Ethernet Switching

QSR-1920, QSR-2920, QSR-3920

Оглавление

1. LINK AGGREGATION 5
1.1. Overview 5
1.1.1. Basic Concepts 5
1.1.2. Link Aggregation Modes 6
1.1.3. Load Balancing Modes of Aggregation Groups 7
1.2. Link Aggregation Function Configuration 8
1.2.1. Configure an Aggregation Group 8
1.2.2. Configure the Load Balancing Mode of an Aggregation Group 10
1.2.3. Configure LACP Priorities 11
1.2.4. Link Aggregation Monitoring and Maintaining 12
1.3. Typical Configuration Example of Link Aggregation 12
1.3.1. Configure a Static Aggregation Group 12
1.3.2. Configure a Dynamic Aggregation Group 15
2. PORT ISOLATION 19
2.1. Overview 19
2.2. Port Isolation Function Configuration 19
2.2.1. Configure Basic Functions of Port Isolation 19
2.2.2. Port Isolation Monitoring and Maintaining 21
2.3. Typical Configuration Example of Port Isolation 21
2.3.1. Configure Port Isolation 21
3. VLAN 23
3.1. Overview 23
3.2. VLAN Function Configuration 24
3.2.1. Configure Basic Attributes of VLANs 24
3.2.2. Configure a Port-Based VLAN 25
3.2.3. VLAN Monitoring and Maintaining 30
3.3. VLAN Typical Configuration Example 31
3.3.1. Configure Port-Based VLANs 31
3.3.2. Configure MAC-Based VLANs 33
3.3.3. Configure IP Subnet-Based VLANs 35
3.3.4. Configure Protocol-Based VLANs 37
4. MAC ADDRESS TABLE MANAGEMENT 40
4.1. Overview 40
4.2. MAC Address Management Function Configuration 41
4.2.1. Configure Management Properties of MAC Addresses 41
4.2.2. Configure MAC Address Learning Limitation 42

4.2.3. Configure Static MAC Addresses 45
4.2.4. MAC Address Management Monitoring and Maintaining 46
5. SPANNING TREE 48
5.1. Overview 48
5.2. Spanning Tree Function Configuration 51
5.2.1. Configure Basic Functions of a Spanning Tree 53
5.2.2. Configure Bridge Properties 54
5.2.3. Configure Spanning Tree Port Properties 57
5.2.4. Configure the Working Mode of a Spanning Tree 64
5.2.5. Configure the Spanning Tree Protection Function 65
5.2.6. Spanning Tree Monitoring and Maintaining 71
5.3. Spanning Tree Typical Configuration Example 72
5.3.1. MSTP Typical Application 72
6. LOOPBACK DETECTION 80
6.1. Overview 80
6.2. Loopback Detection Function Configuration 80
6.2.1. Configure Basic Functions of Loopback Detection 80
6.2.2. Configure Basic Parameters of Loopback Detection 82
6.2.3. Loopback Detection Monitoring and Maintaining 84
6.3. Typical Configuration Example of Loopback Detection 84
6.3.1. Configure Remote Loopback Detection 84
6.3.2. Configure Local Loopback Detection 87
7. ERROR-DISABLE MANAGEMENT 91
7.1. Overview 91
7.2. Error-Disable Management Function Configuration 91
7.2.1. Configure Error-Disable Basic Functions 91
7.2.2. Configure Error-Disable Automatic Recovery 92
7.2.3. Error-Disable Management Monitoring and Maintaining 93
7.3. Typical Configuration Example of Error-Disable Management 93
7.3.1. Combination of Error-Disable, Port Security and Storm Suppression 93
8. VOICE-VLAN 98
8.1. Overview 98
8.2. Voice-VLAN Function Configuration 98
8.2.1. Configure a Voice-VLAN 98
8.2.2. Configure an OUI Address 99
8.2.3. Configure the Aging Time 99
8.2.4. Enable the Voice-VLAN Function 100

8.2.5. Configure the Voice-VLAN Working Mode on the Port 101
8.2.6. Configure Voice-VLAN Security 102
8.2.7. Voice-VLAN Monitoring and Maintaining 103
8.3. Voice-VLAN Typical Configuration Example 103
8.3.1. Configure a Voice-VLAN to Manual Mode 103
8.3.2. Configure a Voice-VLAN to Automatic Mode 105
8.3.3. Configure Voice-VLAN Security Mode 108
9. ОБЩАЯ ИНФОРМАЦИЯ 111
9.1. Замечания и предложения 111
9.2. Гарантия и сервис 111
9.3. Техническая поддержка 111

1. LINK AGGREGATION

1.1. Overview

Through link aggregation, multiple physical links between two devices are bound to form a logic link so as to expand link capacity. Within the logic link, the physical links act as redundancy and dynamic backup of each other, providing higher network connection reliability.

1.1.1. Basic Concepts

Aggregation Group and Member Ports

Multiple physical ports are bound to form an aggregation group, and the physical ports are member ports of the aggregation group.

Member Port Status

The member ports of an aggregation group have the following two statuses:

- Selected: The member ports which are in this status can participate in user service traffic forwarding. The member ports in this status are called "the selected ports".
- Unselected: The member ports which are in this status cannot participate in user service traffic forwarding. The member ports in this status are called "the unselected ports".

The rate and duplex mode of an aggregation group is determined by the selected ports in the aggregation group. The rate of an aggregation group is the sum of all selected ports, and the duplex mode of the aggregation group is the same as the duplex mode of the selected ports.

Operation Key

An operation key is the property configuration of member ports. It consists of the rate, duplex mode, and administrative key (that is, the aggregation group number). In property configuration, change of the duplex mode or rate may cause re-calculation of the operation key.

In one aggregation group, if the duplex mode or rate of member ports are different, then the generated operation keys are different. However, the member ports that are in the selected status must have the same operation key.

LACP

Link Aggregation Control Protocol (LACP) is a protocol that is based on IEEE802.3ad. The LACP protocol exchanges messages with the peer end via the Link Aggregation Control Protocol Data Unit (LACPDU).

LACP Priorities

LACP priorities are categorized into two types: system LACP priorities and port LACP priorities.

- System LACP priorities: They are used to determine the LACP priority order of the devices at two ends.
- Port LACP priorities: They are used to determine the priority order at which the member ports of the local device are selected.

System ID and Port ID

System ID: Aggregation property of a device. It consists of the system LACP priority of the device and the system MAC address. The higher the system LACP priority is, the better the system ID of the device is. If the system LACP priorities are the same, then the smaller the system MAC address is, the better the system ID of the device is.

Port ID: Aggregation property of a port. It consists of the port LACP priority and the port number. The higher the port LACP priority is, the better the port ID is. If the port LACP priorities are the same, then the smaller the port number is, the better the port ID is.

Root Port of an Aggregation Group

The protocols that are applied in an aggregation group receive and send protocol packets through the root port of the aggregation group. The root port of an aggregation group is selected from the member ports of the aggregation group. The physical link of the root port must be in the up status.

1.1.2. Link Aggregation Modes

Link aggregation modes include the static aggregation mode and the dynamic aggregation mode. Aggregation groups are categorized into static aggregation groups and dynamic aggregation groups.

Static Aggregation Mode

In static aggregation mode, the LACP protocol of the member ports of the devices at the two ends are in the disabled status. In the static aggregation group of the local device, set the selected and unselected status for the member ports by following the guidelines as described below:

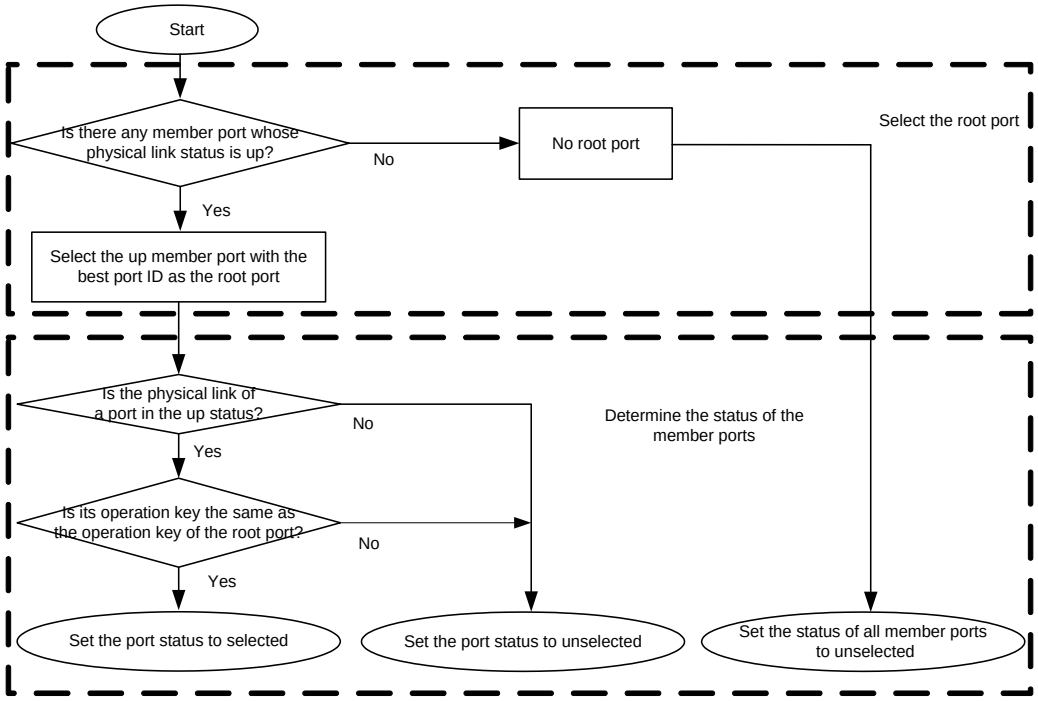


Figure 1-1 Setting the status of member ports in static aggregation mode

Dynamic Aggregation Mode

In dynamic aggregation ports, a port can join in a dynamic aggregation group in two modes, active or passive.

- If the duplex mode of the port is full duplex:

If the port joins in a dynamic aggregation group in active mode, the LACP protocol is enabled for the port.

If the port joins in a dynamic aggregation group in passive mode, the LACP protocol is disabled for the port. After it receives the LACPDU packets from the peer port, the LACP protocol is enabled.

- If the duplex mode of the port is half duplex, no matter the port joins in a dynamic aggregation group in either mode, the LACP protocol is disabled for the port.

In the dynamic aggregation group, set the selected and unselected status for the member ports by following the guidelines as described below:

First determine the device with a better system ID. Then the device determines the statuses of the member ports of the devices at the two ends. The device with the better system ID sets the selected and unselected status for the member ports by following the guidelines as described below:

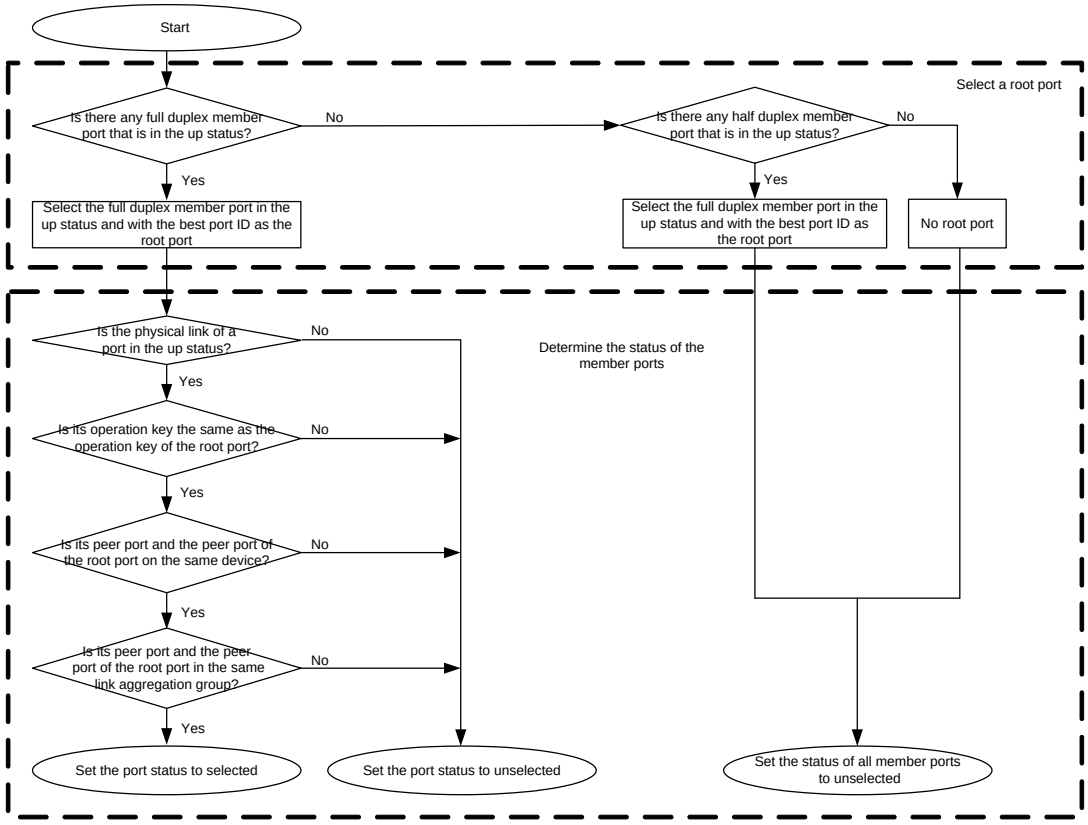


Figure 1-2 Setting the Status of member ports in dynamic aggregation mode

1.1.3. Load Balancing Modes of Aggregation Groups

Six load balancing modes are available, and users can select a mode according to the actual requirement.

- Load balancing based on the destination MAC addresses: The aggregation group implements aggregated load balancing based on the destination MAC addresses of packets.
- Load balancing based on the source and destination MAC addresses: The aggregation group implements aggregated load balancing based on the source and destination MAC addresses of packets.
- Load balancing based on the source MAC addresses: The aggregation group implements aggregated load balancing based on the source MAC addresses of packets.
- Load balancing based on the destination IP addresses: The aggregation group implements aggregated load balancing according to the destination IP addresses of packets.

- Load balancing based on the source and destination IP addresses: The aggregation group implements aggregated load balancing based on the source and destination IP addresses of packets.
- Load balancing based on the source IP addresses: The aggregation group implements aggregated load balancing based on the source IP addresses of packets.

1.2. Link Aggregation Function Configuration

Table 1-1 Link aggregation function list

Configuration Tasks	
Configure an aggregation group.	Create an aggregation group.
	Add ports into the aggregation group.
Configure the load balancing mode of the aggregation group.	Configure the load balancing mode of the aggregation group.
Configure LACP priorities.	Configure the system LACP priority.
	Configure the port LACP priority.

1.2.1. Configure an Aggregation Group

After configuring an aggregation group, you can manage multiple physical ports in a centralized manner. Any configuration on the aggregation group will be applied to each member port.

Note:

- A device supports a maximum of 32 aggregation groups, a maximum of 8 ports can join in the aggregation group at the same time, and a maximum of 8 ports can be in the selected status at the same time.

Configuration Condition

None

Create an Aggregation Group

The aggregation groups at the two ends of an aggregated link must be configured to the same type. Description can be added to each aggregation group to make it easier for network administrators to distinguish the aggregation groups.

Table 1-2 Creating an aggregation group

Step	Command	Description
Enter the global configuration mode.	**configure terminal**	-
Create an aggregation group.	**link-aggregation** *link-aggregation-id* **mode** { **manual** | **lacp** }	Mandatory. By default, no aggregation group is created.
Enter the aggregation group configuration mode.	**link-aggregation** *link-aggregation-id*	-
Configure the description for the aggregation group.	**description** *description-name*	Optional. By default, no description is added to the aggregation group.

Caution:

- The protocols that are applied in an aggregation group receive and send protocol packets through the root port of the aggregation group. In static aggregation mode, because the member ports between the devices at two ends do not exchange LACPDU packets, the root ports of the two devices may be on different physical links. As a result, other protocol packets on the aggregation group may fail to be received or sent. To prevent this problem, ensure that the root ports of the devices at the two ends are on the same physical link. In dynamic aggregation mode, the member ports of the devices at two ends exchange LACPDU packets. The negotiation between the two member ports ensures that the root ports of the two devices are on the same physical link.
- After an aggregation group is deleted, all the member ports of the aggregation group are removed from the aggregation group, and then the all the member ports adopt the default settings. This may result in loops in the network. Therefore, before deleting an aggregation group, ensure that the spanning tree function has been enabled or ensure that no loop may occur in the network.

Add Ports into the Aggregation Group

When an aggregation group is created, it is only a logic interface which contains no physical port. In this case, the aggregation function does not take effect. The aggregation function takes effect after ports are added to a static aggregation group. The aggregation function takes effect after local or peer ports are added into a dynamic aggregation group.

Table 1-3 Adding a port into the aggregation group

Step	Command	Description
Enter the global configuration mode.	**configure terminal**	-
Enter the layer-2 Ethernet interface configuration mode.	**interface** *interface-name*	-
Add the port into the aggregation group.	**link-aggregation** *link-aggregation-id* { **manual** | **active** | **passive** }	By default, a port is not added into any aggregation group.

Note:

- Before adding a port into an aggregation group, the aggregation group must have been created; otherwise, an error message is displayed.
- A port can be added one aggregation group at a time.
- After a port is added into an aggregation group, the some existing configurations (such as loopback detection and VLAN) will be removed from the port.
- Some functions (such as loopback detection) cannot be configured on a member port in an aggregation group; otherwise, an error message is displayed.
- If a port is added into a dynamic aggregation group in passive mode, its peer port must be added into the dynamic aggregation group in active mode. Otherwise, the two ports are both in the unselected status and they cannot participate in user service traffic forwarding.

1.2.2. Configure the Load Balancing Mode of an Aggregation Group

By configuring the load balancing mode of an aggregation group, you can achieve load balancing of service traffic in the aggregation group in a flexible manner.

Configuration Condition

None

Configure the Load Balancing Mode of the Aggregation Group

Table 1-4 Configuring the load balancing mode of the aggregation group

Step	Command	Description
Enter the global configuration mode.	**configure terminal**	-
Configure the load balancing mode of the aggregation group.	**link-aggregation** *link-aggregation-id* **load-balance** {**dst-ip | dst-mac | src-dst-ip | src-ip | src-dst-mac | src-mac** }	Mandatory. By default, the aggregation group implements aggregated load balancing based on the source MAC addresses of packets.

1.2.3. Configure LACP Priorities

Configuration Condition

None

Configure the System LACP Priority

Configuration of the system LACP priority may affect the system ID, and finally affect the selected/unselected status of member ports of dynamic aggregation groups.

Table 1-5 Configuring the system lacp priority

Step	Command	Description
Enter the global configuration mode.	**configure terminal**	-
Configure the system LACP priority.	**lacp system-priority** *system-priority-value*	Mandatory. By default, the system LACP priority is 32768.

Configure the Port LACP Priority

Configuration of the port LACP priority may affect the port ID, and finally affect the selected/unselected status of member ports of aggregation groups.

Table 1-6 Configuring the port LACP priority

Step	Command	Description
Enter the global configuration mode.	**configure terminal**	-
Enter the layer-2 Ethernet interface configuration mode.	**interface** *interface-name*	-
Configure the port LACP priority.	**lacp port-priority** *port-priority-value*	Mandatory. By default, the port LACP priority is 32768.

1.2.4. Link Aggregation Monitoring and Maintaining

Table 1-7 Link Aggregation monitoring and maintaining

Command	Description
show link-aggregation group [*link-aggregation-id*]	Displays brief information about a specified aggregation group or all existing aggregation groups.
show link-aggregation interface [*interface-name*]	Displays the details of a specified member port of an aggregation group or details of all member ports of the aggregation group.

1.3. Typical Configuration Example of Link Aggregation

1.3.1. Configure a Static Aggregation Group

Network Requirements

- Device1 is connected to PC1, Device2 is connected to PC2 and PC3, and the three PCs are in the same network segment. Device1 and Device2 are interconnected through Trunk ports.
- A static aggregation group is configured between Device1 and Device2 for bandwidth increase, load sharing, and service backup.

Network Topology

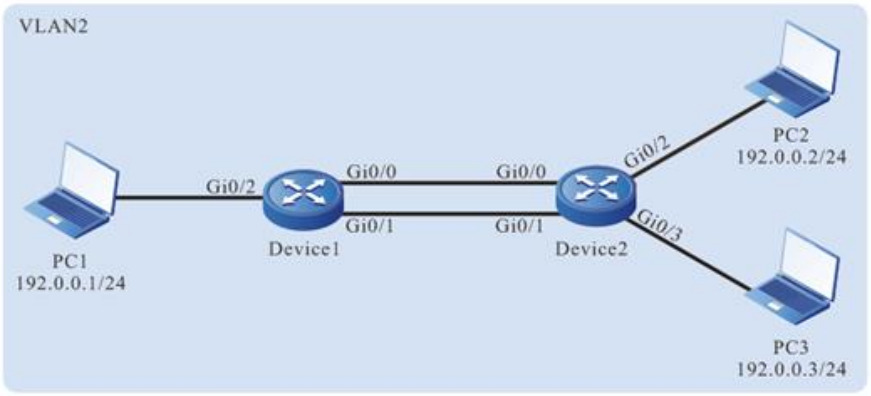


Figure 1-3 Networking for configuring a static aggregation group

Configuration Steps

Step 1: Create a static aggregation group.

#On Device1, create static aggregation group 1.

```
Device1#configure terminal
Device1(config)#link-aggregation 1 mode manual
Device1(config)#exit
```

#On Device2, create static aggregation group 2.

```
Device2#configure terminal
Device2(config)#link-aggregation 1 mode manual
Device2(config)#exit
```

Step 2: Add ports into the aggregation group.

#On Device1, add ports gigabitethernet0/0 and gigabitethernet0/1 into aggregation group 1 in Manual mode.

```
Device1(config)#interface gigabitethernet 0/0,0/1
Device1(config-if-range)#link-aggregation 1 manual
Device1(config-if-range)#exit
```

#On Device2, add ports gigabitethernet0/0 and gigabitethernet 0/1 into aggregation group 1 in Manual mode.

```
Device2(config)#interface gigabitethernet 0/0,0/1
Device2(config-if-range)#link-aggregation 1 manual
Device2(config-if-range)#exit
```

#After the configuration is completed, check the status of aggregation group 1 on the devices.

Here takes Device1 for example:

```
Device#show link-aggregation group 1
 Link Aggregation 1
  Mode: Manual   Description:
  Load balance method: src-mac
  Number of ports in total: 2
  Number of ports attached: 2
  Root port: gigabitethernet0/0
  gigabitethernet0/0: ATTACHED
  gigabitethernet0/1: ATTACHED
```

According to the system display, ports gigabitethernet 0/0 and gigabitethernet 0/1are both in the ATTACHED state in aggregation group 1, and aggregation of aggregation group 1 is successful.

