch is in management.

```
Switch#show stacking status
Switch ID         Config Status          Active Status
------------------------------------------------------------------------------------------------------------------------------------------------------------
1                        Y                  Y
2                        Y                  Y
```

(4) Check the interface information, the switch will show all the interface, the four ports for stacking will not show in the port list.

```
Switch#show interfaces brief
Interface Type
Admin Link-Status Negotiation Speed/Duplex Group
------------------------------------------------------------------------------------------------------------------------------------------------------------
Eth 1/1 1000BASE-T     Up    Down       Auto        None
Eth 1/ 2 1000BASE-T    Up    Down       Auto        None
Eth 1/ 3 1000BASE-T    Up    Down       Auto        None
Eth 1/ 4 1000BASE-T    Up    Down       Auto        None
Eth 1/ 5 1000BASE-T    Up    Down       Auto        None
Eth 1/ 6 1000BASE-T    Up    Down       Auto        None
Eth 1/ 7 1000BASE-T    Up    Down       Auto        None
Eth 1/ 8 1000BASE-T    Up    Down       Auto        None
Eth 1/ 9 1000BASE-T    Up    Down       Auto        None
Eth 1/10 1000BASE-T    Up    Down       Auto        None
Eth 1/11 1000BASE-T    Up    Down       Auto        None
Eth 1/12 1000BASE-T    Up    Down       Auto        None
Eth 1/13 1000BASE-T    Up    Down       Auto        None
Eth 1/14 1000BASE-T    Up    Down       Auto        None
Eth 1/15 1000BASE-T    Up    Down       Auto        None
Eth 1/16 1000BASE-T    Up    Down       Auto        None
Eth 1/17 1000BASE-T    Up    Down       Auto        None
Eth 1/18 1000BASE-T    Up    Down       Auto        None
Eth 1/19 1000BASE-T    Up    Down       Auto        None
Eth 1/20 1000BASE-T    Up    Down       Auto        None
Eth 1/21 1000BASE-T    Up    Down       Auto        None
Eth 1/22 1000BASE-T    Up    Down       Auto        None
Eth 1/23 1000BASE-T    Up    Down       Auto        None
Eth 1/24 1000BASE-T    Up    Down       Auto        None
Eth 1/25 10GBASE SFP+Up    Down       Disable     10Gfull     None
Eth 1/26 10GBASE SFP+Up    Down       Disable     10Gfull     None
Eth 2/1 1000BASE-T     Up    Down       Auto        None
Eth 2/ 2 1000BASE-T    Up    Down       Auto        None
Eth 2/ 3 1000BASE-T    Up    Down       Auto        None
Eth 2/ 4 1000BASE-T    Up    Down       Auto        None
Eth 2/ 5 1000BASE-T    Up    Down       Auto        None
Eth 2/ 6 1000BASE-T    Up    Down       Auto        None
Eth 2/ 7 1000BASE-T    Up    Down       Auto        None
Eth 2/ 8 1000BASE-T    Up    Down       Auto        None
Eth 2/ 9 1000BASE-T    Up    Down       Auto        None
Eth 2/10 1000BASE-T    Up    Down       Auto        None
Eth 2/11 1000BASE-T    Up    Down       Auto        None
Eth 2/12 1000BASE-T    Up    Down       Auto        None
Eth 2/13 1000BASE-T    Up    Down       Auto        None
Eth 2/14 1000BASE-T    Up    Down       Auto        None
Eth 2/15 1000BASE-T    Up    Down       Auto        None
Eth 2/16 1000BASE-T    Up    Down       Auto        None
Eth 2/17 1000BASE-T    Up    Down       Auto        None
Eth 2/18 1000BASE-T    Up    Down       Auto        None
Eth 2/19 1000BASE-T    Up    Down       Auto        None
Eth 2/20 1000BASE-T    Up    Down       Auto        None
Eth 2/21 1000BASE-T    Up    Down       Auto        None
Eth 2/22 1000BASE-T    Up    Down       Auto        None
Eth 2/23 1000BASE-T    Up    Down       Auto        None
Eth 2/24 1000BASE-T    Up    Down       Auto        None
Eth 2/25 10GBASE SFP+Up    Down       Disable     10Gfull     None
Eth 2/26 10GBASE SFP+Up    Down       Disable     10Gfull     None
```

(5) Configure the eth1/21 port and eth 2/21 port as access on the master switch and allow VLAN 10 pass.

```
Switch(config)#interface ethernet 1/21
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access vlan 10
Switch(config)#interface ethernet 2/21
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access vlan 10
```

(6) Configure IP address 10.100.10.4 and mask 255.255.255.0 for the PC.

(7) Connect PC with the eth1/21 of master, and ping VLAN 10 IP address on PC.

```
C:Userss>ping 10.10.10.3
Pinging 10.10.10.3 with 32 bytes of data:
Reply from 10.10.10.3: bytes=32 time=4ms TTL=249
Reply from 10.10.10.3: bytes=32 time=56ms TTL=249
Reply from 10.10.10.3: bytes=32 time=6ms TTL=249
Reply from 10.10.10.3: bytes=32 time=14ms TTL=249
Ping statistics for 10.10.10.3:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 4ms, Maximum = 56ms, Average = 20ms
```

(8) Connect PC with eth2/21 of master, ping VLAN 10 IP address on PC.

```
C:Userss>ping 10.10.10.3
Pinging 10.10.10.3 with 32 bytes of data:
Reply from 10.10.10.3: bytes=32 time=13ms TTL=249
Reply from 10.10.10.3: bytes=32 time=3ms TTL=249
Reply from 10.10.10.3: bytes=32 time=4ms TTL=249
Reply from 10.10.10.3: bytes=32 time=10ms TTL=249
Ping statistics for 10.10.10.3:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 3ms, Maximum = 13ms, Average = 7ms
```

(9) PC can successfully ping master switch and slave switch, suggesting switch stacking is accomplished.

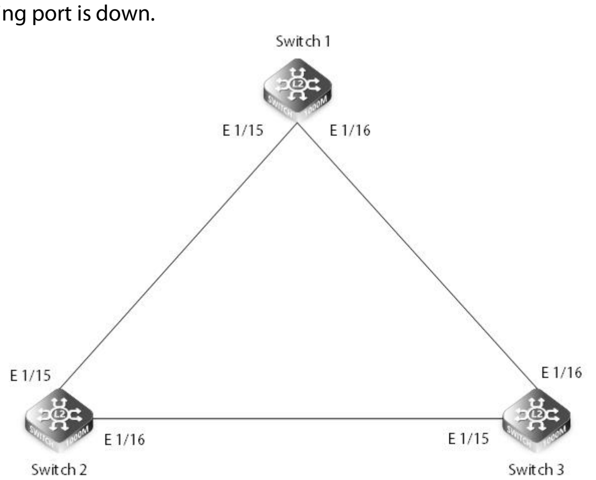
2.24 Non-Spanning Tree Loopback detection

2.24.1 Introduction

During the network deployment process, the TX-RX interface (TX indicates the optical fiber transmitting end, RX indicates the optical fiber receiving end) self-loop problems. For example, the wrong insertion of the optical fiber, and the interface is damaged by high voltage may cause the TX- RX self-loop .

2.24.2 Topology

After“ configuring Non-Spanning Tree Loopback detection”, use three switches to form a loop, and use one of them to send broadcast packets, and check whether the sending port is down.



2.24.3 Configuration

Switch configuration

```
Switch#config t
Switch(config)#loopback-detection            //Enable global loop detection
Switch(config-if)#interface ethernet 1/15
Switch(config-if)# #no spanning-tree loopback-detection
Switch(config-if)#loopback-detection          //Enable loop detection on the interface
```

2.24.4 Verification

```
Switch#show loopback-detection
Loopback Detection Global Information
  Global Status         : Enabled
  Transmit Interval : 10
  Recover Time          : 60
  Action                : Shutdown
  Trap                  : None
Loopback Detection Port Information
  Port        Admin State    Oper State
  --------    -----------    ----------
  Eth 1/ 1    Disabled       Normal
  Eth 1/ 2    Disabled       Normal
  Eth 1/ 3    Disabled       Normal
  Eth 1/ 4    Disabled       Normal
  Eth 1/ 5    Disabled       Normal
  Eth 1/ 6    Disabled       Normal
  Eth 1/ 7    Disabled       Normal
  Eth 1/ 8    Disabled       Normal
  Eth 1/ 9    Disabled       Normal
  Eth 1/10    Disabled       Normal
  Eth 1/11    Disabled       Normal
  Eth 1/12    Disabled       Normal
  Eth 1/13    Disabled       Normal
  Eth 1/14    Disabled       Normal
  Eth 1/15    Enabled        Looped
  Eth 1/16    Enabled        Normal
  Eth 1/17    Disabled       Normal
  Eth 1/18    Disabled       Normal
  Eth 1/19    Disabled       Normal
  Eth 1/20    Disabled       Normal
  Eth 1/21    Disabled       Normal
  Eth 1/22    Disabled       Normal
  Eth 1/23    Disabled       Normal
  Eth 1/24    Disabled       Normal
  Eth 1/25    Disabled       Normal
  Eth 1/26    Disabled       Normal
  Eth 1/27    Disabled       Normal
  Eth 1/28    Disabled       Normal
```

2.25 Port security

2.25.1 Introduction

When using port security, the switch will stop learning the ports specified when the new MAC address reaches the configured maximum number. Only in the dynamic or static address table already stored on that port is the source address authorized to do the following on incoming traffic: access the network.

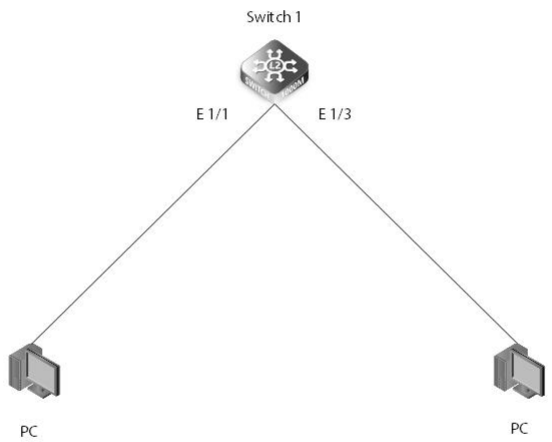
The port will discard any incoming frames that are unknown or previously exist in the source MAC address, learned from another port. If a device with an unauthorized MAC address attempts to use a switch port, an intrusion will be detected and the switch can automatically take action by disabling the port and sending a trap message.

Parameter Description：

Parameter	Parameter Description	Value Range
action	Responses to take action when port security is violated	/
max-mac-count	Sets port maximum MAC address count	0-1024
shutdown	Disables port only	/
trap	Issues SNMP trap message only	/
trap-and-shutdown	Issues SNMP trap message and disables port	/

2.25.2 Topology

Turn on port security on the port of the switch, then switch to a PC on the port and use PC to send messages to see if the switch will bring down the port.



2.25.3 Configuration

Switch1 configuration

Port protection is enabled on the port. Frames set to the source MAC will be dropped

```
switch(config)#interface ethernet 1/5
switch (config-if)#port security
switch (config-if)#port security action trap
```

2.25.4 Verification

```
switch#show port security interface ethernet 1/1
Global Port Security Parameters
  Secure MAC Aging Mode : Enabled

Port Security Details
  Port                               : 1/1
  Port Security                      : Enabled
  Port Status                        : Secure/Up
  Intrusion Action                   : Trap
  Max MAC Count                      : 0
  Current MAC Count                  : 0
  MAC Filter                         : Disabled
  Last Intrusion MAC                 : NA
  Last Time Detected Intrusion MAC   : NA
```

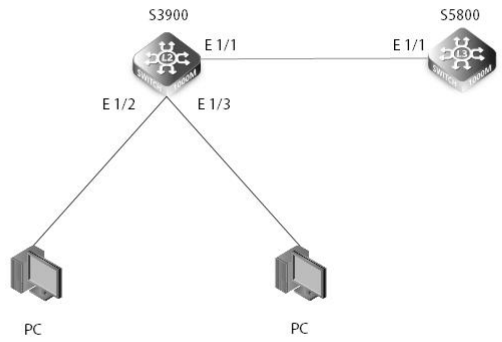
2.26 IP Source Guard

2.26.1 Introduction

IP source protection is mainly to prevent IP address spoofing, according to the IP source binding table IP. Source protection automatically loads the corresponding policies on the port to detect the traffic. The data that meets the requirements is allowed to be sent, and the data that does not comply are discarded.

2.26.2 Topology

After IP Source Guard is configured, PC1 is a legitimate visitor, and PC2 is an illegal counterfeit. PC2 uses the IP of PC1 to access the data on S5800. Check whether S39 will discard the data on PC2.



2.26.3 Configuration

Switch1 configuration

Create VLAN 6 on the S3900 and configure the interface type to allow VLAN 6. Configure the interface to enable IPSG on the S3900, detect IP and MAC, and configure IPSG bindings on the S3900.

```
S3900#configure terminal
S3900(config)#vlan database
S3900(config-vlan)#vlan 6
S3900(config)#int eth 1/1
S3900(config-if)#switchport mode access
S3900(config-if)#switchport access vlan 6
S3900(config-if)#int eth 1/2
S3900(config-if)#switchport mode access
S3900(config-if)#switchport access vlan 6
S3900(config-if)#int eth 1/3
S3900(config-if)#switchport mode access
S3900(config-if)#switchport access vlan 6
S3900(config-if)#int eth 1/2
S3900(config-if)#ip source-guard sip-mac
S3900(config-if)#int eth 1/3
S3900(config-if)#ip source-guard sip-mac
S3900(config)#ip source-guard binding mode mac 8c-ec-4b-ab-d2-57 vlan 6 10.0.0.10 interface ethernet 1/3
```

2.26.4 Verification

```
switch#show ip source-guard binding static
MAC Address         IP Address        Type              VLAN        Interface
----------------- --------------- -------------- --------- ---------
64-9D-99-ab-d2-57 10.0.0.10          static-mac                  6 Eth 1/3
```

2.27 Dynamic Arp Inspection

2.27.1 Introduction

Dynamic ARP detection DAI, using the binding table to prevent man-in-the-middle attacks. When the device receives an ARP packet, it compares the source IP, source MAC, VLAN, interface information, and binding table information corresponding to the ARP packet. If the information matches, it indicates that the user sending the ARP packet is a legitimate user and allows the user's ARP packet to pass, otherwise it is considered an attack and the ARP packet is discarded.

