МИР ДОСТУПНЕЕ

РУКОВОДСТВО ПОЛЬЗОВАТЕЛЯ

Ethernet Switching Configuration

Оглавление

1 CONFIGURING INTERFACES

1.1 Overview

Interfaces are important in implementing data switching on network devices. QTECH devices support two types of interfaces: physical ports and logical interfaces. A physical port is a hardware port on a device, such as the 100M Ethernet interface and gigabit Ethernet interface. A logical interface is not a hardware port on the device. A logical interface, such as the loopback interface and tunnel interface, can be associated with a physical port or independent of any physical port. For network protocols, physical ports and logical interfaces serve the same function.

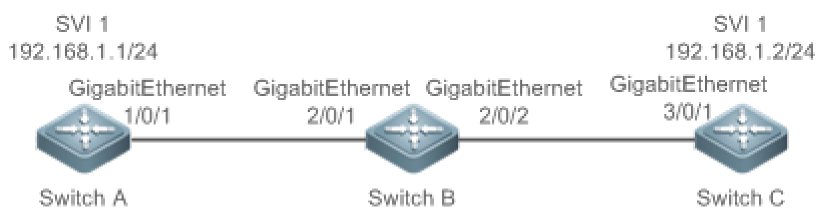
1.2 Applications

Application	Description
L2 Data Switching Through the Physical Ethernet Interface	Implement Layer-2 (L2) data communication of network devices through the physical L2 Ethernet interface.
L3 Routing Through the Physical Ethernet Interface	Implement Layer-3 (L3) data communication of network devices through the physical L3 Ethernet interface.

1.2.1 L2 Data Switching Through the Physical Ethernet Interface

Scenario

Figure 1-1



As shown in Figure 1-1, Switch A, Switch B, and Switch C form a simple L2 data switching network.

Deployment

- Connect Switch A to Switch B through physical ports GigabitEthernet 1/0/1 and GigabitEthernet 2/0/1.
- Connect Switch B to Switch C through physical ports GigabitEthernet 2/0/2 and GigabitEthernet 3/0/1.
- Configure GigabitEthernet 1/0/1, GigabitEthernet 2/0/1, GigabitEthernet 2/0/2, and GigabitEthernet3/0/1 as Trunk ports.
- Create a switch virtual interface (SVI), SVI 1, on Switch A and Switch C respectively, and configure IP addresses from a network segment for the two SVIs. The IP address of SVI 1 on Switch A is 192.168.1.1/24, and the IP address of SVI 1 on Switch C is 192.168.1.2/24.
- Run the **ping 192.168.1.2** command on Switch A and the **ping 192.168.1.1** command on Switch C to implement data switching through Switch B.

1.2.2 L3 Routing Through the Physical Ethernet Interface

Scenario

Figure 1-2

As shown in Figure 1-2, Switch A, Switch B, and Switch C form a simple L3 data communication network.

Deployment

- Connect Switch A to Switch B through physical ports GigabitEthernet 1/0/1 and GigabitEthernet 2/0/1.
- Connect Switch B to Switch C through physical ports GigabitEthernet 2/0/2 and GigabitEthernet 3/0/1.
- Configure GigabitEthernet 1/0/1, GigabitEthernet 2/0/1, GigabitEthernet 2/0/2, and GigabitEthernet3/0/1 as L3 routed ports.
- Configure IP addresses from a network segment for GigabitEthernet 1/0/1 and GigabitEthernet 2/0/1. The IP address of GigabitEthernet 1/0/1 is 192.168.1.1/24, and the IP address of GigabitEthernet 2/0/1 is 192.168.1.2/24.
- Configure IP addresses from a network segment for GigabitEthernet 2/0/2 and GigabitEthernet 3/0/1. The IP address of GigabitEthernet 2/0/2 is 192.168.2.1/24, and the IP address of GigabitEthernet 3/0/1 is 192.168.2.2/24.
- Configure a static route entry on Switch C so that Switch C can directly access the network segment 192.168.1.0/24. Configure a static route entry on Switch A so that Switch C can directly access the network segment 192.168.1.0/24.

- Run the **ping 192.168.2.2** command on Switch A and the **ping 192.168.1.1** command on Switch C to implement L3 routing through Switch B.

1.3 Features

Basic Concepts

Interface Classification

1. Interfaces on QTECH devices fall into three categories:

- L2 interface (Switches or gateway bridge)
- L3 interface (supported by L3 devices)

2. Common L2 interfaces are classified into the following types:

- Switch port
- L2 aggregate port (AP)

3. Common L3 interfaces are classified into the following types:

- Routed port
- L3 AP port
- SVI
- Loopback interface
- Tunnel interface

Switch Port

A switch port is an individual physical port on the device, and implements only the L2 switching function. The switch port is used to manage physical ports and L2 protocols related to physical ports.

L2 AP Port

An AP port is formed by aggregating multiple physical ports. Multiple physical links can be bound together to form a simple logical link. This logical link is called an AP port.

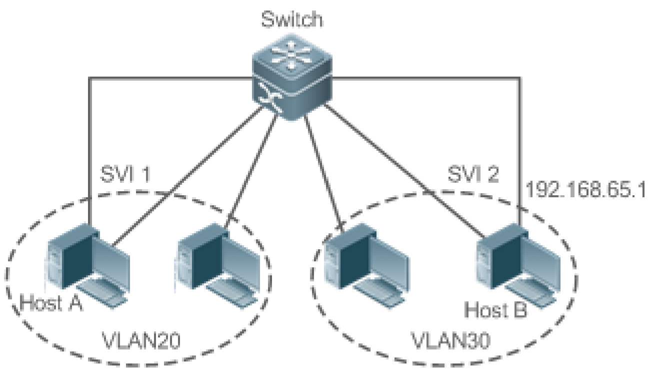
For L2 switching, an AP port is equivalent to a switch port that combines bandwidths of multiple ports, thus expanding the link bandwidth. Frames sent over the L2 AP port are balanced among the L2 AP member ports. If one member link fails, the L2 AP port automatically transfers the traffic on the faulty link to other member links, improving reliability of connections.

SVI

The SVI can be used as the management interface of the local device, through which the administrator can manage the device. You can also create an SVI as a gateway interface, which is mapped to the virtual interface of each VLAN to implement routing across VLANs among L3 devices. You can run the **interface vlan** command to create an SVI and assign an IP address to this interface to set up a route between VLANs.

As shown in Figure 1-3, hosts in VLAN 20 can directly communicate with each other without participation of L3 devices. If Host A in VLAN 20 wants to communicate with Host B in VLAN 30, SVI 1 of VLAN 20 and SVI 2 of VLAN 30 must be used.

Figure 1-3



Routed Port

A physical port on a L3 device can be configured as a routed port, which functions as the gateway interface for L3 switching. A routed port is not related with a specific VLAN. Instead, it is just an access port. The routed port cannot be used for L2 switching. You can run the **no switchport** command to change a switch port to a routed port and assign an IP address to this port to set up a route. Note that you must delete all L2 features of a switch port before running the **no switchport** command.

If a port is a L2 AP member port or a DOT1X port that is not authenticated, you cannot run the **switchport** or **no switchport** command to configure the switch port or routed port.

L3 AP Port

Like the L2 AP port, a L3 AP port is a logical port that aggregates multiple physical member ports. The aggregated ports must be the L3 ports of the same type. The AP port functions as a gateway interface for L3 switching. Multiple physical links are combined into one logical link, expanding the bandwidth of a link. Frames sent over the L3 AP port are balanced among the L3 AP member ports. If one member link fails, the L3 AP port automatically transfers the traffic on the faulty link to other member links, improving reliability of connections.

A L3 AP port cannot be used for L2 switching. You can run the **no switchport** command to change a L2 AP port that does not contain any member port into a L3 AP port, add multiple routed ports to this L3 AP port, and then assign an IP address to this L3 AP port to set up a route.

Loopback Interface

The loopback interface is a local L3 logical interface simulated by the software that is always UP. Packets sent to the loopback interface are processed on the device locally, including the route information. The IP address of the loopback interface can be used as the device ID of the Open Shortest Path First (OSPF) routing protocol, or as the source address used by Border Gateway Protocol (BGP) to set up a TCP connection. The procedure for configuring a loopback interface is similar to that for configuring an Ethernet interface, and you can treat the loopback interface as a virtual Ethernet interface.

Tunnel Interface

The Tunnel interface implements the tunnel function. Over the Tunnel interface, transmission protocols (e.g., IP) can be used to transmit packets of any protocol. Like other logical interfaces, the tunnel interface is also a virtual interface of the system. Instead of specifying any transmission protocol or load protocol, the tunnel interface provides a standard point-to-point (P2P) transmission mode. Therefore, a tunnel interface must be configured for every individual link.

Overview

Feature	Description
Interface Configuration Commands	You can configure interface-related attributes in interface configuration mode. If you enter interface configuration mode of a non-existing logical interface, the interface will be created.
Interface Description and Administrative Status	You can configure a name for an interface to identify the interface and help you remember the functions of the interface. You can also configure the administrative status of the interface.
MTU	You can configure the maximum transmission unit (MTU) of a port to limit the length of a frame that can be received or sent over this port.
Bandwidth	You can configure the bandwidth of an interface.
Load Interval	You can specify the interval for load calculation of an interface.
Carrier Delay	You can configure the carrier delay of an interface to adjust the delay after which the status of an interface changes from Down to Up or from Up to Down.
Link Trap Policy	You can enable or disable the link trap function on an interface.
Interface Index Persistence	You can enable the interface index persistence function so that the interface index remains unchanged after the device is restarted.
Routed Port	You can configure a physical port on a L3 device as a routed port, which functions as the gateway interface for L3 switching.
L3 AP Port	You can configure an AP port on a L3 device as a L3 AP port, which functions as the gateway interface for L3 switching.

Interface Speed, Duplex Mode, Flow Control Mode, and Auto Negotiation Mode	You can configure the speed, duplex mode, flow control mode, and auto negotiation mode of an interface.
Automatic Module Detection	If the interface speed is set to auto, the interface speed can be automatically adjusted based on the type of the inserted module.
Protected Port	You can configure some ports as protected ports to disable communication between these ports. You can also disable routing between protected ports.
Port Errdisable Recovery	After a port is shut down due to a violation, you can run the errdisable recovery command in global configuration mode to recover all the ports in errdisable state and enable these ports.
Port Flapping Protection	You can configure the port flapping protection function so that the system can automatically turn the port into the violation mode when flapping occurs on the port.

1.3.1 Interface Configuration Commands

Run the **interface** command in global configuration mode to enter interface configuration mode. You can configure interface-related attributes in interface configuration mode.

Working Principle

Run the **interface** command in global configuration mode to enter interface configuration mode. If you enter interface configuration mode of a non-existing logical interface, the interface will be created. You can also run the **interface range** or **interface range macro** command in global configuration mode to configure the range (IDs) of interfaces. Interfaces defined in the same range must be of the same type and have the same features.

You can run the **no interface** command in global configuration mode to delete a specified logical interface.

Interface Numbering Rules

In stand-alone mode, the ID of a physical port consists of two parts: slot ID and port ID on the slot. For example, if the slot ID of the port is 2, and port ID on the slot is 3, the interface ID is 2/3.

The slot number rules are as follows: The static slot ID is 0, whereas the ID of a dynamic slot (pluggable module or line card) ranges from 1 to the number of slots. Assume that you are facing the device panel. Dynamic slot are numbered from 1 sequentially from front to rear, from left to right, and from top to bottom.

The ID of a port on the slot ranges from 1 to the number of ports on the slot, and is numbered sequentially from left to right.

The ID of an AP port ranges from 1 to the number of AP ports supported by the device.

The ID of an SVI is the VID of the VLAN corresponding to this SVI.

Configuring Interfaces Within a Range

You can run the **interface range** command in global configuration mode to configure multiple interfaces at a time. Attributes configured in interface configuration mode apply to all these interfaces.

The **interface range** command can be used to specify several interface ranges.

The **macro** parameter is used to configure the macro corresponding to a range. For details, see "Configuring Macros of Interface Ranges."

Ranges can be separated by commas (,).

The types of interfaces within all ranges specified in a command must be the same.

Pay attention to the format of the **range** parameter when you run the **interface range** command.

The following interface range formats are valid:

- **FastEthernet** device/slot/{first port} - {last port};
- **GigabitEthernet** device/slot/{first port} - {last port};
- **TenGigabitEthernet** device/slot/{first port} - {last port};
- **FortyGigabitEthernet** device/slot/{first port} - {last port};
- **AggregatePort** *Aggregate-port ID* (The AP ID ranges from 1 to the maximum number of AP ports supported by the device.)
- **vlan** vlan-ID-vlan-ID (The VLAN ID ranges from 1 to 4,094.)
- **Loopback** loopback-ID (The loopback ID ranges from 1 to 2,147,483,647.)
- **Tunnel** tunnel-ID (The tunnel ID ranges from 0 to the maximum number of tunnel interfaces supported by the device minus 1.)

Interfaces in an interface range must be of the same type, namely, FastEthernet or GigabitEthernet.

Configuring Macros of Interface Ranges

You can define some macros to replace the interface ranges. Before using the **macro** parameter in the **interface range** command, you must first run the **define interface-range** command in global configuration mode to define these macros.

Run the **no define interface-range macro_name** command in global configuration mode to delete the configured macros.

1.3.2 Interface Description and Administrative Status

You can configure a name for an interface to identify the interface and help you remember the functions of the interface.

You can enter interface configuration mode to enable or disable an interface.

Working Principle

Interface Description

You can configure the name of an interface based on the purpose of the interface. For example, if you want to assign GigabitEthernet 1/1 for exclusive use by user A, you can describe the interface as "Port for User A."

Interface Administrative Status

You can configure the administrative status of an interface to disable the interface as required. If the interface is disabled, no frame will be received or sent on this interface, and the interface will loss all its functions. You can enable a disabled interface by configuring the administrative status of the interface. Two types of interface administrative status are defined: Up and Down. The administrative status of an interface is Down when the interface is disabled, and Up when the interface is enabled.

1.3.3 MTU

You can configure the MTU of a port to limit the length of a frame that can be received or sent over this port.

Working Principle

When a large amount of data is exchanged over a port, frames greater than the standard Ethernet frame may exist. This type of frame is called jumbo frame. The MTU is the length of the valid data segment in a frame. It does not include the Ethernet encapsulation overhead.

If a port receives or sends a frame with a length greater than the MTU, this frame will be discarded.

The MTU ranges from 64 bytes to 9,216 bytes, at a step of four bytes. The default MTU is 1500 bytes.

The **mtu** command takes effect only on a physical or AP port.

1.3.4 Bandwidth

Working Principle

The **bandwidth** command can be configured so that some routing protocols (for example, OSPF) can calculate the route metric and the Resource Reservation Protocol (RSVP) can calculate the reserved bandwidth. Modifying the interface bandwidth will not affect the data transmission rate of the physical port.

The **bandwidth** command is a routing parameter, and does not affect the bandwidth of a physical link.

1.3.5 Load Interval

Working Principle

You can run the **load-interval** command to specify the interval for load calculation of an interface. Generally, the interval is 10s.

1.3.6 Carrier Delay

Working Principle

The carrier delay refers to the delay after which the data carrier detect (DCD) signal changes from Down to Up or from Up to Down. If the DCD status changes during the delay, the system will ignore this change to avoid negotiation at the upper data link layer. If this parameter is set to a great value, nearly every DCD change is not detected. On the contrary, if the parameter is set to 0, every DCD signal change will be detected, resulting in poor stability.

If the DCD carrier is interrupted for a long time, the carrier delay should be set to a smaller value to accelerate convergence of the topology or route. On the contrary, if the DCD carrier interruption time is shorter than the topology or route convergence time, the carrier delay should be set to a greater value to avoid topology or route flapping.

1.3.7 Link Trap Policy

You can enable or disable the link trap function on an interface.

Working Principle

When the link trap function on an interface is enabled, the Simple Network Management Protocol (SNMP) sends link traps when the link status changes on the interface.

1.3.8 Interface Index Persistence

Like the interface name, the interface index also identifies an interface. When an interface is created, the system automatically assigns a unique index to the interface. The index of an interface may change after the device is restarted. You can enable the interface index persistence function so that the interface index remains unchanged after the device is restarted.

Working Principle

After interface index persistence is enabled, the interface index remains unchanged after the device is restarted.

1.3.9 Routed Port

Working Principle

A physical port on a L3 device can be configured as a routed port, which functions as the gateway interface for L3 switching. The routed port cannot be used for L2 switching. You can run the **no switchport** command to change a switch port to a routed port and assign an IP address to this port to set up a route. Note that you must delete all L2 features of a switch port before running the **no switchport** command.

1.3.10 L3 AP Port

Working Principle

Like a L3 routed port, you can run the **no switchport** command to change a L2 AP port into a L3 AP port on a L3 device, and then assign an IP address to this AP port to set up a route. Note that you must delete all L2 features of the AP port before running the **no switchport** command.

A L2 AP port with one or more member ports cannot be configured as a L3 AP port. Similarly, a L3 AP port with one or more member ports cannot be changed to a L2 AP port.

1.3.11 Interface Speed, Duplex Mode, Flow Control Mode, and Auto Negotiation Mode

You can configure the interface speed, duplex mode, flow control mode, and auto negotiation mode of an Ethernet physical port or AP port.

Working Principle

Speed

Generally, the speed of an Ethernet physical port is determined through negotiation with the peer device. The negotiated speed can be any speed within the interface capability. You can also configure any speed within the interface capability for the Ethernet physical port.

When you configure the speed of an AP port, the configuration takes effect on all of its member ports. (All these member ports are Ethernet physical ports.)

Duplex Mode

- The duplex mode of an Ethernet physical port or AP port can be configured as follows:
- Set the duplex mode of the interface to full-duplex so that the interface can receive packets while sending packets.
- Set the duplex mode of the interface to half-duplex so that the interface can receive or send packets at a time.
- Set the duplex mode of the interface to auto-negotiation so that the duplex mode of the interface is determined through auto negotiation between the local interface and peer interface.
- When you configure the duplex mode of an AP port, the configuration takes effect on all of its member ports. (All these member ports are Ethernet physical ports.)

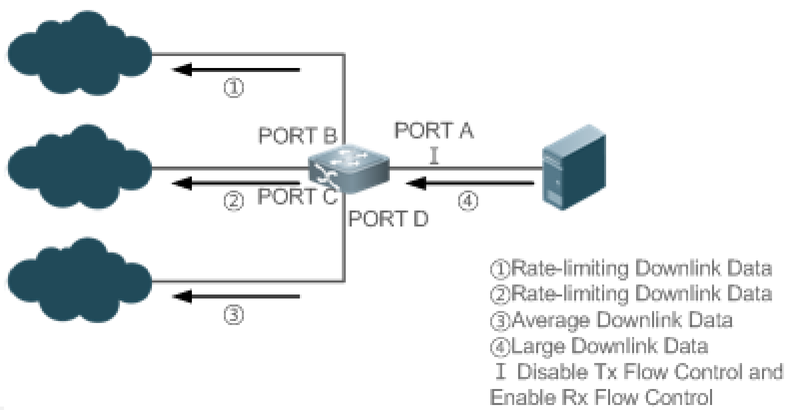
Flow Control

Two flow control modes are defined for an interface:

- Symmetric flow control mode: Generally, after flow control is enabled on an interface, the interface processes the received flow control frames, and sends the flow control frames when congestion occurs on the interface. The received and sent flow control frames are processed in the same way. This is called symmetric flow control mode.
- Asymmetric flow control mode: In some cases, an interface on a device is expected to process the received flow control frames to ensure that no packet is discarded due to congestion, and not to send the flow control frames to avoid decreasing the network speed. In this case, you need to configure asymmetric flow control mode to separate the procedure for receiving flow control frames from the procedure for sending flow control frames.
- When you configure the flow control mode of an AP port, the configuration takes effect on all of its member ports. (All these member ports are Ethernet physical ports.)

As shown in Figure 1-4, Port A of the device is an uplink port, and Ports B, C and D are downlink ports. Assume that Port A is enabled with the functions of sending and receiving flow control frames. Port B and Port C are connected to different slow networks. If a large amount of data is sent on Port B and Port C, Port B and Port C will be congested, and consequently congestion occurs in the inbound direction of Port A. Therefore, Port A sends flow control frames. When the uplink device responds to the flow control frames, it reduces the data flow sent to Port A, which indirectly slows down the network speed on Port D. At this time, you can disable the function of sending flow control frames on Port A to ensure the bandwidth usage of the entire network.