Note:

- For the method of checking Device2, refer to the method of checking Device1.

Step 3: Configure the load balancing mode of the aggregation group.

#On Device1, configure the load balancing mode of aggregation group 1 to the dst-mac mode.

Device1(config)#link-aggregation 1 load-balance dst-mac

Step 4: Configure a VLAN, and configure the link type of the aggregation group and ports.

#On Device1, create VLAN2, configure the VLAN of aggregation group 1 to Trunk and allow services of VLAN2 to pass, and set Port VLAN ID (PVID) to 2.

```
Device1(config)#vlan 2
Device1(config-vlan2)#exit
Device1(config)#link-aggregation 1
Device1(config-link-aggregation1)#switchport mode trunk
Device1(config-link-aggregation1)#switchport trunk allowed vlan add 2
Device1(config-link-aggregation1)#switchport trunk pvid vlan 2
Device1(config-link-aggregation1)#exit
```

#On Device1, configure the VLAN of port gigabitethernet0/2 to Access and allow services of VLAN2 to pass.

```
Device1(config)#interface gigabitethernet 0/2
Device1(config-if-gigabitethernet0/2)#switchport mode access
Device1(config-if-gigabitethernet0/2)#switchport access vlan 2
Device1(config-if-gigabitethernet0/2)#exit
```

#On Device2, create VLAN2, configure the VLAN of aggregation group 1 to Trunk and allow services of VLAN2 to pass, and set PVID to 2. (Omitted)

#On Device2, configure the VLAN of ports gigabitethernet 0/2 and gigabitethernet 0/3 to Access and allow services of VLAN2 to pass. (Omitted)

Step 5: Check the result.

#On the devices, check the aggregated bandwidth of aggregation group 1.

Here takes Device1 for example:

```
Device1#show link-aggregation 1
link-aggregation 1 configuration information
    Description     :
    Status          : Enabled
    Link            : Up
    Act Speed       : 2000
    Act Duplex      : Full
    Port Type       : Nni
    Pvid            : 1
```

According to the system display, the interface bandwidth of aggregation group on Device1 is 2000M.

Note:

- For the method of checking Device2, refer to the method of checking Device1.

#On Device1, check the current load balancing mode.

```
Device1#show link-aggregation group 1
```

```
Link Aggregation 1
Mode: Manual   Description:
Load balance method: dst-mac
Number of ports in total: 2
Number of ports attached: 2
Root port: gigabitethernet0/0
gigabitethernet0/0: ATTACHED
gigabitethernet0/1: ATTACHED
```

According to the system display, the current load balancing mode of aggregation group 1 is dst-mac.

#During the process of service interaction between PC1 and PC2 and PC3, load balancing of data is achieved on the aggregated links. If a link in the aggregation group becomes faulty, the remaining links can perform the service backup.

1.3.2. Configure a Dynamic Aggregation Group

Network Requirements

- Device1 is connected to PC1, Device2 is connected to PC2 and PC3, and the three PCs are in the same network segment. Device1 and Device2 are interconnected through Trunk ports.
- A dynamic aggregation group is configured between Device1 and Device2, so as to realize the functions of adding bandwidth, load balance and service backup.

Network Topology

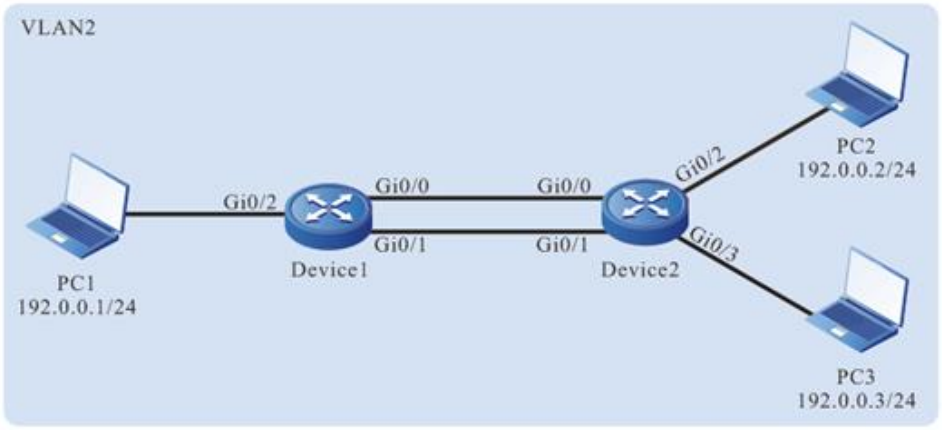


Figure 1-4 Networking for configuring a dynamic aggregation group

Configuration Steps

Step 1: Create a dynamic aggregation group.

#On Device1, create dynamic aggregation group 1.

```
Device1#configure terminal
Device1(config)#link-aggregation 1 lacp
Device1(config)#exit
```

#On Device2, create dynamic aggregation group 1.

```
Device2#configure terminal
Device2(config)#link-aggregation 1 lacp
Device2(config)#exit
```

Step 2: Add ports into the aggregation group.

#On Device1, add ports gigabitethernet0/0 and gigabitethernet0/1 into aggregation group 1 in Active mode.

```
Device1(config)#interface gigabitethernet 0/0,0/1
Device1(config-if-range)#link-aggregation 1 active
Device1(config-if-range)#exit
```

#On Device2, add ports gigabitethernet0/0 and gigabitethernet0/1 into aggregation group 1 in Active mode.

```
Device2(config)#interface gigabitethernet 0/0,0/1
Device2(config-if-range)#link-aggregation 1 active
Device2(config-if-range)#exit
```

#After the configuration is completed, check the status of aggregation group 1 on the devices.

Here takes Device1 for example:

```
Device1#show link-aggregation group 1
Link Aggregation 1
  Mode: LACP   Description:
  Load balance method: src-mac
  Number of ports in total: 2
  Number of ports attached: 2
  Root port: gigabitethernet0/0
  gigabitethernet0/0: ATTACHED
  gigabitethernet0/1: ATTACHED
```

According to the system display, ports gigabitethernet0/0 and gigabitethernet0/1 are both in the ATTACHED state in aggregation group 1, and aggregation of aggregation group 1 is successful.

#View the aggregation bandwidth of the aggregation group 1 on the device.

Here takes Device1 for example:

```
Device1#show link-aggregation 1
link-aggregation 1 configuration information
    Description     :
    Status          : Enabled
    Link            : Up
    Act Speed       : 2000
```

```
Act Duplex      : Full
Port Type       : Nni
Pvid            : 1
```

It can be viewed that the interface bandwidth of aggregation group on Device1 is 2000M.

Note:

- For the method of checking Device2, refer to the method of checking Device1.

Step 3: Configure the load balancing mode of the aggregation group.

#On Device1, configure the load balancing mode of aggregation group 1 to the dst-mac mode.

```
Device1(config)#link-aggregation 1 load-balance dst-mac
```

Step 4: Configure a VLAN, and configure the link type of the aggregation group and ports.

#On Device1, create VLAN2, configure the VLAN of aggregation group 1 to Trunk and allow services of VLAN2 to pass, and set PVID to 2.

```
Device1(config)#vlan 2
Device1(config-vlan2)#exit
Device1(config)#link-aggregation 1
Device1(config-link-aggregation1)#switchport mode trunk
Device1(config-link-aggregation1)#switchport trunk allowed vlan add 2
Device1(config-link-aggregation1)#switchport trunk pvid vlan 2
Device1(config-link-aggregation1)#exit
```

#On Device1, configure the VLAN of port gigabitethernet 0/2 to Access and allow services of VLAN2 to pass.

```
Device1(config)#interface gigabitethernet 0/2
Device1(config-if-gigabitethernet0/2)#switchport mode access
Device1(config-if-gigabitethernet0/2)#switchport access vlan 2
Device1(config-if-gigabitethernet0/2)#exit
```

#On Device2, create VLAN2, configure the VLAN of aggregation group 1 to Trunk and allow services of VLAN2 to pass, and set PVID to 2. (Omitted)

#On Device2, configure the VLAN of ports gigabitethernet0/2 and gigabitethernet0/3 to Access and allow the services of VLAN2 to pass. (Omitted)

Step 5: Check the result.

#On the devices, check the aggregated bandwidth of aggregation group 1.

Here takes Device1 for example:

```
Device1#show link-aggregation 1
link-aggregation 1 configuration information
```

```
Description    :
Status         : Enabled
Link           : Up
Act Speed      : 2000
Act Duplex     : Full
Port Type      : Nni
Pvid           :1
```

According to the system display, the interface bandwidth of the aggregation group on Device1 is 2000M.

Note:

- For the method of checking Device2, refer to the method of checking Device1.

#After the configuration is completed, check the current load balancing mode on Device1.

```
Device1#show link-aggregation group 1
 Link Aggregation 1
  Mode: LACP   Description:
  Load balance method: dst-mac
  Number of ports in total: 2
  Number of ports attached: 2
  Root port: gigabitethernet0/0
  gigabitethernet0/0: ATTACHED
  gigabitethernet0/1: ATTACHED
```

According to the system display, the current load balancing mode of aggregation group 1 is dst-mac.

#During the process of service interaction between PC1 and PC2 and PC3, load balancing of data is achieved on the aggregated links. If a link in the aggregation group becomes faulty, the remaining links can perform the service backup.

2. PORT ISOLATION

2.1. Overview

Port isolation is a security feature that is based on ports. According to the actual requirement, you can configure certain ports to be isolated from a specified port, that is, configure some isolated ports for a specified port. In this way, the packets that are received by the specified port cannot be forwarded to the isolated ports. This enhances the network security, and also provides a flexible networking scheme.

2.2. Port Isolation Function Configuration

Table 2-1 Port Isolation function list

Configuration Tasks	
Configure the basic function of port isolation.	Configure port isolation.

2.2.1. Configure Basic Functions of Port Isolation

The port isolation function realizes a unidirectional packet isolation. Assuming that port B is configured as the isolated port of port A, then if a packet whose target port is port B enters port A, the port is directly discarded. However, if a packet whose target port is port B enters port B, the port is normally forwarded. The isolated port can be a port or an aggregation group.

The port isolation is configured based on the isolation group.

- The ports in one isolation group are isolated from each other.

The ports in the isolation group can be configured as the ingress, egress, both mode, and the resolution is as follows:

Table 2-2 Configure mode forwarding table

Packet Ingress Port mode	**Packet Egress Port Mode**	**Forward Normally**
Ingress	ingress	Yes
ingress	egress	No
ingress	both	No
egress	ingress	Yes
egress	egress	Yes

Packet Ingress Port mode	Packet Egress Port Mode	Forward Normally
egress	both	Yes
both	ingress	Yes
both	egress	No
both	both	No

- The ports in the isolation group communicate with the ports not added to the isolation group normally.
- The ports in different isolation groups can communicate normally.

Configuration Condition

The isolation group is created.

Configure Port Isolation

Table 2-3 Configuring port isolation

Step	Command	Description
Enter the global configuration mode.	**configure terminal**	-
Enter the isolation group configuration mode.	**isolate group** *group-id*	Mandatory
Add the port to the isolation group	**interface** *interface-list* [**ingress | egress | both**]	Mandatory By default, the port is not added to isolation group.
Add the aggregation group to the isolation group	**link-aggregation** *link-aggregation-id* [**ingress | egress | both**]	Mandatory By default, the aggregation group is not added to the isolation group.

Note:

- When adding the port to the isolation group, you need to create the isolation group.

2.2.2. Port Isolation Monitoring and Maintaining

Table 2-4 Port isolation monitoring and maintenance

Command	Description
show isolate { **group [** *group-id*] **| interface** *interface-list* **| link-aggregation** *link-aggregation-id* }	Displays the configuration of port isolation.

2.3. Typical Configuration Example of Port Isolation

2.3.1. Configure Port Isolation

Network Requirements

- PC1 and PC2 are connected to Device, and they communicate with each other in VLAN2.
- On Device, port isolation has been configured; therefore, PC1 and PC2 cannot communicate with each other.

Network Topology

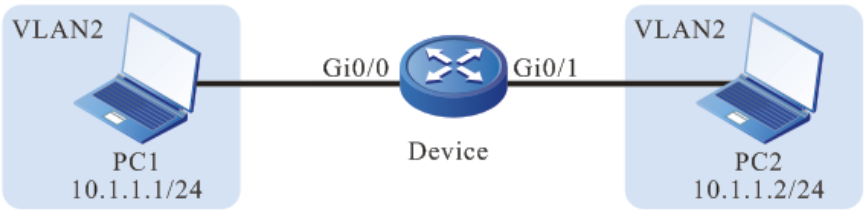


Figure 2-1 Networking for configuring port isolation

Configuration Steps

Step 1: Configure a VLAN, and configure the link type of the ports.

#On Device, create VLAN2.

```
Device#configure terminal
Device(config)#vlan 2
Device(config-vlan2)#exit
```

#On Device, configure the link type of ports gigabitethernet 0/0 and gigabitethernet 0/1 to Access and allow the services of VLAN2 to pass.

```
Device(config)#interface gigabitethernet 0/0-0/1
Device(config-if-range)#switchport mode access
Device(config-if-range)#switchport access vlan 2
Device(config-if-range)#exit
```

Step 2: Configure port isolation.

#On Device, configure port isolation between port gigabitethernet 0/0 and gigabitethernet 0/1.

```
Device(config)#isolate group 1
Device(config-isolate-group1)#interface gigabitethernet 0/0 both
Device(config-isolate-group1)#interface gigabitethernet 0/1 both
Device(config-isolate-group1)#exit
```

#On Device, query the port isolation information.

```
Device#show isolate group 1
------------------------------------------------------------
        isolate group 1
both members: gi0/0-0/1
```

Step 3: Check the result.

#PC1 and PC2 cannot communicate with each other.

3. VLAN

3.1. Overview

In a switched Ethernet, each port in the device is an independent collision domain, but all the ports belong to a broadcast domain. When a terminal device sends broadcast packets, all devices in the Local Area Network (LAN) can receive the packets. This not only wastes network bandwidth, but also brings hidden troubles.

Virtual Local Area Network (VLAN) is a technology through which devices in the same LAN can be divided in a logic manner. The devices in the same VLAN can communicate with each other at layer 2, while the devices from different VLANs are isolated at layer 2. In this way, broadcast packets are limited within a VLAN.

VLANs comply with IEEE 802.1Q. This standard defines a new frame encapsulation format, in which a 4-byte VLAN tag containing VLAN information is added after the source MAC address of a traditional data frame.

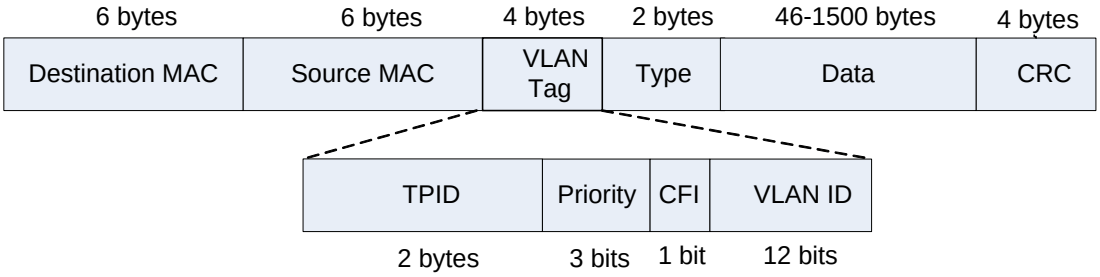


Figure 3-1 IEEE 802.1Q frame encapsulation format

A VLAN tag contains the following four fields:

- Tag Protocol Identifier (TPID): It is used to determine whether a VLAN tag is carried by the data frame. The length is 2 bytes, and the value is fixed to be 0x8100, indicating a standard 802.1Q tag.
- Priority: It is the 802.1p priority. The length is 3 bits and the value range is 0-7. Packets with different priorities can obtain services of different levels.
- Canonical Format Indicator (CFI): It indicates whether the MAC address is encapsulated in a standard format for transmission in different media. The length is 1 bit. The value 0 indicates that the MAC address is encapsulated in a standard format while the value 1 indicates that the MAC address is encapsulated in a non-standard format.
- VLAN ID: It indicates the VLAN to which the packet belongs. The length is 12 bits, and the value range is 0-4095, where 0 and 4095 are protocol reserved values, and the available VLAN IDs are in the range of 1-4094.

VLANs has the following advantages:

- Establishes virtual workgroups flexibly. Users with the same requirements can be divided into one VLAN, without being limited by their physical locations.
- Limits broadcast domains. A VLAN is a broadcast domain. Layer-2 unicast, multicast, and broadcast frames can be forwarded only within the domain, and they cannot enter other VLANs directly. This prevents broadcast storms.
- Improves the network security. Different VLANs are isolated at layer two, and the VLANs cannot communicate with each other directly.

According to applications, VLANs are categorized into the following four types:

- Port-based VLANs

- MAC address-based VLANs
- IP subnet-based VLANs
- Protocol-based VLANs

By default, in the order of priorities from high to low, the four types of VLANs are: MAC address-based VLANs, IP subnet-based VLANs, protocol-based VLANs, and port-based VLANs. On one port, the VLANs takes effect according to the priority levels, and only one type of VLAN takes effect.

3.2. VLAN Function Configuration

Table 3-1 VLAN function list

Configuration Tasks	
Configuring basic attributes of VLANs	Configure a VLAN.
	Configure the VLAN name.
Configure a port-based VLAN.	Configure the port link type.
	Add an Access port into the VLAN.
	Configure a Trunk port to allow services of a VLAN to pass.
	Add a Hybrid port into the VLAN.
	Configure PVIDs for ports.

3.2.1. Configure Basic Attributes of VLANs

Configuration Condition

None

Configure a VLAN

Each VLAN corresponds to a broadcast domain. The users in the same VLAN can communicate with each other at layer 2, while users from different VLANs are isolated from each other at layer 2.

Table 3-2 Configuring a VLAN

Step	Command	Description
Enter the global configuration mode.	**configure terminal**	-

Step	Command	Description
Create a VLAN.	**vlan** *vlan-list*	Mandatory. By default, the system automatically creates VLAN1. In creating a single VLAN, after a VLAN is created, you will enter the VLAN configuration mode. In creating multiple VLANs, after a VLAN is created, you are still in the current configuration mode.

Configure the VLAN Name

To facilitate memory and management, you can configure the name of a VLAN according to the service type, function, and connection of the VLAN.

Table 3-3 Configure the VLAN name.

Step	Command	Description
Enter the global configuration mode.	**configure terminal**	-
Enters the VLAN configuration mode.	**vlan** *vlan-id*	-
Configure the VLAN name.	**name** *vlan-name*	Mandatory. By default, the name of VLAN1 is DEFAULT, and the names of other VLANs follow the format "VLAN*vlan-id*", such as VLAN100.

3.2.2. Configure a Port-Based VLAN

A port-based VLAN, also called port VLAN, is a VLAN of the simplest division type. After a port is added into the VLAN, the port can forward packets that belong to the VLAN.

Configuration Condition

None

Configure the Port Link Type

A port handles VLAN tags in different modes before it forwards packets. According to the VLAN tag handling modes, the following three link types are available:

- Access type: The packets that have been forwarded do not carry VLAN tags. Ports of this type are usually connected to user devices.
- Trunk type: The packets from the VLANs in which the PVID is located do not carry VLAN tags, while the packets from other VLANs still carry VLAN tags.
- Hybrid type: The packets from the specified VLAN can be configured not to carry or carry VLAN tags. Ports of the type can be connected to user devices or interconnected with network devices.

The ports of the Trunk type and the ports of the Hybrid type cannot be converted to each other directly. They need to be converted to the Access type before being converted to another type.

Table 3-4 Configuring the port link type

Step	Command	Description
Enter the global configuration mode.	**configure terminal**	-
Enter the layer-2 Ethernet interface configuration mode.	**interface** *interface-name*	Either. After you enter the layer-2 Ethernet interface configuration mode, the subsequent configuration takes effect only on the current port. After you enter the aggregation group configuration mode, the subsequent configuration takes effect only within the aggregation group.
Enter the aggregation group configuration mode.	**link-aggregation** *link-aggregation-id*	
Configure the port link type.	**switchport mode** { **access** | **hybrid** | **trunk** }	Mandatory. By default, the port link type is the Access type.

Caution:

- Some commands can be configured only on the ports with the specified link type, therefore, if the port link type is converted to another type, the functions that are configured on the port with the original link type may become invalid.

Add an Access Port into the VLAN

One Access port can belong to only one VLAN. When an Access port is added into a specified VLAN, it exits from the current VLAN and then enters the specified VLAN. If the VLAN to which the Access port is to be added does not exists, the VLAN is automatically created.

Table 3-5 Adding an access port into the VLAN

Step	Command	Description
Enter the global configuration mode.	**configure terminal**	-
Enter the layer-2 Ethernet interface configuration mode.	**interface** *interface-name*	Either. After you enter the layer-2 Ethernet interface configuration mode, the subsequent configuration takes effect only on the current port. After you enter the aggregation group configuration mode, the subsequent configuration takes effect only within the aggregation group.
Enter the aggregation group configuration mode.	**link-aggregation** *link-aggregation-id*	
Configure the port link type to the Access type.	**switchport mode access**	Mandatory. By default, the port link type is the Access type.
Add an Access port into the specified VLAN.	**switchport access vlan** *vlan-id*	Mandatory. By default, the Access port is added into VLAN1.

Configure a Trunk Port to Allow Services of a VLAN to Pass

If a Trunk port allows services of an existing VLAN to pass, the port allows forwarding packets of the VLAN. If the VLAN that the Trunk port allows to pass does not exist, the VLAN will not be created automatically, you must create the VLAN before the port allows forwarding packets of the VLAN.

Table 3-6 Configuring a trunk port to allow services of a VLAN to pass

Step	Command	Description
Enter the global configuration mode.	**configure terminal**	-
Enter the layer-2 Ethernet interface configuration mode.	**interface** *interface-name*	Either. After you enter the layer-2 Ethernet interface configuration mode, the subsequent configuration takes effect only on the current port. After you enter the aggregation group configuration mode, the subsequent configuration takes effect only within the aggregation group.
Enter the aggregation group configuration mode.	**link-aggregation** *link-aggregation-id*	
Configure the port link type to the Trunk type.	**switchport mode trunk**	Mandatory. By default, the port link type is the Access type.
Configure a Trunk port to allow a VLAN to pass.	**switchport trunk allowed vlan** { **all** | **add** *vlan-list* }	Mandatory. By default, the Trunk port allows VLAN1 to pass.
Configure the packets from the VLAN in which the PVID is located to be forwarded with VLAN tags reserved.	**vlan dot1q tag pvid**	Optional. By default, the packets from the VLAN in which the PVID is located are forwarded without VLAN tags.