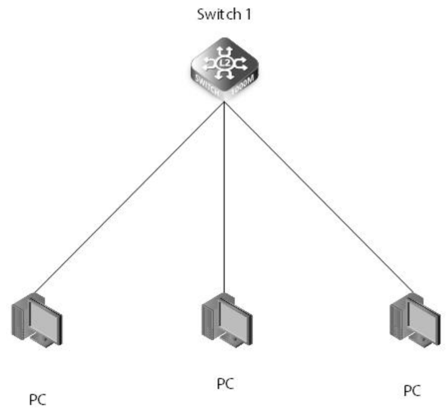
Parameter Description：

Parameter	Parameter Description	Value Range
filter	Applies the ARP ACL rule in specified VLAN(s)	Applies the ARP ACL rule in specified VLAN(s)
log-buffer	Log buffer for saving logs	Log buffer for saving logs
validate	Enable (disable) additional validation	Enable or disables
vlan	Enables (disables) ARP Inspection on VLANs	Enables or disables

2.27.2 Topology

After Dynamic Arp Inspection is configured, when an attacker sends an ARP packet, check whether S39 discards the ARP packet.

2.27.3 Configuration



Enable ARP Inspection

```
switch(config)#ip arp inspection
```

Enable source IP, source mac, vlan verification

```
Switch(config)#ip arp inspection validate ip
Switch(config)#ip arp inspection validate ip src-mac
Switch(config)#ip arp inspection validate src-mac
Switch(config)#ip arp inspection vlan 1
```

2.27.4 Verification

```
Switch#show ip arp inspection configuration
ARP Inspection Global Information:
Global IP DAI Status : disabled
Log Message Interval                    : 10 s
Log Message Number                      : 20
Need Additional Validation(s)       : Yes
Additional Validation Type           : Source MAC address
                                              IP address

Switch#show ip arp inspection vlan

VLAN ID         DAI Status                        ACL Name                        ACL Status
--------      ---------------        --------------------        --------------------
1                   enabled
```

2.28 ERPS

2.28.1 Introduction

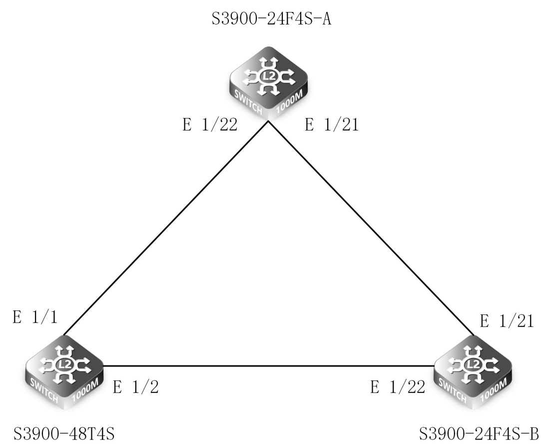
At present, the time required for fault switching in Layer 2 Ethernet is getting higher and higher. The spanning tree protocol cannot meet the convergence performance requirements of the link. ERPS is a standard loop-breaking protocol released by ITU-T. It blocks the specified ports to eliminate loops, and the convergence speed can meet carrier-class reliability requirements. Manufacturers in the network support this protocol, so they can communicate with each other.

Parameter Description:

Parameter	Parameter Description	Value Range
control-vlan	Configures control VLAN	1-4094
enable	Enables ERPS domain	/
guard-timer	Configures guard timer	10-2000
holdoff-timer	Configures hold-off timer	0-10000
major-domain	Configures ERPS major domain	/
node-id	Configures node ID	/
version	Configures ERPS protocol compatible version	1-2
wtr-timer	Configures wait-to-restore timer	5-12

2.28.2 Topology

Use three S3900 switch to form a loop, and configure ERPS, check the ERPS status, whether there are blocked ports, and whether the loop is eliminated.



2.28.3 Configuration

S3900-24F4S-A Configuration

(1) Create VLAN 2 for message transmission

```
S3900-24F4S-A-1(config)#vlan database
S3900-24F4S-A-1(config-vlan)#vlan 2
```

(2) Configure eth2 / 21-22 port to trunk mode and disable spanning tree.

```
S3900-24F4S-A-1(config)#interface ethernet 2/21
S3900-24F4S-A-1(config-if)#switchport mode trunk
S3900-24F4S-A-1(config-if)#switchport allowed vlan add 1-2 tagged
S3900-24F4S-A-1(config-if)#spanning-tree spanning-disabled
```

```
S3900-24F4S-A-1(config-if)#ex
S3900-24F4S-A-1(config)#int ethernet 2/22
S3900-24F4S-A-1(config-if)#switchport mode trunk
S3900-24F4S-A-1(config-if)#switchport allowed vlan add 1-2 tagged
S3900-24F4S-A-1(config-if)#spanning-tree spanning-disabled
```

(3) Create ERPS and enable control VLAN 2

```
S3900-24F4S-A-1(config)#erps
S3900-24F4S-A-1(config)#erps domain 1 id 1
S3900-24F4S-A-1(config-erps)#control-vlan 2
```

(4) Set the east-west port of the switch and enable ERPS

```
S3900-24F4S-A-1(config-erps)#ring-port west interface ethernet 2/22
S3900-24F4S-A-1(config-erps)#ring-port east interface ethernet 2/21
S3900-24F4S-A-1(config-erps)#enable
```

S3900-24F4S-B Configuration

(1) Configure port eth1 / 21-22 as trunk on the switch, allow VLAN 2 to pass, and disable spanning tree on the port.

```
S3900-24F4S-B(config)#int ethernet 1/21
S3900-24F4S-B(config-if)#switchport mode trunk
S3900-24F4S-B(config-if)#switchport allowed vlan add 1-2 tagged
S3900-24F4S-B(config-if)#spanning-tree spanning-disabled
S3900-24F4S-B(config-if)#ex
S3900-24F4S-B(config)#int ethernet 1/22
S3900-24F4S-B(config-if)#switchport mode trunk
S3900-24F4S-B(config-if)#switchport allowed vlan add 1-2 tagged
S3900-24F4S-B(config-if)#spanning-tree spanning-disabled
```

(2) Create VLAN 2

```
S3900-24F4S-B(config)#vlan database
S3900-24F4S-B(config-vlan)#vlan 2
```

(3) Enable ERPS, set the east-west interface, and configure the switch as the rpl owner

```
S3900-24F4S-B(config)#erps
S3900-24F4S-B(config)#erps domain 1 id 1
S3900-24F4S-B(config-erps)#control-vlan 2
S3900-24F4S-B(config-erps)#ring-port west interface ethernet 1/22
S3900-24F4S-B(config-erps)#ring-port east interface ethernet 1/21
S3900-24F4S-B(config-erps)#rpl owner
S3900-24F4S-B(config-erps)#enable
```

S3900-48T4S Configuration

(1) Configure port eth1 / 1-2 in trunk mode and disable spanning tree

```
S3900-48T4S(config)#int ethernet 1/1
S3900-48T4S(config-if)#switchport mode trunk
S3900-48T4S(config-if)#switchport allowed vlan all tagged
S3900-48T4S(config-if)#spanning-tree spanning-disabled
S3900-48T4S(config-if)#ex
S3900-48T4S(config)#int ethernet 1/2
S3900-48T4S(config-if)#switchport mode trunk
S3900-48T4S(config-if)#switchport allowed vlan all tagged
S3900-48T4S(config-if)#spanning-tree spanning-disabled
```

(2) Create VLAN 2

```
S3900-48T4S(config)#vlan database
S3900-48T4S(config-vlan)#vlan 2
```

(3) Create ERPS and create east-west interface

```
S3900-48T4S(config)#erps
S3900-48T4S(config)#erps domain 1 id 1
S3900-48T4S(config-erps)#control-vlan 2
S3900-48T4S(config-erps)#ring-port west interface ethernet 1/1
S3900-48T4S(config-erps)#ring-port east interface ethernet 1/2
S3900-48T4S(config-erps)#enable
```

2.28.4 Verification

```
S3900-24F4S-A#show erps
ERPS status : Enabled
Number of ERPS Domains : 1
Domain    ID    Enabled    ver    MEL Ctrl VLAN state          Type      Revertive
---------------------------------------------------------------------------------------------------------------------------------------------------------
1          1    Yes        2       1       2    Pending          None        Yes
      W/E       Interface Port state    Local SF Local        FS Local MS MEP   RPL
      west      Eth 2/22 Blocking NO    NO     NO        NO
      East      Eth 2/21 Forwarding     NO     NO    NO        NO
S3900-24F4S-A#
S3900-24F4S-B#show erps
ERPS Status        :Enabled
Number of ERPS Domains : 1
Domain    ID    Enabled ver MEL Ctrl VLAN          state  Type  Revertive
---------------------------------------------------------------------------------------------------------------------------------------------------------
1         1     Yes   2     1     2     Idle   RPL Owner  Yes
      W/E       Interface Port state    Local SF Local        FS Local MS MEP   RPL
      west East       Eth 1/22 Blocking Eth 1/21 Forwarding     NO NO      NO NO      NO NO           Yes NO
S39OO-24F4S-B# S3900-48T4S#show              erps
ERPS status        :Enabled
Number of ERPS Domains : 1
Domain    ID    Enabled ver MEL Ctrl VLAN          state  Type  Revertive
---------------------------------------------------------------------------------------------------------------------------------------------------------
1         1     Yes   2     1     2     Idle   None Yes
w/E interface Port state Local SF Local FS Local MS mep rpl
west Eth 1/ 1 Forwarding    No       No    NO
East Eth 1/ 2 Forwarding No    No    No    NO
```

2.29 IEEE 802.1ag CFM

2.29.1 Introduction

Following the IEEE 802.1ag protocol CFM (Connectivity Fault Management) and itu-t's y.1731 protocol, it is an end-to-end OAM mechanism for ethernet-based hosted network connection detection on a two-layer link.It is mainly used to detect link connectivity, confirm fault and locate fault in the two-layer network.

CFM implements end-to-end connectivity fault detection, fault notification, fault confirmation, and fault location functions for the network. It can be used to monitor the connectivity of the entire network, locate network connectivity faults, and cooperate with protection switching technology to improve network reliability.

Y.1731 is an OAM protocol proposed by the ITU-T standards organization. It not only contains the content specified by IEEE802.1ag, but also adds more OAM message combinations. Y.1731, as an extended function of CFM, adds some functions of performance detection on the basis of CFM.

2.29.2 Parameter Description

Command	Purpose
MD（Maintenance Domain）	Maintenance domain MD, indicating the network covered by connectivity error detection
MA（Maintenance Association）	Maintenance alliance MA，it can configure multiple maintenance alliances in the maintenance domain as required.
MEP（Maintenance association End Point）	Maintenance endpoint, which determines the scope and boundary of the MD in the maintenance domain
MIP（Maintenance association Intermediate Point）	Maintenance MIP is located in the maintenance domain. Multiple MIPs can be deployed between MEPs to improve network manageability.

2.29.3 Working Mechanism

Basic CFM functions include connectivity detection (CC), loopback function (LB), link tracking function (LT), and delay measure (DM). The connectivity detection function is used to detect the connectivity status between the maintenance endpoints. The loopback function is 802.1ag MAC Ping function. Similar to the IP layer Ping, it is used to verify the connection status between local and remote devices. The link tracking function is 802.1ag MAC Trac, Similar to Traceroute, it is used to determine the path from the source to the destination maintenance endpoint.