Figure 1-4



Auto Negotiation Mode

- The auto negotiation mode of an interface can be On or Off. The auto negotiation state of an interface is not completely equivalent to the auto negotiation mode. The auto negotiation state of an interface is jointly determined by the interface speed, duplex mode, flow control mode, and auto negotiation mode.
- When you configure the auto negotiation mode of an AP port, the configuration takes effect on all of its member ports. (All these member ports are Ethernet physical ports.)

Generally, if one of the interface speed, duplex mode, and flow control mode is set to auto, or the auto negotiation mode of an interface is On, the auto negotiation state of the interface is On, that is, the auto negotiation function of the interface is enabled. If none of the interface speed, duplex mode, and flow control mode is set to auto, and the auto negotiation mode of an interface is Off, the auto negotiation state of the interface is Off, that is, the auto negotiation function of the interface is disabled.

For a 100M fiber port, the auto negotiation function is always disabled, that is, the auto negotiation state of a 100M fiber port is always Off. For a Gigabit copper port, the auto negotiation function is always enabled, that is, the auto negotiation state of a Gigabit copper port is always On.

1.3.12 Automatic Module Detection

If the interface speed is set to auto, the interface speed can be automatically adjusted based on the type of the inserted module.

Working Principle

Currently, the automatic module detection function can be used to detect only the SFP and SFP+ modules. The SFP is a Gigabit module, whereas SFP+ is a 10 Gigabit module. If the inserted module is SFP, the interface works in Gigabit mode. If the inserted module is SFP+, the interface works in 10 Gigabit mode.

The automatic module detection function takes effect only when the interface speed is set to auto.

1.3.13 Protected Port

In some application environments, it is required that communication be disabled between some ports. For this purpose, you can configure some ports as protected ports. You can also disable routing between protected ports.

Working Principle

Protected Port

After ports are configured as protected ports, protected ports cannot communicate with each other, but can communicate with non-protected ports.

Protected ports work in either of the two modes. In the first mode, L2 switching is blocked but routing is allowed between protected ports. In the second mode, both L2 switching and routing are blocked between protected ports. If a protected port supports both modes, the first mode is used by default.

When two protected port are configured as a pair of mirroring ports, frames sent or received by the source port can be mirrored to the destination port.

Currently, only an Ethernet physical port or AP port can be configured as a protected port. When an AP port is configured as a protected port, all of its member ports are configured as protected ports.

Blocking L3 Routing Between Protected Ports

By default, L3 routing between protected ports is not blocked. In this case, you can run the **protected-ports route-deny** command to block routing between protected ports.

1.3.14 Port Errdisable Recovery

Some protocols support the port errdisable recovery function to ensure security and stability of the network. For example, in the port security protocol, when you enable port security and configure the maximum number of security addresses on the port, a port violation event is generated if the number of addresses learned on this port exceeds the maximum number of security addresses. Other protocols, such as the Spanning Tree Protocol (STP), DOT1X, REUP, and and frequent port flapping support the similar functions, and a violating port will be automatically shut down to ensure security.

Working Principle

After a port is shut down due to a violation, you can run the **errdisable recovery** command in global configuration mode to recovery all the ports in errdisable state and enable these ports. You can manually recover a port, or automatically recover a port at a scheduled time.

1.3.15 Split and Combination of the 100G Port

Working Principle

The 100G Ethernet port is a high-bandwidth port. It is mainly used on devices at the convergence layer or core layer to increase the port bandwidth. 100G port split means that a 100G port is split into four 25G ports. At this time, the 100G port becomes unavailable, and the four 25G ports forward data independently. 100G port combination means that four 25G ports are combined into a 100G port. At this time, the four 25G ports become unavailable, and only the 100G port forwards data. You can flexibly adjust the bandwidth by combining or splitting ports.

1.3.16 SVI or Sub-Interface Sampling

By default, the SVI or sub-interface does not support packet statistics. Information, such as the number of packets received or sent on the SVI or sub-interface and the packet sending/receiving rate, cannot be displayed. You can enable SVI or sub-interface sampling to display these statistics.

1.3.17 Port Flapping Protection

When flapping occurs on a port, a lot of hardware interruptions occur, consuming a lot of CPU resources. On the other hand, frequent port flapping damages the port. You can configure the flapping protection function to protect ports.

Working Principle

By default, the port flapping protection function is enabled. You can disable this function as required. When flapping occurs on a port, the port detects flapping every 2s or 10s. If flapping occurs six times within 2s on a port, the device displays a prompt. If 10 prompts are displayed continuously, that is, port flapping is detected continuously within 20s, the port is turned into the violation mode(the violation cause shows Link Dither). If flapping occurs 10 times within 10s on a port, the device displays a prompt without turning the port into the violation mode.

1.3.18 Syslog

You can enable or disable the syslog function to determine whether to display information about the interface changes or exceptions.

Working Principle

You can enable or disable the syslog function as required. By default, this function is enabled. When an interface becomes abnormal, for example, the interface status changes, or the interface receives error frames, or flapping occurs, the system displays prompts to notify users.

1.3.19 Global MTU

Users can set the global MTU to control the maximum length of frames that can be sent and received over all ports.

Working Principle

When large-throughput data exchange is performed over a port, frames whose length is longer than that of a standard Ethernet frame may exist, and these frames are called jumbo frames. The MTU indicates the length of valid data fields in a frame, excluding the Ethernet encapsulation overhead.

If the length of a frame received or forwarded by a port exceeds the MTU value, the frame will be discarded.

The MTU value ranges from 64 to 9216 bytes. The granularity is four bytes. The default value is 1500 bytes.

- The IP MTU automatically changes to the value of the link MTU of an interface when the globally set link MTU changes.
- The MTU of an interface takes precedence over the global MTU. After the global MTU is configured, the MTU of an interface cannot be set to the default value.

1.3.20 Interface MAC Address

Working Principle

By default, each Ethernet interface has a globally unique MAC address. The MAC addresses of Ethernet interfaces can be modified if required. However, MAC addresses in the same LAN must be unique.

To configure the MAC address of an Ethernet interface, run the **mac-address** command in interface configuration mode:

- Configuration of MAC addresses may affect internal communication in a LAN. Therefore, it is recommended that users do not configure MAC addresses by themselves if unnecessary.

Related Configuration

Configuring MAC Addresses for Interfaces

By default, each interface has a globally unique MAC address.

You can run the **mac-address** ***mac-address*** command in interface configuration mode to modify the MAC address of an interface.

1.3.21 VLAN Encapsulation Flag on Interfaces

Working Principle

Virtual local area network (VLAN) is a logical network divided on a physical network and corresponds to the layer-2 network in the ISO model. In 1999, IEEE released the 802.1Q protocol draft for standardizing the VLAN implementation solution.

The VLAN technology enables the network administrator to divide a physical LAN into multiple broadcast domains (or VLANs). Each VLAN contains a group of workstations with the same requirements and each VLAN has the same attributes as the physical LAN.As VLANs are logically divided, workstations in the same VLAN do not need to be placed in the same physical space, that is, these workstations may belong to different physical LAN network segments. Multicast and unicast traffic in a VLAN will not be forwarded to other VLANs. This helps control traffic, reduce device investment, simplify network management, and improve the network security.

VLAN is a protocol used to solve Ethernet broadcast and security problems. During packet transmission, a VLAN header is added to Ethernet frames. In addition, VLAN IDs are used to classify users to different work groups to restrict layer-2 exchange between users in different work groups. Each work group is a VLAN.VLANs can be used to restrict the broadcast scope and form virtual work groups to manage networks dynamically.

To ensure communication with hosts in a VLAN, users can configure the 802.1Q (VLAN protocol) VLAN encapsulation flag on the Ethernet interface or sub-interface. In this case, when packets are sent over the Ethernet interface, the corresponding VLAN header will be encapsulated. When packets are received, the VLAN header will be deleted from the packet.

Related Configuration

Configuring the VLAN Encapsulation Flag for Interfaces

By default, the 802.1Q encapsulation protocol is disabled for interfaces.

You can run the **encapsulation dot1Q VlanID** command in interface mode for 802.1Q encapsulation for an interface. **VlanID** indicates the encapsulated VLAN ID.

1.3.22 Interface FEC Mode

Working Principle

Forward Error Correction (FEC) is an error code correction method employing the following working principle: The sender adds a redundancy error-correcting code to the data for sending. The receiver performs error detection on the data based on the error-correcting code. If an error is found, the receiver corrects the error. FEC improves signal quality but also causes signal delay. Users can enable or disable this function according to the actual situation.

Different types of ports support different FEC modes. A 25 Gbps port supports the BASE-R mode, while a 100 Gbps port supports the RS mode.

Related Configuration

Configuring Interface FEC Mode

By default, FEC mode is disabled on a 25 Gbps port, and whether the FEC mode is enabled or disabled on a 100 Gbps port is determined by the inserted optical module.

Run the **fec mode {rs | base-r | none | auto}** command in interface mode to configure the FEC mode on an interface.

1.3.23 Statistics Sampling Cycle on Ethernet Ports

Working Principle

The default statistics sampling cycle of Ethernet ports is 5 seconds, which means that the interface statistics are updated every 5 seconds. In scenarios with high requirements for real-time statistics, you can prolong the sampling cycle.

A shorter sampling cycle indicates higher system performance consumption. Therefore, the sampling cycle must be adjusted as required. If the number of physical port exceeds 500, it is recommended to set the sampling cycle to over 10s.

Related Configuration

Configuring Statistics Sampling Cycle on Ethernet Ports

The default statistics sampling cycle of Ethernet ports is 5 seconds.

Run the **ethernet-port counter sample-period [*seconds*]** command in global configuration mode to adjust the sampling cycle on Ethernet ports.

1.4 Limitations

- Optical ports of the QSW-6900 series products do not support the speed of 100 Mbps.

- 10G optical port: When a 10G optical transceiver is inserted into a 10G optical port, the auto-negotiation mode is disabled. When a 1000M optical transceiver is inserted into a 10G optical port, the auto-negotiation mode is enabled by default.
- 40G optical port: When an optical transceiver is inserted into a 40G optical port, the auto-negotiation mode is disabled. When a copper cable is connected to a 40G optical port, the auto-negotiation mode is enabled.

- For QSW-6900 series products, the MTU is converted into a packet length for calculation in chips. The converted packet length used for calculation is 26 bytes (including a 14-byte Ethernet header, a 4-byte FCS, and two tags) greater than the configured MTU.

- When mode switching is configured on 25G ports of the QSW-6900-56F (**port speed-mode 10G/25G**), the modes of four consecutive ports of the configured port are changed at the same time, and no speed can be configured for the 25G ports.

- Ensure that the IP MTU, IPv6 MTU, and link MTU of layer-3 interfaces are set properly and the IP/IPv6 MTU is not greater than the interface MTU. Layer-3 interfaces include routing ports, layer-3 APs, and SVIs.

1.5 Configuration

Configuration	Description and Command	
Performing Basic Configurations	(Optional) It is used to manage interface configurations, for example, creating/deleting an interface, or configuring the interface description.	
	interface	Creates an interface and enters configuration mode of the created interface or a specified interface.
	interface range	Enters an interface range, creates these interfaces (if not created), and enters interface configuration mode.
	define interface-range	Creates a macro to specify an interface range.
	snmp-server if-index persist	Enables the interface index persistence function so that the interface index remains unchanged after the device is restarted.
	description	Configures the interface description of up to 80 characters in interface configuration mode.
	snmp trap link-status	Configures whether to send the link traps of the interface.
	shutdown	Shuts down an interface in interface configuration mode.
	split interface	Splits a 40G port in global configuration mode.
	physical-port dither protect	Configures interface flapping protection in global configuration mode.
	logging [link-updown | error-frame | link-dither | res-lack-frame]	Enables logging of status information on an interface in global configuration mode.

Configuring Interface Attributes	(Optional) It is used to configure interface attributes.	
	bandwidth	Configures the bandwidth of an interface in interface configuration mode.
	carrier-delay	Configures the carrier delay of an interface in interface configuration mode.
	load-interval	Configures the interval for load calculation of an interface.
	duplex	Configures the duplex mode of an interface.
	flowcontrol	Enables or disables flow control of an interface.
	mtu	Configures the MTU of an interface.
	negotiation mode	Configures the auto negotiation mode of an interface.
	speed	Configures the speed of an interface.
	port speed-mode	Configures the speed mode for a 25G port.
	switchport	Configures an interface as a L2 interface in interface configuration mode. (Run the **no switchport** command to configure an interface as a L3 interface.)
	switchport protected	Configures a port as a protected port.
	protected-ports route-deny	Blocks L3 routing between protected ports in global configuration mode.
	errdisable recovery [cause link-state]	Recovers a port in errdisable state in global configuration mode.
	route-sample enable	Enables the sampling function of a SVI/subinterface in interface configuration mode.
	mtu forwarding	Sets the global MTU and IP MTU.

	mac-address	Sets the MAC address of an interface.
	encapsulation dot1Q	Sets the VLAN tag for an interface.
	fec mode	Configures the FEC mode for an interface.
	ethernet-port counter sample-period	Configures the statistics sampling period for an Ethernet port.

1.5.1 Performing Basic Configurations

Configuration Effect

- Create a specified logical interface and enter configuration mode of this interface, or enter configuration mode of an existing physical or logical interface.
- Create multiple specified logical interfaces and enter interface configuration mode, or enter configuration mode of multiple existing physical or logical interfaces.
- The interface indexes remain unchanged after the device is restarted.
- Configure the interface description so that users can directly learn information about the interface.
- Enable or disable the link trap function of an interface.
- Enable or disable an interface.
- Split a 100G port or combine four 25G ports into a 100G port.

Notes

- The no form of the command can be used to delete a specified logical interface or logical interfaces in a specified range, but cannot be used to delete a physical port or physical ports in a specified range.
- The **default** form of the command can be used in interface configuration mode to restore default settings of a specified physical or logical interface, or interfaces in a specified range.

Configuration Steps

Configuring a Specified Interface

- Optional.
- Run this command to create a logical interface or enter configuration mode of a physical port or an existing logical interface.

Command	**interface** ***interface-type interface-number***

Parameter Description	*interface-type interface-number*: Indicates the type and number of the interface. The interface can be an Ethernet physical port, AP port, SVI, or loopback interface.
Defaults	N/A
Command Mode	Global configuration mode
Usage Guide	▪ If a logical interface is not created yet, run this command to create this interface and enter configuration mode of this interface. ▪ For a physical port or an existing logical interface, run this command to enter configuration mode of this interface. ▪ Use the **no** form of the command to delete a specified logical interface. ▪ Use the **default** form of the command to restore default settings of the interface in interface configuration mode.

Configuring Interfaces Within a Range

- Optional.
- Run this command to create multiple logical interfaces or enter configuration mode of multiple physical port or existing logical interfaces.

Command	**interface range { *port-range* | macro *macro_name* }**
Parameter Description	*port-range*: Indicates the type and ID range of interfaces. These interfaces can be Ethernet physical ports, AP ports, SVIs, or loopback interfaces. *macro_name*: Indicates the name of the interface range macro.
Defaults	N/A
Command Mode	Global configuration mode
Usage Guide	▪ If logical interfaces are not created yet, run this command to create these interfaces and enter interface configuration mode. ▪ For multiple physical ports or existing logical interfaces, run this command to enter interface configuration mode. ▪ Use the **default** form of the command to restore default settings of these interfaces in interface configuration mode. ▪ Before using a macro, run the **define interface-range** command to define the interface range as a macro name in global configuration mode, and then run the **interface range macro** *macro_name* command to apply the macro.

Configuring Interface Index Persistence

- Optional.
- Run this command when the interface indexes must remain unchanged after the device is restarted.

Command	**snmp-server if-index persist**
Parameter Description	N/A
Defaults	By default, interface index persistence is disabled.
Command Mode	Global configuration mode
Usage Guide	After this command is executed, current indexes of all interfaces will be saved, and the indexes remain unchanged after the device is restarted. You can use the no or default form of the command to disable the interface index persistence function.

Configuring the Description of an Interface

- Optional.
- Run this command to configure the description of an interface.

Command	**description *string***
Parameter Description	*string:* Indicates a string of up to 80 characters.
Defaults	By default, no description is configured.
Command Mode	Interface configuration mode
Usage Guide	This command is used to configure the description of an interface. You can use the **no** or **default** form of the command to delete the description of an interface.-

Configuring the Link Trap Function of an Interface

- Optional.
- Run this command to obtain the link traps through SNMP.

Command	**snmp trap link-status**
Parameter Description	N/A
Defaults	By default, the link trap function is enabled.

Command Mode	Interface configuration mode
Usage Guide	This command is used to configure the link trap function on an interface. When this function is enabled, the SNMP sends link traps when the link status changes on the interface. You can use the **no** or **default** form of the command to disable the link trap function.

Configuring the Administrative Status of an Interface

- Optional.
- Run this command to enable or disable an interface.
- An interface cannot send or receive packets after it is disabled.

Command	**Shutdown**
Parameter Description	N/A
Defaults	By default, the administrative status of an interface is Up.
Command Mode	Interface configuration mode
Usage Guide	You can run the **shutdown** command to disable an interface, or the **no shutdown** command to enable an interface. In some cases, for example, when an interface is in errdisable state, you cannot run the **no shutdown** command on an interface. You can use the **no** or **default** form of the command to enable the interface.

Splitting a 100G Port or Combining Four 25G Ports into a 100G Port

- Optional.
- Run this command to split a 100G port or combine four 25G ports into a 100G port.

Command	**[no] split interface *interface-type interface-number***
Parameter Description	*interface-type interface-number*: Indicates the type and number of a port. The port must be a 100G port.
Defaults	By default, the ports are combined.
Command Mode	Global configuration mode

Usage Guide	You can run the **split** command to split a 100G port, or the **no split** command to combine the split 100G port. After this command is configured, you generally need to restart the line card or the entire device so that the configuration can take effect.

Configuring the SVI or Sub-Interface Sampling Function

- Optional.
- Run this command to enable the SVI or sub-interface sampling function.

Command	**[no] route-sample enable**
Parameter Description	N/A
Defaults	By default, the SVI or sub-interface does not support sampling.
Command Mode	Interface configuration mode
Usage Guide	N/A

Configuring Port Flapping Protection

- Optional.
- Run this command to protect the port against flapping.

Command	**physical-port dither protect**
Parameter Description	N/A
Defaults	By default, port flapping protection is enabled.
Command Mode	Global configuration mode
Usage Guide	N/A

Configuring the Syslog Function

- Optional.
- Run this command to enable or disable the syslog function on an interface.

Command	[no] logging [link-updown | error-frame | link-dither | res-lack-frame]

Parameter Description	**link-updown**: prints the status change information. **error-frame**: prints the error frame information. **link-dither**: prints the port flapping information. **res-lack-frame**: prints the error frame information received by an inteface due to lack of resource.
Defaults	By default, the syslog function is enabled on an interface.
Command Mode	Global configuration mode
Usage Guide	N/A

Verification

Configuring a Specified Interface

- Run the **interface** command. If you can enter interface configuration mode, the configuration is successful.
- For a logical interface, after the **no interface** command is executed, run the **show running** or **show interfaces** command to check whether the logical interface exists. If not, the logical interface is deleted.
- After the **default interface** command is executed, run the **show running** command to check whether the default settings of the corresponding interface are restored. If yes, the operation is successful.

Configuring Interfaces Within a Range

- Run the **interface range** command. If you can enter interface configuration mode, the configuration is successful.
- After the **default interface range** command is executed, run the **show running** command to check whether the default settings of the corresponding interfaces are restored. If yes, the operation is successful.

Configuring Interface Index Persistence

- After the **snmp-server if-index persist** command is executed, run the **write** command to save the configuration, restart the device, and run the **show interface** command to check the interface index. If the index of an interface remains the same after the restart, interface index persistence is enabled.

Configuring the Link Trap Function of an Interface

- Remove and then insert the network cable on a physical port, and enable the SNMP server. If the SNMP server receives link traps, the link trap function is enabled.

- Run the **no** form of the **snmp trap link-status** command. Remove and then insert the network cable on a physical port. If the SNMP server does not receive link traps, the link trap function is disabled.

Configuring the Administrative Status of an Interface

- Insert the network cable on a physical port, enable the port, and run the shutdown command on this port. If the syslog is displayed on the Console indicating that the state of the port changes to Down, and the indicator on the port is off, the port is disabled. Run the show interfaces command, and verify that the interface state changes to Administratively Down. Then, run the no shutdown command to enable the port. If the syslog is displayed on the Console indicating that the state of the port changes to Up, and the indicator on the port is on, the port is enabled.