Add a Hybrid Port into the VLAN

If the VLAN to which the Access port is to be added does not exist, the VLAN is automatically created.

Table 3-7 Adding a hybrid port into the VLAN

Step	Command	Description
Enter the global configuration mode.	**configure terminal**	-
Enter the layer-2 Ethernet interface configuration mode.	**interface** *interface-name*	Either. After you enter the layer-2 Ethernet interface configuration mode, the subsequent configuration takes effect only on the current port. After you enter the aggregation group configuration mode, the subsequent configuration takes effect only within the aggregation group.
Enter the aggregation group configuration mode.	**link-aggregation** *link-aggregation-id*	
Configure the port link type to the Hybrid type.	**switchport mode hybrid**	Mandatory. By default, the port link type is the Access type.
Add a Hybrid port to a specified VLAN in a specified mode.	**switchport hybrid** { **untagged** | **tagged** } **vlan** *vlan-list*	Mandatory. By default, the Hybrid port is added into VLAN1 in Untagged mode.

Configure PVIDs for Ports

Port VLAN ID (PVID) is an important parameter of a port. When a port receives an Untag packet, it adds a VLAN tag to the packet, and the VLAN ID of the VLAN tag is the PVID of the port.

The PVID of an Access port is the ID of the VLAN to which it belongs, so the PVID of the Access port can be configured only by changing the VLAN to which it belongs. The Trunk port and hybrid port can belong to multiple VLANs, and their PVIDs can be configured according to the actual requirement.

The Trunk port and Hybrid port must be added into the VLAN to which their PVIDs belong; otherwise, packets of the VLAN to which their PVIDs belong cannot be forwarded, and the port discards the received Untag packets.

Table 3-8 Configuring PVIDs for ports

Step	Command	Description
Enter the global configuration mode.	**configure terminal**	-
Enter the layer-2 Ethernet interface configuration mode.	**interface** *interface-name*	Either. After you enter the layer-2 Ethernet interface configuration mode, the subsequent configuration takes effect only on the current port. After you enter the aggregation group configuration mode, the subsequent configuration takes effect only within the aggregation group.
Enter the aggregation group configuration mode.	**link-aggregation** *link-aggregation-id*	
Configuring the PVID for the Trunk port.	**switchport trunk pvid vlan** *vlan-id*	Mandatory. Select one option according to the port link type. By default, the port PVID is VLAN1.
Configuring the PVID for the Hybrid port.	**switchport hybrid pvid vlan** *vlan-id*	

Note:

- In configuring the PVID for a port, the VLAN to which the PVID belongs must have been created; otherwise, the configuration fails, and an error message is prompted.

3.2.3. VLAN Monitoring and Maintaining

Table 3-9 VLAN monitoring and maintaining

Command	Description
show running-config vlan	Displays VLAN configuration information.
show vlan [*vlan-id*]	Displays the information about a specified VLAN or all existing VLANs.
show vlan statistics	Displays the number of existing VLANs.

Command	Description
show { **interface** *interface-name* | **link-aggregation** *link-aggregation-id* } **vlan status**	Displays the VLAN information on the specified port or aggregation group.

3.3. VLAN Typical Configuration Example

3.3.1. Configure Port-Based VLANs

Network Requirements

- Server1 and PC1 are in the office network, while Server2 and PC2 are in the production network.
- You need to configure the port-based VLAN functions to isolate PC1 and PC2 so that PC1 can access only Server1 and PC2 can access only Server2.

Network Topology

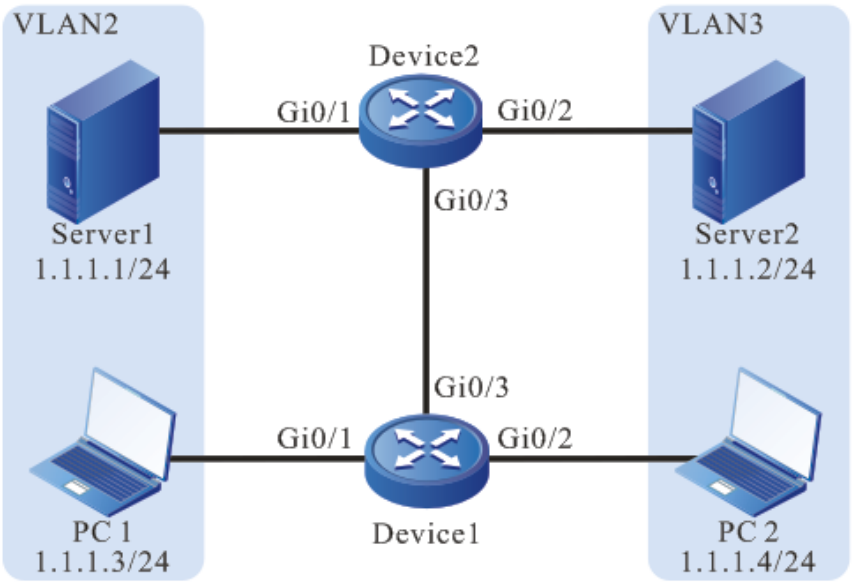


Figure 3-2 Networking for configuring port-based VLANs

Configuration Steps

Step 1: On Device1, configure VLANs, and configure the port link types of the ports.

#On Device1, create VLAN2 and VLAN3.

```
Device1#configure terminal
Device1(config)#vlan 2-3
```

#On Device1, configure the link type of ports gigabitethernet0/1 and gigabitethernet0/2 to Access. Configure gigabitethernet0/1 to allow services of VLAN2 to pass and configure and gigabitethernet0/2 to allow services of VLAN3 to pass.

```
Device1(config)#interface gigabitethernet 0/1
Device1(config-if-gigabitethernet0/1)#switchport mode access
```

```
Device1(config-if-gigabitethernet0/1)#switchport access vlan 2
Device1(config-if-gigabitethernet0/1)#exit
Device1(config)#interface gigabitethernet 0/2
Device1(config-if-gigabitethernet0/2)#switchport mode access
Device1(config-if-gigabitethernet0/2)#switchport access vlan 3
Device1(config-if-gigabitethernet0/2)#exit
```

#On Device1, configure the link type of port gigabitethernet0/3 to Trunk and allow services of VLAN2 and VLAN3 to pass.

```
Device1(config)#interface gigabitethernet 0/3
Device1(config-if-gigabitethernet0/3)#switchport mode trunk
Device1(config-if-gigabitethernet0/3)#switchport trunk allowed vlan add 2-3
Device1(config-if-gigabitethernet0/3)#exit
```

Step 2: On Device3, configure VLANs, and configure the port link types of the ports.

#On Device2, create VLAN2 and VLAN3.

```
Device2#configure terminal
Device2(config)#vlan 2-3
```

#On Device2, configure the link type of ports gigabitethernet0/1 and gigabitethernet0/2 to Access. Configure gigabitethernet0/1 to allow services of VLAN2 to pass and configure gigabitethernet0/2 to allow services of VLAN3 to pass.

```
Device2(config)#interface gigabitethernet 0/1
Device2(config-if-gigabitethernet0/1)#switchport mode access
Device2(config-if-gigabitethernet0/1)#switchport access vlan 2
Device2(config-if-gigabitethernet0/1)#exit
Device2(config)#interface gigabitethernet 0/2
Device2(config-if-gigabitethernet0/2)#switchport mode access
Device2(config-if-gigabitethernet0/2)#switchport access vlan 3
Device2(config-if-gigabitethernet0/2)#exit
```

#On Device2, configure the link type of port gigabitethernet0/3 to Trunk and allow services of VLAN2 and VLAN3 to pass.

```
Device2(config)#interface gigabitethernet 0/3
Device2(config-if-gigabitethernet0/3)#switchport mode trunk
Device2(config-if-gigabitethernet0/3)#switchport trunk allowed vlan add 2-3
Device2(config-if-gigabitethernet0/3)#exit
```

Step 3: Check the result.

#Query the VLAN information on Device1.

```
Device1#show vlan 2
---- ---- ------------------------------ ------- --------- ------------------
-----------
NO. VID  VLAN-Name                      Owner   Mode      Interface
---- ---- ------------------------------ ------- --------- ------------------
-----------
1   2    VLAN0002                        static  Tagged    gi0/3
                                         Untagged  gi0/1
Device1#show vlan 3
---- ---- ------------------------------ ------- --------- ------------------
-----------
NO. VID  VLAN-Name                      Owner   Mode      Interface
---- ---- ------------------------------ ------- --------- ------------------
-----------
1   3    VLAN0003                        static  Tagged    gi0/3
                                         Untagged  gi0/2
```

Query the VLAN information on Device2.

```
Device2#show vlan 2
---- ---- ------------------------------ ------- --------- ------------------
-----------
NO. VID  VLAN-Name                      Owner   Mode      Interface
---- ---- ------------------------------ ------- --------- ------------------
-----------
1   2    VLAN0002                        static  Tagged    gi0/3
                                         Untagged  gi0/1
Device2#show vlan 3
---- ---- ------------------------------ ------- --------- ------------------
-----------
NO. VID  VLAN-Name                      Owner   Mode      Interface
---- ---- ------------------------------ ------- --------- ------------------
-----------
1   3    VLAN0003                        static  Tagged    gi0/3
                                         Untagged  gi0/2
```

#PC1 and PC2 cannot communicate with each other, PC1 can access only Server1, and PC2 can access only Server2.

3.3.2. Configure MAC-Based VLANs

Network Requirements

- PC1 and PC2 can access the network through different ports of Device.

- The MAC-address based VLAN functions need to be configured so that the PCs with the specified MAC addresses can access the server through different ports. PCs which do not have a specified MAC address can access the server only through a specified port.

Network Topology

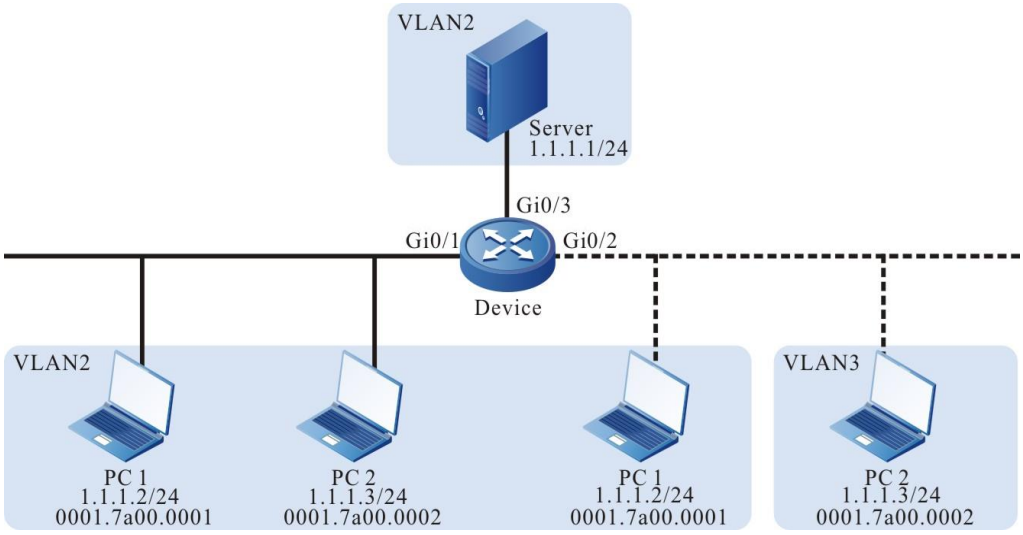


Figure 3-3 Networking for configuring MAC address-based VLANs

Configuration Steps

Step 1: On Device, configure VLANs, and configure the port link types of the ports.

#On Device, create VLAN2 and VLAN3.

```
Device#configure terminal
Device(config)#vlan 2-3
```

#On Device2, configure the link type of ports gigabitethernet0/1 and gigabitethernet0/3 to Access and allow services of VLAN2 to pass.

```
Device(config)#interface gigabitethernet 0/1,0/3
Device(config-if-range)#switchport mode access
Device(config-if-range)#switchport access vlan 2
Device(config-if-range)#exit
```

#On Device, configure the link type of port gigabitethernet0/2 to Hybrid and allow services of VLAN2 and VLAN3 to pass, and set PVID to 3.

```
Device(config)#interface gigabitethernet 0/2
Device(config-if-gigabitethernet0/2)#switchport mode hybrid
Device(config-if-gigabitethernet0/2)#switchport hybrid untagged vlan 2-3
Device(config-if-gigabitethernet0/2)#switchport hybrid pvid vlan 3
Device(config-if-gigabitethernet0/2)#exit
```

Step 2: Configure the MAC address-based VLAN function.

#On Device, configure an MAC address-based VLAN entry so that the packets with the source MAC address 001f.ce00.0001 can be forwarded in VLAN2.

```
Device(config)#mac-vlan mac-address 001f.ce00.0001 vlan 2
```

#On port gigabitethernet0/2 of Device, enable the MAC address-based VLAN function.

```
Device(config)#interface gigabitethernet 0/2
Device(config-if-gigabitethernet0/2)#mac-vlan enable
Device(config-if-gigabitethernet0/2)#exit
```

Step 3: Check the result.

#On Device, query MAC VLAN entries and port enable status.

```
Device#show mac-vlan
                                total 1024,    used 1,    left 1023

--------------------------------MAC-VLAN--------------------------------
NO.   Mac Address     Dynamic Vlan  Static Vlan  Current Pri  Static Pri
----- --------------- ------------- ------------ ------------ -----------
1     001f.ce00.0001  0             2            0            0

----------------------------ENABLE MAC-VLAN-----------------------------
gi0/2
```

#PC1 can access the server through port gigabitethernet0/1 or gigabitethernet0/2, while PC2 can access the server only through port gigabitethernet0/1.

3.3.3. Configure IP Subnet-Based VLANs

Network Requirements

- Server1 is the server in the office network, and Server2 is the server in the production network.
- The IP subnet-based VLAN functions need to be configured so that PC1 can access only Server1 and PC2 can access only Server2.

Network Topology

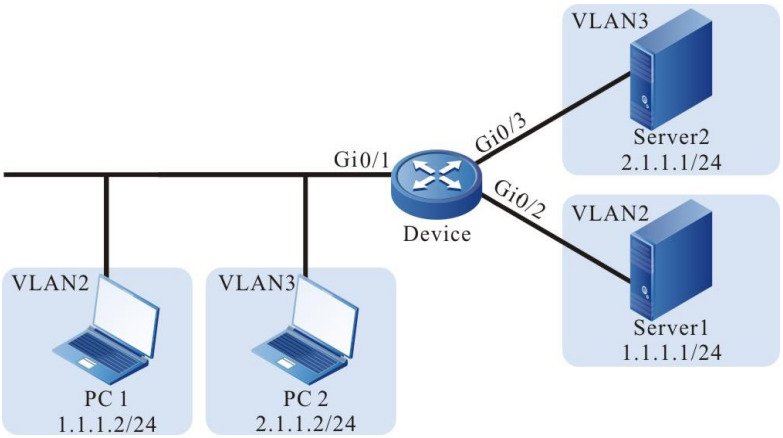


Figure 3-4 Configuring an IP subnet-based VLAN

Configuration Steps

Step 1: On Device, configure VLANs, and configure the port link types of the ports.

#On Device, create VLAN2 and VLAN3.

```
Device#configure terminal
Device(config)#vlan 2-3
```

#On Device, configure the link type of port gigabitethernet0/1 to Hybrid and allow services of VLAN2 and VLAN3 to pass, and set PVID to 2.

```
Device(config)#interface gigabitethernet 0/1
Device(config-if-gigabitethernet0/1)#switchport mode hybrid
Device(config-if-gigabitethernet0/1)#switchport hybrid untagged vlan 2-3
Device(config-if-gigabitethernet0/1)#switchport hybrid pvid vlan 2
Device(config-if-gigabitethernet0/1)#exit
```

#On Device, configure the link type of ports gigabitethernet0/2 and gigabitethernet0/3 to Access. Configure gigabitethernet0/2 to allow services of VLAN2 to pass and configure gigabitethernet0/3 to allow services of VLAN3 to pass.

```
Device(config)#interface gigabitethernet 0/2
Device(config-if-gigabitethernet0/2)#switchport mode access
Device(config-if-gigabitethernet0/2)#switchport access vlan 2
Device(config)#interface gigabitethernet 0/3
Device(config-if-gigabitethernet0/3)#switchport mode access
Device(config-if-gigabitethernet0/3)#switchport access vlan 3
Device(config-if-gigabitethernet0/3)#exit
```

Step 2: Configure IP subnet-based VLAN functions.

#On Device, configure IP subnet-based VLAN entries so that the packets with the source IP address in the 2.1.1.0/24 subnet can be forwarded in VLAN3.

```
Device(config)#ip-subnet-vlan ipv4 2.1.1.0 mask 255.255.255.0 vlan 3
```

#On port gigabitethernet0/1 of Device, enable the IP subnet-based VLAN function.

```
Device(config)#interface gigabitethernet 0/1
Device(config-if-gigabitethernet0/1)#ip-subnet-vlan enable
Device(config-if-gigabitethernet0/1)#exit
```

Step 3: Check the result.

#On Device, query IP subnet VLAN entries and port enable status.

```
Device(config)#show ip-subnet-vlan
-------------------------IP-SUBNET-VLAN-----------------------
NO.   IP              MASK            VLAN   PRI
------ ------------------ ------------------ ------- ----------
1     2.1.1.0         255.255.255.0     3      0

----------------------Enable SUBNET-VLAN----------------------
gi0/1

------------------Enable SUBNET-VLAN Priority-----------------
```

#PC1 can access only Server1 and PC2 can access only Server2.

3.3.4. Configure Protocol-Based VLANs

Network Requirements

- PC is a host in the Ethernet and can only visit Server1.
- The protocol-based VLAN function needs to be configured so that the PC can access only Server 1 before the protocol-based VLAN function is enabled on the port of Device. After the protocol-based VLAN function is enabled on the port, PC can access only Server2.

Network Topology

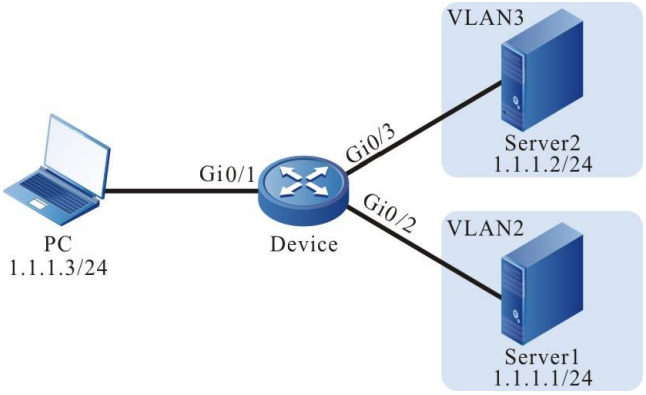


Figure 3-5 Networking for configuring protocol-based VLANs

Configuration Steps

Step 1: On Device, configure VLANs, and configure the port link types of the ports.

#On Device, create VLAN2 and VLAN3.

```
Device#configure terminal
Device(config)#vlan 2-3
```

#On Device, configure the link type of port gigabitethernet0/1 to Hybrid and allow services of VLAN2 and VLAN3 to pass, and set PVID to 2.

```
Device(config)#interface gigabitethernet 0/1
Device(config-if-gigabitethernet0/1)#switchport hybrid untagged vlan 2-3
Device(config-if-gigabitethernet0/1)#switchport hybrid pvid vlan 2
```

#On Device, configure the link type of ports gigabitethernet0/2 and gigabitethernet0/3 to Access. Configure gigabitethernet0/2 to allow services of VLAN2 to pass and configure gigabitethernet0/3 to allow services of VLAN3 to pass.

```
Device(config)#interface gigabitethernet 0/2
Device(config-if-gigabitethernet0/2)#switchport mode access
Device(config-if-gigabitethernet0/2)#switchport access vlan 2
Device(config-if-gigabitethernet0/2)#exit
Device(config)#interface gigabitethernet 0/3
Device(config-if-gigabitethernet0/3)#switchport mode access
Device(config-if-gigabitethernet0/3)#switchport access vlan 3
Device(config-if-gigabitethernet0/3)#exit
```

Step 2: Configure the protocol-based VLAN function.

#On Device, configure a protocol profile for IP(0x0800) packets that are based on ETHERII encapsulation.

```
Device(config)#protocol-vlan profile 1 frame-type ETHERII ether-type 0x0800
```

#On port gigabitethernet0/1 of Device, the packets that match the protocol profile are forwarded in VLAN3.

```
Device(config)#interface gigabitethernet 0/1
Device(config-if-gigabitethernet0/1)#protocol-vlan profile 1 vlan 3
Device(config-if-gigabitethernet0/1)#protocol-vlan enable
Device(config-if-gigabitethernet0/1)#exit
```

Step 3: Check the result.

#On Device, query protocol VLAN entries and port enable status.

```
Device#show protocol-vlan profile
--------------------PROTOCOL-VLAN-TEMPLATE-----------------------
```

```
Profile   Frame-type    Ether-type
------------------------------------------------------------------
1       ETHERII       0x800

-----------------------Enable PROTOCOL-VLAN-----------------------
gi0/1

-------------------Enable PROTOCOL-VLAN Profile-------------------
gi0/1: total-profiles 1
      vlan 3, profile 1
Device#show protocol-vlan
---------------------------PROTOTOCL-VLAN-------------------------
Interface          Profile          VLAN
---------------------- -------------------- --------------------
gi0/1              1              3

-----------------------Enable PROTOCOL-VLAN-----------------------
gi0/1

-------------------Enable PROTOCOL-VLAN Profile-------------------
gi0/1: total-profiles 1
      vlan 3, profile 1
```

#Before the protocol-based VLAN function is enabled on port gigabitethernet0/1, PC can access only Server1. After the protocol-based VLAN function is enabled on port gigabitethernet0/1, PC can access only Server2.

4. MAC ADDRESS TABLE MANAGEMENT

4.1. Overview

A MAC address entry consists of the MAC address of a terminal, the device port that is connected to the terminal, and the ID of the VLAN to which the port belongs. After a device receives a data packet, it matches the destination MAC address of the packet with the MAC address table entries that are saved in the device so as to locate a packet forwarding port efficiently.

MAC addresses are categorized into two types: dynamic MAC addresses and static MAC addresses. Static MAC addresses are categorized into static forwarding MAC addresses and static filtering MAC addresses.

Dynamic MAC address learning is the basic MAC address learning mode of the devices. Each dynamic MAC address entry has aging time. If no packet whose source MAC address matches a MAC address entry is received by the corresponding VLAN and port, the device deletes the MAC address entry.