2.29.4 Configuration

Topology

Configure CFM

Complete VLAN configuration on DUT1 and DUT2. For the configuration of DUT2, refer to the configuration of DUT1.

```
DUT1#
DUT1#conf t
DUT1(config)#vlan database
DUT1(config-vlan)#vlan 6
DUT1(config-vlan)#exi
DUT1(config)#int ethernet 1/6
DUT1(config-if)#switchport mode access
DUT1(config-if)#switchport access vlan 6
```

Configure CFM basic function cross detection on DUT1.

```
DUT1(config)#cfm enable
DUT1(config)#cfm domain index 1 name md1 level 4          Create a maintenance domain "md1"
DUT1(config-ether-cfm)#ma index 1 name ma1 vlan 1         Create a maintenance domain "ma1"
DUT1(config-ether-cfm)#mp crosscheck mpid 2 ma ma1        Remote mpid
DUT1(config)#exit
DUT1(config)#interface ethernet 1/1
DUT1(config-if)#cfm mep mpid 1 md md1 ma ma1              Create mpid 1 on port 1
DUT1(config)#cfm cc md md1 ma ma1 interval 5              ccm message sending interval level is 5 (1s)
DUT1(config)#eth cfm mep crosscheck start-delay 3
```

Configure CFM basic function cross detection on the DUT2 device.

```
DUT2(config)#cfm enable
DUT2(config)#cfm domain index 2 name md1 level 4        Create a maintenance domain "md1"
DUT2(config-ether-cfm)#ma index 2 name ma1 vlan 1       Create a maintenance domain "ma1"
DUT2(config-ether-cfm)#mp crosscheck mpid 1 ma ma1
DUT2(config)#exit
DUT2(config)#interface ethernet 1/1
DUT2(config-if)#cfm mep mpid 2 md md1 ma ma1            Create mep 2 on port 1
DUT2(config)#cfm cc md md1 ma ma1 interval 5            ccm message sending interval level is 5 (1s)
DUT2(config)#eth cfm mep crosscheck start-delay 3
```

2.29.5 CFM Verification

Display local and remote mep information

```
DUT#show cfm maintenance-points local mep
MPID MD Name              Level Direct VLAN Interface CC Status MAC Address
---- --------------- ----- ------ ---- --------- --------- -----------------
   1 md1                      4 Down        6 Eth 1/ 6    Enabled     64-9D-99-10-06-66

DUT1#show cfm maintenance-points remote detail mpid 2
MAC Address              : 64-9D-99-10-0A-D8
Domain/Level             : md1 / 4
MA Name                  : ma1
Primary VLAN             : 6
MPID                     : 2
Incoming Port            : Eth 1/ 6
CC Lifetime              : 3723 seconds
```

```
Age of Last CC Message : 25 seconds
Frame Loss                    : 75
CC Packet Statistics      : 375/75 (Received/Error)
Port State                    : Up
Interface State             : Up
Crosscheck Status          : Enabled

DUT#show cfm maintenance-points remote crosscheck mpid 2
DUT1#show cfm maintenance-points remote crosscheck mpid 1
MPID    MA Name                           Level    VLAN    MEP Up    Remote MAC
----    -----------------------    -----    ----    ------    -----------------
   1    ma1                                    4         6    Yes         64-9D-99-10-0A-D8
```

2.29.6. CFM LB（lookback）Verification

```
DUT1#cfm loopback dest-mep 2 md md1 ma ma1 count 2
Type ESC to abort.
Sending 2 Ethernet CFM loopback message, timeout is 5 sec.
Received 2 Ethernet CFM loopback message in 1 sec.
Received 2 Ethernet CFM loopback message in 5 secs.
Success rate is 100% (2/2).
```

2.29.7. CFM LT（linktrace）Verification

```
DUT1(config)# cfm linktrace dest-mep 2 md md1 ma ma1
DUT1(config)#end
DUT1#show cfm linktrace-cache
Hops MA                    IP / Alias                    Ingress MAC            Ing. Action Relay
                           Forwarded                     Egress MAC             Egr. Action
---- -------------- ----------------------- ----------------- ----------- -----
   1 ma1                   192.168.6.2                   64-9D-99-10-0A-D8 ingOk           Hit
                           Not Forwarded
   1 ma1                   192.168.6.2                   64-9D-99-10-0A-D8 ingOk           Hit
                           Not Forwarded
```

2.29.8. CFM DM（delay measure）Verification

```
DUT1(config)#cfm delay-measure two-way dest-mep 2 md md1 ma ma1 count 5
Type ESC to abort.
Sending 5 Ethernet CFM delay measurement message, timeout is 5 sec.
Sequence    Delay Time (ms.)    Delay Variation (ms.)
--------    ----------------    ---------------------
        1              < 10                       0
        2              < 10                       0
        3              < 10                       0
        4              < 10                       0
        5              < 10                       0
Success rate is 100% (5/5), delay time min/avg/max=0/0/0 ms.
Average frame delay variation is 0 ms.
```

2.30 ITU-T Y.1731 OAM

2.30.1. Introduction

EFM can effectively improve the management and maintenance capabilities of Ethernet and ensure the stable operation of the network. Ethernet technology is easy to use, inexpensive, and the bandwidth can be continuously increased. Whether it is a business or a network structure, it has been widely used in the enterprise network. As the scope of Ethernet promotion gradually expands, the demand for Ethernet management and maintenance functions is also increasing. However, traditional Ethernet is relatively maintainable and operable. The emergence of the last mile Ethernet EFM (Ethernet in the First Mile) solves this problem very well.

Parameters	Description
efm oam critical-link-event	This command enables reporting of critical event or dying gasp. Use the no form to disable this function.
efm oam link-monitor frame	This command enables reporting of errored frame link events. Use the no form to disable this function.
efm oam mode	active - All OAM functions are enabled. passive - All OAM functions are enabled, except for OAM discovery, and sending loopback control OAMPDUs.

2.30.2. Configuration

Topology

Configure EFM

```
dut1:
DUT1(config)#interface ethernet 1/3
DUT1(config-if)#efm oam
DUT1(config-if)#efm oam mode active        //Set oam mode to active

dut2:
DUT2(config)#interface ethernet 1/3
DUT2(config-if)#efm oam
DUT2(config-if)#efm oam mode passive        //Set oam mode to active
```

EFM inspection

```
DUT1#show efm oam counters
DUT1#show efm oam counters interface 1/3
Port OAMPDU Type TX RX
---- --------------------- ---------- ----------
1/3 Information 1121 1444
1/3 Event Notification 0 0
1/3 Loopback Control 1 0
1/3 Organization Specific 76 0

DUT1#show efm oam event-log interface 1/1
```

2.31 UDLD

2.31.1. Introduction

UDLD (UniDirectional Link Detection) is used to monitor the physical configuration of the Ethernet link connected by optical fiber or twisted pair. When a unidirectional link (transmits to one direction only) occurs, UDLD can detect this situation, close the corresponding interface and send a warning message. Unidirectional links can cause many problems, especially spanning trees, which can cause loops.

Note: UDLD requires devices at both ends of the link for normal operation.

Parameters	Description
udld message-interval	This command configures the message interval between UDLD probe messages for ports in advertisement phase and determined to be bidirectional. Use the no form to restore the default setting.
udld aggressive	This command sets UDLD to aggressive mode on an interface. Use the no form to restore the default setting.
udld port	This command enables UDLD on an interface. Use the no form to disable UDLD on an interface.

2.31.2. Configuration

Topology

Configure UDLD

```
DUT1:
DUT1(config)#interface ethernet 1/3
DUT1(config-if)#udld port
DUT1(config-if)#udld aggressive
DUT2:
DUT2(config)#interface ethernet 1/3
DUT2(config-if)#udld port
DUT2(config-if)#udld aggressive
```

UDLD inspection

```
DUT1#show efm oam event-log interface 1/1
Console#show udld
Message Interval : 15
Interface UDLD Mode Oper State Msg Invl
Port State Timeout
--------- -------- ---------- ------------------------------------- --------
Eth 1/ 1 Enabled Aggressive Advertisement 15 s
Bidirectional 5 s
Eth 1/ 2 Disabled Normal Disabled 7 s
Unknown 5 s
Eth 1/ 3 Disabled Normal Disabled 7 s
Unknown 5 s
Eth 1/ 4 Disabled Normal Disabled 7 s
Unknown 5 s
Eth 1/ 5 Disabled Normal Disabled 7 s
Unknown 5 s
...
Console#show udld interface ethernet 1/1
Interface UDLD Mode Oper State Msg Invl
Port State Timeout
--------- -------- ---------- ------------------------------------- --------
Eth 1/ 1 Enabled Aggressive Advertisement 15 s
Bidirectional 5 s
```

```
  Accounting Port Number        : 1813
  Retransmit Times              : 2
  Request Timeout               : 5

Server 1:
  Server IP Address             : 10.1.1.2
  Authentication Port Number    : 1812
  Accounting Port Number        : 1813
  Retransmit Times              : 2
  Request Timeout               : 5

RADIUS Server Group:
Group Name                      Member Index
------------------------- -------------
radius                          1
```

```
Switch#show dot1x

802.1x:          Disabled

EAPOL Pass Through   :        Disabled

Port Brief Information

Port       Type            Operation Mode Control Mode        Authorized
-------- ------------- -------------- ------------------ ----------
Eth 1/ 1 Disabled       Single-Host     Force-Authorized     N/A
Eth 1/ 2 Disabled       Single-Host     Auto                 N/A
Eth 1/ 3 Disabled       Single-Host     Auto                 N/A
Eth 1/ 4 Disabled       Single-Host     Force-Authorized     N/A
Eth 1/ 5 Disabled       Single-Host     Force-Unauthorized   N/A
```

3. Layer 3 Features

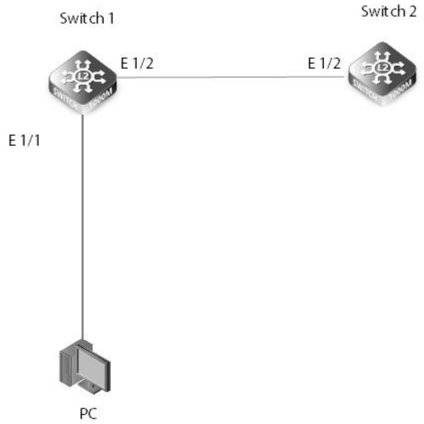
3.1 Static Unicast Routes

3.1.1 Introduction

When the network structure is relatively simple, configuring static routes can facilitate the normal operation of the network. In a large, complex network, because static routes do not change with network topology changes, bandwidth can be guaranteed for important applications when static routes are used. If the destination address of the packet cannot match any interface in the routing table, the packet will choose the default route. If there is no default route and the destination address of the message is not in the routing table, the message will be discarded, and an ICMP response message will be sent to the source to report that the destination address or network is unreachable.

3.1.2 Networking Ideas

Connect two S39s; configure the IP address and gateway of the PC. And configure a static route on the switch; use a PC to send packets to Switch 2 to see if they can communicate.



3.1.3 Configuration

Switch 1 Configuration

```
Switch1(config)#vlan database
Switch1(config-vlan)#vlan 24
Switch1(config-vlan)#vlan 2
Switch1(config)#interface ethernet 1/24
Switch1(config-if)#switchport mode access
Switch1(config-if)#switchport access vlan 24
Switch1(config-if)#interface vlan 24
Switch1(config-if)#ip add 192.168.2.1 255.255.255.0
Switch1(config)#interface ethernet 1/2
Switch1(config-if)#switchport mode access
Switch1(config-if)#switchport access vlan 2
Switch1(config)#interface vlan 2
Switch1(config-if)#ip add 192.168.1.254 255.255.255.0
Switch1(config)#ip route 192.168.2.0 255.255.255.0 192.168.2.2
```

Configure the IP on the PC as 192.168.1.1-253 and the gateway as 192.168.1.254

Switch 2 Configuration

```
Switch2(config)#vlan database
Switch2(config-vlan)#vlan 24
Switch2(config)#interface ethernet 1/24
Switch2(config-if)#switchport mode access
Switch2(config-if)#switchport access vlan 24
Switch2(config-if)#interface vlan 24
Switch2(config-if)#ip add 192.168.2.1 255.255.255.0
Switch2(config)#ip route 192.168.1.0 255.255.255.0 192.168.2.1
```

3.1.4 Verification

```
Switch1#show ip route
Codes: C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default
C        127.0.0.0/8 is directly connected, lo
S        192.168.1.0/24 [1/0] via 192.168.2.1, VLAN24
C        192.168.2.0/24 is directly connected, VLAN24
```

```
Switch2#show ip route
Codes: C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default

C        127.0.0.0/8 is directly connected, lo
S        192.168.2.0/24 [1/0] via 192.168.2.2, VLAN24
C        192.168.2.0/24 is directly connected, VLAN24
```

4. QoS Features

4.1. Function Introduction

Quality of Service (QoS) can be used to give certain traffic priority over other traffic. Without QoS, all traffic in a network has the same priority and chance of being delivered on time. If congestion occurs, all traffic has the same chance of being dropped. With QoS, specific network traffic can be prioritized to receive preferential treatment. In turn, a network performs more predictably, and utilizes bandwidth more effectively.
Classification information can be carried in the Layer-3 IP packet header or the Layer-2 frame. IP packet headers carry the information using 6 bits or 3 bits from the deprecated IP type of service (TOS) field. Layer-2 802.1Q frames carry the information using a 2-byte Tag Control Information field.
All switches and routers accessing the Internet depend on class information to give the same forwarding treatment to packets with the same class information, and give different treatment to packets with different class information. A packet can be assigned class information, as follows:

4.2. Principle Description

4.2.1 ACL

Access control lists (ACLs) classify traffic with the same characteristics. IP traffic is classified using IP ACLs, and non-IP traffic is classified using MAC ACLs. The ACL can have multiple access control entries (ACEs), which are commands that match fields against the contents of the packet.

4.2.2 CoS Value

Class of Service (CoS) is a 3-bit value used to classify the priority of Layer-2 frames upon entry into a network.
QoS classifies frames by assigning priority-indexed CoS values to them, and gives preference to higher-priority traffic.
Layer-2 802.1Q frame headers have a 2-byte Tag Control Information field that carries the CoS values in the 3 most significant bits, called the User Priority bits. On interfaces configured as Layer-2 802.1Q trunks, all traffic is in 802.1Q frames, except for traffic in the native VLAN.
Other frame types cannot carry Layer-2 CoS values. CoS values range from 0 to 7.

4.2.3 DSCP Value

Differentiated Services Code Point (DSCP) is a 6-bit value used to classify the priority of Layer-3 packets upon entry into a network.
DSCP values range from 0 to 63.

4.2.4 IP-Precedence Value

IP-Precedence is a 3-bit value used to classify the priority of Layer-3 packets upon entry into a network.
IP-Precedence values range from 0 to 7.

4.2.5 Classification

Classification distinguishes one kind of traffic from another by examining the fields in the packet. The process generates an internal priority for a packet, which identifies all future QoS actions to be taken on the packet.
Each packet is classified upon entry into the network. At the ingress, the packet is inspected, and the priority is determined based on ACLs or the configuration. The Layer-2 CoS value is then mapped to a priority value.
The classification is carried in the IP packet header using 6 bits or 3 bits from the deprecated IP TOS field to carry the classification information. Classification can also occur in the Layer-2 frame.
Classification is enabled only if QoS is globally enabled on the switch. By default, QoS is globally disabled, thus, no classification occurs.
Classification occurs on an ingress physical port, but not at the switch virtual interface level.
Classification can be based on CoS/inner-CoS/DSCP/IP-Precedence, default port cos, or class maps and policy maps.