Splitting or Combining a 100G Port

- Run the **split** command on a 100G port in global configuration mode. Verify that the related syslog is displayed on the Console. Run the **write** command to save the configuration, and restart the device or line card according to the method described in the syslog. The four 25G ports can be configured as L2 or L3 ports, but the split 100G port cannot be configured as a L2 or L3 port.
- Run the **no split** command on a split 100G port. Verify that the related syslog is displayed on the Console. Run the **write** command to save the configuration, and restart the device or line card according to the method described in the syslog. The four 25G ports cannot be configured as L2 or L3 ports, but the combined 100G port can be configured as a L2 or L3 port.

Configuring the SVI or Sub-Interface Sampling Function

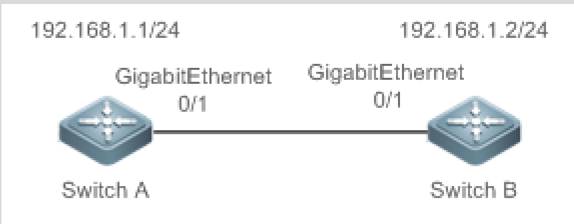
- Run the **route-sample enable** command in SVI or sub-interface configuration mode. Then, run the **show interface** command and verify that the number of sent or received packets and the packet sending/receiving rate are displayed. Run the **no route-sample enable** command. Then, run the **show interface** command and verify that the number of sent or received packets and the packet sending/receiving rate are not displayed.

Configuring Port Flapping Protection

- Run the **physical-port dither protect** command in global configuration mode. Frequently remove and insert the network cable on a physical port to simulate port flapping. Verify that a syslog indicating port flapping is displayed on the Console. After such a syslog is displayed for several times, the system prompts that the port will be turned into the violation mode.

Configuration Example

Configuring Basic Attributes of Interfaces

Scenario Figure 1-5	

Configuration Steps	▪ Connect two devices through the switch ports. ▪ Configure an SVI respectively on two devices, and assign IP addresses from a network segment to the two SVIs. ▪ Enable interface index persistence on the two devices. ▪ Enable the link trap function on the two devices. ▪ Configure the interface administrative status on the two devices.
A	A# configure terminal A(config)# snmp-server if-index persist A(config)# interface vlan 1 A(config-if-VLAN 1)# ip address 192.168.1.1 255.255.255.0 A(config-if-VLAN 1)# exit A(config)# interface gigabitethernet 0/1 A(config-if-GigabitEthernet 0/1)# snmp trap link-status A(config-if-GigabitEthernet 0/1)# shutdown A(config-if-GigabitEthernet 0/1)# end A# write
B	B# configure terminal B(config)# snmp-server if-index persist B(config)# interface vlan 1 B(config-if-VLAN 1)# ip address 192.168.1.2 255.255.255.0 B(config-if-VLAN 1)# exit B(config)# interface gigabitethernet 0/1 B(config-if-GigabitEthernet 0/1)# snmp trap link-status B(config-if-GigabitEthernet 0/1)# shutdown B(config-if-GigabitEthernet 0/1)# end B# write
Verification	Perform verification on Switch A and Switch B as follows: ▪ Run the **shutdown** command on port GigabitEthern 0/1, and check whether GigabitEthern 0/1 and SVI 1 are Down. ▪ Run the **shutdown** command on port GigabitEthern 0/1, and check whether a trap indicating that this interface is Down is sent. ▪ Restart the device, and check whether the index of GigabitEthern 0/1 is the same as that before the restart.
A	A# show interfaces gigabitEthernet 0/1 Index(dec):1 (hex):1

```
GigabitEthernet 0/1 is administratively down  , line protocol is DOWN
Hardware is GigabitEthernet, address is 08c6.b3.de9b (bia 08c6.b3.de9b)
Interface address is: no ip address
  MTU 1500 bytes, BW 1000000 Kbit
  Encapsulation protocol is Bridge, loopback not set
  Keepalive interval is 10 sec , set
  Carrier delay is 2 sec
  Rxload is 1/255, Txload is 1/255
  Queue    Transmitted packets    Transmitted bytes      Dropped packets
Dropped bytes
     0                 0                 0                 0                0
     1                 0                 0                 0                0
     2                 0                 0                 0                0
     3                 0                 0                 0                0
     4                 0                 0                 0                0
     5                 0                 0                 0                0
     6                 0                 0                 0                0
     7                 4               440                 0                0
  Switchport attributes:
    interface's description:""
    lastchange time:0 Day:20 Hour:15 Minute:22 Second
    Priority is 0

    admin speed is AUTO, oper speed is Unknown
    flow control admin status is OFF, flow control oper status is Unknown
    admin negotiation mode is OFF, oper negotiation state is ON
    Storm Control: Broadcast is OFF, Multicast is OFF, Unicast is OFF
  Port-type: access
    Vlan id: 1
   10 seconds input rate 0 bits/sec, 0 packets/sec
   10 seconds output rate 0 bits/sec, 0 packets/sec
    4 packets input, 408 bytes, 0 no buffer, 0 dropped
    Received 0 broadcasts, 0 runts, 0 giants
    0 input errors, 0 CRC, 0 frame, 0 overrun, 0 abort
    4 packets output, 408 bytes, 0 underruns , 0 dropped
```

<table>
<tr><td></td><td>0 output errors, 0 collisions, 0 interface resets
A# show interfaces vlan 1
Index(dec):4097 (hex):1001
VLAN 1 is UP , line protocol is DOWN
Hardware is VLAN, address is 08c6.b3.33af (bia 08c6.b3.33af)
Interface address is: 192.168.1.1/24
ARP type: ARPA, ARP Timeout: 3600 seconds
MTU 1500 bytes, BW 1000000 Kbit
Encapsulation protocol is Ethernet-II, loopback not set
Keepalive interval is 10 sec , set
Carrier delay is 2 sec
Rxload is 0/255, Txload is 0/255</td></tr>
<tr><td>B</td><td>B# show interfaces gigabitEthernet 0/1
Index(dec):1 (hex):1
GigabitEthernet 0/1 is administratively down , line protocol is DOWN
Hardware is GigabitEthernet
Interface address is: no ip address, address is 08c6.b3.de9b (bia 08c6.b3.de9b)
MTU 1500 bytes, BW 1000000 Kbit
Encapsulation protocol is Bridge, loopback not set
Keepalive interval is 10 sec , set
Carrier delay is 2 sec
Rxload is 1/255, Txload is 1/255
Queue Transmitted packets Transmitted bytes Dropped packets Dropped bytes
0 0 0 0 0
1 0 0 0 0
2 0 0 0 0
3 0 0 0 0
4 0 0 0 0
5 0 0 0 0
6 0 0 0 0
7 4 440 0 0
Switchport attributes:
interface's description:""
lastchange time:0 Day:20 Hour:15 Minute:22 Second</td></tr>
</table>

```
  Priority is 0

  admin duplex mode is AUTO, oper duplex is Unknown
  admin speed is AUTO, oper speed is Unknown
  flow control admin status is OFF, flow control oper status is Unknown
  admin negotiation mode is OFF, oper negotiation state is ON
  Storm Control: Broadcast is OFF, Multicast is OFF, Unicast is OFF
 Port-type: access
  Vlan id: 1
 10 seconds input rate 0 bits/sec, 0 packets/sec
 10 seconds output rate 0 bits/sec, 0 packets/sec
  4 packets input, 408 bytes, 0 no buffer, 0 dropped
  Received 0 broadcasts, 0 runts, 0 giants
  0 input errors, 0 CRC, 0 frame, 0 overrun, 0 abort
  4 packets output, 408 bytes, 0 underruns , 0 dropped
    0 output errors, 0 collisions, 0 interface resets
B# show interfaces vlan 1
Index(dec):4097 (hex):1001
VLAN 1 is UP  , line protocol is DOWN
Hardware is  VLAN, address is 08c6.b3.33af (bia 08c6.b3.33af)
Interface address is: 192.168.1.2/24
ARP type: ARPA, ARP Timeout: 3600 seconds
 MTU 1500 bytes, BW 1000000 Kbit
 Encapsulation protocol is Ethernet-II, loopback not set
 Keepalive interval is 10 sec , set
 Carrier delay is 2 sec
 Rxload is 0/255, Txload is 0/255
```

1.5.2 Configuring Interface Attributes

Configuration Effect

- Enable the device to connect and communicate with other devices through the switch port or routed port.
- Adjust various interface attributes on the device.

Configuration Steps

Configuring a Routed Port

- Optional.
- Run this command to configure a port as a L3 routed port.
- After a port is configured as a L3 routed port, L2 protocols running on the port do not take effect.
- This command is applicable to a L2 switch port.

Command	no switchport
Parameter Description	N/A
Defaults	By default, an Ethernet physical port is a L2 switch port.
Command Mode	Interface configuration mode
Usage Guide	On a L3 device, you can run this command to configure a L2 switch port as a L3 routed port. You can run the **switchport** command to change a L3 routed port into a L2 switch port.

Configuring a L3 AP Port

- Optional.
- Run the **no switchport** command in interface configuration mode to configure a L2 AP port as a L3 AP port. Run the **switchport** command to configure a L3 AP port as a L2 AP port.
- After a port is configured as a L3 routed port, L2 protocols running on the port do not take effect.
- This command is applicable to a L2 AP port.

Command	**no switchport**
Parameter Description	N/A
Defaults	By default, an AP port is a L2 AP port.
Command Mode	Interface configuration mode

Usage Guide	After entering configuration mode of a L2 AP port on a L3 device, you can run this command to configure a L2 AP port as a L3 AP port. After entering configuration mode of a L3 AP port, you can run the switchport command to change a L3 AP port into a L2 AP port.

Configuring the Speed of an Interface

- Optional.
- Port flapping may occur if the configured speed of a port changes.
- This command is applicable to an Ethernet physical port or AP port.
- A same speed mode must be configured on four consecutive 25 Gbps ports.

Command	**speed [10 | 100 | 1000 | 10G | 40G | 100G | auto]**
Parameter Description	**10**: Indicates that the speed of the interface is 10 Mbps. **100**: Indicates that the speed of the interface is 100 Mbps. **1000**: Indicates that the speed of the interface is 1000 Mbps. **10G**: Indicates that the speed of the interface is 10 Gbps. **40G**: Indicates that the speed of the interface is 40 Gbps. 100G: Indicates that the speed of the interface is 100 Gbps.
Defaults	By default, the speed of an interface is auto.
Command Mode	Interface configuration mode
Usage Guide	If an interface is an AP member port, the speed of this interface is determined by the speed of the AP port. When the interface exits the AP port, it uses its own speed configuration. You can run **show interfaces** to display the speed configurations. The speed options available to an interface vary with the type of the interface. For example, you cannot set the speed of an SFP interface to 10 Mbps. The speed of a 40G physical port can only be set to 40 Gbps or auto.
Command	**port speed-mode [10G | 25G]**
Parameter Description	**10G**: Indicates that the speed of the interface is 10 Gbps. **25G**: Indicates that the speed of the interface is 25 Gbps.
Defaults	The speed of the interface is **25G** by default.
Command Mode	Interface configuration mode
Usage Guide	Only 25 Gbps ports support this speed mode. A same speed mode must be configured on four consecutive 25 Gbps ports.

	Only 25 Gbps ports with the same speed mode are allowed to join the same aggregation group. Running the **default interface** command does not clear the speed mode configuration on 25 Gbps ports.

Configuring the Duplex Mode of an Interface

- Optional.
- Port flapping may occur if the configured duplex mode of a port changes.
- This command is applicable to an Ethernet physical port or AP port.

Command	**duplex { auto | full | half }**
Parameter Description	**auto**: Indicates automatic switching between full duplex and half duplex. **full**: Indicates full duplex. **half**: Indicates half duplex.
Defaults	By default, the duplex mode of an interface is auto.
Command Mode	Interface configuration mode
Usage Guide	The duplex mode of an interface is related to the interface type. You can run **show interfaces** to display the configurations of the duplex mode.

Configuring the Flow Control Mode of an Interface

- Optional.
- Generally, the flow control mode of an interface is off by default. For some products, the flow control mode is on by default.
- After flow control is enabled on an interface, the flow control frames will be sent or received to adjust the data volume when congestion occurs on the interface.
- Port flapping may occur if the configured flow control mode of a port changes.
- This command is applicable to an Ethernet physical port or AP port.

Command	**flowcontrol { auto | off | on }**
Parameter Description	auto: Indicates automatic flow control. off: Indicates that flow control is disabled. on: Indicates that flow control is enabled.
Defaults	By default, flow control is disabled on an interface.

Command Mode	Interface configuration mode

Configuring the Auto Negotiation Mode of an Interface

- Optional.
- Port flapping may occur if the configured auto negotiation mode of a port changes.
- This command is applicable to an Ethernet physical port or AP port.

Command	**negotiation mode { on | off }**
Parameter Description	**on**: Indicates that the auto negotiation mode is on. **off**: Indicates that the auto negotiation mode is off.
Defaults	By default, the auto negotiation mode is off.
Command Mode	Interface configuration mode
Usage Guide	N/A

Configuring the MTU of an Interface

- Optional.
- You can configure the MTU of a port to limit the length of a frame that can be received or sent over this port.
- This command is applicable to an Ethernet physical port or SVI.

Command	**mtu *num***
Parameter Description	*num*: *64–9216*
Defaults	By default, the MTU of an interface is 1500 bytes.
Command Mode	Interface configuration mode
Usage Guide	This command is used to configure the interface MTU, that is, the maximum length of a data frame at the link layer. Currently, you can configure MTU for only a physical port or an AP port that contains one or more member ports.

Configuring Global MTU

- Optional.
- Users can set the global MTU and IP MTU to control the maximum length of frames that can be sent and received over all ports.
- Support physical Ethernet port.

Command	**mtu forwarding *num***
Parameter Description	*num*: *64–9216*
Defaults	By default, the MTU of an interface is 1500 bytes.
Command Mode	Global configuration mode
Usage Guide	The IP MTU automatically changes to the value of the link MTU of an interface when the globally set link MTU changes.

Configuring the Bandwidth of an Interface

- Optional.
- Generally, the bandwidth of an interface is the same as the speed of the interface.

Command	**bandwidth *kilobits***
Parameter Description	*kilobits*: The value ranges from 1 to 2,147,483,647. The unit is kilo bits.
Defaults	Generally, the bandwidth of an interface matches the type of the interface. For example, the default bandwidth of a gigabit Ethernet physical port is 1,000,000, and that of a 10G Ethernet physical port is 10,000,000.
Command Mode	Interface configuration mode
Usage Guide	N/A

Configuring the Carrier Delay of an Interface

- Optional.
- If the configured carrier delay is long, it takes a long time to change the protocol status when the physical status of an interface changes. If the carrier delay is set to 0, the protocol status changes immediately after the physical status of an interface changes.

Command	**carrier-delay {[milliseconds] *num* | up [milliseconds] *num* down [milliseconds] *num*}**

Parameter Description	*num*: The value ranges from 0 to 60. The unit is second. *milliseconds*: Indicates the carrier delay. The value ranges from 0 to 60,000. The unit is millisecond. *Up*: Indicates the delay after which the state of the DCD changes from Down to Up. *Down*: Indicates the delay after which the state of the DCD changes from Up to Down.
Defaults	By default, the carrier delay of an interface is 2s.
Command Mode	Interface configuration mode
Usage Guide	If millisecond is used as the unit, the configured carrier delay must be an integer multiple of 100 milliseconds.

Configuring the Load Interval of an Interface

- Optional.
- The configured load interval affects computation of the average packet rate on an interface. If the configured load interval is short, the average packet rate can accurately reflect the changes of the real-time traffic.

Command	**load-interval *seconds***
Parameter Description	*seconds*: The value ranges from 5 to 600. The unit is second.
Defaults	By default, the load interval of an interface is 10s.
Command Mode	Interface configuration mode
Usage Guide	N/A

Configuring a Protected Port

- Optional.
- L2 packets cannot be forwarded between protected ports.
- This command is applicable to an Ethernet physical port or AP port.

Command	**switchport protected**
Parameter Description	N/A

Defaults	By default, no protected port is configured.
Command Mode	Interface configuration mode
Usage Guide	N/A

Blocking L3 Routing Between Protected Ports

- Optional.
- After this command is configured, L3 routing between protected ports are blocked.

Command	**protected-ports route-deny**
Parameter Description	N/A
Defaults	By default, the function of blocking L3 routing between protected ports is disabled.
Command Mode	Global configuration mode
Usage Guide	By default, L3 routing between protected ports is not blocked. In this case, you can run this command to block routing between protected ports.

Configuring Port Errdisable Recovery

- Optional.
- By default, a port will be disabled and will not be recovered after a violation occurs. After port errdisable recovery is configured, a port in errdisable state will be recovered and enabled.

Command	**errdisable recovery [interval *time* | cause *link-state*]**
Parameter Description	*time*: Indicates the automatic recovery time. The value ranges from 30 to 86,400. The unit is second. link-state: Restores the port that is set to the errdisable state by the REUP link state tracking function.
Defaults	By default, port errdisable recovery is disabled.
Command Mode	Global configuration mode

Usage Guide	By default, a port in errdisable state is not recovered. You can recover the port manually or run this command to automatically recover the port.

Configuring MAC Addresses for Interfaces

- Optional. If this function is required, run the **mac-address** command in interface configuration mode.
- By default, MAC addresses of interfaces have fixed values.

Command	**mac-address *mac-address***
Parameter Description	***Mac-address***: Indicates a valid MAC address.
Command Mode	Interface configuration mode
Usage Guide	N/A

Configuring the VLAN Encapsulation Flag for Interfaces

- Optional. If this function is required, run the **encapsulation dot1Q** command in interface configuration mode.
- By default, the VLAN encapsulation protocol is disabled for interfaces.

Command	encapsulation dot1Q *VlanID*
Parameter Description	***VlanID***: Indicates the VLAN ID. The value range is from **1** to **4094**.
Command Mode	Interface configuration mode
Usage Guide	N/A

Configuring Interface FEC Mode

- Optional.
- By default, FEC mode is disabled on a 25 Gbps port, and whether the FEC mode is enabled or disabled on a 100 Gbps port is determined by the inserted optical module.

Command	**fec mode {rs | base-r | none | auto}**

Parameter Description	rs: Enable FEC mode by rs. Supported by 100 Gbps port. base-r: Enable FEC mode by base-r. Supported by 25 Gbps port. none: Enable FEC function. auto: Whether the FEC mode is enabled or disabled is determined by the inserted optical module. Supported by 100 Gbps port.
Command Mode	Interface configuration mode
Usage Guide	N/A

Configuring Statistics Sampling Cycle on Ethernet Port

- Optional.
- The default statistics sampling cycle of Ethernet ports is 5 seconds.

Command	**ethernet-port counter sample-period [seconds]**
Parameter Description	seconds: Unit of the sampling cycle.
Defaults	rs: Enable FEC mode by rs. Supported by 100 Gbps port. base-r: Enable FEC mode by base-r. Supported by 25 Gbps port. none: Enable FEC function. auto: Whether the FEC mode is enabled or disabled is determined by the inserted optical module. Supported by 100 Gbps port.
Command Mode	Interface configuration mode
Usage Guide	A shorter sampling cycle indicates higher system performance consumption. Therefore, the sampling cycle must be adjusted as required.

Verification

- Run the show interfaces command to display the attribute configurations of interfaces.

Command	**show interfaces [** ***interface-type interface-number*** **] [description | switchport | trunk]**
Parameter Description	*interface-type interface-number*: Indicates the type and number of the interface. **description**: Indicates the interface description, including the link status. **switchport**: Indicates the L2 interface information. This parameter is effective only for a L2 interface.

	trunk: Indicates the Trunk port information. This parameter is effective for a physical port or an AP port.
Command Mode	Privileged EXEC mode
Usage Guide	Use this command without any parameter to display the basic interface information.