The dynamic MAC address learning/forwarding process is as follows:

- When a device receives a packet, it searches the MAC address table of the corresponding VLAN for the MAC address entry that matches the source MAC address of the packet. If no corresponding matching entry is available, the source MAC address of the packet is written into the MAC address table, and the aging time timer of the new MAC address entry is started. If a matching MAC address entry is found, the aging time of the MAC address entry is updated.
- In the corresponding VLAN, the device searches the MAC address table for MAC address entry that matches the destination MAC address of the packet. If no matching entry is available, the packet is flooded to the other ports with the same VLAN ID. If a matching MAC address entry is available, the packet is forwarded through the specified port.

Static filtering MAC addresses are used to isolate devices which are aggressive, preventing the devices from communicating with external devices.

The configuration/forwarding process of static filtering MAC addresses is as follows:

- Static filtering MAC addresses can only be configured by users.
- If the destination MAC address of a packet matches a static filtering MAC address entry in the corresponding VLAN, the packet is discarded.

Static forwarding MAC addresses are used to control the routing principle of packets, and prevent frequent MAC address migration of MAC address entries in the table. MAC address migration means that: A device learns a MAC address from port A, then the device receives packets whose source MAC address is the same as the MAC address from port B, and port B and port A belong to the same VLAN. At this time, the forwarding port saved in the MAC address entry is updated from port A to port B.

The configuration/forwarding process of static forwarding MAC addresses is as follows:

- Static forwarding MAC addresses are configured by users.
- If the destination MAC address of a packet matches a static MAC address entry in the corresponding VLAN, the packet is forwarded through the specified port.

One port can learn the same MAC address from different VLANs, but one MAC address can only be learnt by one port in one VLAN.

4.2. MAC Address Management Function Configuration

Table 4-1 MAC address management function list

Configuration Tasks	
Configure management properties of MAC addresses.	Configure the MAC address aging time.
	Configure the MAC address learning capability.
Configure limitations on MAC address learning.	Configure limitations on port-based dynamic MAC address learning.
	Configure limitations on VLAN-based dynamic MAC address learning.
	Configure limitations on system-based dynamic MAC address learning.
Configure static MAC addresses.	Configure static filtering MAC addresses.
	Configure static forwarding MAC addresses that are bound to a port.
	Configure static forwarding MAC addresses that are bound to an aggregation group.

4.2.1. Configure Management Properties of MAC Addresses

MAC address management properties include: MAC address aging time, and the MAC address learning capability of ports.

Each dynamic MAC address entry has aging time. If no packet whose source MAC address matches a MAC address entry is received by the specified VLAN, the device deletes the MAC address entry. If the specified VLAN receives a packet whose source MAC address matches a MAC address entry, the device resets the aging time of the MAC address entry.

Static MAC addresses can only be configured and deleted by users, so static MAC addresses cannot age.

If devices in the network have idle ports and the ports do not allow free use, then the MAC address learning capability can be disabled on the port. Then, the packets received by the port will all be discarded. In this way, these ports cannot access the network, and hence the security of the network is improved.

Configuration Condition

None

Configure the MAC Address Aging Time

The dynamic MAC address aging time set in a device takes effect globally. The value range of the MAC address aging time is:

- 0: MAC addresses do not age, that is, the learned dynamic MAC addresses do not age.
- 10-1000000: Aging time of dynamic MAC addresses. Unit: second. Default: 300.

If the aging time is configured too long, the MAC address table in the device may contain a large number of MAC address entries that are no long in use. In this way, the large number of invalid entries may use up MAC address resources, and new valid MAC address entries fail to be added to the device. If the aging time is configured too short, the device may frequently delete valid MAC address entries, affecting the device forwarding performance. Therefore, you need to configure a reasonable value for the aging time according to the actual environment.

Table 4-2 Configuring the MAC address aging time

Step	Command	Description
Enter the global configuration mode.	**configure terminal**	-
Configure the MAC address aging time.	**mac-address aging-time** *aging-time-value*	Mandatory. By default, the MAC address aging time is set to 300 seconds.

4.2.2. Configure MAC Address Learning Limitation

MAC address learning restrictions can be divided into three categories: Port-based dynamic MAC address learning limit, VLAN-based dynamic MAC address learning limit and system-based dynamic MAC address learning limit.

The more dynamic MAC address table items learned in the device, the longer the time for packet forwarding to find MAC address table, which may lead to the decreasing of the device performance. You can configure the ability of dynamic MAC address learning in the device to improve the performance of the device. The dynamic MAC address learning ability limit can be configured under the corresponding port or corresponding VLAN to control the number of the terminals accessed.

Configuration Conditions

None

Configure Port-based Dynamic MAC Address Learning Limitation

After the MAC address table entries learned under the specified port have reached the upper limit, the packets received by this port whose source MAC addresses are not in the MAC address forwarding table will be discarded.

Table 4-3 Configure port-based dynamic MAC address learning limitation

Step	Command	Description
Enter the global configuration mode.	**configure terminal**	-
Enter the L2 Ethernet interface configuration mode	**interface** *interface-name*	Either After entering the L2 Ethernet interface configuration mode, the subsequent configuration only takes effect on the current port; after entering the aggregation group configuration mode, the subsequent configuration only takes effect in the aggregation group.
Enter the aggregation group configuration mode	**link-aggregation** *link-aggregation-id*	
Configure port-based dynamic MAC address learning limitation	**mac-address max-mac-count** *max-mac-count-value*	Mandatory By default, the dynamic MAC address learning in the port is not limited. Configure the value range of the upper limit of the learned dynamic MAC addresses as 1-max. address table entries that can be learned by the hardware chip.

Note:

- When configuring the port-based dynamic MAC address learning limit, if the configured limit is less than the number of existing dynamic MAC addresses in the current port, the device will prompt the user to manually clear the existing dynamic MAC address table entries. After manual clearing, the configuration takes effect immediately.

Configure VLAN-based Dynamic MAC Address Learning Limitation

After the MAC address table entries learned in the specified VLAN have reached the upper limit, the packets received in this VLAN whose source MAC addresses are not in the MAC address forwarding table will be discarded.

Table 4-4 Configure VLAN-based dynamic MAC address learning limitation

Step	Command	Description
Enter the global configuration mode.	**configure terminal**	-
Configure VLAN-based dynamic MAC address learning limitation	**mac-address vlan** *vlan-id* **max-mac-count** *max-mac-count-value*	Mandatory By default, the dynamic MAC address learning in the VLAN is not limited. Configure the value range of the upper limit of the learned dynamic MAC addresses as 1-max. address table entries that can be learned by the hardware chip.

Note:

- When configuring the VLAN-based dynamic MAC address learning limit, if the configured limit is less than the number of existing dynamic MAC addresses in the current VLAN, the device will prompt the user to manually clear the existing dynamic MAC address table entries. After manual clearing, the configuration takes effect immediately.

Configure System-based Dynamic MAC Address Learning Limitation

After the MAC address table entries learned in the system have reached the upper limit, the packets received by the system whose source MAC addresses are not in the MAC address forwarding table will be discarded.

Table 4-5 Configure system-based dynamic MAC address learning limitation

Step	Command	Description
Enter the global configuration mode.	**configure terminal**	-
Configure system-based dynamic MAC address learning limitation	**mac-address system max-mac-count** *max-mac-count-value*	Mandatory By default, the MAC address learning is not limited. Configure the value range of the upper limit of the learned dynamic MAC addresses as 1-max. address table entries that can be learned by the hardware chip.

Note:

- When configuring the system-based dynamic MAC address learning limit, if the configured limit is less than the number of existing dynamic MAC addresses in the current system, the device will prompt the user to manually clear the existing MAC address table entries. After manual clearing, the configuration takes effect immediately.

4.2.3. Configure Static MAC Addresses

Static MAC addresses are categorized into two types: static forwarding MAC addresses and static filtering MAC addresses.

The configured MAC addresses must be legal unicast MAC addresses instead of broadcast, multicast, or all-0 addresses.

One MAC address can only be configured as a static forwarding MAC address or a static filtering MAC address in a VLAN.

Configuration Condition

None

Configure Static Filtering MAC Addresses

After static filtering MAC address entries are configured, if the destination MAC addresses of the packets that are received by the corresponding VLAN match static filtering MAC address entries, the packets are discarded. This function prevents trustless devices from accessing the network, and prevents fraud and attacking activities of illegal users.

Table 4-6 Configuring static filtering MAC addresses

Step	Command	Description
Enter the global configuration mode.	**configure terminal**	-
Configure static filtering MAC addresses.	**mac-address static** *mac-address-value* **vlan** *vlan-id* **drop**	Mandatory. By default, a device is not configured with static filtering MAC addresses.
Configure the description information	**mac-address static** *mac-address-value* **vlan** *vlan-id* **drop description** *description-name*	Optional By default, the corresponding MAC address does not have description information.

Note:

- The static filtering MAC address of MP1800-35E(V2) only supports filtering the destination MAC address.

Configure Static Forwarding MAC Addresses That Are Bound to a Port

With static forwarding MAC address entries configured, after the corresponding VLAN receives packets, the port matches the destination MAC addresses of the packets with the static forwarding MAC address entries that are configured on the device. If they match successfully, the device forwards the packets through the specified port. This function helps to control the

routing principle of packets more flexibly, and prevents frequent migration of MAC address entries in the table.

Table 4-7 Configuring static forwarding MAC addresses that are bound to a port

Step	Command	Description
Enter the global configuration mode.	**configure terminal**	-
Configure static forwarding MAC addresses that are bound to a port.	**mac-address static** *mac-address-value* **vlan** *vlan-id* **[interface** *interface-name* **| link-aggregation** *link-aggregation-id*]	Mandatory. By default, a device is not configured with static forwarding MAC addresses.
Configure the description information	**mac-address static** *mac-address-value* **vlan** *vlan-id* **[interface** *interface-name* | **link-aggregation** *link-aggregation-id*] **description** *description-name*	Optional By default, the corresponding MAC address does not have description information.

4.2.4. MAC Address Management Monitoring and Maintaining

Table 4-8 MAC address management monitoring and maintaining

Command	Description
clear mac-address dynamic { *mac-address-value* **| all** | **interface** *interface-list* | **link-aggregation** *link-aggregation-id* | **vlan** *vlan-id* [*mac-address-value* | **interface** *interface-list* | **link-aggregation** *link-aggregation-id*] }	Clears the MAC address entries that are dynamically learned.
show mac-address interface *interface-list* { **all** | **dynamic** | **static** [**config**] }	Displays MAC address entries on a port.
show mac-address link-aggregation *link-aggregation-id* { **all** | **dynamic** | **static** [**config**] }	Displays MAC address entries in an aggregation group.
show mac-address vlan *vlan-id* { **all** | **dynamic** | **static** [**config**] }	Displays MAC address entries in a VLAN.

Command	Description
show mac-address drop [*mac-address-value* | **config**]	Displays static filtering MAC address entries in the system.
show mac-address dynamic [*mac-address-value*]	Displays dynamic MAC address entries in the system.
show mac-address global learning	Displays whether the global MAC address learning capability is globally enabled in the system.
show mac-address static [*mac-address-value* **| config**]	Displays static forwarding MAC address entries in the system.
show mac-address system-mac	Displays the MAC address of the system.
show mac-address { *mac-address-value* **| all** }	Displays the information about the system MAC address entries or a specified MAC address entry.
show mac-address aging-time	Displays the aging time of dynamic MAC address entries.
show mac-address count [**interface** *interface-name* | **link-aggregation** *link-aggregation-id* | **vlan** *vlan-id*]	Displays MAC address entry statistics in the system.

5. SPANNING TREE

5.1. Overview

IEEE 802.1D defines the standard Spanning Tree Protocol (STP) to eliminate network loops, preventing data frames from circulating or multiplying in loops, which may result in network congestion and affect normal communication in the network. Through the spanning tree algorithm, STP can determine where loops may exist in a network, block ports on redundant links, and trim the network into a tree structure in which no loops exist to prevent devices from receiving duplicated data frames. When the active path is faulty, STP recovers the connectivity of the blocked redundant links to ensure normal services. On the basis of STP, Rapid Spanning Tree Protocol (RSTP) and Multiple Spanning Tree Protocol (MSTP) are developed. The basic principles of the three protocols are the same, while RSTP and MSTP are improved versions of STP.

In STP, the following basic concepts are defined:

- Root bridge: Root of the finally formed tree structure of a network. The device with the highest priority acts as the root bridge.
- Root Port (RP): The port which is nearest to the root bridge. The port is not on the root bridge, and it communicates with the root bridge.
- Designated bridge: If the device sends Bridge Protocol Data Unit (BPDU) configuration information to a directly connected device or directly connected LAN, the device is regarded as the designated bridge of the directly connected device or directly connected LAN.
- Designated port: The designated bridge forwards BPDU configuration information through the designated port.
- Path cost: It indicates the link quality, and it is related to the link rate. Usually, a higher link rate means a smaller path cost, and the link is better.

The devices that run STP implement calculation of the spanning tree by exchanging BPDU packets, and finally form a stable topology structure. BPDU packets are categorized into the following two types:

- Configuration BPDUs: They are also called BPDU configuration messages which are used to calculate and maintain the spanning tree topology.
- Topology Change Notification (TCN) BPDUs: When the network topology structure changes, they are used to inform other devices of the change.

BPDU packets contain information that is required in spanning tree calculation. The major information includes:

- Root bridge ID: It consists of the root bridge priority and the MAC address.
- Root path cost: It is the minimum path cost to the root bridge.
- Designated bridge ID: It consists of the designated bridge priority and the MAC address.
- Designated port ID: It consists of the designated port priority and port number.
- Message Age: Life cycle of BPDU configuration messages while they are broadcast in a network.
- Hello Time: Transmitting cycle of BPDU configuration messages.
- Forward Delay: Delay in port status migration.
- Max Age: Maximum life cycle of configuration messages in a device.

The election process of STP is as follows:

- Initial status.

The local device takes itself as the root bridge to generate BPDU configuration messages and sends the messages. In the BPDU packets, the root bridge ID and designated bridge ID are the local bridge ID, and root path cost is 0, and the specified port is the transmitting port.

Each port of the device generates a port configuration message which is used for spanning tree calculation. In the port configuration message, the root bridge ID and the designated bridge ID are the local bridge ID, the root path cost is 0, and the specified port is the local port.

- Update port configuration messages.

After the local device receives a BPDU configuration message from another device, it compares the message with the port configuration message of the receiving port. If the received configuration message is better, the device uses the received BPDU configuration message to replace the port configuration message. If the port configuration message is better, the device does not perform any operation.

The principle of comparison is as follows: The root bridge IDs, root path cost, designated bridge IDs, designated port IDs, and receiving port IDs should be compared in order. The smaller value is better. If the values of previous item are the same, compare the next item.

- Select the root bridge.

The device that sends the optimal configuration message in the entire network is selected as the root bridge.

- Select port roles and port status.

All ports of the root bridge are designated ports, and the ports are in the Forwarding status. The designated bridge selects the optimal port configuration message from all ports. The receiving port of the message is selected as the root port, and the root port is in the Forwarding status. The other ports calculate designated port configuration messages according to the root port configuration message.

The calculation method is as follows: The root bridge ID is the route ID of the root port configuration message, the root path cost is the sum of the root path cost of the root port configuration message and the root port path cost, the designated bridge ID is the bridge ID of the local device, and the designated port is the local port.

Based on the port configuration message and the calculated designated port configuration message, determine port rules: If the designated port configuration message is better, the local port is selected as the designated port, and the port is in the Forwarding status. Then, the port configuration message is replaced by the designated port configuration message, and the designated port sends port configuration messages periodically at the interval of Hello Time. If the port configuration message is better, the port is blocked. The port is then in the Discarding status, and the port configuration message is not modified.

After the root bridge, root port, and designated port are selected, the tree structure network topology is set up successfully. Only the root port and the designated port can forward data. The other ports are in the Discarding status. They can only receive configuration messages but cannot send configuration messages or forward data.

If the root port of a non-root bridge fails to receive configuration messages periodically, the active path is regarded as faulty. The device re-generates a BPDU configuration message and TCN BPDU with itself as the root bridge and sends the messages. The messages causes re-calculation of the spanning tree and then a new active path is obtained.

Before receiving new configuration messages, the other devices do not find the network topology change, so their root ports and designated port still forward data through the original path. The

newly selected root port and designated port migrate to the Forwarding status after two Forward Delay periods to ensure that the new configuration message has been broadcast to the entire network and prevent occurrence of temporary loops that may be caused if both old and new root ports and designate ports forward data.

RSTP defined in IEEE 802.1w is developed based on STP, and it is the improved version of STP. RSTP realizes fast migration of port status and hence shortens the time required for a network to set up stable topology. RSTP is improved in the following aspects:

- It sets a backup port, that is, alternate port, for the root port. If the root port is blocked, the alternate port can fast switch over to become a new root port.
- It sets a backup port, that is, backup port, for the designated port. If the designated port is blocked, the backup port can fast switch over to become a new designated port.
- In a point-to-point link of two directly-connected devices, the designated port can enter the Forwarding status without delay only after a handshake with the downstream bridge.
- Some ports are not connected to the other bridges or shared links, instead, they are directly connected with user terminals. These ports are defined as edge ports. The status changes of edge ports do not affect the network connectivity, so the ports can enter the Forwarding status without delay.

However, both RSTP and STP form a single spanning tree, which has the following shortages:

- Only one spanning tree is available in the entire network. If the network size is large, the network convergence takes a long time.
- Packets of all VLANs are forwarded through one spanning tree, therefore no load balancing is achieved.

MSTP defined in IEEE 802.1s is an improvement of STP and RSTP, and it is backward compatible with STP and RSTP. MSTP introduces the concept of region and instance. MSTP divides a network into multiple regions. Each region contains multiple instances, one instance can set up mapping with one or more VLANs, and one instance corresponds to one spanning tree. One port may have different port role and status in different instances. In this way, packets of different VLANs are forwarded in their own paths.

In MSTP, definition of the following concepts is added:

- MST region: It consists of multiple devices in the switching network and the network between the devices. The devices in an MST region must meet the following requirements: The spanning tree function has been enabled on the devices. They have the same MST region, MSTP level, and VLAN mapping table. They are directly connected physically.
- Internal Spanning Tree (IST): It is the spanning tree of instance 0 in each region.
- Common Spanning Tree (CST): If each MST region is regarded as a device, then the spanning trees that connect MST regions are CSTs.
- Common and Internal Spanning Tree (CIST): It consists of the ISTs of MST regions and the CSTs between the MST regions. It is a single spanning tree that connects all devices in the network.
- Multiple Spanning Tree Instance (MSTI): Spanning trees in MST regions. Each instance has an independent MSTI.
- Common root: CIST root.
- Region root: Root of each IST and MSTI in MST regions. In MST domains, each instance has an independent spanning tree, so the region roots may be different. The root bridge of instance 0 is the region root of the region.

- Region edge ports: They are located at the edge of an MST region and they are used to connect ports of different MST regions.
- External path cost: It is the minimum path cost from a port to the common root.
- Internal path cost: It is the minimum path cost from a port to the region root.
- Master port: It is the region edge port with the minimum path cost to the common root in an MST region. The role of a master port in an MSTI is the same as its role in a CIST.

The selection rule of MSTP is similar to that of STP, that is, selecting the bridge with the highest priority in the network as the root bridge of CIST by comparing configuration messages. Each MST region calculates its IST, and MST regions calculate CSTs, and all of the constructs CIST in the entire network. Based on mapping between VLANs and spanning tree instances, each MST region calculates an independent spanning tree MSTI for each instance.

5.2. Spanning Tree Function Configuration

Table 5-1 Spanning tree function list

Configuration Tasks	
Configure basic functions of a spanning tree.	Enable the spanning tree function.
	Configure MST regions.
Configure bridge properties.	Configure the priority of a bridge.
	Configure Hello Time.
	Configure Forward Delay.
	Configure Max Age.
	Configure the maximum number of hops in an MST region.
Configure spanning tree port properties.	Configure the priority of a port.
	Configure the default path cost standard for a port.
	Configure the path cost of a port.
	Configure the BPDU packet length check
	Configure the maximum length of the BPDU packet

Configuration Tasks	
	Configure the maximum sending rate of the BPDU packet
	Configure the source mac check of the BPDU packet
	Configure the timeout factor of the BPDU packet
	Configure the edge port
	Configure the auto detection of the edge port
	Force the auto detection of the edge port
	Configure the port link type
Configure the working mode of a spanning tree.	Configure the working mode of a spanning tree.
Configure the spanning tree protection function.	Configure the BPDU Guard function.
	Configure the BPDU Filter function.
	Configure the Flap Guard function.
	Configure the Loop Guard function.
	Configure the Root Guard function.
	Configure the TC Guard function
	Configure the TC protection function.

5.2.1. Configure Basic Functions of a Spanning Tree

Configuration Condition

None

Enable the Spanning Tree Function

After the spanning tree function is enabled, devices start to run the spanning tree protocol. The devices exchange BPDU packets to form a stable tree network topology, and network loops are eliminated.

Table 5-2 Enabling the spanning tree function

Step	Command	Description
Enter the global configuration mode.	**configure terminal**	-
Enabling the spanning tree function globally.	**spanning-tree enable**	Mandatory. By default, the spanning tree function is disabled globally.
Enter the layer-2 Ethernet interface configuration mode.	**interface** *interface-name*	Either. After you enter the layer-2 Ethernet interface configuration mode, the subsequent configuration takes effect only on the current port. After you enter the aggregation group configuration mode, the subsequent configuration takes effect only within the aggregation group.
Enter the aggregation group configuration mode.	**link-aggregation** *link-aggregation-id*	
Enabling the spanning tree function on a port.	**spanning-tree enable**	Optional. By default, the spanning tree function is enabled on a port.

Configure MST Regions

Dividing an entire network into multiple MST regions helps to shorten the network convergence time. VLAN packets are transmitted through the corresponding MSTIs in MST regions and transmitted through CSTs between MST regions.

Table 5-3 Configuring MST regions

Step	Command	Description
Enter the global configuration mode.	**configure terminal**	-
Enter the MST region configuration mode.	**spanning-tree mst configuration**	-
Configure an MST region name.	**region-name** *region-name*	Mandatory. By default, the name of an MST region is the MAC address of the local device.
Configure the MSTP revision level.	**revision-level** *revision-level*	Mandatory. By default, the MSTP revision level is 0.
Configure a VLAN mapping table.	**instance** *instance-id* **vlan** *vlan-list*	Mandatory. By default, all VLANs are mapped to instance 0.
Activate MST region parameter configuration.	**active configuration pending**	Mandatory. By default, MST region parameters do not take effect immediately after modification.

Note:

- MST region parameters do not take effect immediately after they are modified. Instead, you need to run the **active configuration pending** command to activate the parameters and trigger re-calculation of the spanning tree. To cancel MST region parameter configuration, use the **abort configuration pending** command.

5.2.2. Configure Bridge Properties

Configuration Condition

None

Configure the Priority of a Bridge

The bridge priority and MAC address form the bridge ID. A smaller ID indicates a higher priority. The bridge with the highest priority is elected as the root bridge. One device may have different bridge priority in different spanning tree instances.