4.2.6 Policing

Policing determines whether a packet is in or out of profile by comparing the internal priority to the configured policer.
The policer limits the bandwidth consumed by a traffic flow. The result is given to the marker.
There are two types of policers:
- Individual: QoS applies the bandwidth limits specified in the policer, separately, to each matched traffic class. An individual policer is configured within a policy map.
- Aggregate: QoS applies the bandwidth limits specified in an aggregate policer, cumulatively, to all matched traffic flows. An aggregate policer is configured by specifying the policer name within a policy map. The bandwidth limits of the policer are specified. In this way, the aggregate policer is shared by multiple classes of traffic within one or multiple policy map.

4.2.7 Marking

Marking determines how to handle a packet when it is out of profile. It assesses the policer and the configuration information to determine the action required for the packet, and then handles the packet using one of the following methods:
- Let the packet through and mark color down
- Drop the packet

Marking can occur on ingress and egress interfaces.

4.2.8 Queuing

Queuing maps packets to a queue. Each egress port can accommodate up to 8 unicast queues, 4 multicast queues and 1 SPAN queue.
The packet internal priority can be mapped to one of the egress queues. The unit of queue depth is buffer cell. Buffer cell is the granularity, which is 288 bytes, for packet storing.
After the packets are mapped to a queue, they are scheduled.

4.2.9 Tail Drop

Tail drop is the default congestion-avoidance technique on the interface. With tail drop, packets are queued until the thresholds are exceeded. The packets with different priority and color are assigned to different drop precedence. The mapping between priority and color to queue and drop precedence is configurable. You can modify the three tail-drop threshold to every egress queue by using the queue threshold interface configuration command. Each threshold value is packet buffer cell, which ranges from 0 to 16383.

4.2.10 WRED

Weighted Random Early Detection (WRED) differs from other congestion-avoidance techniques because it attempts to anticipate and avoid congestion, rather than controlling congestion when it occurs.
WRED reduces the chances of tail drop by selectively dropping packets when the output interface begins to show signs of congestion. By dropping some packets early rather than waiting until the queue is full, WRED avoids dropping large numbers of packets at once. Thus, WRED allows the transmission line to be fully used at all times. WRED also drops more packets from large users than small. Therefore, sources that generate the most traffic are more likely to be slowed down versus sources that generate little traffic.
You can enable WRED and configure the two thresholds for a drop-precedence assigned to every egress queues. The WRED's color drop precedence map is the same as tail-drop's. Each min-threshold represents where WRED starts to randomly drop packets. After min-threshold is exceeded, WRED randomly begins to drop packets assigned to this threshold. As the queue max-threshold is approached, WRED continues to drop packets randomly with the rate of drop-probability. When the max-threshold is reached, WRED drops all packets assigned to the threshold. By default, WRED is disabled.

4.2.11 Scheduling

Scheduling forwards conditions packets using combination of WDRR and SP. Every queue belongs to a class. The class range from 0 to 7, and 7 is the highest priority. Several queues can be in a same class, or non queue in some class. Packets are scheduled by SP between classes and WDRR between queues in a class.
- Strict Priority-Based (SP), in which any high-priority packets are first transmitted. Lower-priority packets are transmitted only when the higher-priority queues are empty. A problem may occur when too many lower-priority packets are not transmitted.
- Weighted Deficit Round Robin (WDRR), in which each queue is assigned a weight to control the number of packets relatively sent from each queue.

4.2.12 Class Map

A class map names and isolates specific traffic from other traffic. The class map defines the criteria used to match against a specific traffic flow to further classify it. The criteria can match several access groups defined by the ACL.
If there is more than one type of traffic to be classified, another class map can be created under a different name. After a packet is matched against the class-map criteria, it is further classified using a policy map.

4.2.13 Policy Map

A policy map specifies on which traffic class to act. This can be implemented as follows:

Set a specific priority and color in the traffic class.

Set a specific trust policy to map priority and color.

Specify the traffic bandwidth limitations for each matched traffic class (policer) and the action to take (marking) when the traffic is out of profile.

Redirect the matched traffic class to a specific physical interface.

Mirror the matched traffic class to a specific monitor session, which's destination is defined in mirror module(please refer to the "monitor session destination " command).

Enable statistics of matching each ace or each class-map(if the class-map operator is match-any).

Policy maps have the following attributes:

A policy map can contain multiple class statements, each with different match criteria and action.

A separate policy-map class can exist for each type of traffic received through an interface.

There can be only one policy map per interface per direction. The same policy map can be applied to multiple interfaces and directions.

Before a policy map can be effective, it must be attached to an interface.

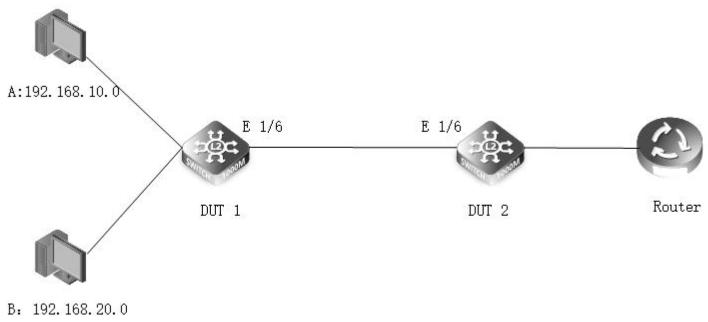
A policy map can be applied on physical interface(not link agg member), link agg interface, or vlan interface.

4.3. Scheduling for priority queues

4.3.1 Networking Ideas

A company has three services: data query, mail processing, and file transfer. Due to the importance of the business, the priority of business processing is also different. When users HostA and HostB access the three service servers, ensure that user A has the highest priority , Followed by user B. User A and user B belong to different network segments. DUT1 sets the priority, and DUT2 trusts the delivery priority.

#The topology is as follows



4.3.2 Configuration

#Set priority

```
DUT1#conf t
DUT1(config)#ip access-list acl
DUT1(config-std-acl)#permit 192.168.10.0 255.255.255.0
DUT1(config-std-acl)#exi
DUT1(config)#class-map cmap
DUT1(config-cmap)#match access-list acl
DUT1(config-cmap)#exi
DUT1(config)#policy-map pmap
DUT1(config-pmap)#class cmap
DUT1(config-pmap-c)#set ip dscp 48
```

#Apply to interface

```
DUT1(config)#interface ethernet 1/6
DUT1(config-if)#service-policy output pmap
```

#Priority of trust transfer

```
DUT2(config)#interface ge1/6
DUT2(config-if)#qos map trust-mode dscp
```

4.3.3 Verification

```
Switch-2#show policy-map
Policy Map pmap
Description:
 class cmap
  set IP DSCP 48
```

4.4. DiffServ Configuration

4.4.1 Networking Ideas

At present, the performance of the DUT2 device first needs to perform flow control on the data transmitted by DUT1 on the 10.0.0.0 network segment. The maximum traffic that can be transmitted on the entire network segment is 100M, and the burst traffic can reach 150M.

#The topology is as follows

4.4.2 Configuration

#ACL Traffic matching

```
DUT1#
DUT1#conf t
DUT1(config)#ip access-list extended ip-acl
DUT1(config-ext-acl)#permit any 10.0.0.0 255.255.255.0
DUT1(config-ext-acl)#exi
```

#Configuration Class Map

```
DUT1(config)#class-map cmap
DUT1(config-cmap)#match access-list acl
DUT1(config-cmap)#exi
```

#Configuration Polocy Map

```
DUT1(config)#policy-map pmap
DUT1(config-pmap)#class cmap
DUT1(config-pmap-c)#police flow 100000 150000 conform-action transmit violate-action drop
DUT1(config-pmap-c)#exit
DUT1(config-pmap)#exit
```

#Apply configuration policy

```
DUT1(config)#interface ethernet 1/6
DUT1(config-if)#service-policy output pmap
```

4.4.3 Verification

```
Switch#show policy-map
Policy Map fsmap
Description:
  class fsclass
Policy Map 12
Description:
  class 12
Policy Map pmap
Description:
  class cmap
    police flow 100000 200000 conform-action transmit violate-action drop
```

5. Security

5.1 Radius client

5.1.1 Introduction

The system can use AAA authentication to authenticate users who access the network and network services. RADIUS authentication is one of the AAA authentication methods. RADIUS is a distributed client / server system that prevents unauthorized access and ensures network security. RADIUS is a widely used protocol in network environments. It is usually used for embedded network devices such as routers, modem servers, switches, etc. RADIUS clients typically run on routers and switches that support RADIUS. The client sends an authentication request to the RADIUS server. The RADIUS server contains all user authentication and network service access information.

Users are under the same switch, and the Switch serves as the destination network access server. Users need to pass the remote authentication of the server to access the destination network through the Switch. The remote authentication method on the Switch is as follows:
- The Switch first authenticates the access user with a RADIUS server. If the authentication fails, the local authentication.
- The RADIUS server 10.32.120.37/24 acts as the authentication server and accounting server.

The topology diagram is shown below:

5.1.2 Networking ideas

Configuration ideas for user authentication and accounting using the RADIUS protocol.
(1) Configure the IP address of the RADIUS server and the IP address of the switch.
(2) Configure authentication scheme, authorization scheme, and accounting scheme.
(3) Apply authorization and charging policies in line vty.

5.1.3 Configuration

(1) Set the IP address of the switch and radius-server

```
Switch#configure terminal
Switch(config)#interface vlan 1
Switch(config-if)#ip add 10.32.120.100/24
Switch(config-if)#exit
Switch-4(config)#radius-server 1 host 10.32.120.37 key keyname
```

(2) Configure authentication scheme, authorization scheme, and accounting scheme

```
Switch-4(config)#authentication login radius local
Switch-2(config)#aaa authorization login default list radius
Switch-2(config)#aaa accounting login default start-stop list radius
```

(3) Apply authorization and charging policies in line vty

```
Switch-2(config)#line vty
Switch-4(config-line-vty)#authorization login default
Switch-2(config-line-vty)#accounting login default
```

5.1.4 Verification

```
Switch-2#show radius-server

Remote RADIUS Server Configuration:

Global Settings:
  Authentication Port Number : 1812
  Accounting Port Number     : 1813
  Retransmit Times           : 2
  Request Timeout            : 5

Server 1:
```

```
 Server IP Address                : 10.32.120.37
 Authentication Port Number : 1812
 Accounting Port Number         : 1813
 Retransmit Times                   : 2
 Request Timeout                      : 5

RADIUS Server Group:
Group Name                              Member Index
------------------------- -------------
radius                                   1
```

```
Switch-2#show authorization
-----------------------------------------------
Authorization Type : Login
   Method List      : default
   Group List        : radius
   Interface : VTY
```

```
Switch-2#show accounting login
------------------------------------------------------------
Accounting Type : Login
   Method List      : default
   Group List: radius
   Interface : VTY
```

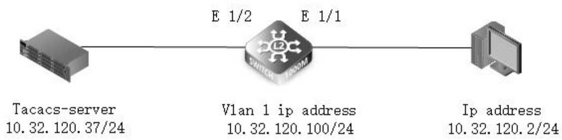
5.2 Tacacs+ client

5.2.1 Introduction

The system can use AAA authentication to authenticate users accessing the network and network services. TACACS + authentication is one of the AAA authentication methods. TACACS + is a distributed client / server system that prevents unauthorized access while ensuring network security. TACACS + is a widely used protocol in network environments. It is usually used for clients running on embedded network equipment such as routers, modem servers, switches, etc. that support TACACS + routers and switches. The client sends an authentication request to the TACACS + server. The TACACS + server contains all user authentication and network service access information.
Users are under the same switch, and the Switch serves as the destination network access server. Users need to pass the remote authentication of the server to access the destination network through the Switch. The remote authentication method on the Switch is as follows:

- Switch authenticates access users with tacacs + server first;

Tacacs + server 10.32.120.168/24



5.2.2 Networking ideas

Configuration ideas for user authentication and accounting using the RADIUS protocol.
(1) Configure the IP address of the RADIUS server and the IP address of the switch;
(2) Configure authentication scheme, authorization scheme, and accounting scheme;
(3) Apply authorization and charging policies in line vty.

5.2.3 Configuration

(1) Set the switch's IP address and tacacs-server's IP address

```
Switch#configure terminal
Switch(config)#interface vlan 1
Switch(config-if)#ip add 10.32.120.100/24
Switch(config-if)#exit
Switch(config)#tacacs-server 1 host 10.32.120.100 key keyname
```

(2) Configure authentication scheme, authorization scheme, and accounting scheme

```
Switch(config)#authentication login tacacs local
Switch(config)#aaa authorization login default list tacacs+
Switch(config)#aaa accounting login default start-stop list tacacs+
```

(3) Apply authorization and charging policies in line vty

```
Switch-2(config)#line vty
Switch-4(config-line-vty)#authorization login default
Switch-2(config-line-vty)#accounting login default
```

5.2.4 Verification

```
Switch-2#show tacacs-server

Remote TACACS+ Server Configuration:

Global Settings:
  Server Port Number : 49
  Retransmit Times      : 2
  Timeout                      : 5

Server 1:
  Server IP Address    : 10.32.120.100
  Server Port Number : 49
  Retransmit Times      : 2
  Timeout                      : 5

TACACS Server Group:
Group Name                          Member Index
------------------------- -------------
tacacs+                              1
```

```
Switch-2#show accounting login
-----------------------------------------------------------
Accounting Type : Login
    Method List      : default
    Group List: tacacs+
    Interface : VTY
```

```
Switch-2#show authorization
-----------------------------------------------
Authorization Type : Login
    Method List      : default
    Group List        : tacacs+
    Interface : VTY
```

5.3 802.1X

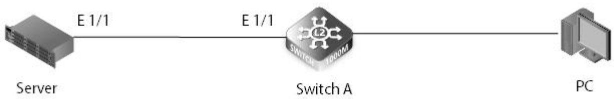
5.3.1 Introduction

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

802.1X protocol is a port-based network access control protocol. "Port-based network access control" refers to the authentication of the accessed user equipment at the port level of the LAN access device to control access to network resources.