	SwitchA#show interfaces GigabitEthernet 0/1
	Index(dec):1 (hex):1
	GigabitEthernet 0/1 is DOWN, line protocol is DOWN
	  Hardware is Broadcom 5464 GigabitEthernet, address is 08c6.b3.de9b (bia 08c6.b3.de9b)
	  Interface address is: no ip address
	  Interface IPv6 address is:
	    No IPv6 address
	  MTU 1500 bytes, BW 1000000 Kbit
	  Encapsulation protocol is Ethernet-II, loopback not set
	  Keepalive interval is 10 sec, set
	  Carrier delay is 2 sec
	  Ethernet attributes:
	    Last link state change time: 2012-12-22 14:00:48
	    Time duration since last link state change: 3 days, 2 hours, 50 minutes, 50 seconds
	    Priority is 0
	    Medium-type is Copper
	    Admin duplex mode is AUTO, oper duplex is Unknown
	    Admin speed is AUTO, oper speed is Unknown
	    Flow receive control admin status is OFF,flow send control admin status is OFF
	    Flow receive control oper status is Unknown,flow send control oper status is Unknown
	    Storm Control: Broadcast is OFF, Multicast is OFF, Unicast is OFF
	  Bridge attributes:
	    Port-type: trunk
	    Native vlan:1
	    Allowed vlan lists:1-4094 //Allowed VLAN list of the Trunk port
	    Active vlan lists:1, 3-4 //Active VLAN list (indicating that only VLAN 1, VLAN 3, and VLAN 4 are created on the device)

	Rxload is 1/255,Txload is 1/255 5 minutes input rate 0 bits/sec, 0 packets/sec 5 minutes output rate 0 bits/sec, 0 packets/sec 0 packets input, 0 bytes, 0 no buffer, 0 dropped Received 0 broadcasts, 0 runts, 0 giants 0 input errors, 0 CRC, 0 frame, 0 overrun, 0 abort 0 packets output, 0 bytes, 0 underruns, 0 dropped 0 output errors, 0 collisions, 0 interface resets

- Run the **show eee interfaces status** command to display the EEE status of an interface.

Command	**show eee interfaces { interface-type interface-number | status }**
Parameter Description	*interface-type interface-number*: Indicates the type and number of an interface. ***status*:** Indicates the EEE status of all interfaces.
Command Mode	Privileged EXEC mode
Usage Guide	If the interface is specified, the EEE status of the specified interface is displayed; otherwise, the EEE status of all interfaces is displayed.
	1. Display the EEE status of GigabitEthernet 0/1. QTECH#show eee interface gigabitEthernet 0/1 Interface : Gi0/1 EEE Support : Yes Admin Status : Enable Oper Status : Disable Remote Status : Disable Trouble Cause : Remote Disable Interface — Indicates the interface information. EEE Support — Indicates whether EEE is supported. Admin Status — Indicates the administrative status. Oper Status — Indicates the operational status. Trouble Cause — Indicates the reason why the EEE status of an interface is abnormal. 2. Display the EEE status of all interfaces.

```
QTECH#show eee interface status
Interface EEE     Admin    Oper     Remote   Trouble
          Support Status   Status   Status   Cause
--------- ------- -------- -------- -------- --------------------
Gi0/1     Yes     Enable   Disable  Disable  Remote Disable
Gi0/2     Yes     Enable   Disable  Unknown  None
Gi0/3     Yes     Enable   Enable   Enable   None
Gi0/4     Yes     Enable   Enable   Enable   None
Gi0/5     Yes     Enable   Enable   Enable   None
Gi0/6     Yes     Enable   Enable   Enable   None
Gi0/7     Yes     Enable   Enable   Enable   None
Gi0/8     Yes     Enable   Enable   Enable   None
Gi0/9     Yes     Enable   Enable   Enable   None
Gi0/10    Yes     Enable   Enable   Enable   None
```

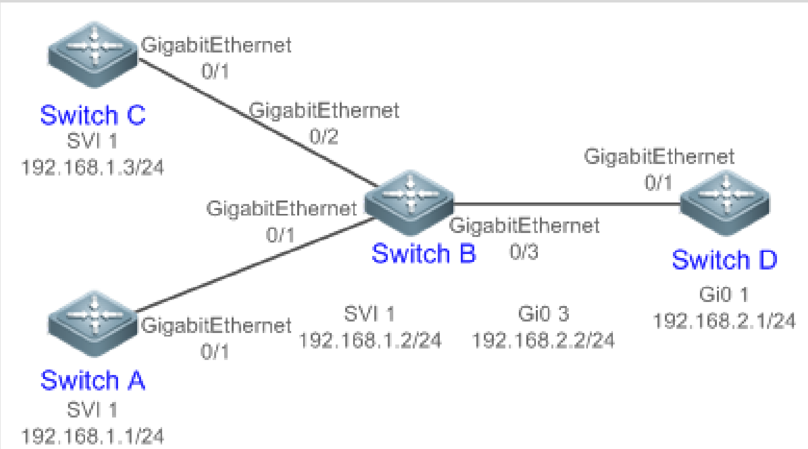
Interface	Indicates the interface information.
EEE Support	Indicates whether EEE is supported.
Admin Status	Indicates the administrative status.
Oper Status	Indicates the operational status.
Trouble Cause	Indicates the reason why the EEE status of an interface is abnormal.

Configuration Example

Configuring Interface Attributes

Scenario

Figure 1-1



Configuration Steps	▪ On Switch A, configure GigabitEthernet 0/1 as an access mode, and the default VLAN ID is 1. Configure SVI 1, assign an IP address to SVI 1, and set up a route to Switch D. ▪ On Switch B, configure GigabitEthernet 0/1 and GigabitEthernet 0/2 as Trunk ports, and the default VLAN ID is 1. Configure SVI 1, and assign an IP address to SVI 1. Configure GigabitEthernet 0/3 as a routed port, and assign an IP address from another network segment to this port. ▪ On Switch C, configure GigabitEthernet 0/1 as an Access port, and the default VLAN ID is 1. Configure SVI 1, and assign an IP address to SVI 1. ▪ On Switch D, configure GigabitEthernet 0/1 as a routed port, assign an IP address to this port, and set up a route to Switch A.
A	A# configure terminal A(config)# interface GigabitEthernet 0/1 A(config-if-GigabitEthernet 0/1)# switchport mode access A(config-if-GigabitEthernet 0/1)# switchport access vlan 1 A(config-if-GigabitEthernet 0/1)# exit A(config)# interface vlan 1 A(config-if-VLAN 1)# ip address 192.168.1.1 255.255.255.0 A(config-if-VLAN 1)# exit A(config)# ip route 192.168.2.0 255.255.255.0 VLAN 1 192.168.1.2
B	B# configure terminal B(config)# interface GigabitEthernet 0/1 B(config-if-GigabitEthernet 0/1)# switchport mode trunk B(config-if-GigabitEthernet 0/1)# exit B(config)# interface GigabitEthernet 0/2 B(config-if-GigabitEthernet 0/2)# switchport mode trunk B(config-if-GigabitEthernet 0/2)# exit B(config)# interface vlan 1 B(config-if-VLAN 1)# ip address 192.168.1.2 255.255.255.0 B(config-if-VLAN 1)# exit B(config)# interface GigabitEthernet 0/3 B(config-if-GigabitEthernet 0/3)# no switchport B(config-if-GigabitEthernet 0/3)# ip address 192.168.2.2 255.255.255.0 B(config-if-GigabitEthernet 0/3)# exit
C	C# configure terminal C(config)# interface GigabitEthernet 0/1

	C(config-if-GigabitEthernet 0/1)# port-group 1 C(config-if-GigabitEthernet 0/1)# exit C(config)# interface aggregateport 1 C(config-if-AggregatePort 1)# switchport mode access C(config-if-AggregatePort 1)# switchport access vlan 1 C(config-if-AggregatePort 1)# exit C(config)# interface vlan 1 C(config-if-VLAN 1)# ip address 192.168.1.3 255.255.255.0 C(config-if-VLAN 1)# exit
D	D# configure terminal D(config)# interface GigabitEthernet 0/1 D(config-if-GigabitEthernet 0/1)# no switchport D(config-if-GigabitEthernet 0/1)# ip address 192.168.2.1 255.255.255.0 D(config-if-GigabitEthernet 0/1)# exit A(config)# ip route 192.168.1.0 255.255.255.0 GigabitEthernet 0/1 192.168.2.2
Verification	Perform verification on Switch A, Switch B, Switch C, and Switch D as follows: ▪ On Switch A, ping the IP addresses of interfaces of the other three switches. Verify that you can access the other three switches on Switch A.. ▪ Verify that switch B and Switch D can be pinged mutually. ▪ Verify that the interface status is correct.

A	A# show interfaces gigabitEthernet 0/1
	Index(dec):1 (hex):1
	GigabitEthernet 0/1 is UP, line protocol is UP
	Hardware is GigabitEthernet, address is 08c6.b3.de90 (bia 08c6.b3.de90)
	Interface address is: no ip address
	  MTU 1500 bytes, BW 100000 Kbit
	  Encapsulation protocol is Ethernet-II, loopback not set
	  Keepalive interval is 10 sec, set
	  Carrier delay is 2 sec
	  Ethernet attributes:
	    Last link state change time: 2012-12-22 14:00:48
	    Time duration since last link state change: 3 days, 2 hours, 50 minutes, 50 seconds
	    Priority is 0
	    Admin medium-type is Copper, oper medium-type is Copper

	Admin duplex mode is AUTO, oper duplex is Full Admin speed is AUTO, oper speed is 100M Flow control admin status is OFF, flow control oper status is OFF Admin negotiation mode is OFF, oper negotiation state is ON Storm Control: Broadcast is OFF, Multicast is OFF, Unicast is OFF **Bridge attributes:** **Port-type: access** **Vlan id: 1** Rxload is 1/255, Txload is 1/255 10 seconds input rate 0 bits/sec, 0 packets/sec 10 seconds output rate 67 bits/sec, 0 packets/sec 362 packets input, 87760 bytes, 0 no buffer, 0 dropped Received 0 broadcasts, 0 runts, 0 giants 0 input errors, 0 CRC, 0 frame, 0 overrun, 0 abort 363 packets output, 82260 bytes, 0 underruns, 0 dropped 0 output errors, 0 collisions, 0 interface resets
B	B# show interfaces gigabitEthernet 0/1 Index(dec):1 (hex):1 GigabitEthernet 0/1 is UP, line protocol is UP Hardware is GigabitEthernet, address is 08c6.b3.de91 (bia 08c6.b3.de91) Interface address is: no ip address MTU 1500 bytes, BW 100000 Kbit Encapsulation protocol is Ethernet-II, loopback not set Keepalive interval is 10 sec, set Carrier delay is 2 sec Ethernet attributes: Last link state change time: 2012-12-22 14:00:48 Time duration since last link state change: 3 days, 2 hours, 50 minutes, 50 seconds Priority is 0 Admin medium-type is Copper, oper medium-type is Copper Admin duplex mode is AUTO, oper duplex is Full Admin speed is AUTO, oper speed is 100M Flow control admin status is OFF, flow control oper status is OFF Admin negotiation mode is OFF, oper negotiation state is ON

	Storm Control: Broadcast is OFF, Multicast is OFF, Unicast is OFF Bridge attributes: **Port-type: trunk** **Native vlan: 1** **Allowed vlan lists: 1-4094** **Active vlan lists: 1** Rxload is 1/255, Txload is 1/255 10 seconds input rate 0 bits/sec, 0 packets/sec 10 seconds output rate 67 bits/sec, 0 packets/sec 362 packets input, 87760 bytes, 0 no buffer, 0 dropped Received 0 broadcasts, 0 runts, 0 giants 0 input errors, 0 CRC, 0 frame, 0 overrun, 0 abort 363 packets output, 82260 bytes, 0 underruns, 0 dropped 0 output errors, 0 collisions, 0 interface resets
C	C# show interfaces gigabitEthernet 0/1 Index(dec):1 (hex):1 GigabitEthernet 0/1 is UP, line protocol is UP Hardware is GigabitEthernet, address is 08c6.b3.de92 (bia 08c6.b3.de92) Interface address is: no ip address MTU 1500 bytes, BW 100000 Kbit Encapsulation protocol is Ethernet-II, loopback not set Keepalive interval is 10 sec, set Carrier delay is 2 sec Ethernet attributes: Last link state change time: 2012-12-22 14:00:48 Time duration since last link state change: 3 days, 2 hours, 50 minutes, 50 seconds Priority is 0 Admin medium-type is Copper, oper medium-type is Copper Admin duplex mode is AUTO, oper duplex is Full Admin speed is AUTO, oper speed is 100M Flow control admin status is OFF, flow control oper status is OFF Admin negotiation mode is OFF, oper negotiation state is ON Storm Control: Broadcast is OFF, Multicast is OFF, Unicast is OFF Rxload is 1/255, Txload is 1/255

	10 seconds input rate 0 bits/sec, 0 packets/sec 10 seconds output rate 67 bits/sec, 0 packets/sec 362 packets input, 87760 bytes, 0 no buffer, 0 dropped Received 0 broadcasts, 0 runts, 0 giants 0 input errors, 0 CRC, 0 frame, 0 overrun, 0 abort 363 packets output, 82260 bytes, 0 underruns, 0 dropped 0 output errors, 0 collisions, 0 interface resets
D	D# show interfaces gigabitEthernet 0/1 Index(dec):1 (hex):1 GigabitEthernet 0/1 is UP, line protocol is UP Hardware is GigabitEthernet, address is 08c6.b3.de93 (bia 08c6.b3.de93) **Interface address is: 192.168.2.1/24** MTU 1500 bytes, BW 100000 Kbit Encapsulation protocol is Ethernet-II, loopback not set Keepalive interval is 10 sec, set Carrier delay is 2 sec Ethernet attributes: Last link state change time: 2012-12-22 14:00:48 Time duration since last link state change: 3 days, 2 hours, 50 minutes, 50 seconds Priority is 0 Admin medium-type is Copper, oper medium-type is Copper Admin duplex mode is AUTO, oper duplex is Full Admin speed is AUTO, oper speed is 100M Flow control admin status is OFF, flow control oper status is OFF Admin negotiation mode is OFF, oper negotiation state is ON Storm Control: Broadcast is OFF, Multicast is OFF, Unicast is OFF Rxload is 1/255, Txload is 1/255 10 seconds input rate 0 bits/sec, 0 packets/sec 10 seconds output rate 67 bits/sec, 0 packets/sec 362 packets input, 87760 bytes, 0 no buffer, 0 dropped Received 0 broadcasts, 0 runts, 0 giants 0 input errors, 0 CRC, 0 frame, 0 overrun, 0 abort 363 packets output, 82260 bytes, 0 underruns, 0 dropped 0 output errors, 0 collisions, 0 interface resets

1.6 Monitoring

Clearing

Running the **clear** commands may lose vital information and thus interrupt services.

Description	Command
Clears the counters of a specified interface.	**clear counters** [*interface-type interface-number*]
Resets the interface hardware.	**clear interface** *interface-type interface-number*
Clears the statistics of link status change.	**clear link-state-change statistics** [*interface-type interface-number*]

Displaying

Displaying Interface Configurations and Status

Description	Command
Displays all the status and configuration information of a specified interface.	**show interfaces** [*interface-type interface-number*]
Displays the interface status.	**show interfaces** [*interface-type interface-number*] **status**
Displays the interface errdisable status.	**show interfaces** [*interface-type interface-number*] **status err-disable**
Displays the link status change time and count of a specified port.	**show interfaces** [*interface-type interface-number*] **link-state-change statistics**
Displays the administrative and operational states of switch ports (non-routed ports).	**show interfaces** [*interface-type interface-number*] **switchport**
Displays the description and status of a specified interface.	**show interfaces** [*interface-type interface-number*] **description**

Displays the counters of a specified port, among which the displayed speed may have an error of ±0.5%.	**show interfaces** [*interface-type interface-number*] **counters**
Displays the number of packets increased in a load interval.	**show interfaces** [*interface-type interface-number*] **counters increment**
Displays statistics about error packets.	**show interfaces** [*interface-type interface-number*] **counters error**
Displays the packet sending/receiving rate of an interface.	**show interfaces** [*interface-type interface-number*] **counters rate**
Displays the packet sending/receiving rate of an interface at the physical layer. The packet sending/receiving rate at the physical layer refers to the sending/receiving rate of packets that contain interframe spacing.	**show interfaces** [*interface-type interface-number*] **counters rate physical-layer**
Displays a summary of interface information.	**show interfaces** [*interface-type interface-number*] **counters summary**
Displays the bandwidth usage of an interface.	**show interfaces** [*interface-type interface-number*] **usage**
Displays the global MTU information.	**show interface** [*interface-type interface-number*] **mtu forwarding**
Displays the sub VLAN interface information.	**show vlans**

Displaying Optical Module Information

Description	Command
Displays basic information about the optical module of a specified interface.	**show interfaces** [*interface-type interface-number*] **transceiver**

Displays the fault alarms of the optical module on a specified interface. If no fault occurs, "None" is displayed.	**show interfaces** [*interface-type interface-number*] **transceiver alarm**
Displays the optical module diagnosis values of a specified interface.	**show interfaces** [*interface-type interface-number*] **transceiver diagnosis**

2 CONFIGURING SINGLE FIBER

2.1 Overview

Single Fiber (SF) is a function developed to meet the special requirement for only receiving packets but not sending packets. In normal cases, when Ethernet standard devices interwork with each other by using optical transceivers, dual-fiber optical transceivers must be used so that the link becomes up and packets are forwarded normally. The disadvantage, however, is that physical isolation cannot be smoothly achieved in the transmission direction when Ethernet standard devices send data through dual fibers. As a result, the peer switch may receive unpredictable packets, affecting the switch security. For this, the SF mode can be configured to physically isolate data in the transmission direction to ensure data security. The application of SF-mode ports does not conform to the link specifications of Ethernet device ports. Therefore, for the implementation of SF receiving, a single-core fiber needs to be connected to the Rx end of a switch port so that data from the Tx end of the peer optical transceiver can be received normally.

2.2 Applications

Application	Description
SF Receiving	The Rx end of a switch port is connected to the Tx end of an optical splitter through a single-core fiber.

2.2.1 SF Receiving

Scenario

The Rx end of a switch port is connected to the Tx end of an optical splitter through a single-core fiber, and the Rx end of the optical splitter is not connected to the Tx end of the connected switch, to ensure physical isolation.

Figure 14-1

Deployment

- The switch can only receive packets from the optical splitter but cannot send packets to the optical splitter.

2.3 Configuration

Configuration	Description and Command	
Configuring the SF Mode	(Mandatory) It is used to configure the SF mode.	
	transport mode { rx }	Configures the SF Rx mode.
	no transport mode	Restores the default mode, that is, dual-fiber bidirectional Rx/Tx mode.

2.3.1 Configuring the SF Mode

Configuration Effect

Configure a port of the switch to support the SF mode and the Rx direction only.

Notes

Configuration Steps

Configuring the SF Mode

- Mandatory.
- The SF mode should be configured on the port that requires the SF Rx function unless otherwise stated.

Command	transport mode {rx}
Parameter Description	**rx**: Indicates the mode in which only packets are received.
Defaults	The SF mode is disabled by default.

Command Mode	Interface configuration mode
Usage Guide	N/A

Verification

Verify the SF configuration:

- Check whether the port on which the SF Rx function is configured can be up normally.
- Check whether the light emission function is disabled for the port on which the SF Rx function is configured.
- Verify that the port on which the SF Rx function is configured can only receive packets but cannot send packets.

2.4 Monitoring

Displaying

Description	Command
Displays information about the port on which the SF Rx function is configured.	**show transport mode** {rx}

3 CONFIGURING MAC ADDRESS

3.1. Overview

A MAC address table contains the MAC addresses, interface numbers and VLAN IDs of the devices connected to the local device.

When a device forwards a packet, it finds an output port from its MAC address table according to the destination MAC address and the VLAN ID of the packet.

After that, the packet is unicast, multicast or broadcast.

This document covers dynamic MAC addresses, static MAC addresses and filtered MAC addresses. For the management of multicast MAC addresses, please see *Configuring IGMP Snooping Configuration*.

Protocols and Standards

- IEEE 802.3: Carrier sense multiple access with collision detection (CSMA/CD) access method and physical layer specifications
- IEEE 802.1Q: Virtual Bridged Local Area Networks

2.5 Applications

Application	Description
MA.C Address Learning	Forward unicast packets through MAC addresses learning.
MAC Address Change Notification	Monitor change of the devices connected to a network device through MAC address change notification.

2.5.1 MAC Address Learning

Scenario

Usually a device maintains a MAC address table by learning MAC addresses dynamically. The operating principle is described as follows:

As shown in the following figure, the MAC address table of the switch is empty. When User A communicates with User B, it sends a packet to the port GigabitEthernet 0/2 of the switch, and the switch learns the MAC address of User A and stores it in the table.

As the table does not contain the MAC address of User B, the switch broadcasts the packet to the ports of all connected devices except User A, including User B and User C.