Table 5-4 Configuring the priority of a bridge

Step	Command	Description
Enter the global configuration mode.	**configure terminal**	-
Configure the priority of a bridge.	**spanning-tree mst instance** *instance-id* **priority** *priority-value*	Mandatory. By default, the priority of the bridge in all spanning tree instances is 32768.

Note:

- The step of bridge priorities is 4096, that is, the valid values include: 0, 4096, 8192, 12288, 16384, 20480, 24576, 28673, 32768, 36864, 40960, 45056, 49152, 53248, 57344, and 61440.

Configure Hello Time

After the network topology becomes stable, the root bridge sends BPDU packets at the interval of Hello Time to inform other bridges of its role as the root bridge so that the other bridges can recognize its role. The designated bridge maintains the existing spanning tree topology according to the BPDU packet, and it forwards the BPDU packet to other devices. If the designated bridge does not receive BPDU packets at a period of time as long is three times Hello Time, it regards the link as faulty. In this way, the spanning tree re-calculates the network topology to obtain a new active path, ensuring the network connectivity.

Table 5-5 Configuring hello time

Step	Command	Description
Enter the global configuration mode.	**configure terminal**	-
Configure Hello Time.	**spanning-tree mst hello-time** *seconds*	Mandatory. By default, Hello Time is 2 seconds.

Note:

- Forward Delay, Hello Time, and Max Age must meet the following requirement; otherwise, frequent network flapping may be cause.
- 2 × (Forward_Delay – 1.0seconds) ≥ Max_Age
- Max_Age ≥ 2 × (Hello_Time + 1.0seconds)

Configure Forward Delay

In STP, when the root port or designated port migrates from the Discarding status to the Forwarding status, the topology change cannot be learned by the entire network immediately.

To prevent temporary loops, the port migrates to the Learning status in the first Forward Delay, and then waits another Forward Delay to migrate to the Forwarding status.

Table 5-6 Configuring forward delay

Step	Command	Description
Enter the global configuration mode.	**configure terminal**	-
Configure Forward Delay.	**spanning-tree mst forward-time** *seconds*	Mandatory. By default, Forward Delay is 15 seconds.

Configure Max Age

Max Age refers to the life cycle of BPDU configuration messages while they are broadcast in a network. When a configuration message is transmitted crossing regions, after it passes through an MST region, one is added to Message Age in the configuration message. If the device receives a configuration message and finds that the value of Message Age in the configuration message is larger than the value of Max Age, the device discards the configuration message, and the configuration message is no longer used in spanning tree calculation.

Table 5-7 Configuring max age

Step	Command	Description
Enter the global configuration mode.	**configure terminal**	-
Configure Max Age.	**spanning-tree mst max-age** *seconds*	Mandatory. By default, Max Age is 20 seconds.

Configure the Maximum Number of Hops in an MST Region

You can limit the size of an MST region by configuring the maximum number of hops in the MST region. A larger number of hops in an MST region means a larger MST region. In one MST region, starting from the region root, once the configuration message is forwarded by a device, the number of hops is decreased by one. If the number of hops of a configuration message is 0, the device discards the configuration message. Therefore, the device which is beyond the maximum number of hops cannot participate in spanning tree calculation in the region.

Table 5-8 Configuring the maximum number of hops in an MST region

Step	Command	Description
Enter the global configuration mode.	**configure terminal**	-
Configure the maximum number of hops in an MST region.	**spanning-tree mst max-hops** *max-hops-value*	Mandatory. By default, the maximum number of hops in an MST region is 20.

5.2.3. Configure Spanning Tree Port Properties

Configuration Condition

None

Configure the Priority of a Port

A port ID consists of port priority and port index. Port ID affects election of the port role. A smaller port ID indicates a higher priority. One port may have different port priority in different spanning tree instances.

Table 5-9 Configuring the priority of a port

Step	Command	Description
Enter the global configuration mode.	**configure terminal**	-
Enter the layer-2 Ethernet interface configuration mode.	**interface** *interface-name*	Either. After you enter the layer-2 Ethernet interface configuration mode, the subsequent configuration takes effect only on the current port. After you enter the aggregation group configuration mode, the subsequent configuration takes effect only within the aggregation group.
Enter the aggregation group configuration mode.	**link-aggregation** *link-aggregation-id*	
Configuring the priority of a port.	**spanning-tree mst instance** *instance-id* **port-priority** *priority-value*	Mandatory. By default, the priority of the port in all spanning tree instances is 128.

Note:

- The step of port priorities is 16, that is, the valid values include: 0, 16, 32, 48, 64, 80, 96, 112, 128, 144, 160, 176, 192, 208, 224, and 240.

Configure the Default Path Cost Standard for a Port

Compared with the path cost calculated based on the IEEE 802.1D-1998 standard, the path cost calculated based on the IEEE 802.1T-2001 is larger. With the increase of the link rate, the path cost value quickly decreases.

Table 5-10 Configuring the default path cost standard for a port

Step	Command	Description
Enter the global configuration mode.	**configure terminal**	-
Configure the default path cost standard for a port.	**spanning-tree pathcost method** { **dot1D-1998 | dot1T-2001** }	Mandatory. By default, the IEEE 802.1T-2001 standard is used to calculate the default path cost of the port.

Configure the Path Cost of a Port

The port path cost affects election of the port role. A smaller port path cost means a better link. One port may have different port path cost in different spanning tree instances.

Table 5-11 Configuring the path cost of a port

Step	Command	Description
Enter the global configuration mode.	**configure terminal**	-
Enter the layer-2 Ethernet interface configuration mode.	**interface** *interface-name*	Either. After you enter the layer-2 Ethernet interface configuration mode, the subsequent configuration takes effect only on the current port. After you enter the aggregation group configuration mode, the subsequent configuration takes effect only within the aggregation group.
Enter the aggregation group configuration mode.	**link-aggregation** *link-aggregation-id*	

Step	Command	Description
Configure the path cost of a port.	**spanning-tree mst instance** *instance-id* **cost** *cost-value*	Mandatory. By default, the path cost is automatically calculated according to the port rate.

Configure BPDU Packet Length Check

Configure the BPDU packet length check and you can let the port check the length of the received BPDU packet, so as to prevent the attack of the BPDU packet with the invalid length.

Table 5-12 Configuring the BPDU packet length check

Step	Command	Description
Enter the global configuration mode.	**configure terminal**	-
Configure the BPDU packet length check	**spanning-tree bpdu length-check**	Mandatory By default, do not enable the BPDU packet length check

Configure Maximum Length of BPDU Packet

Configure the maximum length of the BPDU packet when performing the BPDU packet length check.

Table 5-13 Configuring the maximum length of the BPDU packet

Step	Command	Description
Enter the global configuration mode.	**configure terminal**	-
Configure the maximum length of the BPDU packet	**spanning-tree bpdu max-length** *max-length*	Mandatory By default, the maximum length od is 1500 bytes.

Configure the Maximum Transmitting Rate of BPDU Packets

The maximum transmitting rate of BPDU packets limits the number of BPDU packets that can be transmitted during the Hello Time of a device. This prevents the device from sending too many BPDU packets which may cause frequent spanning tree calculation for other devices.

Table 5-14 Configuring the maximum transmitting rate of BPDU packets

Step	Command	Description
Enter the global configuration mode.	**configure terminal**	-
Enter the layer-2 Ethernet interface configuration mode.	**interface** *interface-name*	Either. After you enter the layer-2 Ethernet interface configuration mode, the subsequent configuration takes effect only on the current port. After you enter the aggregation group configuration mode, the subsequent configuration takes effect only within the aggregation group.
Enter the aggregation group configuration mode.	**link-aggregation** *link-aggregation-id*	
Configure the maximum transmitting rate of BPDU packets.	**spanning-tree transmit hold-count** *hold-count-number*	By default, a port can send a maximum of 6 BPDU packets within Hello Time.

Configure Source MAC Address Check of BPDU Packet

Configure the source MAC address check of the BPDU packet and you can let the port check the source MAC address of the received BPDU packet, so as to prevent the attack of the BPDU packet from the invalid device.

Table 5-15 Configuring the source MAC check of the BPDU packet

Step	Command	Description
Enter the global configuration mode.	**configure terminal**	-
Enter the layer-2 Ethernet interface configuration mode.	**interface** *interface-name*	Either After you enter the layer-2 Ethernet interface configuration mode, the subsequent configuration takes effect only on the current port. After you enter the aggregation group configuration mode, the subsequent configuration
Enter the aggregation group configuration mode.	**link-aggregation** *link-aggregation-id*	

Step	Command	Description
		takes effect only within the aggregation group.
Configure the source mac check of the BPDU packet	**spanning-tree bpdu src-mac-match** *src-mac*	Mandatory By default, the port does not enable the source MAC address check of the BPDU packet.

Configure Timeout Factor of BPDU Packet

When the network topology is stable, the specified port will send on BPDU packet with a HELLO TIME interval. If the device does not receive the BPDU packet sent by the upstream device within three multiples of HELLO TIME, regard that the network topology changes and trigger the re-election of the spanning tree.

When the network topology is stable and if the downstream device does not receive the BPDU packet in time because the upstream device is busy or other reasons and triggers the re-election, you can configure the timeout factor to avoid the un-necessary calculation.

Table 5-16 Configure the timeout factor of the BPDU packet

Step	Command	Description
Enter the global configuration mode.	**configure terminal**	-
Configure the time factor of the BPDU packet	**spanning-tree timer-facor** *times-number*	By default, if the device does not receive the BPDU packet sent by the upstream device within three multiples of HELLO TIME, regard that the network topology changes and trigger the re-election of the spanning tree. In the stacking environment, it is suggested to configure the timeout factor as 6.

Configure an Edge Port

Edge ports are the ports that are directly connected to user terminals. If an edge port is UP/DOWN, it does not cause temporary loops. Therefore, an edge port can quickly migrate from the Discarding status to the Forwarding status without delay time. In addition, if an edge port is UP/DOWN, it does not send TC BPDUs. This prevents unnecessary spanning tree re-calculation.

If an edge port receives BPDU packets, it becomes a non-edge port again. Then, the port can become the edge port again only after it is reset.

Table 5-17 Configuring edge ports

Step	Command	Description
Enter the global configuration mode.	**configure terminal**	-
Enter the layer-2 Ethernet interface configuration mode.	**interface** *interface-name*	Either After you enter the layer-2 Ethernet interface configuration mode, the subsequent configuration takes effect only on the current port. After you enter the aggregation group configuration mode, the subsequent configuration takes effect only within the aggregation group.
Enter the aggregation group configuration mode.	**link-aggregation** *link-aggregation-id*	
Configure an edge port.	**spanning-tree portfast edgeport**	Mandatory. By default, a port is a not an edge port.

Configure Auto Detection of Edge Port

You can configure the auto detection of the edge port to let the port connected to the terminal be automatically identified as edge port, so as to prevent the online/offline of the terminal device from causing spanning tree re-calculation and network shock.

If receiving the BPDU packet after being identified as the edge port, re-change to the non-edge port.

Table 5-18 Configure the auto detection of the edge port

Step	Command	Description
Enter the global configuration mode.	**configure terminal**	-
Enter the layer-2 Ethernet interface configuration mode.	**interface** *interface-name*	Either After you enter the layer-2 Ethernet interface configuration mode, the subsequent configuration takes effect only on the current port. After you enter the aggregation group configuration mode, the subsequent configuration takes
Enter the aggregation group configuration mode.	**link-aggregation** *link-aggregation-id*	

Step	Command	Description
		effect only within the aggregation group.
Configure the auto detection of the edge port	**spanning-tree portfast autoedge**	Mandatory By default, the port disables the auto detection of the edge port.

Force Auto Detection of Edge Port

Because of the configuration or environment, the current port may be identified as the edge port or non-edge port wrongly. Here, the user can execute the command to trigger the port to detect the edge port, making the port correctly identify itself as the edge port.

Table 5-19 Configure the auto detection of the edge port

Step	Command	Description
Enter the global configuration mode.	**configure terminal**	-
Enter the layer-2 Ethernet interface configuration mode.	**interface** *interface-name*	Either After you enter the layer-2 Ethernet interface configuration mode, the subsequent configuration takes effect only on the current port. After you enter the aggregation group configuration mode, the subsequent configuration takes effect only within the aggregation group.
Enter the aggregation group configuration mode.	**link-aggregation** *link-aggregation-id*	
Force the auto detection of the edge port	**spanning-tree portfast autoedge force**	Mandatory

Note:

- The command can take effect only when the port is enabled with the auto edge port detection.

Configure the Port Link Type

If two devices are directly connected, you can configure the port link type to point-to-point link. The ports of the point-to-point link type can quickly migrate from the Discarding status to the Forwarding status without delay time.

Table 5-20 Configuring the port link type

Step	Command	Description
Enter the global configuration mode.	**configure terminal**	-
Enter the layer-2 Ethernet interface configuration mode.	**interface** *interface-name*	Either. After you enter the layer-2 Ethernet interface configuration mode, the subsequent configuration takes effect only on the current port. After you enter the aggregation group configuration mode, the subsequent configuration takes effect only within the aggregation group.
Enter the aggregation group configuration mode.	**link-aggregation** *link-aggregation-id*	
Configure the port link type.	**spanning-tree link-type** { **point-to-point | shared** }	Mandatory. By default, the port link type is set according to the port duplex mode. If the port works in the full duplex mode, the port is set to the point-to-point link type. If the port works in the half duplex mode, the port is set to the shared link type.

Note:

- The port link type should be configured according to the actual physical link. If the actual physical link of the port is not point-to-point link, but is configured as the point-to-point link wrongly, it may cause the temporary loop.
- When the local port link type is the shared link type, the local port does not support the auto identify function of the edge port. If the peer port performs the auto identify function of the edge port, it may make the peer port be identified as the edge port wrongly.

5.2.4. Configure the Working Mode of a Spanning Tree

The working mode of a spanning tree determines the mode in which devices run and determines the encapsulation format of BPDU packets that are sent out. If a port that works in the MSTP mode is found to be connected to a device that runs RSTP, the port automatically migrates to the RSTP mode. If a port that works in the MSTP mode or MSTP mode is found to be connected to a device that runs STP, the port automatically migrates to the STP compatible mode.

Configuration Condition

None

Configure the Working Mode of a Spanning Tree

Table 5-21 Configuring the working mode of a spanning tree

Step	Command	Description
Enter the global configuration mode.	**configure terminal**	-
Configure the working mode of a spanning tree.	**spanning-tree mode** { **stp | rstp | mstp** }	Mandatory. By default, the working mode of a spanning tree is MSTP.

5.2.5. Configure the Spanning Tree Protection Function

Configuration Condition

None

Configure the BPDU Guard Function

For an access layer device, the access port is usually directly connected to the user terminal or file server. At this time, the port is set to the edge port to realize fast migration of port statuses. When an edge port receives BPDU packets, it automatically changes to a non-edge port to cause re-generation of the spanning tree. Normally, an edge port does not receive BPDU packets. However, if someone send faked BPDU packets to attack the device in a malicious manner, network flapping may be caused. The BPDU Guard function is used to prevent such attacks. If an edge port on which the BPDU Guard function is enabled receives BPDU packets, the port is closed.

Table 5-22 Configuring the BPDU guard function

Step	Command	Description
Enter the global configuration mode.	**configure terminal**	-
Enter the layer-2 Ethernet interface configuration mode.	**interface** *interface-name*	Either. After you enter the layer-2 Ethernet interface configuration mode, the subsequent configuration takes effect only on the current port. After you enter the aggregation group configuration mode, the subsequent configuration takes effect only within the aggregation group.
Enter the aggregation group configuration mode.	**link-aggregation** *link-aggregation-id*	

Step	Command	Description
Configure the BPDU Guard function.	**spanning-tree bpdu guard**	Mandatory. By default, the BPDU Guard function is disabled on the port.

Configure the BPDU Filter Function

After the BPDU Filter function is enabled on an edge port, the port does not send or receive BPDU packets.

Table 5-23 Configuring the BPDU filter function

Step	Command	Description
Enter the global configuration mode.	**configure terminal**	-
Enter the layer-2 Ethernet interface configuration mode.	**interface** *interface-name*	Either. After you enter the layer-2 Ethernet interface configuration mode, the subsequent configuration takes effect only on the current port. After you enter the aggregation group configuration mode, the subsequent configuration takes effect only within the aggregation group.
Enter the aggregation group configuration mode.	**link-aggregation** *link-aggregation-id*	
Configure the BPDU Filter function.	**spanning-tree bpdu filter**	Mandatory. By default, the BPDU Filter function is disabled.

Configure the Flap Guard Function

In a stable topology environment, the root port is usually not changed. However, if the links in the network are not stable or the network experiences attacks with external BPDU packets, frequent switchover of root ports may be caused, and finally network flapping is caused.

The Flap Guard function prevent frequent switchover of root ports. After the Flap Guard function is enabled, if the root port role change frequency of a spanning tree instance exceeds the specified threshold, the root port of the instance enters the Flap Guard status. In this case, the root port is always in the Discarding status, and it starts normal spanning tree calculation only after the recovery time times out.

Table 5-24 Configuring the flap guard function

Step	Command	Description
Enter the global configuration mode.	**configure terminal**	-
Enable the Flap Guard function.	**spanning-tree flap-guard enable**	Mandatory. By default, the Flap Guard function is disabled.
Configure the maximum number of root port changes that are allowed within a detection period.	**spanning-tree flap-guard max-flaps** *max-flaps-number* **time** *seconds*	Optional. By default, after the Flap Guard function is enabled, if five root port role changes occurs for an instance within 10 seconds, the port enters the Flap Guard status.
Configure the Flap Guard recovery time.	**spanning-tree flap-guard max-flaps** *count* **time** *seconds*	Optional. By default, the Flap Guard recovery time is 30 seconds.

Configure the Loop Guard Function

The local device maintains the statuses of the root port and other blocked ports according to the BPDU packets that are periodically sent by the upstream device. In the case of link congestion or unidirectional link failure, the ports fail to receive BPDU packets from the upstream device, the spanning tree message on the port times out. Then, the downstream devices re-elect port roles. The downstream device ports that fail to receive BPDU packets change to designated port, while blocked ports migrate to the Forwarding status, resulting in loops in the switching network.

The Loop Guard function can restrain generation of such loops. After the Loop Guard function is enabled on a port, if the port times out owing to the failure to receive BPDU packets from the upstream device, in re-calculating the port role, the port is set to the Discarding status, and the port does not participate in spanning tree calculation. If an instance on the port receives BPDU packets again, the port participates in spanning tree calculation again.

Table 5-25 Configuring the loop guard function

Step	Command	Description
Enter the global configuration mode.	**configure terminal**	-
Enter the layer-2 Ethernet interface configuration mode.	**interface** *interface-name*	Either.

Step	Command	Description
Enter the aggregation group configuration mode.	**link-aggregation** *link-aggregation-id*	After you enter the layer-2 Ethernet interface configuration mode, the subsequent configuration takes effect only on the current port. After you enter the aggregation group configuration mode, the subsequent configuration takes effect only within the aggregation group.
Configure the Loop Guard function.	**spanning-tree guard** { **loop** | **root** | **none** }	Mandatory. By default, the Loop Guard function is disabled on the port.

Note:

- On a port, either the Root Guard function or the Loop Guard function can be enabled at a time.

Configure the Root Guard Function

The root bridge and backup root bridge of a spanning tree must be in the same region, especially the CIST root bridge and its backup bridge. In network design, usually the CIST root bridge and its backup bridge are placed in the core region with high bandwidth. However, owning to incorrect configuration or malicious attacks in the network, the legal root bridge in the network may receive a BPDU packet with a higher priority. In this way, the current legal bridge may lose its role as the root bridge, and improper change of the network topology is caused. The illegal change may lead the traffic that should be transmitted through a high-speed link to a low-speed link, causing network congestion.

The Root Guard function prevents occurrence of such case. If the Root Guard function is enabled on a port, the port can only act as the designated port in all instances. If the port receives a better BPDU configuration message, the port is set to the Discarding status. If it does not receive better BPDU configuration message in a period of time, the port resumes its previous status. It is recommended that you enable the Root Guard function on the specified port of the root bridge.

Table 5-26 Configuring the root guard function

Step	Command	Description
Enter the global configuration mode.	**configure terminal**	-
Enter the layer-2 Ethernet interface configuration mode.	**interface** *interface-name*	Either. After you enter the layer-2 Ethernet interface configuration mode, the subsequent configuration takes effect only on the current port. After you enter the aggregation group configuration mode, the subsequent configuration takes effect only within the aggregation group.
Enter the aggregation group configuration mode.	**link-aggregation** *link-aggregation-id*	
Configure the Root Guard function.	**spanning-tree guard** { **loop** | **root** | **none** }	Mandatory. By default, the Root Guard function is disabled on the port.

Note:

- On a port, either the Root Guard function or the Loop Guard function can be enabled at a time.

Configure TC Guard Function

When the device discovers the network topology change, generate the TC packet to inform the other devices in the environment of the network topology change. When the device receives the TC packet, refresh the address. When the topology is not stable or the TC packet is man-made to attack, generate TC in the network frequently and as a result, the device refreshes the address repeatedly, affecting the spanning tree calculation and resulting in the high CPU occupation.

TC GUARD can effectively prevent the case. After configuring TC GUARD on the current port and the device receives the TC packet, do not process the TC tag or spreading TC any more, so as to prevent the attack of the TC packet for the network.

Table 5-27 Configure the TC Guard function

Step	Command	Description
Enter the global configuration mode.	**configure terminal**	-
Enter the layer-2 Ethernet interface configuration mode.	**interface** *interface-name*	Either. After you enter the layer-2 Ethernet interface configuration mode, the subsequent configuration takes effect only on the current port. After you enter the aggregation group configuration mode, the subsequent configuration takes effect only within the aggregation group.
Enter the aggregation group configuration mode.	**link-aggregation** *link-aggregation-id*	
Configure the TC Guard function	**spanning-tree tc-guard enable**	Mandatory By default, do not enable the TC Guard function of the port.

Configure the TC Protection Function

If the network topology changes, to ensure normal forwarding of service data during the topology change process, when devices handle TC packets, they will refresh the MAC addresses. Attacks with faked TC packets may cause the devices to refresh MAC addresses frequently. This affects calculation of the spanning tree and leads to a high CPU occupancy.

The TC protection function prevents occurrence of such case. After the TC protection function is enabled, once a TC packet is received within the TC protection interval, the TC counter counts one. If the TC counter is equal to or larger than the threshold, it enters a suppressed status. Then, the devices do not refresh MAC addresses in handling later TC packets. After the TC protection interval, the suppressed status is changed to the normal status, the TC counter is cleared and started again.