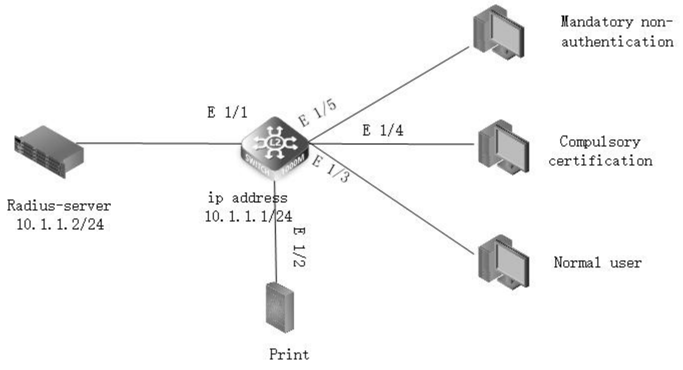
As shown in Figure 1, the 802.1X system is a typical Client / Server structure and includes three entities: Client, Device, and Authentication Server.

Figure 1 Schematic diagram of 802.1X authentication system



Networking requirements:

Attack users cannot access the network. Normal users access the network by username and password. Forced authentication users log in to the network without authentication. Printers access the network through Mac authentication.



5.3.2 Networking ideas

(1) Configure an IP address on the switch and specify the IP address of the radius-server;
(2) Configure the corresponding dot1x mode on the port.

5.3.3 Configuration

(1) Configure the IP address of the switch and the IP address of radius-server and enable dot1x

```
Switch#configure terminal
Switch(config)#interface vlan 1
Switch(config-if)#ip add 10.1.1.1/24
Switch(config-if)#exit
Switch(config)#radius-server 1 host 10.1.1.2 key keyname
switch-A(config)#dot1x system-auth-control
```

(2) Configure the corresponding dot1x mode under the port

```
Switch(config)#interface ethernet 1/2
Switch(config-if)#dot1x port-control auto
Switch(config-if)#network-access mode mac-authentication
Switch(config-if)#exit
Switch(config)#interface ethernet 1/3
Switch(config-if)#dot1x port-control auto
Switch(config)#interface ethernet 1/4
Switch(config-if)#dot1x port-control force-authorized
Switch(config-if)#exit
Switch(config)#interface ethernet 1/5
Switch(config-if)#dot1x port-control force-unauthorized
Switch(config-if)#exit
```

5.3.4 Verification

```
Switch#show radius-server
Remote RADIUS Server Configuration:

Global Settings:
  Authentication Port Number : 1812
  Accounting Port Number     : 1813
  Retransmit Times           : 2
  Request Timeout            : 5

Server 1:
  Server IP Address          : 10.1.1.2
  Authentication Port Number : 1812
  Accounting Port Number     : 1813
  Retransmit Times           : 2
  Request Timeout            : 5

RADIUS Server Group:
```

```
Group Name                    Member Index
------------------------- -------------
radius                        1
```

```
Switch#show dot1x

802.1x:          Disabled

EAPOL Pass Through   :        Disabled

Port Brief Information

Port       Type              Operation Mode Control Mode          Authorized
-------- ------------- -------------- ------------------ ----------
Eth 1/ 1 Disabled        Single-Host      Force-Authorized       N/A
Eth 1/ 2 Disabled        Single-Host      Auto                   N/A
Eth 1/ 3 Disabled        Single-Host      Auto                   N/A
Eth 1/ 4 Disabled        Single-Host      Force-Authorized       N/A
Eth 1/ 5 Disabled        Single-Host      Force-Unauthorized     N/A
```

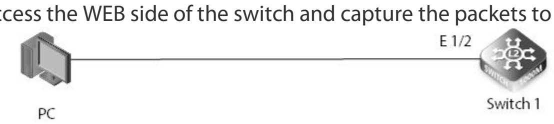
5.4 HTTPS and SSL (v3)

5.4.1 Introduction

This command provides secure access by enabling Secure Hypertext Transfer Protocol (HTTPS) via Secure Sockets Layer (SSL)(Ie encrypted connection) to the network interface of the switch.

5.4.2 Networking ideas

After configuring HTTPS, use a PC to access the WEB side of the switch and capture the packets to see if it is HTTPS.



5.4.3 Configuration

Switch Configuration
Enable HTTPS

```
Switch#config t
Switch(config)#server https enable
```

5.4.4 Verification

```
Switch#show system
 System Up Time              : 0 days, 1 hours, 18 minutes, and 38.58 seconds
 System Name                 :
 System Location             :
 System Contact              :
 MAC Address (Unit 1)        : 64-9D-99-10-06-60
 System OID String    : 1.3.6.1.4.1.52642.2.1.45.101
 http Server          : Enabled
 http Server Port     : 80
 https Server         : Enabled
 https Server Port    : 443
 Telnet Server        : Enabled
 Telnet Server Port : 23
```

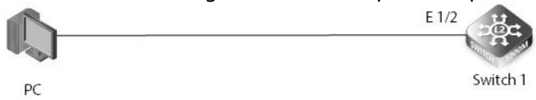
5.5 SSH V2.0

5.5.1 Introduction

SSH is short for Secure Shell. When users log in to the device remotely through a network environment that cannot guarantee security, SSH can use encryption and strong authentication to provide security and protect the device from attacks such as IP address fraud and clear text password interception. The device supports the SSH server function and can accept connections from multiple SSH clients. At the same time, the device also supports the SSH client function, allowing users to establish an SSH connection with a device that supports the SSH server function, thereby enabling SSH login from a local device to a remote device.

5.5.2 Networking ideas

After configuring SSH, use a PC to connect to the switch through SSH 2.0, and capture the packet to see if it is SSH 2.0.



5.5.3 Configuration

Switch1 Configuration
Enable SSH service globally

```
switch#config t
switch(config)#ip ssh server enable
```

5.5.4 Verification

```
switch#show ip ssh
SSH Enabled - Version RSA V1.5, RSA V2.0, DSA V2.0
Negotiation Timeout : 120 seconds; Authentication Retries : 3
```

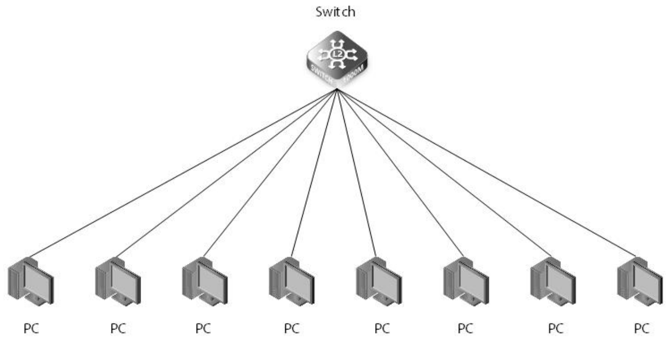
5.6 DoS Protection

5.6.1 Introduction

The full name of the DoS attack is Denial of Service. A denial of service attack refers to a deliberate attack on a network protocol implementation defect or a brutal exhaustion of the victim's resources directly through brutal means. The purpose is to make the target computer or network unable to provide normal services or Resource access makes the target system service system stop responding or even crash, and this attack does not include intrusion into the target server or target network equipment. These service resources include network bandwidth, file system space capacity, open processes or allowed connections. This kind of attack will lead to a lack of resources. No matter how fast the computer can process, how much memory capacity, and how fast the network bandwidth is, the consequences of this attack cannot be avoided.

5.6.2 Networking ideas

The switch is connected to multiple PCs, and multiple PCs request access to the switch at the same time. Check whether the switch discards the request packets.



5.6.3 Configuration

Switch Configuration
Enable dos protection

```
switch (config)#dos-protection land
switch (config)#dos-protection tcp-null-scan
switch (config)#dos-protection tcp-syn-fin-scan
switch (config)#dos-protection tcp-xmas-scan
```

5.6.4 Verification

```
switch#show dos-protection
Global DoS Protection:

LAND Attack              : Enabled
TCP Null Scan            : Enabled
TCP SYN/FIN Scan         : Enabled
TCP XMAS Scan            : Enabled
```

6. ACL

6.1 L2/L3/L4

6.1.1 Introduction

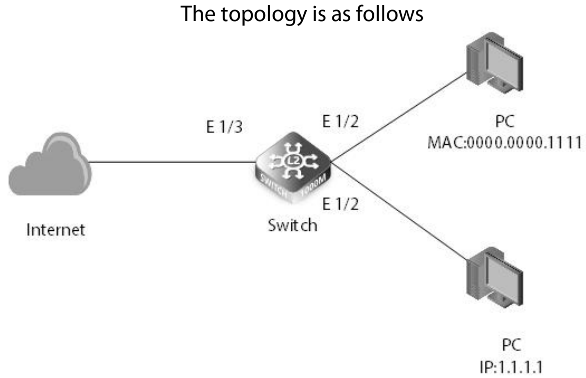
Access Control Lists (ACL) provide packet filtering for IPv4 frames (based on address, protocol, Layer 4 protocol port number or TCP control code), IPv6 frames (based on address, DSCP traffic class, or next header type), or any frames (based on MAC address or Ethernet type). To filter packets, first create an access list, add the required rules, and then bind the list to a specific port. This section describes the Access Control List commands.

IPv4 ACLs The commands in this section configure ACLs based on IPv4 addresses, TCP/UDP port number, protocol type, and TCP control code. To configure IPv4 ACLs, first create an access list containing the required permit or deny rules, and then bind the access list to one or more ports.

6.1.2 Basic acl

In the following example, a basic MAC ACL is used on port eth1/1 to allow packets with a source MAC address of 0000.0000.1111 to pass, and reject other packets. The basic IPv4 ACL is used on eth1/2 to allow the packets with the source IP address 1.1.1.1/24 to pass and deny other packets.

The topology is as follows



Configuration ideas:
- Create acl
- Apply acl to the port

Configuration steps:

(1) Create mac-acl

```
Switch(config)#mac access-list basic
Switch(config-mac-acl)# permit host 000000001111 any
Switch(config-mac-acl)#deny any any
Switch(config-mac-acl)#exit
```

(2) Application of mac-acl under the interface

```
Switch(config)#interface ethernet 1/1
Switch(config-if)#mac service-acl basic in
```

(3) Create basic acl

```
Switch(config)#ip access-list v4basic
Switch(config-std-acl)# permit host 1.1.1.1
Switch(config-std-acl)#deny any
Switch(config-std-acl)#exit
```

(4) Apply basic acl under the interface

```
Switch(config)#interface ethernet 1/2
Switch(config-if)#ip service-acl v4basic in
```

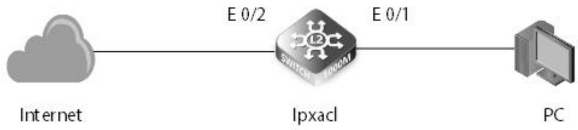
(5) Configuration verification

```
Switch#show mac access-list basic
MAC access-list basic:
 permit host 00-00-00-00-11-11 any
   deny any any
```

```
Switch#show ip access-list standard v4basic
IP standard access-list v4basic:
   permit host 1.1.1.1
   deny any
```

6.1.3 Extended acl

The following example describes how to extend the IPV4 ACL to allow packets with a source MAC of 0.0.1111 on port eth-0-1, allow all TCP packets, and prohibit other packets from entering the system.



Configuration ideas：

- Create extension acl
- Application extension acl under interface

Configuration steps:

(1) Create extension acl

```
Switch(config)#ip access-list extended ipxacl
Switch(config-ext-acl)#permit tcp any any
Switch(config-ext-acl)#deny any any
Switch(config-ext-acl)#exit
```

(2) Application extension acl under interface

```
Switch(config)#interface ethernet 1/12
Switch(config-if)#ip service-acl ipxacl in
```

(3) Configuration verification:

```
Switch#show ip access-list extended ipxacl
IP extended access-list ipxacl:
   permit TCP any any
   deny any any
```

7. IPv6

7.1 IPv6 Address Type

7.1.1 Introduction

There are three types of IPv6 addresses: unicast addresses, anycast addresses, and multicast addresses. Compared with IPv4, the broadcast address type is canceled, replaced by a richer multicast address, and the anycast address type is added.

7.1.2 Address format

Category	Reference format	Description
Unicast address	2001:0:0:0:0DB8:800:200C:417A/64	2001: 0: 0: 0: 0DB8: 800: 200C: 417A is the address. Also specify the prefix length of the address (eg 64 in the reference format)
Multicast address	FF01:0:0:0:0:0:0:101	Multicast addresses start with FF
Anycast Address	2002:0:0:0:0DB8:800:200C:417A/64	The format is the same as the unicast address. Different VLAN ports can be configured with the same anycast address. Messages sent to anycast addresses will be "routed" to the VLAN port closest to the sender configured with anycast addresses

The IPv6 address-related settings of the switch are valid only in the interface VLAN. IPv6 addresses cannot be configured on physical ports.