Figure 2-1 Step 1 of MAC Address Learning

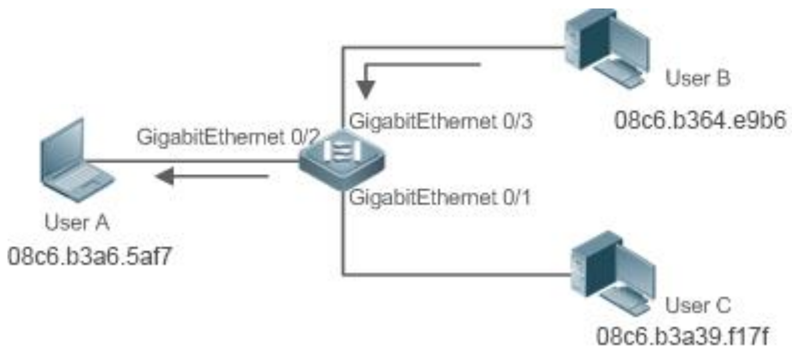


Figure 2-2 MAC Address Table 1

Status	VLAN	MAC address	Interface
Dynamic	1	08c6.b3.5af7	GigabitEthernet 0/2

When User B receives the packet, it sends a reply packet to User A through port GigabitEthernet 0/3 on the switch. As the MAC address of User A is already in the MAC address table, the switch send the reply unicast packet to port GigabitEthernet 0/2 port and learns the MAC address of User B. User C does not receive the reply packet from User B to User A.

Figure 2-3 Step 2 of MAC Address Learning

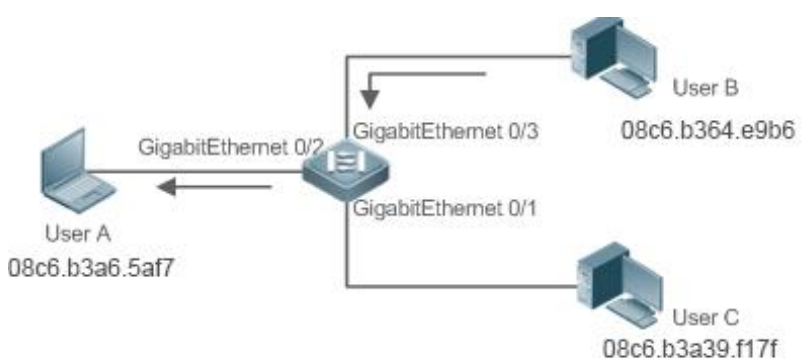


Figure 2-4 MAC Address Table 2

Status	VLAN	MAC address	Interface

Dynamic	1	08c6.b3.5af7	GigabitEthernet 0/2
Dynamic	1	08c6.b3.e9b6	GigabitEthernet 0/3

Through the interaction between User A and User B, the switch learns the MAC addresses of User A and User B. After that, packets between User A and User B will be exchanged via unicast without being received by User C.

Deployment

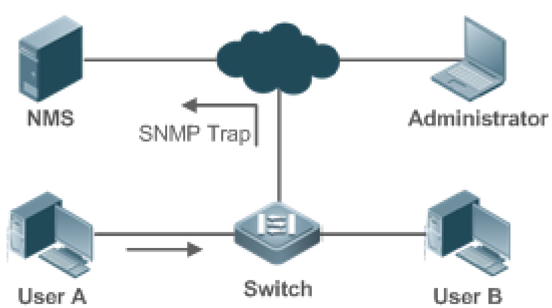
- With MAC address learning, a layer-2 switch forwards packets through unicast, reducing broadcast packets and network load.

2.5.2 MAC Address Change Notification

MAC address change notification provides a mechanism for the network management system (NMS) to monitor the change of devices connected to a network device.

Scenario

Figure 2-5 MAC Address Change Notification



After MAC address change notification is enabled on a device, the device generates a notification message when the device learns a new MAC address or finishes aging a learned MAC address, and sends the message in an SNMP Trap message to a specified NMS.

A notification of adding a MAC address indicates that a new user accesses the network, and that of deleting a MAC address indicates that a user sends no packets within an aging time and usually the user exits the network.

When a network device is connected to a number of devices, a lot of MAC address changes may occur in a short time, resulting in an increase in traffic. To reduce traffic, you may configure an interval for sending MAC address change notifications. When the interval expires, all notifications generated during the interval are encapsulated into a message.

When a notification is generated, it is stored in the table of historical MAC address change notifications. The administrator may know recent MAC address changes by checking the table of notification history even without NMS.

A MAC address change notification is generated only for a dynamic MAC address.

Deployment

- Enable MAC address change notification on a layer-2 switch to monitor the change of devices connected to a network device.

2.6 Features

Basic Concepts

Dynamic MAC Address

A dynamic MAC address is a MAC address entry generated through the process of MAC address learning by a device.

Address Aging

A device only learns a limited number of MAC addresses, and inactive entries are deleted through address aging.

A device starts aging a MAC address when it learns it. If the device receives no packet containing the source MAC address, it will delete the MAC address from the MAC address table when the time expires.

Forwarding via Unicast

If a device finds in its MAC address table an entry containing the MAC address and the VLAN ID of a packet and the output port is unique, it will send the packet through the port directly.

Forwarding via Broadcast

If a device receives a packet containing the destination address ffff.ffff.ffff or an unidentified destination address, it will send the packet through all the ports in the VLAN where the packet is from, except the input port.

Overview

Feature	Description
Dynamic Address Limit for VLAN	Limit the number of dynamic MAC addresses in a VLAN.

Dynamic Address Limit for Interface	Limit the number of dynamic MAC addresses on an interface.

2.6.1 Dynamic Address Limit for VLAN

Working Principle

The MAC address table with a limited capacity is shared by all VLANs. Configure the maximum number of dynamic MAC addresses for each VLAN to prevent one single VLAN from exhausting the MAC address table space.

A VLAN can only learn a limited number of dynamic MAC addresses after the limit is configured. The packets exceeding the limit are broadcast.

- If the number of learned MAC addresses is greater than the limit, a device will stop learning the MAC addresses from the VLAN and will not start learning again until the number drops below the limit after address aging.
- The MAC addresses copied to a specific VLAN are not subject to the limit.

2.6.2 Dynamic Address Limit for Interface

Working Principle

An interface can only learn a limited number of dynamic MAC addresses after the limit is configured. The packets exceeding the limit are broadcast

- If the number of learned MAC addresses is greater than the limit, a device will stop learning the MAC addresses from the interface and will not start learning again until the number drops below the limit after address aging.

2.7 Limitations

QSW-6900 series products do not learn or forward packets whose source MAC address and destination MAC address is all 0.

2.8 Configuration

Configuration	Description and Command

Configuring Dynamic MAC Address	(Optional) It is used to enable MAC address learning.	
	mac-address-learning	Configures MAC address learning globally or on an interface.
	mac-address-table aging-time	Configures an aging time for a dynamic MAC address.
Configuring a Static MAC Address	(Optional) It is used to bind the MAC address of a device with a port of a switch.	
	mac-address-table static	Configures a static MAC address.
Configuring a MAC Address for Packet Filtering	(Optional) It is used to filter packets.	
	mac-address-table filtering	Configures a MAC address for packet filtering.
Configuring MAC Address Change Notification	(Optional) It is used to monitor change of devices connected to a network device.	
	mac-address-table notification	Configures MAC address change notification globally.
	snmp trap mac-notification	Configures MAC address change notification on an interface.
Configuring a Management VLAN for an AP Port	(Optional) It is used to configure a management VLAN for an AP port.	
	aggregateport-admin vlan	Configures a management VLAN for an AP port.
Configuring the Alarm Logging Function for MAC Address Drift	(Optional) It is used to configure the alarm logging function for detected MAC address drift.	
	mac-address-table flapping-logging	
Configuring the Maximum Number of Learned MAC Addresses	(Optional) It is used to configure the maximum number of learned MAC addresses.	

	max-dynamic-mac-count *count*	
Configuring Packet Discarding When the Number of Learned MAC Addresses Exceeds the Address Limit	(Optional) It is used to configure the packet processing method when the number of learned MAC addresses exceeds the address limit.	
	max-dynamic-mac-count exceed-action *forward | discard*	

2.8.1 Configuring Dynamic MAC Address

Configuration Effect

Learn MAC addresses dynamically and forward packets via unicast.

Configuration Steps

Configuring Global MAC Address Learning

- Optional.
- You can perform this configuration to disable global MAC address learning.
- Configuration:

Command	**mac-address-learning { enable | disable }**
Parameter Description	**enable**: Enables global MAC address learning. **disable**: Disable global MAC address learning.
Defaults	Global MAC address learning is enabled by default.
Command Mode	Global configuration mode
Usage Guide	N/A

By default, global MAC address learning is enabled. When global MAC address learning is enabled, the MAC address learning configuration on an interface takes effect; when the function is disabled, MAC addresses cannot be learned globally.

Configuring MAC Address Learning on Interface

- Optional.

- You can perform this configuration to disable MAC address learning on an interface.
- Configuration:

Command	**mac-address-learning**
Parameter Description	N/A
Defaults	MAC address learning is enabled by default.
Command Mode	Interface configuration mode
Usage Guide	Perform this configuration on a layer-2 interface, for example, a switch port or an AP port.

By default, MAC address learning is enabled. If DOT1X, IP SOURCE GUARD, or a port security function is configured on a port, MAC address learning cannot be enabled. Access control cannot be enabled on a port with MAC address learning disabled.

Configuring an Aging Time for a Dynamic MAC Address

- Optional.
- Configure an aging time for dynamic MAC addresses.
- Configuration:

Command	**mac-address-table aging-time *value***
Parameter Description	*value*: Indicates the aging time. The value is either 0 or in the range from 10 to 1000,000.
Defaults	The default is 300s.
Command Mode	Global configuration mode
Usage Guide	If the value is set to 0, MAC address aging is disabled and learned MAC addresses will not be aged.

The actual aging time may be different from the configured value, but it is not more than two times of the configured value.

Verification

- Check whether a device learns dynamic MAC addresses.
- Run the **show mac-address-table dynamic** command to display dynamic MAC addresses.
- Run the **show mac-address-table aging-time** command to display the aging time for dynamic MAC addresses.

Command	**show mac-address-table dynamic [address *mac-address*] [interface *interface-id*] [vlan *vlan-id*]**
Parameter Description	**address** *mac-address*: Displays the information of a specific dynamic MAC address. **interface** *interface-id*: Specifies a physical interface or an AP port. **vlan** *vlan-id*: Displays the dynamic MAC addresses in a specific VLAN.
Command Mode	Privileged EXEC mode/Global configuration mode/Interface configuration mode
Usage Guide	N/A
	QTECH# show mac-address-table dynamic Vlan MAC Address Type Interface ---- ------------ ------ ------------------ **1 0000.0000.0001 DYNAMIC GigabitEthernet 1/1** **1 0001.960c.a740 DYNAMIC GigabitEthernet 1/1** **1 0007.95c7.dff9 DYNAMIC GigabitEthernet 1/1** **1 0007.95cf.eee0 DYNAMIC GigabitEthernet 1/1** **1 0007.95cf.f41f DYNAMIC GigabitEthernet 1/1** **1 0009.b715.d400 DYNAMIC GigabitEthernet 1/1** **1 0050.bade.63c4 DYNAMIC GigabitEthernet 1/1**

Field	**Description**
Vlan	Indicates the VLAN where the MAC address resides.
MAC Address	Indicates a MAC Address.
Type	Indicates a MAC address type.

	Interface	Indicates the interface where the MAC address resides.

Command	show mac-address-table aging-time
Parameter Description	N/A
Command Mode	Privileged EXEC mode/Global configuration mode/Interface configuration mode
Usage Guide	N/A
	QTECH# show mac-address-table aging-time **Aging time : 300**

Configuration Example

Configuring Dynamic MAC Address

Scenario **Figure 2-6**	
Configuration Steps	▪ Enable MAC address learning on an interface. ▪ Configure the aging time for dynamic MAC addresses to 180s. ▪ Delete all dynamic MAC addresses in VLAN 1 on port GigabitEthernet 0/1.
	QTECH# configure terminal QTECH(config-if-GigabitEthernet 0/1)# mac-address-learning QTECH(config-if-GigabitEthernet 0/1)# exit QTECH(config)# mac aging-time 180 QTECH# clear mac-address-table dynamic interface GigabitEthernet 0/1 vlan 1

Verification	▪ Check MAC address learning on an interface. ▪ Display the aging time for dynamic MAC addresses. ▪ Display all dynamic MAC addresses in VLAN 1 on port GigabitEthernet 0/1.
	QTECH# show mac-address-learning **GigabitEthernet 0/1 learning ability: enable** QTECH# show mac aging-time Aging time : **180 seconds** QTECH# show mac-address-table dynamic interface GigabitEthernet 0/1 vlan 1 Vlan MAC Address Type Interface ---------- -------------------- -------- ------------------- **1 08c6.b3.1001 STATIC GigabitEthernet 1/1**

Common Errors

Configure MAC address learning on an interface before configuring the interface as a layer-2 interface, for example, a switch port or an AP port.

2.8.2 Configuring a Static MAC Address

Configuration Effect

Bind the MAC address of a network device with a port of a switch.

Configuration Steps

Configuring a Static MAC address

- Optional.
- Bind the MAC address of a network device with a port of a switch.
- Configuration:

Command	mac-address-table static *mac-address* vlan *vlan-id* interface *interface-id*
Parameter Description	**address** *mac-address*: Specifies a MAC address. **vlan** *vlan-id*: Specifies a VLAN where the MAC address resides. **interface** *interface-id*: Specifies a physical interface or an AP port.
Defaults	By default, no static MAC address is configured.

Command Mode	Global configuration mode
Usage Guide	When the switch receives a packet containing the specified MAC address on the specified VLAN, the packet is forwarded to the bound interface.

Verification

- Run the **show mac-address-table static** command to check whether the configuration takes effect.

Command	**show mac-address-table static [address** ***mac-address*** **] [interface** ***interface-id*** **] [vlan** ***vlan-id*** **]**
Parameter Description	**address** *mac-address*: Specifies a MAC address. **interface** *interface-id*: Specifies a physical interface or an AP port. **vlan** *vlan-id*: Specifies a VLAN where the MAC address resides.
Command Mode	Privileged EXEC mode/Global configuration mode /Interface configuration mode
Usage Guide	N/A
	QTECH# show mac-address-table static Vlan MAC Address Type Interface ----- ----------- -------- ------------------ **1 08c6.b3.1001 STATIC GigabitEthernet 1/1** **1 08c6.b3.1002 STATIC GigabitEthernet 1/1** **1 08c6.b3.1003 STATIC GigabitEthernet 1/1**

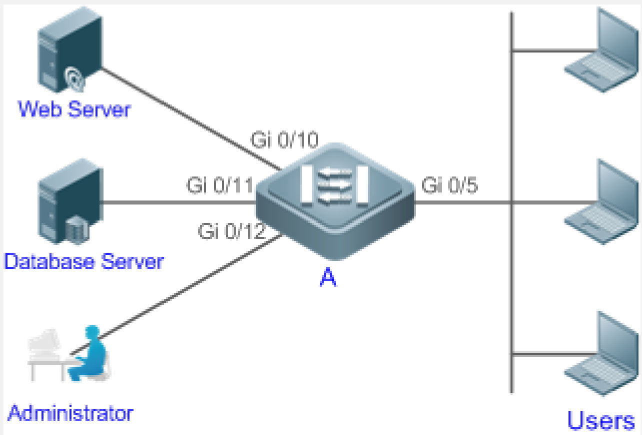
Configuration Example

Configuring a Static MAC address

In the above example, the relationship of MAC addresses, VLAN and interfaces is shown in the following table.

Role	MAC Address	VLAN ID	Interface ID

Web Server	08c6.b332.0001	VLAN2	Gi0/10
Database Server	08c6.b332.0002	VLAN2	Gi0/11
Administrator	08c6.b332.1000	VLAN2	Gi0/12

Scenario Figure 2-7	
Configuration Steps	▪ Specify destination MAC addresses (*mac-address*). ▪ Specify the VLAN (*vlan-id*) where the MAC addresses reside. ▪ Specify interface IDs (*interface-id*).
A	A# configure terminal A(config)# mac-address-table static 08c6.b3.3232.0001 vlan 2 interface gigabitEthernet 0/10 A(config)# mac-address-table static 08c6.b3.3232.0002 vlan 2 interface gigabitEthernet 0/11 A(config)# mac-address-table static 08c6.b3.3232.1000 vlan 2 interface gigabitEthernet 0/12
Verification	Display the static MAC address configuration on a switch.
A	A# show mac-address-table static Vlan MAC Address Type Interface ---------- -------------------- -------- ------------------- **2 08c6.b3.3232.0001 STATIC GigabitEthernet 0/10** **2 08c6.b3.3232.0002 STATIC GigabitEthernet 0/11** **2 08c6.b3.3232.1000 STATIC GigabitEthernet 0/12**

Common Errors

- Configure a static MAC address before configuring the specific port as a layer-2 interface, for example, a switch port or an AP port.

2.8.3 Configuring a MAC Address for Packet Filtering

Configuration Effect

- If a device receives packets containing a source MAC address or destination MAC address specified as the filtered MAC address, the packets are discarded.

Configuration Steps

Configuring a MAC Address for Packet Filtering

- Optional.
- Perform this configuration to filter packets.
- Configuration:

Command	**mac-address-table filtering *mac-address* vlan *vlan-id***
Parameter Description	**address** *mac-address*: Specifies a MAC address. **vlan** *vlan-id*: Specifies a VLAN where the MAC address resides.
Defaults	By default, no filtered MAC address is configured.
Command Mode	Global configuration mode
Usage Guide	If a device receives packets containing a source MAC address or destination MAC address specified as the filtered MAC address, the packets are discarded.

Verification

- Run the **show mac-address-table filter** command to display the filtered MAC address.

Command	**show mac-address-table filter [address *mac-address*] [vlan *vlan-id*]**
Parameter Description	**address** *mac-address*: Specifies a MAC address. **vlan** *vlan-id*: Specifies a VLAN where the MAC address resides.

Command Mode	Privileged EXEC mode/Global configuration mode /Interface configuration mode
Usage Guide	N/A
	QTECH# show mac-address-table filtering Vlan MAC Address Type Interface ------ -------------------- -------- ----------- **1 0000.2222.2222 FILTER**

Configuration Example

- Configuring a MAC Address for Packet Filtering

Configuration Steps	- **Specify a destination MAC address (*mac-address*) for filtering.** - **Specify a VLAN where the MAC addresses resides.**
	QTECH# configure terminal QTECH(config)# mac-address-table static 08c6.b3.3232.0001 vlan 1
Verification	Display the filtered MAC address configuration.
	QTECH# show mac-address-table filter Vlan MAC Address Type Interface ---------- -------------------- -------- ------------------- **1 08c6.b3.3232.0001 FILTER**

2.8.4 Configuring MAC Address Change Notification

Configuration Effect

- Monitor change of devices connected to a network device.

Configuration Steps

Configuring NMS

- Optional.
- Perform this configuration to enable an NMS to receive MAC address change notifications.
- Configuration:

Command	**snmp-server host** ***host-addr*** **traps [version { 1 | 2c | 3 [auth | noauth | priv] }]** ***community-string***
Parameter Description	**host** *host-addr*: Specifies the IP address of a receiver. ▪ **version** { **1** | **2c** | **3** [**auth** | **noauth** | **priv**] }: Specifies the version of SNMP TRAP messages. You can also specify authentication and a security level for packets of Version 3. *community-string*: Indicates an authentication name.
Defaults	By default, the function is disabled.
Command Mode	Global configuration mode
Usage Guide	N/A

- Enabling SNMP Trap
- Optional.
- Perform this configuration to send SNMP Trap messages.
- Configuration:

Command	**snmp-server enable traps**
Parameter Description	N/A
Defaults	By default, the function is disabled.
Command Mode	Global configuration mode
Usage Guide	N/A

- Configuring Global MAC Address Change Notification
- Optional.
- If MAC address change notification is disabled globally, it is disabled on all interfaces.
- Configuration:

Command	mac-address-table notification
Parameter Description	N/A
Defaults	By default, MAC address change notification is disabled globally.
Command Mode	Global configuration mode
Usage Guide	N/A

Configuring MAC Address Change Notification On Interface

- Optional.
- Perform this configuration to enable MAC address change notification on an interface.
- Configuration:

Command	snmp trap mac-notification { added | removed }
Parameter Description	**added**: Generates a notification when an MAC address is added. **removed**: Generates a notification when an MAC address is deleted.
Defaults	By default, MAC address change notification is disabled on an interface.
Command Mode	Interface configuration mode
Usage Guide	N/A

Configuring Interval for Generating MAC Address Change Notifications and Volume of Notification History

- Optional.
- Perform this configuration to modify the interval for generating MAC address change notifications and the volume of notification history.
- Configuration:

Command	mac-address-table notification { interval *value* | history-size *value* }
Parameter Description	**interval** *value*: (Optional) Indicates the interval for generating MAC address change notifications. The value ranges from 1 to 3600 seconds,. **history-size** *value*: Indicates the maximum number of entries in the table of notification history. The value ranges from 1 to 200.
Defaults	The default interval is 1 second. The default maximum amount of notifications is 50.
Command Mode	Global configuration mode
Usage Guide	N/A

Verification

- Run the **show mac-address-table notification** command to check whether the NMS receives MAC address change notifications.