Table 5-28 Configuring the TC protection function

Step	Command	Description
Enter the global configuration mode.	**configure terminal**	-
Enable the TC protection function.	**spanning-tree tc-protection enable**	Optional. By default, the TC protection function is enabled.
Enter the layer-2 Ethernet interface configuration mode.	**interface** *interface-name*	Either. After you enter the layer-2 Ethernet interface configuration mode, the subsequent configuration takes effect only on the current port. After you enter the aggregation group configuration mode, the subsequent configuration takes effect only within the aggregation group.
Enter the aggregation group configuration mode.	**link-aggregation** *link-aggregation-id*	
Configure a TC protection interval.	**spanning-tree tc-protection interval** *seconds*	Mandatory. By default, the TC protection interval is 2 seconds.
Configure the TC protection threshold.	**spanning-tree tc-protection threshold** *threshold-value*	Mandatory. By default, the TC protection threshold is 3.

5.2.6. Spanning Tree Monitoring and Maintaining

Table 5-29 Spanning tree monitoring and maintaining

Command	Description
clear spanning-tree detected-protocols	Performs the mCheck operation globally or on a specified port.
clear spanning-tree bpdu statistics [interface *interface-name* **| link-aggregation** *link-aggregation-id* **]**	Clears the BPDU statistics information on all or specified ports

Command	Description
show spanning-tree detail	Displays the detailed status information of the spanning tree
show spanning-tree guard [configuration | interface *interface-name* **| link-aggregation** *link-aggregation-id***]**	Displays the configuration and status information of the spanning tree protection function on the port
show spanning-tree { interface *interface-name* | **link-aggregation** *link-aggregation-id* **} [detail]**	Displays the spanning tree status information of the specified port or aggregation group
show spanning-tree mst [**configuration** [**current | pending**] | **detail | instance** *instance-id* [**detail**] | { **interface** *interface-name* | **link-aggregation** *link-aggregation-id* } [**instance** *instance-id*]]	Displays the configuration and status information about the spanning tree.
show configuration { current | pending }	Displays the configuration of MST regions.

5.3. Spanning Tree Typical Configuration Example

5.3.1. MSTP Typical Application

Network Requirements

- Four devices in the network are in the same MST domain. Device1 and Device2 convergence layer devices, while Device3 and Device4 are access layer devices.
- To reasonably balance traffic on the links to realize load sharing and redundancy backup, configure packets of VLAN2 to be forwarded following instance 1. The root bridge of instance 1 is Device1. Packets of VLAN3 are forwarded following instance 2. The root bridge of instance 2 is Device2. Packets of VLAN4 are forwarded following instance 0.

Network Topology

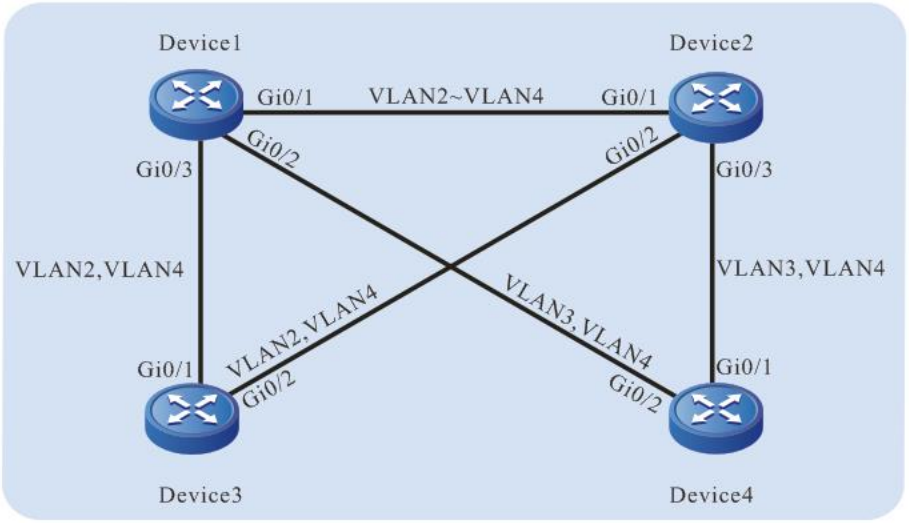


Figure 5-1 Networking for MSTP typical application

Configuration Steps

Step 1: Configure VLANs, and configure the link type of the ports.

#On Device1, create VLAN2-VLAN4, configure the link type of port gigabitethernet0/1 to Trunk and allow services of VLAN2-VLAN4 to pass.

```
Device1(config)#vlan 2-4
Device1(config)#interface gigabitethernet 0/1
Device1(config-if-gigabitethernet0/1)#switchport mode trunk
Device1(config-if-gigabitethernet0/1)#switchport trunk allowed vlan add 2-4
Device1(config-if-gigabitethernet0/1)#exit
```

#On Device1, configure the link type of port gigabitethernet0/2 to Trunk and allow services of VLAN3 and VLAN4 to pass. Configure the link type of port gigabitethernet0/3 to Trunk and allow services of VLAN2 and VLAN4 to pass. (Omitted)

#On Device2, create VLAN2-VLAN4. Configure the link type of ports gigabitethernet0/1-gigabitethernet0/3 to Trunk, configure gigabitethernet0/1 to allow services of VLAN2-VLAN4 to pass, gigabitethernet0/2 to allow services of VLAN2 and VLAN4 to pass, and gigabitethernet0/3 to allow services of VLAN3 and VLAN4 to pass. (Omitted)

#On Device3, create VLAN2-VLAN4, configure the link type of port gigabitethernet0/1-gigabitethernet0/2 to Trunk and allow services of VLAN2-VLAN4 to pass. (Omitted)

#On Device4, create VLAN3 and VLAN4, configure the link type of port gigabitethernet0/1-gigabitethernet0/2 to Trunk and allow services of VLAN3 and VLAN4 to pass. (Omitted)

Step 2: Configure an MST region.

#On Device1, configure an MST region. Set the domain name to admin, the revision level to 1, map instance 1 to VLAN2, map instance 2 to VLAN3, and activate the MST region.

```
Device1#configure terminal
Device1(config)#spanning-tree mst configuration
Device1(config-mst-region)#region-name admin
```

```
Device1(config-mst-region)#revision-level 1
Device1(config-mst-region)#instance 1 vlan 2
Device1(config-mst-region)#instance 2 vlan 3
Device1(config-mst-region)#active configuration pending
Device1(config-mst-region)#exit
```

Note:

- The MST region configuration of Device2, Device3, and Device 4 is far different from that of Device1. (Omitted)

#On Device1, configure the priority of MSTI 1 to 0. On Device2, configure the priority of MSTI 2 to 0.

```
Device1(config)#spanning-tree mst instance 1 priority 0
Device2(config)#spanning-tree mst instance 2 priority 0
```

#On Device1, enable the spanning tree globally.

```
Device1(config)#spanning-tree enable
```

Note:

- The configuration for enabling the spanning tree globally on Device2, Device3, and Device 4 is far different from that on Device1. (Omitted)

Step 3: Check the result.

#After the network topology is stable, check the calculation result of all spanning tree instances.

```
Device1#show spanning-tree mst
Spanning-tree enabled protocol mstp
MST Instance 00        vlans mapped: 1,4-4094
 Bridge              address 0000.0000.008b priority 32768
 Region root         address 0000.0000.008b priority 32768
Designated root      address 0000.0000.008b priority 32768
                     root: 0, rpc: 0, epc: 0, hop: 20
 Operational  hello time 2, forward time 15, max age 20
 Configured   hello time 2, forward time 15, max age 20, max hops 20, hold count 6
 Flap guard : admin false, max count 5, detect period 10s, recovery period 30s
 Tc protection: admin true, threshold 3, interval 2s, rxTcCnt 0, status:NORMAL
 Bpdu length-check: true, allowed bpdu max length is 1600, bpdu illegal length
packets count: 0
 Autoedge swap-check: true
 Swap-delay time: 30
 Configured timer factor: 3
 Topology Change Count:4, last change occured:0 hour 1 minute 0 second(60
seconds)
        Interface  Role  Sts     Cost  Prio.Nbr Type
```

```
-------------------- ----- ---- --------- --------- --------------------------
gi0/1              Desg  FWD    20000   128.001 P2P
gi0/2              Desg  FWD    20000   128.002 P2P
gi0/3              Desg  FWD    20000   128.003 P2P
MST Instance 01        vlans mapped: 2
 Bridge ID           address 0000.0000.008b priority 1/0
 Designated root     address 0000.0000.008b priority 1
                  root: 0, rpc: 0, hop: 20
Topology Change Count:4, last change occured:0 hour 1 minute 0 second(60
seconds)
        Interface  Role  Sts     Cost  Prio.Nbr Type
-------------------- ----- ---- --------- --------- --------------------------
gi0/1              Desg  FWD    20000   128.001 P2P
gi0/3              Desg  FWD    20000   128.003 P2P
MST Instance 02        vlans mapped: 3
 Bridge ID           address 0000.0000.008b priority 32770/32768
 Designated root     address 001f.ce54.5c96 priority 2
                  root: 32769, rpc: 20000, hop: 19
Topology Change Count:4, last change occured:0 hour 1 minute 0 second(60
seconds)
        Interface  Role  Sts     Cost  Prio.Nbr Type
-------------------- ----- ---- --------- --------- --------------------------
gi0/1              Root  FWD    20000   128.001 P2P
gi0/2              Desg  FWD    20000   128.002 P2P
```

#On Device2, query the calculation result of all spanning tree instances. According to the result, port gigabitethernet0/2 of Device2 are blocked in both instance 0 and instance 1.

```
Device2#show spanning-tree mst
Spanning-tree enabled protocol mstp
MST Instance 00        vlans mapped:  1,4-4094
 Bridge              address 001f.ce54.5c96 priority 32768
 Region root         address 0000.0000.008b priority 32768
Designated root      address 0000.0000.008b priority 32768
                  root: 32769, rpc: 20000, epc: 0, hop: 19
 Operational  hello time 2, forward time 15, max age 20
 Configured   hello time 2, forward time 15, max age 20, max hops 20, hold count 6
 Flap guard : admin false, max count 5, detect period 10s, recovery period 30s
 Tc protection: admin true, threshold 3, interval 2s, rxTcCnt 0, status:NORMAL
```

```
 Bpdu length-check: true, allowed bpdu max length is 1600, bpdu illegal length packets count: 0
 Autoedge swap-check: true
 Swap-delay time: 30
 Configured timer factor: 3
 Topology Change Count:4, last change occured:0 hour 1 minute 0 second(60 seconds)
        Interface  Role  Sts     Cost  Prio.Nbr Type
------------------- ----- ---- --------- --------- -------------------------
gi0/1              Root  FWD     20000   128.001 P2P
gi0/2              Alte  DIS     20000   128.002 P2P
gi0/3              Desg  FWD     20000   128.003 P2P
MST Instance 01        vlans mapped:  2
 Bridge ID           address 001f.ce54.5c96 priority 32769/32768
 Designated root     address 0000.0000.008b priority 1
                  root: 32769, rpc: 20000, hop: 19
Topology Change Count:4, last change occured:0 hour 1 minute 0 second(60 seconds)
        Interface  Role  Sts     Cost  Prio.Nbr Type
------------------- ----- ---- --------- --------- -------------------------
gi0/1              Root  FWD     20000   128.001 P2P
gi0/2              Alte  DIS     20000   128.002 P2P
MST Instance 02        vlans mapped:  3
 Bridge ID           address 001f.ce54.5c96 priority 2/0
 Designated root     address 001f.ce54.5c96 priority 2
                  root: 0, rpc: 0, hop: 20
Topology Change Count:4, last change occured:0 hour 1 minute 0 second(60 seconds)
        Interface  Role  Sts     Cost  Prio.Nbr Type
------------------- ----- ---- --------- --------- -------------------------
gi0/1              Desg  FWD     20000   128.001 P2P
gi0/3              Desg  FWD     20000   128.003 P2P
```

#On Device3, query the calculation result of all spanning tree instances.

```
Device3#show spanning-tree mst
Spanning-tree enabled protocol mstp
MST Instance 00        vlans mapped: 1,4-4094
 Bridge              address 0000.0305.070a priority 32768
 Region root         address 0000.0000.008b priority 32768
```

```
Designated root      address 0000.0000.008b priority 32768
                     root: 32769, rpc: 20000, epc: 0, hop: 19
 Operational  hello time 2, forward time 15, max age 20
 Configured   hello time 2, forward time 15, max age 20, max hops 20, hold count 6
 Flap guard : admin false, max count 5, detect period 10s, recovery period 30s
 Tc protection: admin true, threshold 3, interval 2s, rxTcCnt 0, status:NORMAL
 Bpdu length-check: true, allowed bpdu max length is 1600, bpdu illegal length packets count: 0
 Autoedge swap-check: true
 Swap-delay time: 30
 Configured timer factor: 3
 Topology Change Count:4, last change occured:0 hour 1 minute 0 second(60 seconds)
        Interface  Role  Sts     Cost  Prio.Nbr Type
-------------------- ----- ---- --------- --------- --------------------------
gi0/1              Root  FWD     20000   128.001 P2P
gi0/2              Desg  FWD     20000   128.002 P2P
MST Instance 01       vlans mapped: 2
 Bridge ID           address 0000.0305.070a priority 32769/32768
 Designated root      address 0000.0000.008b priority 1
                     root: 32769, rpc: 20000, hop: 19
Topology Change Count:4, last change occured:0 hour 1 minute 0 second(60 seconds)
        Interface  Role  Sts     Cost  Prio.Nbr Type
-------------------- ----- ---- --------- --------- --------------------------
gi0/1              Root  FWD     20000   128.001 P2P
gi0/2              Desg  FWD     20000   128.002 P2P
```

#On Device4, query the calculation result of all spanning tree instances. According to the result, port gigabitethernet0/1 of Device4 is blocked in instance 0, and port gigabitethernet0/2 is blocked in instance 2.

```
Device4#show spanning-tree mst
Spanning-tree enabled protocol mstp
MST Instance 00       vlans mapped:  1,4-4094
 Bridge              address 001f.ce58.dc0c priority 32768
 Region root         address 0000.0000.008b priority 32768
Designated root      address 0000.0000.008b priority 32768
                     root: 32769, rpc: 20000, epc: 0, hop: 19
 Operational  hello time 2, forward time 15, max age 20
 Configured   hello time 2, forward time 15, max age 20, max hops 20, hold count 6
```

Flap guard : admin false, max count 5, detect period 10s, recovery period 30s

Tc protection: admin true, threshold 3, interval 2s, rxTcCnt 0, status:NORMAL

Bpdu length-check: true, allowed bpdu max length is 1600, bpdu illegal length packets count: 0

Autoedge swap-check: true

Swap-delay time: 30

Configured timer factor: 3

Topology Change Count:4, last change occured:0 hour 1 minute 0 second(60 seconds)

Interface Role Sts Cost Prio.Nbr Type

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

gi0/1 Alte DIS 20000 128.001 P2P

gi0/2 Root FWD 20000 128.002 P2P

MST Instance 02 vlans mapped: 3

Bridge ID address 001f.ce58.dc0c priority 32770/32768

Designated root address 001f.ce54.5c96 priority 2

root: 32769, rpc: 20000, hop: 19

Topology Change Count:4, last change occured:0 hour 1 minute 0 second(60 seconds)

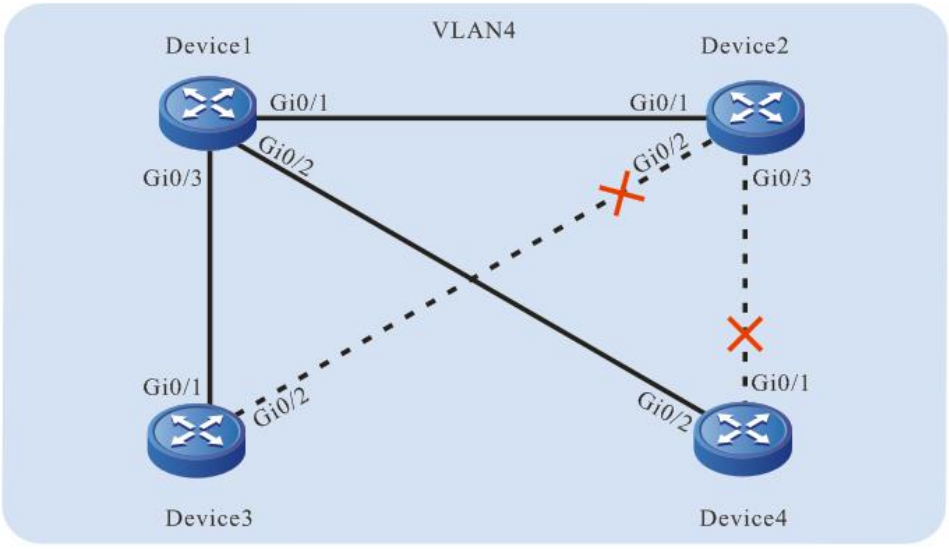
Interface Role Sts Cost Prio.Nbr Type

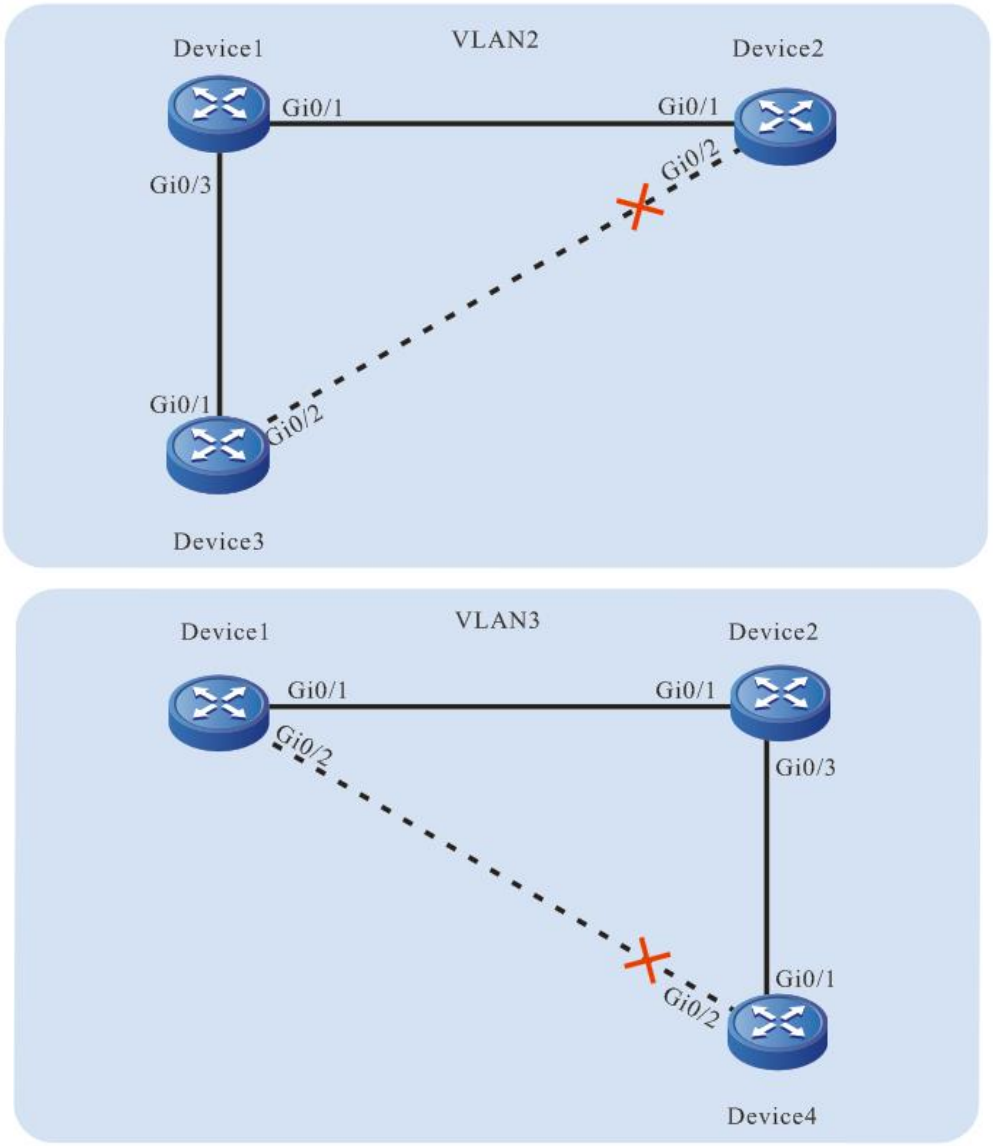
---------- ----- ---- --------- --------- -------------------------

gi0/1 Root FWD 20000 128.001 P2P

gi0/2 Alte DIS 20000 128.002 P2P

Based on the spanning tree calculation result of the four devices, the tree diagrams corresponding to MSTI 0 (mapped to VLAN4), MSTI 1 (mapped to VLAN2), MSTI 2 (mapped to VLAN3) are obtained, as shown in the following figure.




VLAN2
Device1
Device2
Gi0/1
Gi0/1
Gi0/3
Gi0/2
Gi0/1
Gi0/2
Device3
VLAN3
Device1
Device2
Gi0/1
Gi0/1
Gi0/2
Gi0/3
Gi0/1
Gi0/2
Device4

6. LOOPBACK DETECTION

6.1. Overview

In the Ethernet, if the destination of some packet fails to be recognized, they will be flooded in a VLAN. If a loop exists in the network, the packets circulate and multiply without limit, and finally they will use up the bandwidth. Then, the network fails to provide normal communication.

There are two types of loops, loop between different Ethernet interfaces of a device, and loop on one Ethernet interface of a device. The two types of loops can be detected through loopback detection.

After the loopback detection function is enabled, the Ethernet port sends loopback detection packets with an interval to check whether a loop exists in the network. When the Ethernet port receives the loopback detection packet sent by the local device, it determines that a loop exists in the network. Then, disable the Ethernet port to prevent the local loop from affecting the entire network.

6.2. Loopback Detection Function Configuration

Table 6-1 Loopback Detection Function List

Configuration Tasks	
Configure basic functions of loopback detection.	Enable the global loopback detection control switch.
	Enable the loopback detection control switch of an Ethernet port or aggregation group.
Configure basic parameters of loopback detection.	Configure the interval at which loopback detection packets are sent.
	Configure the Error-Disable action on an Ethernet port.

6.2.1. Configure Basic Functions of Loopback Detection

Configuration Condition

None

Enable the Global Loopback Detection Control Switch

The global loopback detection control switch is used to enable the global loopback detection function. The loopback detection configuration of an Ethernet port takes effect only after the global loopback detection control switch is enabled.

Table 6-2 Enabling the Global Loopback Detection Control Switch

Step	Command	Description
Enter the global configuration mode.	**configure terminal**	-
Enable the global loopback detection control switch.	**loopback-detection enable**	Mandatory. By default, the global loopback detection control switch is disabled.

Enable the Loopback Detection Control Switch of an Ethernet Port or Aggregation Group

After the loopback detection function is enabled, the Ethernet port sends loopback detection packets with an interval to check whether a loop exists in the network.