7.1.3 Configuration

Manually configure an IPv6 global unicast address

```
Switch(config-if)#ipv6 add {pv6-address prefix-length}
```

Use EUI-64 format to form IPv6 global unicast addresses

```
Switch(config-if)#ipv6 add {ipv6-address prefix-length} eui-6
```

Configure the link-local address of the interface

```
Switch(config-if)#ipv6 add {ipv6-address} link-local
```

7.1.4 Verification

View interface IPv6 address

```
Switch#show ipv6 interface brief
Interface          Status      IPv6         IPv6 Address
-------------- ---------- ---------- ---------------------------------------
VLAN 1              Up           Up           2001::db8:800:200c:417a/64
VLAN 1              Up           Up           fe80::1/64
```

7.2 IPv4/IPv6 Dual Protocol Stack

7.2.1 Introduction

Dual protocol stack technology refers to enabling both the IPv4 protocol stack and the IPv6 protocol stack on one device. In this case, this device can communicate with both IPv4 and IPv6 networks.

7.2.2 Features

Multiple link protocols (such as Ethernet) support dual protocol stacks: The link layer is Ethernet. On an Ethernet frame, if the value of the protocol ID field is 0x0800, it indicates that the network layer received an IPv4 packet. 0x86DD, indicating that the network layer is an IPv6 packet.
Multiple applications (such as DNS / FTP / Telnet, etc.) support dual protocol stacks: upper-layer applications (such as DNS) can choose TCP or UDP as the transport layer protocol, but prefer the IPv6 protocol stack instead of the IPv4 protocol stack as the network layer protocol.

Configuration

Configure interface IPv4 address Switch(config-if)#ip add {ip-address prefix-length}
Configure the interface IPv6 address Switch(config-if)#ipv6 add {pv6-address prefix-length}

7.2.3 Networking ideas

As the picture shows:

Device name	IPv4 address	IPv6 address	Device port
SwitchA	172.16.1.1/24	1：：1/64	Eth1/1
PC	172.16.1.2	1：：2/64	Network port

Configuration idea:
Configure IPV4 and IPV6 addresses for the same interface of the switch, and configure IPV4 and IPV6 addresses for the PC network card.

7.2.4 Configuration

(1) Enter the CLI interface to create a vlan for the switch, and configure ipv4 and ipv6 addresses on the vlan if interface.

```
SwitchA#configure terminal
SwitchA(config)# vlan database#
SwitchA(config-vlan)#vlan 10
SwitchA(config-vlan)#exit
SwitchA(config)#interface vlan 10
SwitchA(config-if)#ip add 172.16.1.1 255.255.255.0
SwitchA(config-if)#ipv6 enable
SwitchA(config-if)#ipv6 add 1::1/64
SwitchA(config-if)#exit
```

(2) Add the corresponding interface to the corresponding vlan

```
SwitchA(config)#interface ethernet 1/1
SwitchA(config-if)#switchport mode access
SwitchA(config-if)#switchport access vlan 10
```

7.2.5 Verification

Use show ipv6 interface brief to view the ipv6 address of the interface

```
Switch#show ipv6 interface brief
Interface       Status     IPv6       IPv6 Address
VLAN 10           Up         Up           1::1/64
VLAN 10           Up         Up           fe80::669d:99ff:fe10:abc/64
```

Use show ip int brief to view the ipv4 address of the interface

```
Switch# show ip int brief
VLAN 10 is Administrative Up - Link UP
  Address is 64-9D-99-10-0A-BC
  Index: 1010, MTU: 1500
  Address Mode is Static
  IP Address: 172.16.1.1 Mask: 255.255.255.0
  Proxy ARP is disabled
  DHCP Client Vendor Class ID (text): S3900-48T4S
  DHCP Relay Server:
```

The PC uses the local IPv4 and IPv6 addresses to execute the ping command to access the switch.

7.3 Internet Control Message Protocol for the IPv6

7.3.1 Introduction

In addition to the commonly used ICMPv4 functions, ICMPv6 is also the basis for other functions, such as neighbor discovery, stateless address configuration (including duplicate address detection), and PMTU discovery.
Neighbor Discovery Protocol
The Neighbor Discovery Protocol (NDP) defines the use of ICMPv6 packets to implement address resolution, track neighbor status, duplicate address detection, router discovery, and redirection.

Address resolution

NS（Neighbor Solicitation）and NA（Neighbor Advertisement）.

NS packet: Its role in address resolution is similar to the ARP request packet in IPv4.
NA message: Its role in address resolution is similar to the ARP response message in IPv4.

Duplicate Address Detect
Before the interface uses an IPv6 unicast address, it is mainly used to detect whether other nodes use the address. Especially in the automatic address configuration, DAD detection is necessary.

Router discovery
Used to discover devices connected to the local link, and obtain prefixes and other configuration parameters related to automatic address configuration.
Router Advertisement (RA) messages: In order to let hosts and devices on the Layer 2 network know their existence, each device periodically sends RA messages. The RA messages carry network prefix information and other Flag bit information.
Router Request RS (RouterSolicitation) message: In many cases, the host wants to obtain the network prefix for communication as soon as possible after accessing the network. At this time, the host can immediately send an RS message, and the device on the network will respond to the RA message.

Address auto-configuration
IPv4 uses DHCP to implement automatic configuration, including IP address, default gateway, and other information, simplifying network management. The IPv6 address grows to 128 bits and there are many terminal nodes. The requirement for automatic configuration is more urgent. In addition to retaining DHCP as stateful autoconfiguration, stateless autoconfiguration is also added. Stateless auto-configuration means that link-local addresses are automatically generated. Hosts automatically configure global unicast addresses, etc. based on the prefix information of RA messages, and obtain other relevant information.

7.3.2 Configure

Configure static neighbors

```
Switch(config)# ipv6 neighbor ipv6 address vlan vlanid mac-address
```

Configure neighbor discovery

```
Switch(config)#interface vlan vlan id
Switch(config-if)#ipv6 enable
```

Configure optional parameters for neighbor discovery

Configure IPv6 MTU for the interface
```
Switch(config-if)#ipv6 mtu bytes
```

Configure the number of times that the system sends neighbor solicitation messages during duplicate address detection
```
Switch(config-if)#ipv6 nd dad attempts {num}
```

Configure the "M flag" in RA messages
```
Switch(config-if)#ipv6 nd managed-config-flag
```

Configure the interval for sending NS packets
```
Switch(config-if)#ipv6 nd ns-interval {interval}
```

Configure the "O flag" in RA messages
```
Switch(config-if)#ipv6 nd other-config-flag
```

Configure the interval for sending RA messages on the port
```
Switch(config-if)#ipv6 nd prefix X:X;X;X;;X/<0-0> valid-lifetime
```

Configure the interval for sending RA messages on the port
```
Switch(config-if)#ipv6 nd ra interval Maximum RA interval
```

Configure RA packet lifetime
```
Switch(config-if)#ipv6 nd ra lifetime router lifetime
```

Configure the value of the switch priority field in the RA message sent on this port Switch(config-if)#ipv6 nd ra router-preference {preference}
Configure the port to stop being the interface advertised by the switch; only "advertised interfaces can send RA messages" Switch(config-if)#ipv6 nd ra suppres

7.3.3 Verification

Use show ipv6 neighbors to view ipv6 neighbors

```
Switch#show ipv6 neighbors
State: I1 - Incomplete, I2 - Invalid, R - Reachable, S - Stale, D - Delay,
           P1 - Probe, P2 - Permanent, U - Unknown
IPv6 Address                                  Age    Link-layer Addr      State Interface
---------------------------------------- ---- ----------------- ----- ---------
fe80::3076:c8:83bb:baa4                         0 F4-8E-38-B8-D2-58 D          VLAN 1
```

Use show ipv6 interface to view ipv6 interface information

```
Switch#show ipv6 interface
VLAN 1 is up
IPv6 is enabled.
Link-local address:
   fe80::1%1/64
Global unicast address(es):
   2001::db8:800:200c:417a/64, subnet is 2001::/64
Joined group address(es):
ff02::1:ff00:0
ff02::1:ff00:1
ff02::1:ff0c:417a
ff02::1:2
ff02::2
ff02::1
IPv6 link MTU is 1500 bytes
ND DAD is enabled, number of DAD attempts: 1.
ND retransmit interval is 1000 milliseconds
ND advertised retransmit interval is 0 milliseconds
ND reachable time is 30000 milliseconds
ND advertised reachable time is 0 milliseconds
ND advertised router lifetime is 1800 seconds
```

7.4 Neighbor Discovery Snooping

7.4.1 Introduction

ND snooping is to establish a prefix management table and an ND snooping dynamic binding table by listening to ND packets based on ICMPv6, so that the device can manage the IPv6 address of the access user according to the prefix management table; meanwhile, according to the ND snooping dynamic binding table To filter illegal ND packets received by untrusted interfaces to prevent ND attacks.

7.4.2 Interface Role

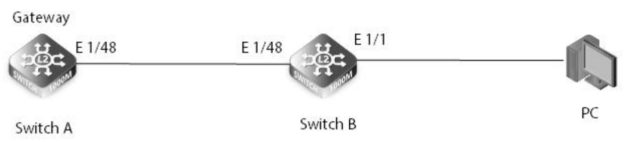
ND Snooping trusted interface: This type of interface is used to connect to trusted IPv6 nodes. The device forwards ND packets received from this type of interface normally. At the same time, the device creates a prefix management table based on the received RA packets.

ND Snooping untrusted interface: This type of interface is used to connect untrusted IPv6 nodes. The device considers that the RA message received from this type of interface is an illegal message and directly discards it. For the received NA / NS / RS message, if This interface enables the ND packet validity check function. The device checks the binding table for matching with the NA / NS / RS packet based on the ND Snooping dynamic binding table. When the packet does not meet the binding table relationship, the device considers that The packet is directly discarded by an illegal user. The device forwards other types of ND packets normally.

7.4.3 Networking Ideas

Example for Configuring ND Snooping

Device name	Interface	Interface Type	Vlan
SwitchA	Eth48	Trunk	20
SwitchB	Eth48	Trunk	20
	Eth1/1	Access	20
PC1	Network port	/	20



7.4.4 Configuration

(1) Create vlan10 and put the interface in the corresponding vlan

```
SwitchA#configure terminal
SwitchA(config)#vlan database
SwitchA(config-vlan)#vlan 20
SwitchA(config)#interface ethernet 1/48
SwitchA(config-if)#switchport trunk allowed vlan add 20

SwitchB#configure terminal
SwitchB(config)#vlan database
SwitchB(config-vlan)#vlan 20
SwitchB(config-vlan)#exit
SwitchB(config)#int ethernet 1/48
SwitchB(config-if)#switchport mode trunk
SwitchB(config-if)#switchport trunk allowed vlan add 20
SwitchB(config-if)#exit
SwitchB(config)#int ethernet 1/1
SwitchB(config-if)#switchport mode access
SwitchB(config-if)#switchport access vlan 20
```

(2) Configure the gateway address for the switch so that the PC can obtain the address automatically

```
SwitchA(config)#interface vlan 20
SwitchA(config-if)#ipv6 add 2001::1/64
```

(3) Globally enable ND Snooping and bind VLAN

```
SwitchA(config)#ipv6 nd snooping
SwitchB(config)# ipv6 nd snooping
SwitchB(config)#ipv6 nd snooping vlan 20
```

(4) Configure the interface as a trusted interface

```
Switch(config)#int ethernet 1/48
Switch(config)# ipv6 nd snooping
Switch(config)# ipv6 nd snooping trust
```

(5) Configuration check

Use show ipv6 nd snooping binding to view the binding relationship

```
Switch#show ipv6 nd snooping binding
MAC Address       IPv6 Address                                  Lifetime     VLAN Interface
-------------- --------------------------------------- ---------- ---- ---------
649D-99b8-d258                2001::289e:d276:f163:737d        2592000      20 Eth 1/1
649D-99b8-d258                2001::3076:c8:83bb:baa4          2592000      20 Eth 1/1
```

7.5 IPv6 DHCP Snooping

7.5.1 Introduction

DHCPv6 snooping allows the switch to protect the network from rogue DHCPv6 servers or other sending device related to the port, and information is sent to the DHCPv6 server. This information is helpful for tracing IP addresses back to physical ports.

7.5.2 Features

The trust function of DHCPV6 Snooping can ensure that the client obtains an IP (Internet Protocol) address from a legitimate server.The DHCPV6 Snooping trust function divides interfaces into trusted interfaces and untrusted interfaces:
The trusted interface receives DHCPACK, DHCPNAK, and DHCPOffer messages from the DHCP server. In addition, the device will only send DHCP request messages from the DHCP client to the legitimate DHCP server through the trusted interface. After receiving the DHCP ACK, DHCP NAK, and DHCP Offer message from the DHCP server, the untrusted interface discards the message.

7.5.3 Introduction to Configuration Commands

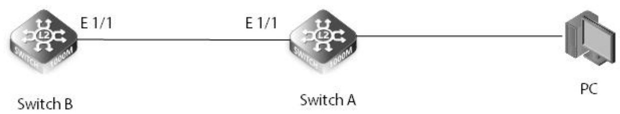
Enable DHCPV6 Snooping globally Switch(config)#ipv6 dhcp snooping
Enable DHCPV6 Snooping on the specified vlan Switch(config)# ipv6 dhcp snooping vlan {vlan-id | vlan-range}
Sets the maximum number of entries that can be stored in the interface's binding database. (Default is 5) Switch(config-if)#ipv6 dhcp snooping max-binding {count}
Configures the specified interface as a trusted interface Switch(config-if)#ipv6 dhcp snooping trust
This command clears the DHCPv6 snoop binding table entry from RAM Switch#clear ipv6 dhcp snooping binding [mac-address ipv6-address]
This command deletes all dynamically learned listening entries from flash Switch (config)#clear ipv6 dhcp snooping database flash

7.5.4 Verification Command Introduction

This command shows the DHCPv6 snooping configuration settings Switch#show ipv6 dhcp snooping
This command displays DHCPv6 snoop binding table entries Switch#show ipv6 dhcp snooping binding
This command displays the statistics of DHCPv6 snooping client, server and relay packets Switch#show ipv6 dhcp snooping statistics

7.5.5 Configuration Example

Topology introduction: SwitchB functions as a DHCPV6 server, and PC functions as a client.Configure DHCPV6 Snooping.