Command	▪ **show mac-address-table notification [interface [*interface-id*] | history]**
Parameter Description	**Interface**:Displays the configuration of MAC address change notification on all interfaces. ***interface-id***: Displays the configuration of MAC address change notification on a specified interface. **history**: Displays the history of MAC address change notifications.
Command Mode	Privileged EXEC mode/Global configuration mode /Interface configuration mode
Usage Guide	N/A

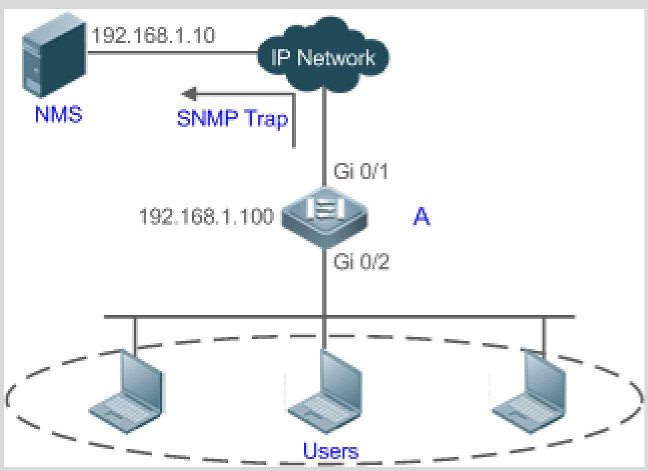
Usage Guide	Display the configuration of global MAC address change notification. QTECH#show mac-address-table notification MAC Notification Feature : **Enabled** Interval(Sec): **300** Maximum History Size : **50** Current History Size : **0**

Field	Description
Interval(Sec)	Indicates the interval for generating MAC address change notifications.
Maximum History Size	Indicates the maximum number of entries in the table of notification history.
Current History Size	Indicates the current notification entry number.

Configuration Example

Scenario

Figure 2-8



The figure shows an intranet of an enterprise. Users are connected to A via port Gi0/2.

The Perform the configuration to achieve the following effects:

When port Gi0/2 learns a new MAC address or finishes aging a learned MAC address, a MAC address change notification is generated.

Meanwhile, A sends the MAC address change notification in an SNMP Trap message to a specified NMS.

In a scenario where A is connected to a number of Users, the configuration can prevent MAC address change notification burst in a short time so as to reduce the network flow.

Configuration Steps	▪ Enable global MAC address change notification on A, and configure MAC address change notification on port Gi0/2. ▪ Configure the IP address of the NMS host, and enable A with SNMP Trap. A communicates with the NMS via routing. ▪ Configure the interval for sending MAC address change notifications to 300 seconds (1 second by default).
A	QTECH# configure terminal QTECH(config)# mac-address-table notification QTECH(config)# interface gigabitEthernet 0/2 QTECH(config-if-GigabitEthernet 0/2)# snmp trap mac-notification added QTECH(config-if-GigabitEthernet 0/2)# snmp trap mac-notification removed QTECH(config-if-GigabitEthernet 0/2)# exit QTECH(config)# snmp-server host 192.168.1.10 traps version 2c comefrom2 QTECH(config)# snmp-server enable traps QTECH(config)# mac-address-table notification interval 300
Verification	▪ **Check t whether MAC address change notification is enabled globally .** ▪ **Check whether MAC address change notification is enabled on the interface.** ▪ **Display the MAC addresses of interfaces, and run the clear mac-address-table dynamic command to simulate aging dynamic MAC addresses.** ▪ **Check whether global MAC address change notification is enabled globally.** ▪ **Display the history of MAC address change notifications.**
A	QTECH# show mac-address-table notification MAC Notification Feature : Enabled Interval(Sec): 300 Maximum History Size : 50 Current History Size : 0 QTECH# show mac-address-table notification interface GigabitEthernet 0/2 Interface MAC Added Trap MAC Removed Trap ----------- -------------- -------------- GigabitEthernet 0/2 Enabled Enabled QTECH# show mac-address-table interface GigabitEthernet 0/2 Vlan MAC Address Type Interface ---------- -------------------- -------- -------------------

	08c6.b332.0001 DYNAMIC GigabitEthernet 0/2 QTECH# show mac-address-table notification MAC Notification Feature : Enabled Interval(Sec): 300 Maximum History Size : 50 Current History Size : 1 QTECH# show mac-address-table notification history History Index : 0 Entry Timestamp: 221683 MAC Changed Message : Operation:DEL Vlan:1 MAC Addr: 08c6.b332.0003 GigabitEthernet 0/2

2.8.5 Configuring a Management VLAN for an AP Port

Configuration Effect

- Enable an AP port to process the packets from a management VLAN as management packets, and those from a non-management VLAN as data packets.

Configuration Steps

Configuring a Management VLAN for an AP Port

- Optional.
- Perform this configuration to enable an AP port to distinguish management packets from data packets.
- Configuration:

Command	**aggregateport-admin vlan *vlan-list***
Parameter Description	*vlan-list*: Indicates a VLAN or a range of VLANs separated by "-".
Defaults	By default, no management VLAN is configured for an AP port.
Command Mode	Global configuration mode

Usage Guide	An AP port processes the packets received on the management VLAN as management packets.

Verification

An AP port processes the packets from a management VLAN as management packets, and those from a non-management VLAN as data packets.

Configuration Example

Configuring a Management VLAN for an AP Port

Configuration Steps	▪ **Specify management VLANs for an AP port.**
	QTECH# configure terminal QTECH(config)# aggregateport-admin vlan 1-20
Verification	Run the **show running** command to display the configuration.

2.8.6 Configuring MAC Address Flapping Check

Configuration Effect

- Print a syslog alarm when MAC address flapping occurs, that is, a MAC address is leaned by more than one port in a short time in a VLAN.

Configuration Steps

Configuring MAC Address Flapping Check

- Optional.
- Configure this configuration to print a syslog alarm upon MAC address flapping.
- Configuration:

Command	**mac-address-table flapping-logging**
Parameter Description	N/A

Defaults	By default, the function is disabled.
Command Mode	Global configuration mode
Usage Guide	N/A

Verification

- Run the **show run** command to display the configuration.
- Print syslog to check the MAC address flapping.

Configuration Example

- Configuring Syslog Printing upon MAC Address Flapping

Configuration Steps	▪ **Enable syslog printing upon MAC address flapping.**
	QTECH# configure terminal QTECH(config)# mac-address-table flapping-logging
Verification	Run the show running command to display the configuration.

2.8.7 Configuring the MAC Address Flapping Protection Policy

Configuration Effect

- When MAC address flapping is detected on a port with the MAC address flapping protection policy configured, the port will be shut down.

Notes

- The MAC address flapping detection function must be enabled.

Configuration Steps

Configuring the MAC Address Flapping Protection Policy

- Optional
- Perform this operation to prevent MAC address flapping between different ports.
- Perform this operation on the switch.

Command	**mac-address-table flapping action [error-down | priority *priotiry-num*]**
Parameter Description	**error-down**: Specifies the policy that a port is shut down if MAC address flapping is detected on the port. **priority** *priotiry-num*: Indicates the priority of the port shutdown policy. The default value is **0** (the lowest priority). The value ranges from 0 to 5. A larger value indicates a higher priority.
Defaults	By default, the MAC address flapping protection function is disabled.
Command Mode	Interface configuration mode
Usage Guide	The MAC address flapping check function must be enabled first. Otherwise, the configuration does not take effect.

Verification

- Run **show run** to query the configuration result.

Configuration Example

- Configuring the MAC Address Flapping Protection Policy

Configuration Steps	▪ **Enable the MAC address flapping detection function.**
	QTECH# configure terminal QTECH(config)# mac-address-table flapping-logging
	▪ Configure the MAC address flapping protection policy. QTECH(config)# interface GigabitEthernet 1/1 QTECH(config-if-GigabitEthernet 1/1)# mac-address-table flapping action error-down QTECH(config-if-GigabitEthernet 1/1)# mac-address-table flapping action priority 2
Verification	Run **show running** on the switch to query the configuration.

Common Errors

None

2.8.8 Configuring the Maximum Number of MAC Addresses Learned by a Port

Configuration Effect

- Only a limited number of dynamic MAC addresses can be learned by a port.

Notes

None

Configuration Steps

Configuring the Maximum Number of MAC Addresses Learned by a Port

- Optional
- Perform this operation on the switch.

Command	**max-dynamic-mac-count** ***count***
Parameter Description	count: Indicates the maximum number of MAC addresses learned by a port.
Defaults	By default, the number of MAC addresses learned by a port is not limited. After the number of MAC addresses learned by a port is limited and after the maximum number of MAC addresses exceeds the limit, packets from source MAC addresses are forwarded by default.
Command Mode	Interface configuration mode
Usage Guide	

Verification

- Run **show run** to query the configuration result.

Configuration Example

- Configuring the Maximum Number of MAC Addresses Learned by a Port

Configuration Steps	▪ **Configure the maximum number of MAC addresses learned by a port.**
	▪ Configure the maximum number of MAC addresses learned by a port and the countermeasure for the case that the number of MAC addresses exceeds the limit. QTECH(config)# interface GigabitEthernet 1/1 QTECH(config-if-GigabitEthernet 1/1)# max-dynamic-mac-count 100 QTECH(config-if-GigabitEthernet 1/1)# max-dynamic-mac-count exceed-action discard
Verification	Run **show running** on the switch to query the configuration.

Common Errors

None

2.8.9 Configuring the Maximum Number of MAC Addresses Learned by a VLAN

Configuration Effect

- Only a limited number of dynamic MAC addresses can be learned by a VLAN.

Notes

None

Configuration Steps

Configuring the Maximum Number of MAC Addresses Learned by a VLAN

- Optional
- Perform this operation on the switch.

Command	**max-dynamic-mac-count exceed-action *forward | discard***
Parameter Description	**Forward/dis**card: Indicates that packets are forwarded or discarded when the number of MAC addresses learned by a VLAN exceeds the limit.
Defaults	By default, the number of MAC addresses learned by a VLAN is not limited. After the number of MAC addresses learned by a VLAN is limited and after the maximum number

	of MAC addresses exceeds the limit, packets from source MAC addresses are forwarded by default.
Command Mode	VLAN configuration mode
Usage Guide	N/A

Verification

- Run **show run** to query the configuration result.

Configuration Example

- Configuring the Maximum Number of MAC Addresses Learned by a VLAN

Configuration Steps	▪ Configure the maximum number of MAC addresses learned by a VLAN.
	▪ Configure the maximum number of MAC addresses learned by a VLAN and the countermeasure for the case that the number of MAC addresses exceeds the limit. QTECH(config)# vlan 2 QTECH(config-vlan)#max-dynamic-mac-count 100 QTECH(config-vlan)# max-dynamic-mac-count exceed-action discard
Verification	Run **show running** on the switch to query the configuration.

Common Errors

None

2.9 Monitoring

Clearing

⚠ Running the clear commands may lose vital information and interrupt services.

Description	Command

Clears dynamic MAC addresses.	**clear mac-address-table dynamic** [**address** *mac-address*] [**interface** *interface-id*] [**vlan** *vlan-id*]

Displaying

Description	Command
Displays the MAC address table.	**show mac-address-table** { **dynamic** | **static** | **filter** } [**address** *mac-address* **]** [**interface** *interface-id*] [**vlan** *vlan-id*]
Displays the aging time for dynamic MAC addresses.	**show mac-address-table aging-time**
Displays the maximum number of dynamic MAC addresses.	**show mac-address-table max-dynamic-mac-count**
Displays the configuration and history of MAC address change notifications.	**show mac-address-table notification** [**interface** [*interface-id*] **|** **history**]

Debugging

System resources are occupied when debugging information is output. Therefore, disable debugging immediately after use.

Description	**Command**
Debugs MAC address operation.	**debug bridge mac**

3 CONFIGURING AGGREGATE PORT

3.1 Overview

An aggregate port (AP) is used to bundle multiple physical links into one logical link to increase the link bandwidth and improve connection reliability.

An AP port supports load balancing, namely, distributes load evenly among member links. Besides, an AP port realizes link backup. When a member link of the AP port is disconnected, the load carried by the link is automatically allocated to other functional member links. A member link does not forward broadcast or multicast packets to other member links.

For example, the link between two devices supports a maximum bandwidth of 1,000 Mbps. When the service traffic carried by the link exceeds 1,000 Mbps, the traffic in excess will be discarded. Port aggregation can be used to solve the problem. For example, you can connect the two devices with network cables and combine multiple links to form a logical link capable of multiples of 1,000 Mbps.

For example, there are two devices connected by a network cable. When the link between the two ports of the devices is disconnected, the services carried by the link will be interrupted. After the connected ports are aggregated, the services will not be affected as long as one link remains connected.

Protocols and Standards

IEEE 802.3ad

3.2 Applications

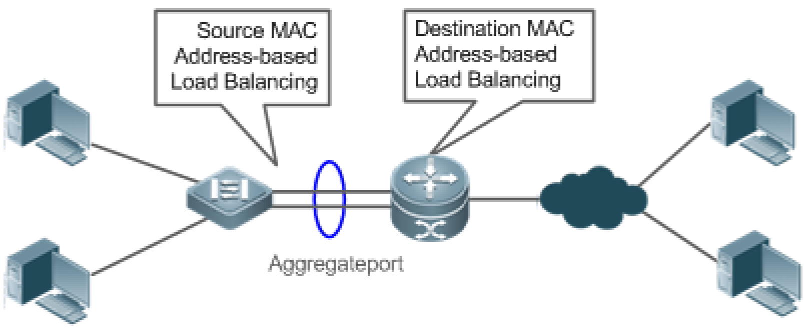
Applications	Description
AP Link Aggregation and Load Balancing	A large number of packets are transmitted between an aggregation device and a core device, which requires a greater bandwidth. To meet this requirement, you can bundle the physical links between the devices into one logical link to increase the link bandwidth, and configure a proper load balancing algorithm to distribute the work load evenly to each physical link, thus improving bandwidth utilization.

3.2.1 AP Link Aggregation and Load Balancing

Scenario

In Figure 31, the switch communicates with the router through an AP port. All the devices on the intranet (such as the two PCs on the left) use the router as a gateway. All the devices on the extranet (such as the two PCs on the right) send packets to the internet devices through the router, with the gateway's MAC address as its source MAC address. To distribute the load between the router and other hosts to other links, configure destination MAC address-based load balancing. On the switch, configure source MAC address-based load balancing.

Figure 3-1 AP Link Aggregation and Load Balancing



Deployment

- Configure the directly connected ports between the switch and router as a static AP port or a Link Aggregation Control Protocol (LACP) AP port.
- On the switch, configure a source MAC address-based load balancing algorithm.
- On the router, configure a destination MAC address-based load balancing algorithm.
- Features

3.3 Features

Basic Concepts

Static AP

The static AP mode is an aggregation mode in which physical ports are directly added to an AP aggregation group through manual configuration to allow the physical ports to forward packets when the ports are proper in link state and protocol state.

An AP port in static AP mode is called a static AP, and its member ports are called static AP member ports.

LACP

LACP is a protocol about dynamic link aggregation. It exchanges information with the connected device through LACP data units (LACPDUs).

An AP port in LACP mode is called an LACP AP port, and its member ports are called LACP AP member ports.

AP Member Port Mode

There are three aggregation modes available, namely, active, passive, and static.

AP member ports in active mode initiate LACP negotiation. AP member ports in passive mode only respond to received LACPDUs. AP member ports in static mode do not send LACPDUs for negotiation. The following table lists the requirements for peer port mode.

Port Mode	Peer Port Mode
Active mode	Active or passive mode
Passive mode	Active mode
Static Mode	Static Mode

AP Member Port State

There are two kinds of AP member port state available:

- When a member port is Down, the port cannot forward packets. The Down state is displayed.
- When a member port is Up and the link protocol is ready, the port can forward packets. The Up state is displayed.

There are three kinds of LACP member port state:

- When the link of a port is Down, the port cannot forward packets. The Down state is displayed.
- When the link of a port is Up and the port is added to an aggregation group, the bndl state is displayed.
- When the link of a port is Up but the port is suspended because the peer end is not enabled with LACP or the attributes of the ports are inconsistent with those of the master port, the susp state is displayed. (The port in susp state does not forward packets.)

Only full-duplex ports are capable of LACP aggregation.

LACP aggregation can be implemented only when the rates, flow control approaches, medium types, and Layer-2/3 attributes of member ports are consistent.

If you modify the preceding attributes of a member port in the aggregation group, LACP aggregation will fail.

The ports which are prohibited from joining or exiting an AP port cannot be added to or removed from a static AP port or an LACP AP port.

AP Capacity Mode

The maximum number of member ports is fixed, which is equal to the maximum number of AP ports multiplied by the maximum number of member ports supported by a single AP port. If you want to increase the maximum number of AP ports, the maximum number of member ports supported by a single AP port must be reduced, and vice versa. This concerns the AP capacity mode concept. Some devices support the configuration of the AP capacity mode. For example, if the system supports 16,384 member ports, you can select the 1024 x 16, 512 x 32, and other AP capacity modes (Maximum number of AP ports multiplied by the maximum number of member ports supported by a single AP port).

LACP System ID

By default, all the LACP ports on a device belong to the same LACP aggregation system.

One device can be configured with only one LACP aggregation system. The system is identified by a system ID and each system has a priority, which is a configurable value. The system ID consists of the LACP system priority and MAC address of the device. A lower system priority indicates a higher priority of the system ID. If the system priorities are the same, a smaller MAC address of the device indicates a higher priority of the system ID. The system with an ID of a higher priority determines the port state. The port state of a system with an ID of a lower priority keeps consistent with that of a higher priority.

The LACP system ID can be configured when LACP ports of multiple (a maximum of four) independent devices need to negotiate with the LACP port of a specific device (for example, LACP ports of two independent ASWs need to negotiate with the LACP port of the NC). You can set the system IDs of the LACP ports of independent devices to the same MAC address and configure different device IDs to implement normal negotiation.

LACP Device ID

The LACP device ID can be configured when LACP ports of multiple independent devices need to negotiate with the LACP port of a specific device. It must be configured together with the system ID.

LACP Port ID

Each port has an independent LACP port priority, which is a configurable value. The port ID consists of the LACP port priority and port number. A smaller port priority indicates a higher priority of the port ID. If the port priorities are the same, a smaller port number indicates a higher priority of the port ID.

LACP Master Port

When dynamic member ports are Up, LACP selects one of those ports to be the master port based on the rates and duplex modes, ID priorities of the ports in the aggregation group, and the bundling state of the member ports in the Up state. Only the ports that have the same attributes as the master port are in Bundle state and participate in data forwarding. When the attributes of ports are changed, LACP reselects a master port. When the new master port is not in Bundle state, LACP disaggregates the member ports and performs aggregation again.

Minimum Number of AP Member Ports

An AP can be configured with a minimum number of AP member ports. When a member port exits the AP aggregation group, causing the number of member ports to be smaller than the minimum number, the other member ports in the group are unbundled (Down Status). When the member port rejoins the group, causing the number of member ports to be greater than the minimum number, the member ports in the group are automatically bundled (Up Status).

LACP Independent Ports

In normal cases, LACP independent ports are used for interworking between access switches and servers with two NICs. If the OS is not pre-installed when a server with two NICs starts, the OS needs to be installed via the remote PXE OS installation device. Before the OS is installed, the server with two NICs cannot perform LACP negotiation with the access device, and only one NIC can work. In this case, the port on the access device must be able to change to a common Ethernet physical port automatically to ensure normal communication between the server and the remote PXE OS installation device. After the OS is installed and both NICs can run the LACP, the port on the access device must be able to enable the LACP again for negotiation.

⚠ LACP independent ports can work only at layer 2. After an LACP independent port is enabled, if the LACP independent port does not receive LACP packets, it automatically changes to a common Ethernet port, which automatically copies the rate, duplex mode, flow control, and VLAN configuration from the AP port to ensure port forwarding capabilities.

⚠ An LACP independent port automatically changes to a common Ethernet port only if it does not receive LACP packets within the set time-out period. After the port receives LACP packets, it changes to an LACP member port again.

Overview

Overview	Description
Link Aggregation	Aggregates physical links statically or dynamically to realize bandwidth extension and link backup.
Load Balancing	Balances the load within an aggregation group flexibly by using different load balancing methods.

3.3.1 Link Aggregation

Working Principle

There are two kinds of AP link aggregation. One is static AP, and the other is dynamic aggregation through LACP.