Table 6-3 Enabling the Loopback Detection Control Switch of an Ethernet Port or Aggregation Group

Step	Command	Description
Enter the global configuration mode.	**configure terminal**	-
Enter the L2 Ethernet interface configuration mode.	**interface** *interface-name*	Either After you enter the L2 Ethernet interface configuration mode, the subsequent configuration takes effect only on the current Ethernet port. After you enter the aggregation group configuration mode, the subsequent configuration takes effect only within the aggregation group.
Enter the aggregation group configuration mode.	**link-aggregation** *link-aggregation-id*	
Enable the loopback detection control	**loopback-detection enable**	Mandatory.

Step	Command	Description
switch of an Ethernet port or aggregation group.		By default, the loopback detection control switch of an Ethernet port or aggregation group is disabled.

Note:

- In loopback detection configuration task, you must enable the global loopback detection control switch before the loopback detection configuration on an Ethernet port takes effect.

6.2.2. Configure Basic Parameters of Loopback Detection

Configuration Condition

None

Configure the Interval at Which Loopback Detection Packets Are Sent

In a loopback detection, loopback detection packets are sent periodically to detect loops in the network. You can modify the interval at which loopback detection packets are sent according to the actual network requirement.

Table 6-4 Configuring the Interval at Which Loopback Detection Packets Are Sent

Step	Command	Description
Enter the global configuration mode.	**configure terminal**	-
Enter the L2 Ethernet interface configuration mode.	**interface** *interface-name*	Either After you enter the L2 Ethernet interface configuration mode, the subsequent configuration takes effect only on the current Ethernet port. After you enter the aggregation group configuration mode, the subsequent configuration takes effect only within
Enter the aggregation group configuration mode.	**link-aggregation** *link-aggregation-id*	

Step	Command	Description
		the aggregation group.
Configure the interval at which loopback detection packets are sent.	**loopback-detection enable interval-time** *interval-time-value*	Mandatory. By default, the interval at which loopback detection packets are sent is 30 seconds.

Configure the Error-Disable Action on an Ethernet Port

If the Ethernet port allows the Error-Disable action, the Ethernet port is controlled. After an Ethernet port detects a loop, it performs the Error-Disable action to close the Ethernet port so as to eliminate the loop. If the Ethernet port is not in the controlled status, the Ethernet port only prints loop prompt message instead of closing the Ethernet port. In this case, the loop has not been eliminated.

Table 6-5 Configuring the Error-Disable Action on the Ethernet port

Step	Command	Description
Enter the global configuration mode.	**configure terminal**	-
Enter the L2 Ethernet interface configuration mode.	**interface** *interface-name*	Either After entering the L2 Ethernet interface configuration mode, the subsequent configuration takes effect only on the current Ethernet interface. After entering the aggregation group configuration mode, the subsequent configuration takes effect only on the aggregation group.
Enter the aggregation group configuration mode.	**link-aggregation** *link-aggregation-id*	
Configure whether the Ethernet port	**loopback-detection enable control**	Mandatory. By default, after the Ethernet port

Step	Command	Description
allows the Error-Disable function.		detects a loop, it performs the Error-Disable action.

6.2.3. Loopback Detection Monitoring and Maintaining

Table 6-6 Loopback Detection Monitoring and Maintaining

Command	Description
show loopback-detection [**interface** *interface-name* | **link-aggregation** *link-aggregation-id*]	Displays the configuration information of all Ethernet ports or a specified Ethernet port in loopback detection.

6.3. Typical Configuration Example of Loopback Detection

6.3.1. Configure Remote Loopback Detection

Network Requirements

- Device1 and Device2 are directly connected, and Device2 has two L2 Ethernet ports which form a self-loop.
- On Device1, loopback detection has been enabled.
- After Device1 detects a loop, it closes the interconnected Ethernet ports to eliminate the loop.

Network Topology

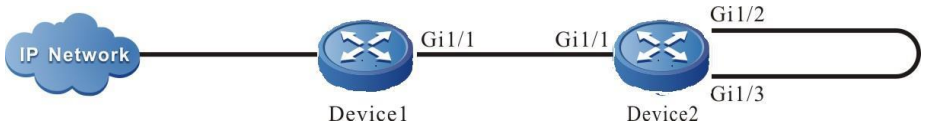


Figure 6-1 Networking for Configuring the Remote Loopback Detection Function

Configuration Steps of L2 Ethernet Interface

Step 1: Configure VLANs, and configure the link type of the L2 Ethernet port.

#On Device1, create VLAN2.

```
Device1#configure terminal
Device1(config)#vlan 2
Device1(config-vlan2)#exit
```

#On Device1, configure the link type of L2 Ethernet port gigabitethernet1/1 to Trunk and allow services of VLAN2 to pass.

```
Device1(config)#interface gigabitethernet 1/1
Device1(config-if-gigabitethernet1/1)#switchport mode trunk
Device1(config-if-gigabitethernet0/1)#switchport trunk allowed vlan add 2
```

```
Device1(config-if-gigabitethernet1/1)#exit
```

#On Device2, create VLAN2.

```
Device2#configure terminal
Device2(config)#vlan 2
Device2(config-vlan2)#exit
```

#On Device2, configure the link type of L2 Ethernet port gigabitethernet1/1, gigabitethernet1/2, and gigabitethernet1/3 as Trunk, permitting the services of VLAN2 to pass; disable the spanning tree on L2 Ethernet interface gigabitethernet1/2 and gigabitethernet1/3.

```
Device2(config)#interface gigabitethernet 1/1-1/3
Device2(config-if-range)#switchport mode trunk
Device2(config-if-range)#no switchport trunk allowed vlan 1

Device2(config-if-range)#switchport trunk allowed vlan add 2
Device2(config-if-range)#exit
Device2(config)#interface gigabitethernet 1/2-1/3
Device2(config-if-range)#no spanning-tree enableDevice2(config-if-range)#exit
```

Step 2: Enable the loopback detection function.

#On Device1, enable the loopback detection function globally.

```
Device1(config)#loopback-detection enable
```

#On Device1, view the loopback detection status.

```
Device1#show loopback-detection
------------------------------------------------------------
Global loopback-detection : ENABLE
------------------- -------- ------- ------------ -------
Interface          Loopback  Time(s) State       Control
------------------- -------- ------- ------------ -------
gi0/1              DISABLE   30      NORMAL      TRUE
gi0/2              DISABLE   30      NORMAL      TRUE
```

#On the L2 Ethernet interface gigabitethernet1/1 of Device1, enable the loopback detection function.

```
Device1(config)#interface gigabitethernet 1/1
Device1(config-if-gigabitethernet1/1)#loopback-detection enable
Device1(config-if-gigabitethernet1/1)#exit
```

Step 3: Check the result.

#On Device1, view the loopback detection status.

After detecting the loop:

```
Device1#show loopback-detection
------------------------------------------------------------
Global loopback-detection : ENABLE
------------------- -------- ------- ------------ -------
Interface          Loopback  Time(s) State       Control
------------------- -------- ------- ------------ -------
gi1/1              ENABLE    30      ERR-DISABLE  TRUE
gi1/2              DISABLE   30      NORMAL       TRUE
```

#On Device1, detect the loop, close L2 Ethernet port gigabitethernet1/1, and output the following prompt information on the device.

```
Jul 30 2014 03:30:30 Device1 MPU0 %LBD-3:%LOOP-BACK-DETECTED : loop-back send tag packet in vlan2 on interface gigabitethernet1/1, detected in vlan2 from interface gigabitethernet1/1

Jul 30 2014 03:30:30 Device1 MPU0 %PORTMGR-LINEPROTO_DOWN-3:Line protocol on interface gigabitethernet1/1, changed state to down

Jul 30 2014 03:30:30 Device1 MPU0 %LBD-3:%LINEPROTO-5-UPDOWN : interface gigabitethernet1/1 link-status changed to err-disable
```

#On Device1, view the status of L2 Ethernet port gigabitethernet1/1, and you can see that the status of L2 Ethernet port gigabitethernet1/1 changes to Down.

```
Device1#show interface gigabitethernet 1/1
Gigabitethernet1/1 configuration information
    Description     :
    Status          : Enabled
    Link            : Down  (Err-disabled)
    Set Speed       : Auto
    Act Speed       : Unknown
    Set Duplex      : Auto
    Act Duplex      : Unknown
    Set Flow Control : Off
    Act Flow Control : Off
    Mdix            : Auto
    Mtu             : 1824
    Port mode       : LAN
    Port ability    : 10M HD,10M FD,100M HD,100M FD,1000M FD
    Link Delay      : No Delay
```

```
        Storm Control   : Unicast Disabled
        Storm Control   : Broadcast Disabled
        Storm Control   : Multicast Disabled
        Storm Action    : None
    Port Type       : Nni
        Pvid        : 1
        Set Medium      : Copper
        Act Medium      : Copper
        Mac Address     : 0000.0000.008b
```

6.3.2. Configure Local Loopback Detection

Network Requirements

- Device1 and Device2 are loop-connected via two links, and all loop-connected L2 Ethernet ports are in one VLAN.
- On Device1, loopback detection has been enabled.
- After Device1 detects a loop, it closes the interconnected L2 Ethernet ports to eliminate the loop.

Network Topology

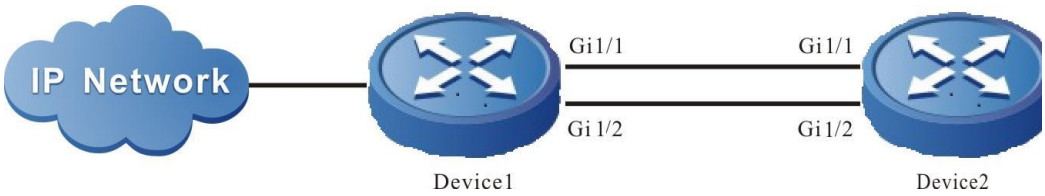


Figure 6-2 Configure the local loopback detection function

Configuration Steps of L2 Ethernet Interface

Step 1: Configure the VLAN and link type of the L2 Ethernet interface.

#Create VLAN2 on Device1.

```
Device1#configure terminal
Device1(config)#vlan 2
Device1(config-vlan2)#exit
```

#On Device1, configure the link type of L2 Ethernet port gigabitethernet1/1 and gigabitethernet1/2 as Trunk, permitting the services of VLAN2 to pass.

```
Device1(config)# interface gigabitethernet 1/1-1/2
Device1(config-if-range)#switchport mode trunk
Device1(config-if-range)#switchport trunk allowed vlan add 2
Device1(config-if-range)#exit
```

#On Device2, create VLAN2.

```
Device2#configure terminal
```

```
Device2(config)#vlan 2
Device2(config-vlan2)#exit
```

#Configure the link type of L2 Ethernet port gigabitethernet1/1 and gigabitethernet1/2 as Trunk, permit the services of VLAN2 to pass, and disable the spanning tree.

```
Device2(config)# interface gigabitethernet 1/1-1/2
Device2(config-if-range)#switchport mode trunk
Device2(config-if-range)#no switchport trunk allowed vlan 1
Device2(config-if-range)#switchport trunk allowed vlan add 2
Device2(config-if-range)#no spanning-tree enable
Device2(config-if-range)#exit
```

Step 2: Enable the loopback detection function.

#On Device1, enable the loopback detection function globally.

```
Device1(config)#loopback-detection enable
```

#On Device1, view the loopback detection status.

```
Device1#show loopback-detection
------------------------------------------------------------
Global loopback-detection : ENABLE
------------------- -------- ------- ------------ -------
Interface          Loopback  Time(s) State       Control
------------------- -------- ------- ------------ -------
gi1/1              DISABLE   30      NORMAL      TRUE
gi1/2              DISABLE   30      NORMAL      TRUE
```

#Enable the loopback detection function on port gigabitethernet1/1 of Device1.

```
Device1(config)#interface gigabitethernet 1/1
Device1(config-if-gigabitethernet1/1)#loopback-detection enable
Device1(config-if-gigabitethernet1/1)#exit
```

Step 3: Check the result.

#On Device1, view the loopback detection status.

After detecting the loop:

```
Device1#show loopback-detection
------------------------------------------------------------
Global loopback-detection : ENABLE
```

```
-------------------- -------- ------- ------------ -------
Interface          Loopback  Time(s) State       Control
-------------------- -------- ------- ------------ -------
gi1/1              ENABLE    30      ERR-DISABLE  TRUE
gi1/2              DISABLE   30      NORMAL       TRUE
```

On Device1, detect the loop, close L2 Ethernet port gigabitethernet1/1, and output the following prompt information on the device:

Jul 30 2014 03:29:59: %LOOP-BACK-DETECTED : loop-back send tag packet in vlan2 on gigabitethernet1/1, detected in vlan2 from gigabitethernet1/2

Jul 30 2014 03:29:59: %LINK-INTERFACE_DOWN-4: interface gigabitethernet1/1, changed state to down

Jul 30 2014 03:29:59: %LINEPROTO-5-UPDOWN : gigabitethernet1/1 link-status changed to err-disable

#On Device1, view the status of L2 Ethernet port gigabitethernet1/1, and you can see that the status of L2 Ethernet port gigabitethernet1/1 changes to Down.

```
Device1#show interface gigabitethernet 1/1
Gigabitethernet1/1 configuration information
    Description     :
    Status          : Enabled
    Link            : Down  (Err-disabled)
    Set Speed       : Auto
    Act Speed       : Unknown
    Set Duplex      : Auto
    Act Duplex      : Unknown
    Set Flow Control : Off
    Act Flow Control : Off
    Mdix            : Auto
    Mtu             : 1824
    Port mode       : LAN
    Port ability    : 10M HD,10M FD,100M HD,100M FD,1000M FD
    Link Delay      : No Delay
    Storm Control   : Unicast Disabled
    Storm Control   : Broadcast Disabled
    Storm Control   : Multicast Disabled
    Storm Action    : None
Port Type       : Nni
```

Pvid : 1

Set Medium : Copper

Act Medium : Copper

Mac Address : 0000.0000.008b

Caution:

- When gigabitethernet 1/1 or gigabitethernet 1/2 of Device1 is L3 Ethernet interface, there is no loop in the networking environment.

7. ERROR-DISABLE MANAGEMENT

7.1. Overview

The Error-Disable function is an error detection and fault recovery mechanism on ports.

Exceptions on ports may degrade the performance of the entire network or bring down the entire network. The Error-Disable function can limit the abnormality within a single device or part of the network, preventing the abnormality from affecting other normal ports and preventing the abnormality from spreading.

If an exception is detected on an open port, the port is automatically closed so that the port will not forward packets. That is, if an error condition is triggered on the port, the port is automatically disabled. This is the Error-Disable management function, and the port status is the Error-Disabled status.

Currently, the following functions are supported: storm suppression, port security, link flapping, DHCP rate limit, BPDU Guard, ARP detection, L2 protocol tunnel, loopback detection (MP1800X does not support storm control action due to chip reasons, so the configuration linked with errdisable can be issued, but it will not take effect.), OAM, and Monitor Link.

If an exception is detected on a port through the above functions, the port is automatically closed, and it is set to the Error-Disabled status. However, this status cannot continue. After the fault is eliminated, the port needs to be enabled again, and the Error-Disabled status of the port needs to be cleared so that the port can continue to forward packets. Here the automatic recovery mechanism of the Error-Disable management function is involved.

7.2. Error-Disable Management Function Configuration

Table 7-1 Error-disable management function list

Configuration Tasks	
Configure Error-Disable basic functions.	Configure Error-Disable error detection.
Configure Error-Disable automatic recovery.	Configure Error-Disable automatic recovery.
	Configure the interval for Error-Disable automatic discovery.

7.2.1. Configure Error-Disable Basic Functions

Configuration Condition

None

Configure Error-Disable Error Detection

After the Error-Disable detection of the specification function is configured, if an exception is detected on the port, the system automatically close the port and set the port to the Error-Disabled status.

Table 7-2 Configuring error-disable error detection

Step	Command	Description
Enter the global configuration mode.	**configure terminal**	-
Configure Error-Disable error detection.	**errdisable detect cause** { **all** | **bpduguard | dai | dhcp-snooping | loopback-detect | storm-control** | **link-flap** | **port-security** }	Mandatory. By default, it is allowed that all the listed functions close a port and set the port to the Error-Disabled status.

7.2.2. Configure Error-Disable Automatic Recovery

Configure Error-Disable Automatic Recovery

The Error-Disable error detection mechanism enables specified functions to close a port. To quickly recover the port so that it can continue to forward packets, an automatic recovery mechanism is provided. With the mechanism, the port is automatically re-enabled after a specified interval.

Table 7-3 Configuring error-disable automatic recovery

Step	Command	Description
Enter the global configuration mode.	**configure terminal**	-
Configure Error-Disable automatic recovery.	**errdisable recovery cause** { **all** | **bpduguard | dai | dhcp-snooping | loopback-detect | storm-control** | **link-flap** | **port-security** }	Mandatory. By default, a port cannot be automatically enabled, and the Error-Disabled status set by the listed functions cannot be automatically cleared. However, by default, a port can be automatically enabled and the Error-Disabled status can be automatically cleared if its status is set by the Link-Flap function.

Configure the Interval for Error-Disable Automatic Discovery

You can configure the interval for a port to automatically recover normal after it port is closed by the Error-Disable error detection mechanism.

Table 7-4 Configuring the interval for error-disable automatic discovery

Step	Command	Description
Enter the global configuration mode.	**configure terminal**	-
Configure the interval for Error-Disable automatic discovery.	**errdisable recovery interval** *interval-value*	Mandatory. By default, the interval at which a port is enabled and its Error-Disabled status is cleared is 300 seconds.

7.2.3. Error-Disable Management Monitoring and Maintaining

Table 7-5 Error-disable management monitoring and maintaining

Command	Description
show errdisable detect	Displays whether it is allowed that all the listed functions close a port and set the port to the Error-Disabled status.
show errdisable recovery	Displays whether a port can be automatically enabled, and whether the Error-Disabled status set by the listed functions can be cleared automatically.
show { **interface** *interface-list* | **link-aggregation** *link-aggregation-id* } **status err-disabled**	Displays the information about Error-Disabled status setting of a specified port or aggregation group.

7.3. Typical Configuration Example of Error-Disable Management

7.3.1. Combination of Error-Disable, Port Security and Storm Suppression

Network Requirements

- PC accesses IP Network through Device. On Device, the port security function, the storm suppression and Error-Disable functions have been enabled.
- When the PC that does not comply with the security policy is connected to the device, close the port via Error-Disable; when the PC that complies with the security policy is connected to the device, but the port receives excessive broadcast packets, disable the port via Error-Disable. Error-Disable can re-enable the port according to the policy.

Network Topology

Figure 7-1 Networking for combination of error-disable, port security and storm suppression

Configuration Steps

Step 1: Configure a VLAN, and configure the link type of the ports.

#On Device, create VLAN2.

```
Device#configure terminal
Device(config)#vlan 2
Device(config-vlan2)#exit
```

#On Device, configure the link type of port gigabitethernet0/1 to Access and allow services of VLAN2 to pass.

```
Device(config)#interface gigabitethernet 0/1
Device(config-if-gigabitethernet0/1)#switchport mode access
Device(config-if-gigabitethernet0/1)#switchport access vlan 2
Device(config-if-gigabitethernet0/1)#exit
```

Step 2: Configure the port security function and storm suppression function.

#On port gigabitethernet0/1 of Device, enable the port security function, permitting the PC with the source MAC address 1.1.1 to access; when the event that does not comply with security happens, enable the storm suppression function, and the pps mode is used to suppress broadcast packets, and the suppression rate is 20pps. When the storm happens, shut down the port.

```
Device(config)#interface gigabitethernet 0/1
Device(config-if-gigabitethernet0/1)# port-security enablestorm-control action shutdown
Device(config-if-gigabitethernet0/1)# port-security permit mac-address 1.1.1storm-control broadcast pps 20
Device(config-if-gigabitethernet0/1)#exit
```

Step 3: Configure the Error-Disable function.

#Enable the port security function and the storm suppression recovery function in Error-Disable, and set the recovery time to 30 seconds.

```
Device(config)#errdisable recovery cause port-securitystorm-control
Device(config)#errdisable recovery interval 30
```

Step 4: Check the result.

#Query the configuration related to Error-Disable.

```
Device#show errdisable recovery

Error disable auto recovery config
interval:30 seconds
ErrDisable Reason   Timer Status
---------------     ------------
bpduguard           Disabled
dai                 Disabled
dhcp-snooping       Disabled
link-flap           Enabled
loopback-detect     Disabled
port-security       Enabled
storm-control       Enabled
```

#When PC1 whose source MAC is not 1.1.1 is connected to the network and sends a large number of broadcast packets, port gigabitethernet0/1 is closed, and the following information is printed:

```
Jan 22 1970 07:00:07: %PORTSEC-5-VIOLATE: Receive unallowed packet, shut downNov 24 2014 15:37:13: %STORM_CONTROL-3: A storm detected on interface gigabitethernet0/1, ActionType:shutdown, StormType: broadcast storm

Jan 22 1970 07:00:07Nov 24 2014 15:37:13: %PORTMGR-LINEPROTO_DOWN-3: Line protocol on interface gigabitethernet0/1, changed state to down.
```

#Query the status of port gigabitethernet0/1.

```
Device#show interface gigabitethernet 0/1

gigabitethernet0/1 configuration information
    Description     :
    Status          : Enabled
    Link            : Down (Err-disabled)
    Set Speed       : Auto
    Act Speed       : 1000Unknown
    Def Speed Set Duplex      : Auto
    DefAct Duplex       : AutoUnknown
    Set Flow Control : Off
    Act Flow Control : Off
    Mdix            : Auto
```

Mtu : 20001824
Port mode : LAN
Port ability : 10M HD,10M FD,100M HD,100M FD,1000M FD
Link Delay : No Delay
Storm Control : AllUnicast Disabled
Storm Control : Broadcast Pps 20
Storm Control : Multicast Disabled
Storm Action : Shutdown
Port Type : Nni
Pvid : 1002
Set Medium : Copper
Act Medium : Copper
Mac Address : 001f.ce20.52f5 7a54.5ca5

#After 30 seconds, port gigabitethernet0/1 will be enabled, and the following prompt information is printed :

Jan 22 1970 07:07:09Nov 24 2014 15:37:43: %PORTMGR-AUTO_RECOVERY-5: auto recovery timer expired on interface gigabitethernet0/1, module: PORT SECURITYSTROM CONTROL ACTION.

Jan 22 1970 07:07:13Nov 24 2014 15:37:45: %PORTMGR-LINEPROTO_UP-5: Line protocol on interface gigabitethernet0/1, changed state to up.

#Query the status of port gigabitethernet0/1.