Configuration steps:

(1) Enable DHCPV6 Snooping globally

```
Switch A#configure terminal
Switch A(config)#ipv6 dhcp snooping
```

(2) Configure SwitchA's interface as a trusted port

```
Switch A(config)#interface ethernet 1/1
Switch A(config-if)#ipv6 dhcp snooping trust
```

(3) View configuration settings with show ipv6 dhcp snooping

```
Switch A#show ipv6 dhcp snooping
Global DHCPv6 Snooping status: enabled
DHCPv6 Snooping remote-id option status: disabled
DHCPv6 Snooping remote-id policy: drop
DHCPv6 Snooping is configured on the following VLANs:

Interface          Trusted      Max-binding   Current-binding
---------          ---------    -----------   ---------------
Eth 1/1            Yes                    5                 0
```

7.6 MVR over IPv6

7.6.1 Introduction

The Multicast LAN Registration (MVR) function solves the flooding problem of receivers in different VLANs. It uses a dedicated manually configured VLAN, the multicast VLAN, to forward multicast traffic in a Layer 2 network. It can simultaneously communicate with IGMP Snooping collaboration.

7.6.2 Features

MVR port type: source port and receive port

Source port: The source port is the port through which the multicast stream in the multicast VLAN passes.

Receive port: It is a port that monitors the switch to which the multicast host is connected. It can be placed in any VLAN or no VLAN except the multicast vlan (no VLAN usually refers to VLAN 1, untagged traffic). This implies that the switch with MVR enabled performs VLAN tag replacement, replacing the VLAN tag of the multicast receiving port with the source port VLAN tag.

MVR has two configuration modes: compatible mode and dynamic mode

Compatible mode: In compatible mode, the CPU of the MVR switch normally forwards the router's query messages and processes the client's join messages to form a dynamically learned multicast forwarding table, but the CPU will not forward the join messages to the router. Port, so the upper-layer router will not receive the following join packets, which will cause the router's data to be forwarded to the switch. In this mode, you need to manually configure the router's multicast forwarding table to forward the data to the switch.

Dynamic mode: The only difference between dynamic mode and compatible mode is that the cpu can forward the join packet to the router port in the dynamic mode, so that the upper-level router can dynamically learn the multicast forwarding table, without the need to manually configure the router. Multicast forwarding table to forward data to the switch.

7.6.3 Introduction to Configuration Commands

This command binds the MVR group address specified in the configuration file to the MVR domain Switch(config)#mvr6 domain {domain-id} associated-profile {profile-name}
This command enables multicast VLAN registration (MVR) for a specific domain Switch(config)#mvr6 domain {domain-id }
This command maps a series of MVR group addresses to a configuration file Switch(config)# mvr6 profile profile-name start-ip-address end-ip-address
This command configures expected packet loss and thus the number of times reports and group-specific queries are generated Switch(config)#mvr6 robustness-value {value}
This command configures the switch to forward only multicast streams that the source port has dynamically joined Switch(config)#mvr6 source-port-mode dynamic
This command configures the source IPv6 address assigned to all MVR control packets sent upstream from the specified domain Switch(config)#mvr6 domain domain-id upstream-source-ip source-ip-address
This command specifies the VLAN through which MVR multicast data is received Switch(config)#mvr6 domain domain-id vlan vlan-id

This command causes the switch to remove the interface from the multicast stream immediately after receiving the leave message Switch(config)#mvr6 domain domain-id immediate-leave
This command configures the interface as an MVR sink or source port Switch(config)#interface Ethernet {Unit number} Switch(config-if)#mvr6 domain domain-id type {receiver | source}
This command statically binds a multicast group to a port that will receive long-term multicast streams associated with a stable port Switch(config-if)# mvr6 domain domain-id vlan vlan-id group ip-address

7.6.4 Verification Command Introduction

This command displays information about MVR domain settings Switch#show mvr6
This command shows that the configuration file is bound to the specified domain Switch# show mvr6 [domain domain-id] associated-profile
This command displays the MVR configuration settings of the interface connected to the MVR VLAN Switch#show mvr6 [domain domain-id] interface
This command displays information about the current number of entries in the forwarding database, or about a specific multicast address Switch#show mvr6 [domain domain-id] members [ip-address]
This command displays all configured MVR profiles Switch#show mvr6 profile
This command displays the MVR protocol related statistics of the specified interface Switch#show mvr6 statistics {input | output} [interface interface] Switch#show mvr6 domain domain-id statistics {input [interface interface] | output [interface interface] | query}

7.7 SNMP over IPv6

7.7.1 Introduction

SNMP commands use Simple Network Management Protocol (SNMP) to control access to this switch from the management station.

7.7.2 Features

MIB is a collection of managed objects. It defines a series of attributes of managed objects, including the name of the object, the access rights of the object, the data type of the object, and the structure of management information (SMI) specifies the managed object. How to define and organize, it defines a series of data types that MIB can use, such as Counter, Gauge, etc. The MIB specifies the variables maintained by the network elements, that is, information that can be queried and set by the NMS, and gives the data structure of a set of all possible managed objects in a network.

7.7.3 Introduction to Basic Configuration

This command enables the SNMPv3 engine and services for all management clients (ie versions 1, 2c, 3).
Switch (config)#snmp-server server
This command defines the authorized access string using SNMP v1 or v2c client.
Switch (config)#snmp-server community string [ro | rw]
This command specifies the recipients of the Simple Network Management Protocol notification operation
Switch (config)#snmp-server host host-addr [inform [retry retries | timeout seconds]] community-string [version {1 | 2c | 3 {auth | noauth | priv} [udp-port port]}

7.7.4 Verification Command Introduction

This command can be used to check the status of SNMP communication
Switch#show snmp

This command displays information about the SNMP view.
Switch#show snmp view

7.8 HTTP over IPV6

7.8.1 Introduction

The HTTP protocol works on a client-server architecture. The browser acts as an HTTP client and sends all requests to the HTTP server or web server through the URL.

7.8.2 Command Introduction

Configure the interface IPv6 address Switch(config-if)#ipv6 add {pv6-address prefix-length}
Enable HTTP service Switch A (config)#server http enable

7.8.3 Configuration Example

As shown in the figure, the PC is connected to Eth1 / 1 of SwitchA,

Device name	IPV6 address	Interface
SwitchA	2001::1/64	Eth1/1
PC	2001::2/64	Network port

Configuration ideas:
Create a VLAN, configure an IPv6 address, and enable the HTTP service globally.

Configuration steps:

(1) Enter the CLI interface and open the switch configuration management port ipv6 address / mask, http server

```
Switch A #configure terminal
Switch A (config)#int vlan 1
Switch A (config-if)#ipv6 add 2001::1/64
Switch A (config)#exit
Switch A (config)#server http enable
```

(2) Configure the IPv6 address of the PC and the IPv6 address of the switch on the same network segment, and enter the management port IP address in the URL field of the browser.

```
http://[2001::1]/home/login_ec.htm
```

8. Management

8.1 IP clustering (32 members)

8.1.1 Introduction

Switch Clustering is a method of grouping switches together to enable centralized management through a single unit. Switches that support clustering can be grouped together regardless of physical location or switch type, as long as they are connected to the same local network. Using Switch Clustering.

- A switch cluster has a primary unit called the “Commander” which is used to manage all other “Member” switches in the cluster. The management station can use either Telnet or the web interface to communicate directly with the Commander through its IP address, and then use the Commander to manage the Member switches through the cluster’s “internal” IP addresses.
- Clustered switches must be in the same Ethernet broadcast domain. In other words, clustering only functions for switches which can pass information between the Commander and potential Candidates or active Members through VLAN 4093.
- Once a switch has been configured to be a cluster Commander, it automatically discovers other cluster-enabled switches in the network. These “Candidate” switches only become cluster Members when manually selected by the administrator through the management station.

NOTE: Cluster Member switches can be managed either through a Telnet connection to the Commander, or through a web management connection to the Commander. When using a console connection, from the Commander CLI prompt, use the rcommand to connect to the Member switch.

Configure the topology:

8.1.2 Networking Ideas

(1) Confirm the MAC address of the switch
(2) Turn on the cluster function
(3) Add cluster member mac-address

8.1.3 Configuration

(1) View the MAC addresses of the two switches

```
SwitchA#show mac-address-table
 Interface MAC Address          VLAN Type        Life Time
 --------- ----------------- ---- -------- -----------------
 CPU          64-9D-99-10-0A-D2       1 CPU          Delete on Reset
```

```
SwitchB#show mac-address-table
 Interface MAC Address          VLAN Type        Life Time
 --------- ----------------- ---- -------- -----------------
   CPU          64-9D-99-10-0A-BC       1 CPU          Delete on Reset
```

(2) Enable the cluster function on the switch

```
SwitchA(config)#cluster
SwitchB(config)#cluster
```

(3) Enable the commander function on a switch

```
SwitchA(config)#cluster commander
```

(4) Add the member Mac addresses of the cluster on the commander switch

```
SwitchA(config)#cluster member mac-address 64-9D-99-10-0A-BC id 2
```

(5) Command verification

```
SwitchA#show cluster members
Cluster Members:
ID               : 2
Role             : Active member
IP Address    : 10.1.1.4
MAC Address : 64-9D-99-10-0A-BC
Description : S3900-48T4S
```

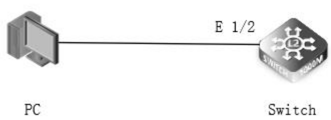
8.1.4 Verification

```
SwitchA#rcommand id 2
SwitchA#
        CLI session with the S3900-48T4S is opened.
        To end the CLI session, enter [Exit].
```

8.2 Firmware upgrade via TFTP/HTTP/FTP server

8.2.1 Introduction

Software upgrade is that users upload the files to be upgraded to the device for upgrade. After the upgrade is complete, the system will automatically restart and load to the latest upgrade version. TFTP/FTP/HTTP and other methods are provided for upgrade.



8.2.2 Configuration

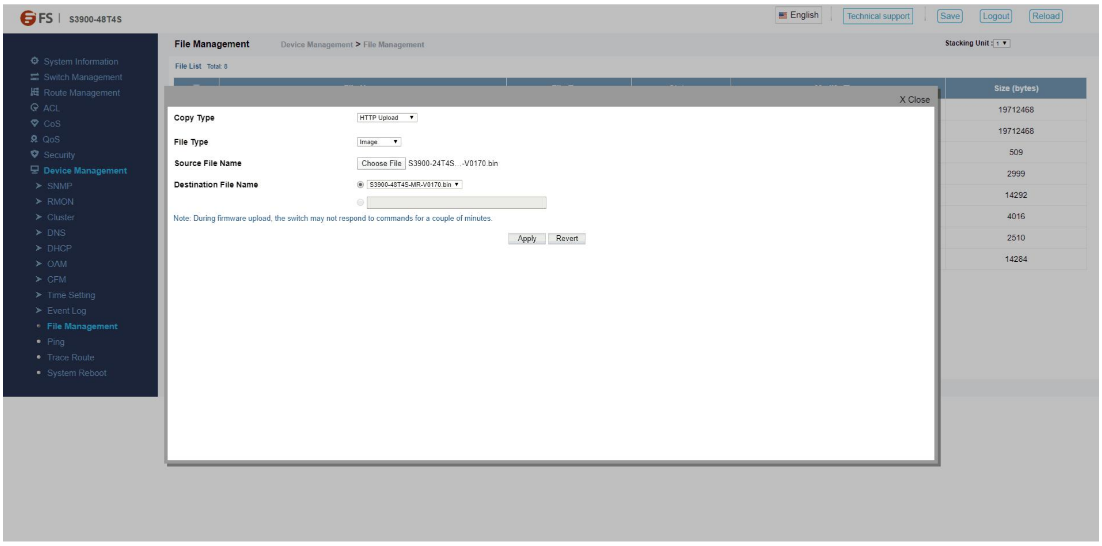
TFTP Configuration

Configure the same IP on the PC as the service port of the switch, and set the corresponding IP and directory on the TFTP software.