Static AP

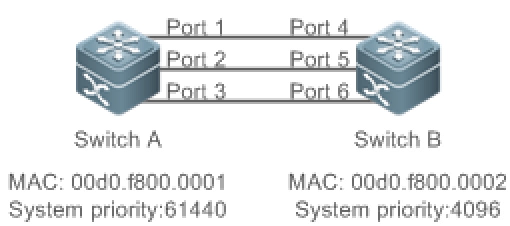
The static AP configuration is simple. Run a command to add the specified physical port to the AP port. After joining the aggregation group, a member port can receive and transmit data and participate in load balancing within the group.

Dynamic AP (LACP)

An LACP-enabled port sends LACPDUs to advertise its system priority, system MAC address, port priority, port number, and operation key. When receiving the LACPDU from the peer end, the device compares the system priorities of both ends based on the system ID in the packet. The end with a higher system ID priority sets the ports in the aggregation group to Bundle state based on the port ID priorities in a descending order, and sends an updated LACPDU. When receiving the LACPDU, the peer end sets corresponding ports to Bundle state so that both ends maintain consistency when a port exits or joins the aggregation group. The physical link can forward packets only after the ports at both ends are bundled dynamically.

After link aggregation, the LACP member ports periodically exchange LACPDUs. When a port does not receive an LACPDU in the specified time, a timeout occurs and the links are unbundled. In this case, the member ports cannot forward packets. There are two timeout modes: long timeout and short timeout. In long timeout mode, a port sends a packet every 30s. If it does not receive a packet from the peer end in 90s, a timeout occurs. In short timeout mode, a port sends a packet every 1s. If it does not receive a packet from the peer end in 3s, a timeout occurs. (The default timeout time in LACP short timeout mode is 3 seconds. The value is changeable.)

Figure 3-2 LACP Negotiation



In Figure 1-2, Switch A is connected to Switch B through three ports. Set the system priorities of Switch A and Switch B to 61440 and 4096 respectively. Enable LACP on the Ports 1–6, set the aggregation mode to the active mode, and set the port priority to the default value 32768.

When receiving an LACPDU from Switch A, Switch B finds that it has a higher system ID priority than Switch A (the system priority of Switch B is higher than that of Switch A). Switch B sets Port 4, Port 5, and Port 6 to Bundle state based on the order of port ID priorities (or in an ascending order of port numbers if the port priorities are the same). When receiving an updated LACPDU from Switch B, Switch A finds that Switch B has a higher system ID priority and has set Port 4, Port 5, and Port 6 to Bundle state. Then Switch A also sets Port 1, Port 2, and Port 3 to Bundle state.

3.3.2 Load Balancing

Working Principle

AP ports segregate packet flows by using load balancing algorithms based on packet features, such as the source and destination MAC addresses, source and destination IP addresses, and Layer-4 source and destination port numbers. The packet flow with the consistent feature is transmitted by one member link, and different packet flows are evenly distributed to member links. For example, in source MAC address-based load balancing, packets are distributed to the member links based on the source MAC addresses of the packets. Packets with different source MAC addresses are evenly distributed to member links. Packets with the identical source MAC address are forwarded by one member link.

Currently, there are several AP load balancing modes as follows:

- Source MAC address or destination MAC address
- Source MAC address + destination MAC address
- Source IP address or destination IP address
- Source IP address + destination IP address
- Layer-4 source port number or Layer-4 destination port number
- Layer-4 source port number + Layer-4 destination port number
- Source IP address + Layer-4 source port number
- Source IP address + Layer-4 destination port number
- Destination IP address + Layer-4 source port number
- Destination IP address + Layer-4 destination port number
- Source IP address + Layer-4 source port number + Layer-4 destination port number
- Destination IP address + Layer-4 source port number + Layer-4 destination port number
- Source IP address + destination IP address + Layer-4 source port number
- Source IP address + destination IP address + Layer-4 destination port number
- Source IP address + destination IP address + Layer-4 source port number + Layer-4 destination port number
- Panel port for incoming packets
- Labels of Multiprotocol Label Switching (MPLS) packets
- Aggregation member port polling
- Enhanced mode

Load balancing based on IP addresses or port numbers is applicable only to Layer-3 packets. When a device enabled with this load balancing method receives Layer-2 packets, it automatically switches to the default load balancing method.

All the load balancing methods use a load algorithm (hash algorithm) to calculate the member links based on the input parameters of the methods. The input parameters include the source MAC address, destination MAC address, source MAC address + destination MAC address, source IP address, destination IP address, source IP address + destination IP addresses, source IP address + destination IP address + Layer-4 port number and so on. The algorithm ensures that packets with different input parameters are evenly distributed to member links. It does not indicate that these packets are always distributed to different member links. For example, in IP address-based load balancing, two packets with different source and destination IP addresses may be distributed to the same member link through calculation.

Different products may support different load balancing algorithms.

Enhanced Load Balancing

Enhanced load balancing allows the combination of multiple fields in different types of packets. These fields include **src-mac**, **dst-mac**, **l2-protocol**, and **src-port** in Layer-2 packets, **src-ip**, **dst-ip**, **protocol**, **l4-src-port**, **l4-dst-port**, and **src-port**, in IPv4 packets, **src-ip**, **dst-ip**, **protocol**, **l4-src-port**, **l4-dst-port**, and **src-port** in IPv6 packets; **top-label**, **2nd-label**, **3rd-label**, **src-ip**, **dst-ip**, **vlan**, **src-port**, **src-mac**, **dst-mac**, **protocol**, **l4-src-port**, **l4-dst-port**, and **l2-etype** in MPLS packets; and **vlan**, **src-port**, **src-id**, **rx-id**, **ox-id**, **fabric-id**, and **dst-id** in FCoE packets.

A device enabled with enhanced load balancing first determines the type of packets to be transmitted and performs load balancing based on the specified fields in the packets. For example, the AP port performs source IP-based load balancing on the packets containing an ever-changing source IPv4 address.

All the load balancing methods are applicable to Layer-2 and Layer-3 AP ports. You need to configure proper load distribution methods based on different network environments to fully utilize network bandwidth.

Perform enhanced load balancing based on the src-mac, dst-mac, and vlan fields in Layer-2 packets, and the src-ip field in IPv4 packets. If the incoming packet is an IPv4 packet with an ever-changing source MAC address, the enhanced balancing algorithm does not take effect, because the device will perform load balancing only based on the src-ip field in the IPv4 packet after finding that it is an IPv4 packet.

In enhanced load balancing, the MPLS balancing algorithm takes effect only for MPLS Layer-3 VPN packets, but does not take effect for MPLS Layer-2 VPN packets.

Hash Load Balancing Control

Hash load balancing enables users to control load balancing flexibly in different scenarios. Currently, QTECH adopts the following hash load balancing control functions:

- Hash disturbance factor: Traffic over AP ports is hashed for balancing. For two devices of the same type, the same path will be calculated for load balancing for the same stream. When the ECMP is deployed, the same stream of the two devices may be balanced to the same destination device, resulting in hash polarization. The hash disturbance factor is used to affect the load balancing algorithm. Different disturbance factors are configured for different devices to ensure that different paths are provided for the same stream.

- Hash synchronization: To ensure network security, a firewall cluster is deployed between the internal and external networks for traffic cleaning. This requires that both the uplink and downlink traffic of a session is transmitted to the same device in the firewall cluster for processing. The source and destination IP addresses contained in the uplink and downlink streams of a session are reversed. The uplink and downlink streams will be directed to different firewalls in the firewall cluster based on the traditional hash algorithm. The hash synchronization function ensures that uplink and downlink streams of a session be transmitted over the same path.
- Hash algorithm mode: Apply the most appropriate hash algorithm mode to different traffic, so that when traffic changes, balance can still be kept. For example, if the source and destination MAC addresses of a stream increase 1 at the same time, configure the algorithm based on the source and destination MAC addresses cannot keep stream balance. At the moment, a suitable hash algorithm mode needs to be applied.
- Hash factor acquisition mode: There are an inner layer and an outer layer in the header in each of VXLAN packets, GRE packets, and other tunnel packets. It can be specified to obtain the hash factor from the inner layer or outer layer, to achieve a better balancing effect. For example, in some scenarios, tunnel packets share the same outer IP address but have different inner IP addresses. In this case, the inner IP address can be specified as the hash factor to optimize traffic balancing.

3.3.3 Member Port BFD Detection

Working Principle

Bidirectional Forwarding Detection (BFD) is a protocol that delivers fast detection of path failures. According to RFC7130, LACP takes 3s to detect link failures even in short timeout mode. The packets distributed to the faulty link during the 3-second period will be lost. BFD delivers faster failure detection. You can configure BFD on member ports to detect link failure and switch load to other member links in case of a link failure.

Because BFD is a Layer-3 protocol, you need to configure BFD on Layer-3 AP ports. BFD is classified into IPv4 detection and IPv6 detection, which detect IPv4 and IPv6 paths respectively. When BFD detects that the path on a member port fails, the packets will not be distributed to the member port.

After BFD is enabled on an AP port, BFD sessions are set up on its member ports in forwarding state independently.

3.4 Limitations

- Each AP of the QSW-6900 series products contains up to eight member ports, and each device supports up to 256 APs by default.
- For QSW-6900 series products, the capacity mode of APs can be set to any one of the following: 255*16, 127*32, 63*64, and 31*128. In these modes, the maximum number of member ports supported by each AP is 16, 32, 64, and 128 respectively, and the maximum

number of supported APs is 255, 127, 63, and 31 respectively. The default configuration is 255*16.

- When the QSW-6900 series products adopt load balancing that is based on the source MAC address, destination MAC address, or source MAC address + destination MAC address, the devices also use the Ethernet type field and VLAN field of unicast packets as balancing factors by default.
- The QSW-6900 series products adopt the non-enhanced load balancing mode. With the Internet Group Management Protocol snooping (IGMP snooping) or multicast routing enabled, the keywords for load balancing of multicast packets are src-ip, dst-ip, or src-ip+dst-ip. The keywords for load balancing of other multicast packets, unknown unicast packets, and broadcast packets are src-mac, dst-mac, or src-mac+dst-mac. For example, when layer-3 packets (unknown unicast, multicast, and broadcast packets) are forwarded at layer 2, load balancing cannot be performed based on src-ip or dst-ip. In this case, the enhanced mode can be adopted because load balancing is performed based on the packet type in this mode.
- In load balancing mode based on src-dst-ip-l4port, L4port changes on the QSW-6900 series products are valid only to unicast packets.
- The QSW-6900 series products support AP-based load balancing algorithms. AP-based load balancing algorithms support load balancing based only on SMAC, DMAC, SMAC+DMAC, SIP, DIP, and SIP+DIP.
- The QSW-6900 series products do not support the Round Robin (RR) load balancing algorithm.
- Enhanced load balancing templates of the QSW-6900 series products support the following fields:
- L2 template: src-mac dst-mac vlan l2-protocol src-port
- IPv4 template: src-ip dst-ip protocol vlan l4-src-port l4-dst-port src-port
- IPv6 template: src-ip dst-ip protocol vlan l4-src-port l4-dst-port src-port

3.5 Configuration

Configuration	Description and Command	
Configuring Static AP Ports	(Mandatory) It is used to configure link aggregation manually.	
	interface aggregateport	Creates an Ethernet AP port.
	interface san-port-channel	Creates an FC AP port.
	port-group	Configures static AP member ports.
	(Mandatory) It is used to configure link aggregation dynamically.	

Configuring LACP AP Ports	**port-group mode**	Configures LACP member ports.
	lacp system-priority	Configures the LACP system priority.
	lacp short-timeout period	Configures the timeout time of the LACP system in short timeout mode.
	lacp port-priority	Configures the port priority.
	lacp short-timeout	Configures the short timeout mode on a port.
Enabling LinkTrap	(Optional) It is used to enable LinkTrap.	
	snmp trap link-status	Enables LinkTrap advertisement for an AP port.
	aggregateport member linktrap	Enables LinkTrap t for AP member ports.
Configuring a Load Balancing Mode	(Optional) It is used to configure a load balancing mode for an aggregated link.	
	aggregateport load-balance	Configures a load balancing algorithm for an AP port or AP member ports.
	(Optional) It is used to configure the profile of enhanced load balancing.	
	load-balance-profile	Renames the profile of enhanced load balancing.
	l2 field	Configures a load balancing mode for Layer-2 packets.
	ipv4 field	Configures a load balancing mode for IPv4 packets.
	ipv6 field	Configures a load balancing mode for IPv6 packets.
	mpls field	Configures a load balancing mode for MPLS packets.
	trill field	Configures a load balancing mode for TRILL packets.

	fcoe field	Configures a load balancing mode for FCoE packets.
	(Optional) It is used to control load balancing policy.	
	aggregateport hash-elasticity enable	Configures flexible hash.
	hash-disturb *string*	Configures hash disturbance factor.
	hash-symmetrical [ipv4 | ipv6 | fcoe| on]	Configures hash synchronization.
	aggregateport hash-header {inner | outer | inner-outer}	Configures the balancing factor acquisition mode for tunnel packet.
Configuring an AP Capacity Mode	(Optional) It is used to configure the AP capacity mode.	
	aggregateport capacity mode	Configures an AP capacity mode in global configuration mode.
Enabling BFD for AP Member Ports	(Optional) It is used to enable BFD for AP member ports.	
	aggregate bfd-detect ipv4	Enables IPv4 BFD for AP member ports.
Configuring a Preferred AP Member Port	(Optional) It is used to configure an AP member port as the preferred port.	
	aggregateport primary-port	Configures an AP member port as the preferred port.
Configuring the Minimum Number of AP Member Ports	**Aggregateport member minimum**	Configures the minimum number of AP member ports.
Configuring the Minimum Number of AP Member Ports (Action)	**Aggregateport member minimum action**	Triggers action when the number of AP member ports in the Up state is less than the minimum number of the AP member ports.
Enabling the LACP Independent Port Function	**lacp individual enable**	Enables the LACP independent port function.

3.5.1 Configuring Static AP Ports

Configuration Effect

- Configure multiple physical ports as AP member ports to realize link aggregation.
- The bandwidth of the aggregation link is equal to the sum of the member link bandwidths.
- When a member link of the AP port is disconnected, the load carried by the link is automatically allocated to other functional member links.

Notes

- Only physical ports can be added to an AP port.
- The ports of different media types or port modes cannot be added to the same AP port.
- Layer-2 ports can be added to only a Layer-2 AP port, and Layer-3 ports can be added to only a Layer-3 AP port. The Layer-2/3 attributes of an AP port that contains member ports cannot be modified.
- After a port is added to an AP port, the attributes of the port are replaced by those of the AP port.
- After a port is removed from an AP port, the attributes of the port are restored.

After a port is added to an AP port, the attributes of the port are consistent with those of the AP port. Therefore, do not perform configuration on the AP member ports or apply configuration to a specific AP member port. However, some configurations (the **shutdown** and **no shutdown** commands) can be configured on AP member ports. When you use AP member ports, check whether the function that you want to configure can take effect on a specific AP member port, and perform this configuration properly.

Configuration Steps

Creating an Ethernet AP Port

- Mandatory.
- Perform this configuration on an AP-enabled device.

Command	**interface aggregateport *ap-number***
Parameter Description	*ap-number*: Indicates the number of an AP port.
Defaults	By default, no AP port is created.
Command Mode	Global configuration mode

Usage Guide	To create an Ethernet AP port, run **interfaces aggregateport** in global configuration mode. To delete the specified Ethernet AP port, run **no interfaces aggregateport** *ap-number* in global configuration mode.

- Run **port-group** to add a physical port to a static AP port in interface configuration mode. If the AP port does not exist, it will be created automatically.
- Run **port-group mode** to add a physical port to an LACP AP port in interface configuration mode. If the AP port does not exist, it will be created automatically.
- The AP feature must be configured on the devices at both ends of a link and the AP mode must be the same (static AP or LACP AP).

Configuring Static AP Member Ports

- Mandatory.
- Perform this configuration on AP-enabled devices.

Command	**port-group** ***ap-number***
Parameter Description	**port-group** *ap-number*: Indicates the number of an AP port.
Defaults	By default, no ports are added to any static AP port.
Command Mode	Interface configuration mode of the specified Ethernet port
Usage Guide	To add member ports to an AP port, run **port-group** in interface configuration mode. To remove member ports from an AP port, run **no port-group** in interface configuration mode.

- The static AP member ports configured on the devices at both ends of a link must be consistent.
- After a member port exits the AP port, the default settings of the member port are restored. Different functions deal with the default settings of the member ports differently. It is recommended that you check and confirm the port settings after a member port exits an AP port.
- After a member port exits an AP port, the port is disabled by using the **shutdown** command to avoid loops. After you confirm that the topology is normal, run **no shutdown** in interface configuration mode to enable the port again.

Converting Layer-2 APs to Layer-3 APs

- Optional.
- When you need to enable Layer-3 routing on an AP port, for example, to configure IP addresses or static route entries, convert the Layer-2 AP port to a Layer-3 AP port and enable routing on the Layer-3 AP port.
- Perform this configuration on AP-enabled devices that support Layer-2 and Layer-3 features, such as Layer-3 switches or wireless access controllers (ACs).

Command	**no switchport**
Parameter Description	N/A
Defaults	By default, the AP ports are Layer-2 AP ports.
Command Mode	Interface configuration mode of the specified AP port
Usage Guide	The Layer-3 AP feature is supported by only Layer-3 devices.

The AP port created on a Layer-3 device that does not support Layer-2 feature is a Layer-3 AP port. Otherwise, the AP port is a Layer-2 AP port.

Creating an Ethernet AP Subinterface

- Optional.
- On a device that supports subinterface configuration, run **interface aggregateport** *sub-ap-number* to create a subinterface.
- Perform this configuration on AP-enabled devices that support Layer-2 and Layer-3 features, such as Layer-3 switches.

Command	**interface aggregateport *sub-ap-number***
Parameter Description	*sub-ap-number*: Indicates the number of an AP subinterface.
Defaults	By default, no subinterfaces are created.
Command Mode	Interface configuration mode of the specified AP port

Usage Guide	You need to convert the master port of the AP port to a Layer-3 port before creating a subinterface.

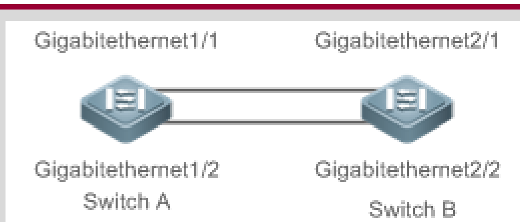
Verification

- Run **show running** to display the configuration.
- Run **show aggregateport summary** to display the AP configuration.

Command	**show aggregateport *aggregate-port-number* [load-balance | summary]**
Parameter Description	*aggregate-port-number*: Indicates the number of an AP port. **load-balance**: Displays the load balancing algorithm. **summary**: Displays the summary of each link.
Command Mode	Any mode
Usage Guide	The information on all AP ports is displayed if you do not specify the AP port number.
	QTECH# show aggregateport 1 summary AggregatePort MaxPorts SwitchPort Mode Load balance Ports ------------- --------------- ---------- ------ --------------------------- ------------------------ **Ag1** 8 Enabled ACCESS **dst-mac** **Gi0/2**

Configuration Example

- Configuring an Ethernet Static AP Port

Scenario **Figure 3-2**	
Configuration Steps	- Add the GigabitEthernet 1/1 and GigabitEthernet 1/2 ports on Switch A to static AP port 3. - Add the GigabitEthernet 2/1 and GigabitEthernet 2/2 ports on Switch B to static AP port 3.

Switch A	SwitchA# configure terminal SwitchA(config)# interface range GigabitEthernet 1/1-2 SwitchA(config-if-range)# port-group 3
Switch B	SwitchB# configure terminal SwitchB(config)# interface range GigabitEthernet 2/1-2 SwitchB(config-if-range)# port-group 3
Verification	▪ Run **show aggregateport summary** to check whether AP port 3 contains member ports GigabitEthernet 1/1 and GigabitEthernet 1/2.
Switch A	SwitchA# show aggregateport summary AggregatePort MaxPorts SwitchPort Mode Ports ------------- -------- ---------- ------ ---------------------------------- **Ag3** 8 Enabled ACCESS **Gi1/1,Gi1/2**
Switch B	SwitchB# show aggregateport summary AggregatePort MaxPorts SwitchPort Mode Ports ------------- -------- ---------- ------ ---------------------------------- **Ag3** 8 Enabled ACCESS **Gi2/1,Gi2/2**

3.5.2 Configuring LACP AP Ports

Configuration Effect

- Connected devices perform autonegotiation through LACP to realize dynamic link aggregation.
- The bandwidth of the aggregation link is equal to the sum of the member link bandwidths.
- When a member link of the AP port is disconnected, the load carried by the link is automatically allocated to other functional member links.
- It takes LACP 90s to detect a link failure in long timeout mode and 3s in short timeout mode.