Device#show interface gigabitethernet 0/1

gigabitethernet0/1 configuration information
Description :
Status : Enabled
Link : Up
Set Speed : Auto
Act Speed : 1000
Def Speed : Auto
Set Duplex : Auto
Act Duplex : Full
Def Duplex : Auto
Set Duplex : Auto
Act Duplex : Full
Set Flow Control : Off
Act Flow Control : Off

Mdix : Auto
Mtu : 20001824
Port mode : LAN
Port ability : 10M HD,10M FD,100M HD,100M FD,1000M FD
Link Delay : No Delay
Storm Control : AllUnicast Disabled
Storm Control : Broadcast Pps 20
Storm Control : Multicast Disabled
Storm Action : Shutdown
Port Type : Nni
Pvid : 1002
Set Medium : Copper
Act Medium : Copper
Mac Address : 001f.ce20.52f57a54.5ca5

8. VOICE-VLAN

8.1. Overview

Voice-VLAN is a mechanism that provides security and Quality of Service (QoS) guarantee for voice data flows. In a network, usually two types of traffic coexists, voice data and service data. During transmission, voice data has a higher priority than service data so as to reduce delay and packet loss that may occur during the transmission process. Voice-VLAN can automatically recognize voice traffic and distribute the voice traffic to a specific VLAN with QoS guarantee.

8.2. Voice-VLAN Function Configuration

Table 8-1 Voice-VLAN Function List

Configuration Tasks	
Configure a voice-VLAN.	Configure a voice-VLAN.
Configure an OUI address.	Configure an OUI address.
Configure the aging time.	Configure the aging time of voice-VLAN entries.
Enable the voice-VLAN function of a port.	Enable the voice-VLAN function of a port.
Configure the voice-VLAN working mode on the port.	Configure a voice-VLAN to automatic mode.
	Configure a voice-VLAN to manual mode.

8.2.1. Configure a Voice-VLAN

A voice VLAN is used to transmit voice packets. The 802.1 priorities of the recognized voice packets are replaced with the priority of the voice-VLAN. Then the packets are distributed into the voice VLAN for forwarding. A device supports a maximum of one voice-VLAN.

Configuration Condition

Before configuring a voice-VLAN, ensure that:

- The VLAN to be configured as a voice-VLAN has already been created.

Configure a Voice-VLAN

Table 8-2 Configuring a Voice-VLAN

Step	Command	Description
Enter the global configuration mode.	**configure terminal**	-
Configure a specified VLAN to voice-VLAN.	**voice vlan** *vlan-id* **cos** *priority*	Mandatory. By default, voice-VLAN is not configured, that is, the voice-VLAN function is not globally enabled.

8.2.2. Configure an OUI Address

Configuration Condition

Before configuring an OUI address, ensure that:

- The voice-VLAN function is globally enabled.
- The voice-VLAN function is enabled on the port.

Configure an OUI Address

Organizationally Unique Identifiers (OUIs) are used to identify voice packets that are sent by voice devices of manufacturers. After a port that works in voice-VLAN automatic mode receives an Untag packet, it takes out the MAC address of the packet and performs the AND operation with the OUI mask. If the obtained address range is the same as the OUI address, it indicates that matching the OUI address succeeds, and the packet is recognized as a voice packet.

Table 8-3 Configuring an OUI Address

Step	Command	Description
Enter the global configuration mode.	**configure terminal**	-
Configure an OUI address.	**voice vlan oui-mac** *oui-mac-address* **mask** *mask* **name** *oui-name*	Mandatory. By default, five OUI addresses are available. A device supports a maximum of 16 OUI addresses.

8.2.3. Configure the Aging Time

Configuration Condition

Before configuring the aging time, ensure that:

- The voice-VLAN function is globally enabled.

Configure the Aging Time of Voice-VLAN Entries

After a port in the voice-VLAN automatic mode receives Untag packets that match the OUI address from the source MAC address, it records a voice-VLAN entry and starts a timer. After the aging time times out, the port deletes the entry. If the port receives the same packets before aging time times out, it start the timer again.

Table 8-4 Configuring the Aging Time

Step	Command	Description
Enter the global configuration mode.	**configure terminal**	-
Configure the aging time of voice-VLAN entries.	**voice vlan aging** *aging-time*	Mandatory. By default, the aging time of voice-VLAN entries is one minute.

8.2.4. Enable the Voice-VLAN Function

After the voice-VLAN function is enabled on a port, the port uses a method according to the voice-VLAN working mode to automatically recognize the received packets.

Configuration Condition

Before enabling the voice-VLAN function of a port, ensure that:

- The voice-VLAN function has been globally enabled.
- The port has been added into the voice-VLAN.

Enable the Voice-VLAN Function of a Port

Table 8-5 Enabling the Voice-VLAN Function of a Port

Step	Command	Description
Enter the global configuration mode.	**configure terminal**	-
Enter the L2 Ethernet interface configuration mode.	**interface** *interface-name*	Either After entering the L2 Ethernet interface configuration mode, the subsequent configuration takes effect only on the current port. After entering the aggregation group configuration mode, the subsequent configuration
Enter the aggregation group configuration mode.	**link-aggregation** *link-aggregation-id*	

Step	Command	Description
		takes effect only on the aggregation group.
Enable the voice-VLAN function of a port.	**voice vlan enable**	Mandatory. By default, the voice-VLAN function is disabled on the port.

8.2.5. Configure the Voice-VLAN Working Mode on the Port

The voice-VLAN of a port can work in automatic mode or manual mode. The ports working in different voice-VLAN modes recognize voice packets in different ways.

- Automatic mode: If the packets received by the port are Untag packets and the source MAC address of the packets matches an OUI address, the packets are regarded as voice packets.
- Manual mode: If the packets received by the port are Untag packets, or Tag packets with the VLAN ID being the port PVID, the packets are regarded as voice packets.

Configuration Condition

Before configuring the voice-VLAN working mode of a port, ensure that:

- The voice-VLAN function has been globally enabled.
- The voice-VLAN function of the port has been enabled.

Configure a Voice-VLAN to Automatic Mode

Table 8-6 Configuring a Voice-VLAN to Automatic Mode

Step	Command	Description
Enter the global configuration mode.	**configure terminal**	-
Enter the L2 Ethernet interface configuration mode.	**interface** *interface-name*	Either After entering the L2 Ethernet interface configuration mode, the subsequent configuration takes effect only on the current port. After entering the aggregation group configuration mode, the subsequent configuration takes effect only on the aggregation group.
Enter the aggregation group configuration mode.	**link-aggregation** *link-aggregation-id*	

Step	Command	Description
Configure the port to work in voice-VLAN automatic mode.	**voice vlan mode auto**	Mandatory. By default, the port works in the voice-VLAN automatic mode.

Configure a Voice-VLAN to Manual Mode

Table 8-7 Configuring a Voice-VLAN to Manual Mode

Step	Command	Description
Enter the global configuration mode.	**configure terminal**	-
Enter the L2 Ethernet interface configuration mode.	**interface** *interface-name*	Either After entering the L2 Ethernet interface configuration mode, the subsequent configuration takes effect only on the current port. After entering the aggregation group configuration mode, the subsequent configuration takes effect only on the aggregation group.
Enter the aggregation group configuration mode.	**link-aggregation** *link-aggregation-id*	
Configure the port to work in voice-VLAN manual mode.	**no voice vlan mode auto**	Mandatory. By default, the port works in the voice-VLAN automatic mode.

8.2.6. Configure Voice-VLAN Security

In order to better separate the user voice flow from data flow, voice VLAN provides security function. When voice VLAN security is enabled, the device only allows the data whose source address is the recognizable voice oui address to pass, and the packet with invalid source address will be discarded directly (including some authentication packets, such as 802.1x authentication packet). By default, voice VLAN security is enabled with the creation of Voice-VLAN. It is recommended that users should try not to transmit voice and service data simultaneously in voice VLAN. If you do need this, make sure that voice VLAN security is disabled.

Configuration Conditions

- Enable Voice-VLAN function

Enable Voice-VLAN Security Function

Table 8-8 Enable the Voice-VLAN Security function

Step	Command	Description
Enter the global configuration mode.	**configure terminal**	-
Enable the Voice-VLAN Security function	**voice vlan security enable**	Mandatory The Voice-VLAN Security function is disabled by default.

Disable Voice-VLAN Security Function

Table 8-9 Disable the Voice-VLAN Security function

Step	Command	Description
Enter the global configuration mode.	**configure terminal**	-
Disable the Voice-VLAN Security function	**no voice vlan security enable**	Mandatory By default, the Voice-VLAN Security function-n is disabled.

8.2.7. Voice-VLAN Monitoring and Maintaining

Table 8-10 Voice-VLAN Monitoring and Maintaining

Command	Description
show voice vlan { **all** | **interface** [*interface-name*] | **link-aggregation** [*link-aggregation-id*] | **mac** [*mac-address*] | **oui** }	Displays the information about the voice-VLAN.

8.3. Voice-VLAN Typical Configuration Example

8.3.1. Configure a Voice-VLAN to Manual Mode

Network Requirements

- IP Phone and PC can access IP Network through Device.
- The voice-VLAN in manual mode has been configured on Device. If the network is normal, IP Phone and PC can normally access IP Network. If the network is congested, IP Phone has a higher priority than PC in accessing IP Network.

Network Topology

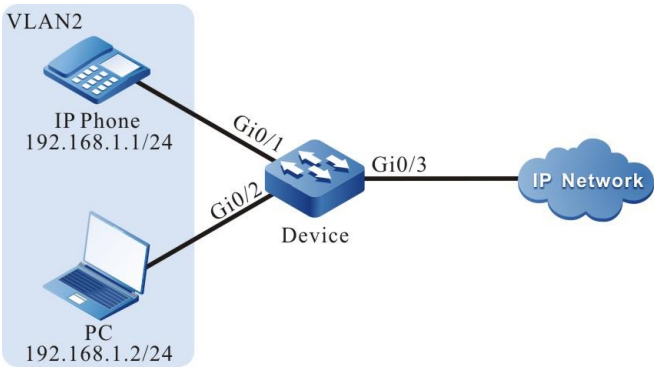


Figure 8-1 Networking for Configure a Voice-VLAN to Manual Mode

Configuration Steps

Step 1: Configure a VLAN, and configure the link type of the ports.

#On Device, create VLAN2.

```
Device#configure terminal
Device(config)#vlan 2
Device(config-vlan2)#exit
```

#On Device2, configure the link type of ports gigabitethernet0/1 and gigabitethernet0/2 to Access and allow services of VLAN2 to pass.

```
Device(config)#interface gigabitethernet 0/1,0/2
Device(config-if-range)#switchport mode access
Device(config-if-range)#switchport access vlan 2
Device(config-if-range)#exit
```

#On Device, configure the link type of port gigabitethernet0/3 to Trunk and allow services of VLAN2 to pass.

```
Device(config)#interface gigabitethernet 0/3
Device(config-if-gigabitethernet0/3)#switchport mode trunk
Device(config-if-gigabitethernet0/3)#switchport trunk allowed vlan add 2
Device(config-if-gigabitethernet0/3)#exit
```

Step 2: Configure the voice-VLAN function.

#On Device, configure VLAN2 to voice-VLAN, and configure the Cos value to 7.

```
Device(config)#voice vlan 2 cos 7
```

#On port gigabitethernet0/1 of Device, configure the voice-VLAN mode to manual mode.

```
Device(config)#interface gigabitethernet 0/1
Device(config-if-gigabitethernet0/1)#voice vlan enable
Device(config-if-gigabitethernet0/1)#no voice vlan mode auto
Device(config-if-gigabitethernet0/1)#exit
```

#On Device, query the voice-VLAN information.

```
Device#show voice vlan all
Voice Vlan Global Information:  Voice Vlan enable
Voice Vlan VID: 2, Cos: 7
Default OUI number: 5
User config OUI number: 0
Learned phone MAC address: 0
Aging time: 1 minute

Voice vlan interface information:
 Interface          Mode
 ------------------------------------
 gi0/1              Manual-Mode

Voice Vlan OUI information: Total: 5
 MacAddr        Mask          Name
 ------------------------------------------------------------
 0003.6b00.0000   ffff.ff00.0000   Cisco-phone  default
 006b.e200.0000   ffff.ff00.0000   H3C-Aolynk-phone  default
 00d0.1e00.0000   ffff.ff00.0000   Pingtel-phone  default
 00e0.7500.0000   ffff.ff00.0000   Polycom-phone  default
 00e0.bb00.0000   ffff.ff00.0000   3Com-phone  default

Voice Vlan MAC information: Total: 0
     No any MAC enable
```

Step 3: Check the result.

#The 802.1 priority of the packets that are sent to IP Phone is modified to 7, and the 802.1P priority of the packets sent by PC to IP Network is not modified.

#When the network is normal, IP Phone and PC can normally access IP Network.

#If the network is congested, IP Phone can access IP Network with a priority higher than PC.

8.3.2. Configure a Voice-VLAN to Automatic Mode

Network Requirements

- IP Phone and PC access IP Network through port gigabitethernet0/1 of Device. The MAC address of IP Phone is 0001.0001.0001, and the MAC address of PC is 0002.0002.0002.

- The voice-VLAN in automatic mode has been configured. In this way, if the network is normal, IP Phone and PC can normally access IP network. If the network is congested, IP Phone has a higher priority than PC in accessing IP Network.

Network Topology

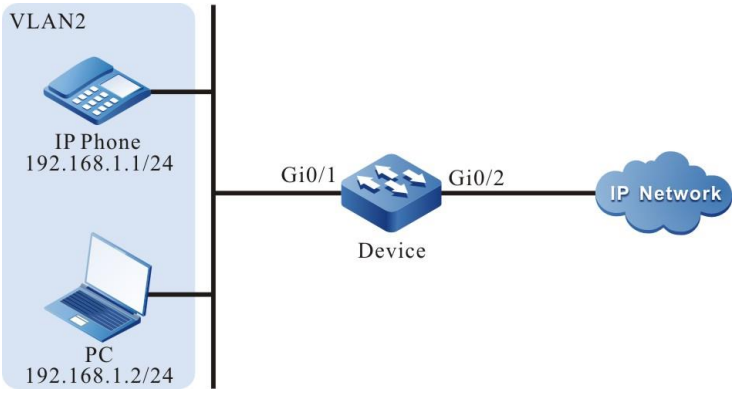


Figure 8-2 Networking for Configure a Voice-VLAN to Automatic Mode

Configuration Steps

Step 1: Configure a VLAN, and configure the link type of the ports.

#On Device, create VLAN2.

```
Device#configure terminal
Device(config)#vlan 2
Device(config-vlan2)#exit
```

#On Device, configure the link type of port gigabitethernet0/1 to Access and allow services of VLAN2 to pass.

```
Device(config)#interface gigabitethernet 0/1
Device(config-if-gigabitethernet0/1)#switchport mode access
Device(config-if-gigabitethernet0/1)#switchport access vlan 2
Device(config-if-gigabitethernet0/1)#exit
```

Step 2: Configure the voice-VLAN function.

#On Device, configure VLAN2 to voice-VLAN, and modify the Cos value to 7.

```
Device(config)#voice vlan 2 cos 7
```

#On port gigabitethernet0/1 of Device, configure the voice-VLAN mode to automatic mode.

```
Device(config)# interface gigabitethernet 0/1
Device(config-if-gigabitethernet0/1)#voice vlan enable
Device(config-if-gigabitethernet0/1)#voice vlan mode auto
Device(config-if-gigabitethernet0/1)#exit
```

#On Device, configure the OUI address corresponding to the MAC address 0001.0001.0001 of IP Phone.

```
Device(config)#voice vlan oui-mac 0001.0001.0001 mask ffff.ffff.0000 name voice-vlan
```

#On Device, query the voice-VLAN information.

```
Device#show voice vlan all
 Voice Vlan Global Information:  Voice Vlan enable
 Voice Vlan VID: 2, Cos: 7
 Default OUI number: 5
 User config OUI number: 1
 Learned phone MAC address: 0
 Aging time: 1 minute

 Voice vlan interface information:
  Interface          Mode
  ------------------------------------
  gi0/1              Auto-Mode

 Voice Vlan OUI information: Total: 6
  MacAddr        Mask          Name
  ------------------------------------------------------------
  0001.0001.0000   ffff.ffff.0000   voice-vlan
  0003.6b00.0000   ffff.ff00.0000   Cisco-phone  default
  006b.e200.0000   ffff.ff00.0000   H3C-Aolynk-phone  default
  00d0.1e00.0000   ffff.ff00.0000   Pingtel-phone  default
  00e0.7500.0000   ffff.ff00.0000   Polycom-phone  default
  00e0.bb00.0000   ffff.ff00.0000   3Com-phone  default

 Voice Vlan MAC information: Total: 0
      No any MAC enable
```

Step 3: Check the result.

#The 802.1 priority of the packets that are sent to IP Phone is modified to 7, and the 802.1P priority of the packets sent by PC to IP Network is not modified.

```
Device#show voice vlan mac

Voice Vlan MAC information: Total: 1

 MacAddr        Vid   Interface          AgeTime(min)
```

```
-----------------------------------------------------------
0001.0001.0001  2    gi0/1              0
```

#When the network is normal, IP Phone and PC can normally access IP Network.

#If the network is congested, IP Phone can access IP Network with a priority higher than PC.

8.3.3. Configure Voice-VLAN Security Mode

Network Requirements

- IP Phone and PC access IP Network through port gigabitethernet0/1 of Device. The MAC address of IP Phone is 0001.0001.0001, and the MAC address of PC is 0002.0002.0002.
- On Device, configure the Voice-VLAN security mode, IP Phone can access IP Network normally, and PC cannot access IP Network.

Network Topology

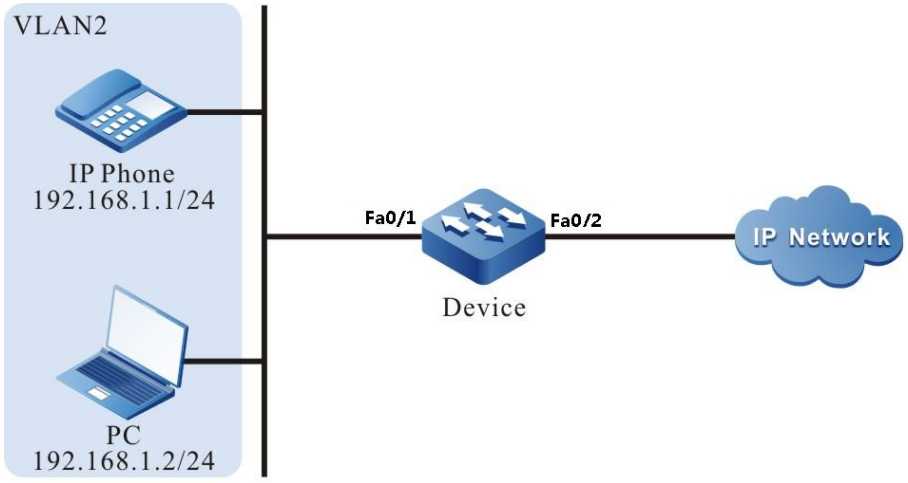


Figure 8-3 Networking for configuring Voice-VLAN auto mode

Configuration Steps

Step 1: Configure the VLAN and port link type.

#On Device, create VLAN2.

```
Device#configure terminal
Device(config)#vlan 2
Device(config-vlan2)#exit
```

#On Device, configure the link type of port fastethernet 0/1 as Access, permitting the services of VLAN2 to pass.

```
Device(config)#interface fastethernet 0/1
Device(config-if-fastethernet0/1)#switchport mode access
Device(config-if-fastethernet0/1)#switchport access vlan 2
Device(config-if-fastethernet0/1)#exit
```

Step 2: Configure the Voice-VLAN function.

#On Device, configure VLAN2 as Voice-VLAN, and modify the corresponding CoS value to 7.

```
Device(config)#voice vlan 2 cos 7
```

#On Device, configure Voice-Vlan and enable the security mode.

```
Device(config)#voice vlan security enable
```

#On port fastethernet 0/1 of Device, configure Voice-VLAN auto mode.

```
Device(config)# interface fastethernet 0/1
Device(config-if-fastethernet0/1)#voice vlan enable
Device(config-if-fastethernet0/1)#voice vlan mode auto
Device(config-if-fastethernet0/1)#exit
```

#On Device, configure the corresponding OUI address of the MAC address 0001.0001.0001 of IP Phone.

```
Device(config)#voice vlan oui-mac 0001.0001.0001 mask ffff.ffff.0000 name voice-vlan
```

#On Device, view the Voice-VLAN information.

```
Device#show voice vlan all
 Voice Vlan Global Information:  Voice Vlan enable
Voice Vlan Security Information:  Voice Vlan Security enable
 Voice Vlan VID: 2, Cos: 7
 Default OUI number: 5
 User config OUI number: 1
Learned phone MAC address: 0
 Aging time: 1 minute


 Voice vlan interface information:
  Interface          Mode
  ------------------------------------
  fa0/1              Auto-Mode

 Voice Vlan OUI information: Total: 6
  MacAddr        Mask          Name
  ------------------------------------------------------------
  0001.0001.0000   ffff.ffff.0000   voice-vlan
  0003.6b00.0000   ffff.ff00.0000   Cisco-phone  default
  006b.e200.0000   ffff.ff00.0000   H3C-Aolynk-phone  default
```

```
00d0.1e00.0000  ffff.ff00.0000  Pingtel-phone  default
00e0.7500.0000  ffff.ff00.0000  Polycom-phone  default
00e0.bb00.0000  ffff.ff00.0000  3Com-phone  default
```

Step 3: Check the result.

#The 802.1P priority of the packet sent by IP Phone to IP Network is modified to 7, and IP Network cannot be accessed.

9. ОБЩАЯ ИНФОРМАЦИЯ

9.1. Замечания и предложения

Мы всегда стремимся улучшить нашу документацию и помочь вам работать лучше, поэтому мы хотим услышать вас. Мы всегда рады обратной связи, в особенности:

- ошибки в содержании, непонятные или противоречащие места в тексте;
- идеи по улучшению документации, чтобы находить информацию быстрее;
- неработающие ссылки и замечания к навигации по документу.

Если вы хотите написать нам по поводу данного документа, то используйте, пожалуйста, форму обратной связи на qtech.ru.

9.2. Гарантия и сервис

Процедура и необходимые действия по вопросам гарантии описаны на сайте QTECH в разделе «Поддержка» −> «Гарантийное обслуживание».

Ознакомиться с информацией по вопросам тестирования оборудования можно на сайте QTECH в разделе «Поддержка» −> «Взять оборудование на тест».

Вы можете написать напрямую в службу сервиса по электронной почте sc@qtech.ru.

9.3. Техническая поддержка

Если вам необходимо содействие в вопросах, касающихся нашего оборудования, то можете воспользоваться нашей автоматизированной системой запросов технического сервис-центра helpdesk.qtech.ru.

Телефон Технической поддержки +7 (495) 797-33-11 доб. 0