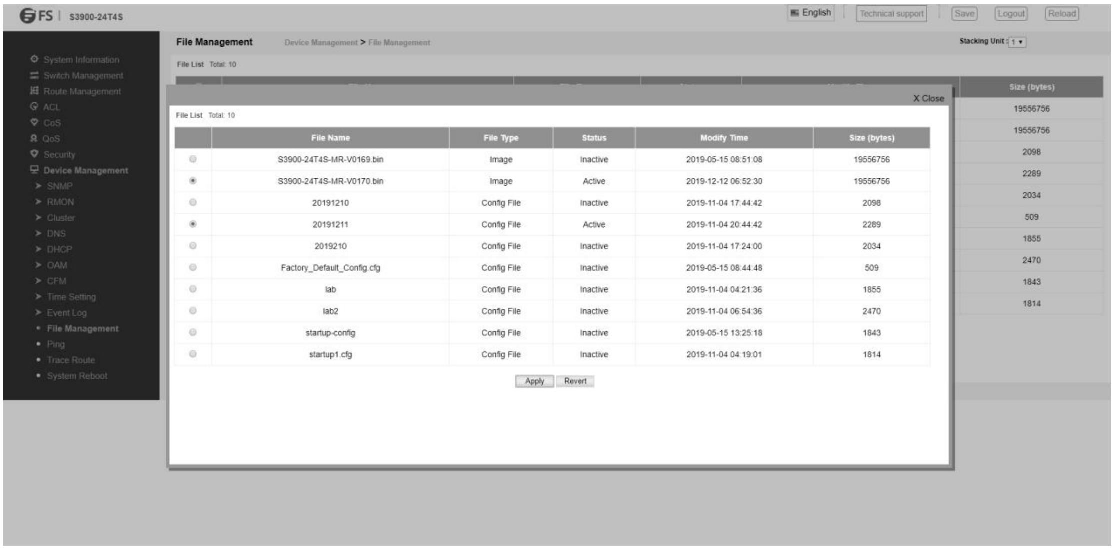
```
Switch#copy tftp file
Copy to which unit: <1-6>: 1
TFTP server IP address: 10.32.120.150
Choose file type:
  1. config; 2. image: 2
Source file name: S3900-24T4S-MR-V0170.bin
Destination file name: S3900-24T4S-MR-V0170.bin
Flash programming started.
Flash programming completed.
Success.
Switch#config t
Switch(config)#boot system image:S3900-24T4S-MR-V0170.bin
```

HTTP Configuration

Select HTTP upload in file management



Select firmware for next startup



FTP Configuration

Configure the same IP on the PC as the service port of the switch, and set the corresponding IP and directory on the FTP software.

```
Switch#copy ftp file
Copy to which unit: <1-6>: 1
FTP server IP address: 10.32.120.150
User [Anonymous]: admin
Password:
Choose file type:
  1. config; 2. image: 2
Source file name: S3900-24T4S-MR-V0170
Destination file name: S3900-24T4S-MR-V0170
Flash programming started.
Flash programming completed.
Success.
Switch#config t
Switch(config)#boot system image:S3900-24T4S-MR-V0170.bin
```

8.2.3 Verification

FTP/TFTP Verification

```
Switch#show version
Unit 1 ----------------------------
 Serial Number             : CG1903190122N0129
 Hardware Version          : 1.0
 Number of Ports           : 28
 Loader Version            : 1.4
 Operation Code Version : 1.7.0
```

HTTP Verification

8.3 Dual images

8.3.1 Introduction

Two firmwares can be stored in the flash of the switch. This prevents BUGs that affect normal services after the firmware is upgraded. The system can be rolled back in time, increasing network reliability.

8.3.2 Configuration

TFTP Configuration
Configure the same IP on the PC as the service port of the switch, and set the corresponding IP and directory on the TFTP software.

```
Switch#copy tftp file
Copy to which unit: <1-6>: 1
TFTP server IP address: 10.32.120.150
Choose file type:
  1. config; 2. image: 2
Source file name: S3900-24T4S-MR-V0170.bin
Destination file name: S3900-24T4S-MR-V0170.bin
Flash programming started.
Flash programming completed.
Success.
```

8.3.3 Configuration Verification

```
Switch#dir

Unit 1:
File Name                              Type     Status        Size       Modified
-------------------------------------------------------------------------------
FSOS-S3900-24T4S-MR-V0169R2.bin Image    InActive      19560852 2019-12-12 07:34:29
S3900-24T4S-MR-V0170.bin              Image    Active        19556756 2019-12-12 06:52:30
20191210                               Config InActive         2098 2019-11-04 17:44:42
20191211                               Config Active           2289 2019-11-04 20:44:42
2019210                                Config InActive         2034 2019-11-04 17:24:00
Factory_Default_Config.cfg             Config InActive          509 2019-11-04 04:18:53
lab                                    Config InActive         1855 2019-11-04 04:21:36
lab2                                   Config InActive         2470 2019-11-04 06:54:36
startup-config                         Config InActive         1843 2019-05-15 13:25:18
startup1.cfg                           Config InActive         1814 2019-11-04 04:19:01
```

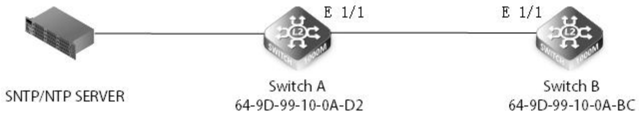
8.4 SNTP/NTP

8.4.1 Introduction

The SNTP / NTP client is connected to the SNTP/NTP server. They all have their own independent system clock. Now the system clock is automatically synchronized through SNTP/NTP.

8.4.2 Networking ideas

Connect PC to SNTP / NTP server, configure NTP protocol for time synchronization, and use NTP broadcast mode with authentication to meet customer needs.



8.4.3 Configuration

(1) NTP Configuration Command

```
Switch B#configure terminal
Switch B(config)#ntp client
Switch B(config)#ntp server 120.25.115.20
Switch B(config)#exit
```

(2) SNTP Configuration Command

```
Switch B#configure terminal
Switch B(config)#sntp client
Switch B(config)#sntp server 120.25.115.20
Switch B(config)#
Switch B(config)#exit
```

8.4.4 Verification

(1) NTP Verification

```
Switch B#show ntp
Current Time                    : Dec 12 03:38:18 2019
Polling                         : 1024 seconds
Current Mode                     : unicast
NTP Status                      : Enabled
NTP Authenticate Status    : Disabled
Last Update NTP Server      : 120.25.115.20              Port: 123
Last Update Time              : Dec 12 03:38:00 2019 UTC
NTP Server 120.25.115.20 version 3
```

(2) SNTP Verification

```
Switch B#show sntp
Current Time      : Dec 12 03:53:13 2019
Poll Interval    : 16 seconds
Current Mode      : Unicast
SNTP Status        : Enabled
SNTP Server        : 120.25.115.20
Current Server : 120.25.115.20
```

8.5 Ping

8.5.1 Introduction

The ping command is used to check the IP network connection and whether the host is reachable.

Format:
ping [ip] [*host address/name*] [count *count*] [size *size*]
ping [ipv6] [*host address/name*/X:X:X:X::X%<1-4094>] [count *count*] [size *size*]

8.5.2 Parameter Description

Parameter	Parameter Description	Value Ranges
ip	Internet protocol	/
ipv6	Sends ICMPv6 echo request packets to another host	/
count	Specifies the number of packets to send	1-16
size	Specifies the size of the data portion	32-512
host	Destination IP/IPv6 address or Destination host name	/
X:X:X:X::X%<1-4094>	Specifies IPv6 link-local address with ZoneID as the destination address	/

8.5.3 Networking Ideas

The ping command is the most common debugging tool used to detect the accessibility of network devices. It uses ICMP message information to detect:

- remote equipment availability;
- Round-trip delay in communication with remote host;
- Packet loss case;
- Whether the network connection is faulty；

8.5.4 Configuration Example

```
# Check whether the host with the IP address 10.32.120.97 is reachable.
Switch#ping ip 10.32.120.97
Press "ESC" to abort.
Ping to 10.32.120.97 by 5 32-byte payload ICMP packets, timeout is 3 seconds
response time: 0 ms
response time: 0 ms
response time: 0 ms
response time: 0 ms
response time: 0 ms
Ping statistics for 10.32.120.97:
  5 packets transmitted, 5 packets received (100%), 0 packets lost (0%)
Approximate round trip times:
  Minimum = 0 ms, Maximum = 0 ms, Average = 0 ms
Switch#
```

8.6 Traceroute

8.6.1 Introduction

Traceroute command is used to check the IP network connection and whether the host is reachable.

Format:
Traceroute [ip] [*host address/name*]
Traceroute [ipv6] [*host address/name/*X:X:X:X::X%<1-4094>] [max-failures/<cr>]

8.6.2 Parameter Description

Parameter	Parameter Description	Value Ranges
ip	Internet protocol	/
ipv6	Sends ICMPv6 echo request packets to another host	/
count	Specifies the number of packets to send	1-16

Parameter	Parameter Description	Value Ranges
size	Specifies the size of the data portion	32-512
host	Destination IP/IPv6 address or Destination host name	/
X:X:X:X::X%<1-4094>	Specifies IPv6 link-local address with ZoneID as the destination address	/
max-failures	Specifies the maximum number of consecutive timeouts allowed before termination	1-255

8.6.3 Networking ideas

For faults in the network, you can run the ping command to check the network connectivity based on the response packets. Then use the tracert command to view the location of the fault in the network to provide a basis for fault diagnosis.

8.6.4 Configuration example

```
# Check whether the host with the IP address 10.32.120.97 is reachable.
Switch-2#traceroute ip 10.32.133.42
Press "ESC" to abort.
Traceroute to 10.32.133.42, 30 hops max, timeout is 3 seconds
Hop Packet 1 Packet 2 Packet 3 IP Address
--- -------- -------- -------- ---------------
  1    <10 ms    <10 ms    <10 ms 10.32.120.254
  2    <10 ms    <10 ms    <10 ms 10.32.133.42

Trace completed.
Switch-2#
```

8.6.5 Verification

Run the tracert command to find out that the network is faulty. The following information symbols may be output. The detailed information is as follows:

- * - No Response
- H - Host Unreachable
- N - Network Unreachable
- P - Protocol Unreachable
- O - Other

8.7 sFlow

8.7.1 Introduction

Flow Sampling (sFlow) can be used with a remote sFlow Collector to provide an accurate, detailed, and real-time type overview. The level of traffic present on the network. The sFlow agent samples one of the n packets from the switch, repacks these samples into sFlow packets, and sends them to the sFlow Collector. This sampling occurs at the internal hardware level, where all traffic can be seen, while traditional probes only have a partial traffic view when sampling on a monitored interface. Since no local analysis is performed, the processor and memory load imposed by the sFlow agent is minimal.

8.7.2 Parameter Description

sflow owner

This command creates an sFlow Collector on the switch. Use the no form to delete the sFlow receiver.

sflow polling

This command enables the sFlow polling data source for the specified interface. The data source polls periodically according to the specified interval. Use the no form to delete the polled data source instance from the sFlow configuration of the switch.

sflow sampling

This command enables an sFlow data source instance for a specific interface, which is periodically sampled based on the number of packets processed. Use noform to delete the sample data source instance from the sFlow configuration of the switch.

8.7.3 Configuration

Configuration sflow owner

sflow owner *owner-name* timeout *timeout-value* [destination *{ipv4-address* | *ipv6-address}*][port*destination-udp-port*][max-datagram-size*max-datagram-size*] [version {v4 | v5}]

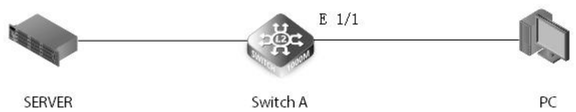
Parameter Description

Parameter	Parameter Description	Value Ranges
name	Name of the collector	1-30
timeout-value	The length of time the sFlow interface is available to send samples to a receiver, after which the owner and associated polling and sampling data source instances are removed from the configuration.	30-10000000
ipv4-address	IPv4 address of the sFlow collector.	/
ipv6-address	IPv6 address of the sFlow collector.	/
destination-udp-port	The UDP port on which the collector is listening for sFlow streams.	1-65535
max-datagram-size	The maximum size of the sFlow datagram payload.	200-1500
version {v4 | v5}	Sends either v4 or v5 sFlow datagrams to the receiver.	

Default Configuration:

No owner is configured
UDP Port: 6343
Version: v4
Maximum Datagram Size: 1400 bytes

Configuration example:



Sflow collector created on the switch

```
Switch(config)#sflow owner stat_server1 timeout 100 destination 192.168.220.225 port 22500 max-datagram-size 512 version v5
```

Configuration sflow polling
sflow polling {interface ethernet *unit/port*} instance *instance-id* receiver *owner-name* polling-interval *seconds*

Parameter Description

Parameter	Parameter Description	Value Ranges
interface	The source from which the samples will be taken at specified intervals and sent to a collector.	/
ethernet unit/port	unit - Unit identifier. port - Port number.	/
instance-id	An instance ID used to identify the sampling source.	1
owner-name	The associated receiver, to which the samples will be sent.	1-30
polling-interval	The time interval at which the sFlow process adds counter values to the sample datagram.	0-10000000

Default Configuration:
No sFlow polling instance is configured.

Configuration example:

This example sets the polling interval to 10 seconds.
Switch(config)#sflow polling interface ethernet 1/1 instance 1 receiver test polling-interval 10

Configuration sflow sampling
Format:
Sflow sampling {interface *interface*} instance *instance-id* receiver *owner-name* sampling-rate *sample-rate* [max-header-size *max-header-size*]
no sflow sample {interface *interface*} instance *instance-id*

Parameter Description

Parameter	Parameter Description	Value Ranges
interface	The source from which the samples will be taken at specified intervals and sent to a collector.	/
ethernet unit/port	unit - Unit identifier. port - Port number.	/
instance-id	An instance ID used to identify the sampling source.	1
owner-name	The associated receiver, to which the samples will be sent.	1-30
polling-interval	The time interval at which the sFlow process adds counter values to the sample datagram.	0-10000000
sample-rate	The packet sampling rate, or the number of packets out of which one sample will be taken.	256-16777215
max-header-size	The maximum size of the sFlow datagram header.	64-256

Default Configuration:

No sFlow sampling instance id configured.
Maximum Header Size: 128 bytes

Configuration example:

This example enables a sampling data source on Ethernet interface 1/1, an associated receiver named “owner1”, and a sampling rate of one out of 300. The maximum header size is also set to 200 bytes.
Switch(config)#sflow sampling interface ethernet 1/1 instance 1 receiver sampling-rate 300 max-header-size 200

View sflow command
This command shows the global and interface settings for the sFlow process.

Format:
show sflow [owner *owner-name* | interface *interface*]

Parameter Description:

Parameter	Parameter Description	Value Ranges
owner-name	The associated receiver, to which the samples will be sent.	1-30
ethernet unit/port	unit - Unit identifier. port - Port number.	/

Configuration example:

Switch#show sflow interface ethernet 1/1
Switch#show sflow owner stat_server1 interface ethernet 1/1

https://www.fs.com

All statements, technical information, and recommendations related to the products here are based upon information believed to be reliable or accurate. However, the accuracy or completeness thereof is not guaranteed, and no responsibility is assumed for any inaccuracies. Please contact FS for more information.