Notes

- After a port exits an LACP AP port, the default settings of the port may be restored. Different functions deal with the default settings of the member ports differently. It is recommended that you check and confirm the port settings after a member port exits an LACP AP port.
- Changing the LACP system priority may cause LACP member ports to be disaggregated and aggregated again.

- Changing the priority of an LACP member port may cause the other member ports to be disaggregated and aggregated again.

Configuration Steps

- Configuring LACP Member Ports
- Mandatory.
- Perform this configuration on LACP-enabled devices.

Command	**port-group *key-number* mode { active | passive }**
Parameter Description	*Key-number*: Indicates the management key of an AP port. In other words, it is the LACP AP port number. The maximum value is subject to the number of AP ports supported by the device. **active**: Indicates that ports are added to a dynamic AP port actively. **passive**: Indicates that ports are added to a dynamic AP port passively.
Defaults	By default, no physical ports are added to any LACP AP port.
Command Mode	Interface configuration mode of the specified physical port
Usage Guide	Use this command in interface configuration mode to add member ports to an LACP AP port.

The LACP member port configuration at both ends of a link must be consistent.

- Configuring the LACP System ID
- Optional.
- Configure the LACP system ID when LACP ports of multiple (a maximum of four) independent devices need to negotiate with the LACP port of a specific device. Configure the LACP system ID together with the LACP device ID.

Command	**lacp system-id *system-id***
Parameter Description	*system-id*: Indicates the system ID of an aggregation group. It must be a valid unicast MAC address.
Defaults	The LACP system ID is the MAC address of device by default.

Command Mode	Interface configuration mode
Usage Guide	Use this command in interface configuration mode to configure the LACP system ID.

- Configuring the LACP Device ID
- Optional.
- Configure the LACP device ID when LACP ports of multiple (a maximum of four) independent devices need to negotiate with the LACP port of a specific device. Configure the LACP device ID together with the LACP system ID.

Command	**lacp device *number***
Parameter Description	*number*: Indicates the device ID of an aggregation group. The value ranges from 0 to 3.
Defaults	The LACP device ID is 0 by default.
Command Mode	Interface configuration mode
Usage Guide	Use this command in interface configuration mode to configure the LACP device ID.

- Configuring the LACP System Priority
- Optional.
- Perform this configuration when you need to adjust the system ID priority. A smaller value indicates a higher system ID priority. The device with a higher system ID priority selects an AP port.
- Perform this configuration on LACP-enabled devices.

Command	**lacp system-priority *system-priority***
Parameter Description	*system-priority*: Indicates the LACP system priority. The value ranges from 0 to 65535.
Defaults	By default, the LACP system priority is 32768.
Command Mode	Global configuration mode

Usage Guide	Use this command in global configuration mode to configure the LACP system priority. All the dynamic member links share one LACP system priority. Changing the LACP system priority will affect all member links. To restore the default settings, run **no lacp system-priority** in interface configuration mode.

- Configuring the Priority of an LACP Member Port
- Optional.
- Perform this configuration when you need to specify the port ID priority. A smaller value indicates a higher port ID priority. The port with the highest port ID priority will be selected as the master port.
- Perform this configuration on LACP-enabled devices.

Command	**lacp port-priority *port-priority***
Parameter Description	*port-priority*: Indicates the priority of an LACP member port. The value ranges from 0 to 65535.
Defaults	By default, the priority of an LACP member port is 32768.
Command Mode	Interface configuration mode of the specified physical port
Usage Guide	Use this command in global configuration mode to configure the priority of an LACP member port. To restore the settings, run **no lacp port-priority** in interface configuration mode.

- Configuring the Timeout Mode of LACP Member Ports
- Optional.
- When you need to implement real-time link failure detection, configure the short timeout mode. It takes LACP 90s to detect a link failure in long timeout mode and 3s in short timeout mode. (The default timeout time in LACP short timeout mode is 3 seconds. The value is changeable.)
- Perform this configuration on LACP-enabled devices, such as switches.

Command	**lacp short-timeout**
Parameter Description	N/A
Defaults	By default, the timeout mode of LACP member ports is long timeout.

Command Mode	Interface configuration mode
Usage Guide	The timeout mode is supported only by physical ports. To restore the default settings, run **no lacp short-timeout** in interface configuration mode.

- Configuring the Timeout Time of the LACP System in Short Timeout Mode
- Optional.
- Configure this function when the timeout time of a device in LACP short timeout mode needs to be adjusted.
- Configure this function on devices that support the LACP function.

Command	**lacp short-timeout period *value***
Parameter Description	*value*: Indicates the timeout time in short timeout mode. The value ranges from 3 seconds to 90 seconds.
Defaults	The default timeout time in LACP short timeout mode is 3 seconds.
Command Mode	Global configuration mode
Usage Guide	In global configuration mode, run the command to configure the timeout time in LACP short timeout mode. All dynamic link groups configured on a device share the same timeout time in LACP short timeout mode. Changing the value will affect all aggregate groups on the switch. In interface configuration mode, run the **no lacp short-timeout period** command to restore the timeout time in LACP short timeout mode to the default value.

Verification

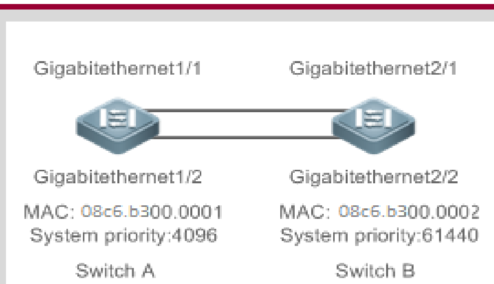
- Run **show running** to display the configuration.
- Run **show lacp summary** to display LACP link state.

Command	**show lacp summary [*key-number*]**
Parameter Description	*key-name*: Indicates the number of an LACP AP port.

Command Mode	Any mode
Usage Guide	The information on all LACP AP ports is displayed if you do not specify *key-name*. The system ID and device ID are displayed if configured.
	QTECH#show lacp summary **System Id:32768, 0000.1236.54aa** Flags: S - Device is requesting Slow LACPDUs F - Device is requesting Fast LACPDUs. A - Device is in active mode. P - Device is in passive mode. **Aggregate port 2:** **System Id: 0000.1236.54aa Device num : 1** **Local information:** LACP port Oper Port Port Port Flags State Priority Key Number State -- **Te1/0/1 SA down 32768 0x2 0x4001 0x45** Partner information: LACP port Oper Port Port Port Flags Priority Dev ID Key Number State --- **Te1/0/1 SP 0 0000.0000.0000 0x0 0x0 0x0**

Configuration Example

Configuring LACP

Scenario **Figure 3-3**	

Configuration Steps	▪ On Switch A, set the LACP system priority to 4096. ▪ Enable dynamic link aggregation on the GigabitEthernet1/1 and GigabitEthernet1/2 ports on Switch A and add the ports to LACP AP port 3. ▪ On Switch B, set the LACP system priority to 61440. ▪ Enable dynamic link aggregation on the GigabitEthernet2/1 and GigabitEthernet2/2 ports on Switch B and add the ports to LACP AP port 3.
Switch A	SwitchA# configure terminal SwitchA(config)# lacp system-priority 4096 SwitchA(config)# interface range GigabitEthernet 1/1-2 SwitchA(config-if-range)# port-group 3 mode active SwitchA(config-if-range)# end
Switch B	SwitchB# configure terminal SwitchB(config)# lacp system-priority 61440 SwitchB(config)# interface range GigabitEthernet 2/1-2 SwitchB(config-if-range)# port-group 3 mode active SwitchB(config-if-range)# end
Verification	▪ Run **show lacp summary 3** to check whether LACP AP port 3 contains member ports GigabitEthernet2/1 and GigabitEthernet2/2.
Switch A	SwitchA# show LACP summary 3 System Id:32768, 08c6.b3.0001 Flags: S - Device is requesting Slow LACPDUs F - Device is requesting Fast LACPDUs. A - Device is in active mode. P - Device is in passive mode. Aggregated port 3: Local information: LACP port Oper Port Port Port Flags State Priority Key Number State -- Gi1/1 SA bndl 32768 0x3 0x1 0x3d Gi1/2 SA bndl 32768 0x3 0x2 0x3d Partner information:

	LACP port Oper Port Port Port Flags Priority Dev ID Key Number State --- Gi1/1 SA 32768 08c6.b3.0002 0x3 0x1 0x3d Gi1/2 SA 32768 08c6.b3.0002 0x3 0x2 0x3d
Switch B	SwitchB# show LACP summary 3 System Id:32768, 08c6.b3.0002 Flags: S - Device is requesting Slow LACPDUs F - Device is requesting Fast LACPDUs. A - Device is in active mode. P - Device is in passive mode. Aggregated port 3: Local information: LACP port Oper Port Port Port Flags State Priority Key Number State --- Gi2/1 SA bndl 32768 0x3 0x1 0x3d Gi2/2 SA bndl 32768 0x3 0x2 0x3d Partner information: LACP port Oper Port Port Port Flags Priority Dev ID Key Number State --- Gi2/1 SA 32768 08c6.b3.0001 0x3 0x1 0x3d Gi2/2 SA 32768 08c6.b3.0001 0x3 0x2 0x3d

3.5.3 Enabling LinkTrap

Configuration Effect

Enable the system with LinkTrap to send LinkTrap messages when aggregation links are changed.

Configuration Steps

Enabling LinkTrap for an AP Port

- Optional.

- Enable LinkTrap in interface configuration mode. By default, LinkTrap is enabled. LinkTrap messages are sent when the link state or protocol state of the AP port is changed.
- Perform this configuration on AP-enabled devices.

Command	**snmp trap link-status**
Parameter Description	N/A
Defaults	By default, LinkTrap is enabled.
Command Mode	Interface configuration mode of the specified AP port
Usage Guide	Use this command in interface configuration mode to enable LinkTrap for the specified AP port. After LinkTrap is enabled, LinkTrap messages are sent when the link state of the AP port is changed. Otherwise, LinkTrap messages are not sent. By default, LinkTrap is enabled. To disable LinkTrap for an AP port, run **no snmp trap link-status** in interface configuration mode. LinkTrap cannot be enabled for a specific AP member port. To enable LinkTrap for all AP member ports, run **aggregateport member linktrap** in global configuration mode.

Enabling LinkTrap for AP Member Ports

- Optional.
- By default, LinkTrap is disabled for AP member ports.
- Perform this configuration on AP-enabled devices.

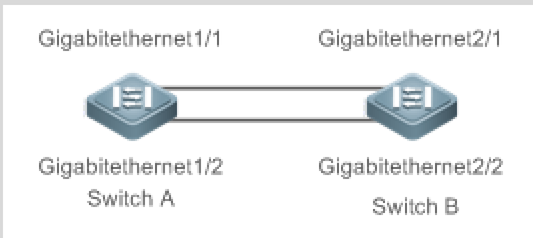
Command	**aggregateport member linktrap**
Parameter Description	N/A
Defaults	By default, LinkTrap is disabled for AP member ports.
Command Mode	Global configuration mode
Usage Guide	Use this command in global configuration mode to enable LinkTrap for all AP member ports. By default, LinkTrap messages are not sent when the link state of AP member ports is changed. To disable LinkTrap for all AP member ports, run **no aggregateport member linktrap** in global configuration mode.

Verification

- Run **show running** to display the configuration.
- After LinkTrap is enabled, you can monitor this feature on AP ports or their member ports by using the MIB software.

Configuration Example

- Enabling LinkTrap for AP Member Ports

Scenario **Figure 3-4**	
Configuration Steps	▪ Add the GigabitEthernet 1/1 and GigabitEthernet 1/2 ports on Switch A to static AP port 3. ▪ Add the GigabitEthernet 2/1 and GigabitEthernet 2/2 ports on Switch B to static AP port 3. ▪ On Switch A, disable LinkTrap for AP port 3 and enable LinkTrap for its member ports. ▪ On Switch B, disable LinkTrap for AP port 3 and enable LinkTrap its AP member ports.
Switch A	SwitchA# configure terminal SwitchA(config)# interface range GigabitEthernet 1/1-2 SwitchA(config-if-range)# port-group 3 SwitchA(config-if-range)# exit SwitchA(config)# aggregateport member linktrap SwitchA(config)# interface Aggregateport 3 SwitchA(config-if-AggregatePort 3)# no snmp trap link-status
Switch B	SwitchB# configure terminal SwitchB(config)# interface range GigabitEthernet 2/1-2 SwitchB(config-if-range)# port-group 3 SwitchB(config-if-range)# exit

	SwitchB(config)# aggregateport member linktrap SwitchB(config)# interface Aggregateport 3 SwitchB(config-if-AggregatePort 3)# no snmp trap link-status
Verification	▪ Run **show running** to check whether LinkTrap is enabled for AP port 3 and its member ports.
Switch A	SwitchA# show run | include AggregatePort 3 Building configuration... Current configuration: 54 bytes interface AggregatePort 3 no snmp trap link-status SwitchA# show run | include AggregatePort aggregateport member linktrap
Switch B	SwitchB# show run | include AggregatePort 3 Building configuration... Current configuration: 54 bytes interface AggregatePort 3 no snmp trap link-status SwitchB# show run | include AggregatePort aggregateport member linktrap

3.5.4 Configuring a Load Balancing Mode

Configuration Effect

- The system distributes incoming packets among member links by using the specified load balancing algorithm. The packet flow with the consistent feature is transmitted by one member link, whereas different packet flows are evenly distributed to various links. A device enabled with enhanced load balancing first determines the type of packets to be transmitted and performs load balancing based on the specified fields in the packets. For example, the AP port performs source IP-based load balancing on the packets containing an ever-changing source IPv4 address.
- In enhanced load balancing mode, configure the hash disturbance factor to ensure that same packets from two devices of the same type will be balanced to different links.

- In enhanced load balancing mode, enable hash synchronization to ensure that uplink and downlink packets of the same type will be transmitted over the same link. For example, in load balancing based on the source and destination IP addresses, enable hash synchronization for IPv4 packets to ensure that the uplink and downlink IPv4 packets will be transmitted over the same path.

Notes

- Different disturbance factors may lead to the same disturbance effect.
- Enable or disable hash synchronization for IPv4, IPv6, FCoE and On as required.

Configuration Steps

- Configuring the Global Load Balancing Algorithm of an AP port
- (Optional) Perform this configuration when you need to optimize load balancing.
- Perform this configuration on AP-enabled devices.

Command	**aggregateport load-balance { dst-mac | src-mac | src-dst-mac | dst-ip | src-ip | src-dst-ip | src-dst-ip-l4port | enhanced profile *profile-name* }**
Parameter Description	**dst-mac**: Indicates that load is distributed based on the destination MAC addresses of incoming packets. **src-mac**: Indicates that load is distributed based on the source MAC addresses of incoming packets. **src-dst-ip**: Indicates that load is distributed based on source and destination IP addresses of incoming packets. **dst-ip**: Indicates that load is distributed based on the destination IP addresses of incoming packets. **src-ip**: Indicates that load is distributed based on the source IP addresses of incoming packets. **src-dst-mac**: Indicates that load is distributed based on source and destination MAC addresses of incoming packets. **src-dst-ip-l4port**: Indicates that load is distributed based on source IP and destination IP addresses as well as Layer-4 source and destination port numbers. **enhanced profile** *profile-name*: Indicates the name of the enhanced load balancing profile.
Defaults	Load balancing can be based on source and destination MAC addresses (applicable to switches), source and destination IP addresses (applicable to gateways), or the profile of enhanced load balancing (applicable to switches with CB line cards).

Command Mode	Global configuration mode
Usage Guide	To restore the default settings, run **no aggregateport load-balance** in global configuration mode. You can run **aggregateport load-balance** in interface configuration mode of an AP port on devices that support load balancing configuration on a specific AP port. The configuration in interface configuration mode prevails. To disable the load balancing algorithm, run **no aggregateport load-balance** in interface configuration mode of the AP port. After that, the load balancing algorithm configured in global configuration mode takes effect. You can run **aggregateport load-balance** in interface configuration mode of an AP port on devices that support load balancing configuration on a specific AP port.

- Renaming the Profile of Enhanced Load Balancing
- By default, if a device supports enhanced load balancing, the system creates a profile named **default** for enhanced load balancing. Perform this configuration when you need to rename the profile or restore the default settings. In other cases, the configuration is optional.
- Perform this configuration on devices that support enhanced load balancing, such as aggregation switches and core switches.

Command	**load-balance-profile** ***profile-name***
Parameter Description	*profile-name*: Indicates the profile name, which contains up to 31 characters.
Defaults	The default profile name is **default**.
Command Mode	Global configuration mode
Usage Guide	To enter default profile mode, run **load-balance-profile default**. To rename the enhanced load balancing profile, run **load-balance-profile** *profile-nam*. To restore the default profile name, run **default load-balance-profile** in global configuration mode. To restore the default load balancing settings, run **default load-balance-profile** *profile-name* in global configuration mode. Only one profile is supported globally. Please do not delete the profile. To display the enhanced load balancing profile, run **show load-balance-profile**.

Configuring the Layer-2 Packet Load Balancing Mode

- (Optional) Perform this configuration to specify the Layer-2 packet load balancing mode.

- Perform this configuration on devices that support enhanced load balancing, such as aggregation switches and core switches.

Command	**l2 field { [src-mac] [dst-mac] [l2-protocol] [src-port] [dst-port] }**
Parameter Description	**src-mac**: Indicates that load is distributed based on the source MAC addresses of incoming Layer-2 packets. **dst-mac**: Indicates that load is distributed based on the destination MAC addresses of incoming Layer-2 packets. **l2-protocol**: Indicates that load is distributed based on the Layer-2 protocol types of incoming Layer-2 packets. **src-port**: Indicates that load is distributed based on the panel port for incoming Layer-2 packets.
Defaults	By default, the load balancing mode of Layer-2 packets is **src-mac** and **dst-mac**.
Command Mode	Profile configuration mode
Usage Guide	To restore the default settings, run **no l2 field** in profile configuration mode.

Configuring the IPv4 Packet Load Balancing Mode

- Optional.
- Perform this configuration to specify the IPv4 packet load balancing mode.
- Perform this configuration on devices that support enhanced load balancing, such as aggregation switches and core switches.

Command	**ipv4 field {[src-ip] [dst-ip] [protocol] [l4-src-port][l4-dst-port] [src-port] }**
Parameter Description	**src-ip**: Indicates that load is distributed based on the source IP addresses of incoming IPv4 packets. **dst-ip**: Indicates that load is distributed based on the destination IP addresses of incoming IPv4 packets. **protocol**: Indicates that load is distributed based on the protocol types of incoming IPv4 packets.

	l4-src-port: Indicates that load is distributed based on the Layer-4 source port numbers of incoming IPv4 packets. **l4-dst-port**: Indicates that load is distributed based on the Layer-4 destination port numbers of incoming IPv4 packets. **src-port**: Indicates that load is distributed based on the panel port for incoming IPv4 packets.
Defaults	By default, the load balancing mode of IPv4 packets is **src-ip** and **dst-ip**.
Command Mode	Profile configuration mode
Usage Guide	To restore the default settings, run **no ipv4 field** in profile configuration mode.

Configuring the IPv6 Packet Load Balancing Mode

- Optional.
- Perform this configuration to specify the IPv6 packet load balancing mode.
- Perform this configuration on devices that support IPv6 packet load balancing, such as aggregation switches and core switches.

Command	**ipv6 field { [src-ip] [dst-ip] [protocol] [l4-src-port][l4-dst-port] [src-port]}**
Parameter Description	**src-ip**: Indicates that load is distributed based on the source IP addresses of incoming IPv6 packets. **dst-ip**: Indicates that load is distributed based on the destination IP addresses of incoming IPv6 packets. **protocol**: Indicates that load is distributed based on the protocol types of incoming IPv6 packets. **l4-src-port**: Indicates that load is distributed based on the Layer-4 source port numbers of incoming IPv6 packets. **l4-dst-port**: Indicates that load is distributed based on the Layer-4 destination port numbers of incoming IPv6 packets. **src-port**: Indicates that load is distributed according to the source port numbers of incoming IPv6 packets.
Defaults	By default, the load balancing mode of IPv6 packets is **src-ip** and **dst-ip**.

Command Mode	Profile configuration mode
Usage Guide	To restore the default settings, run **no ipv6 field** in profile configuration mode.

Configuring the MPLS Packet Load Balancing Mode

- Optional.
- Perform this configuration to specify the MPLS packet load balancing mode.
- Perform this configuration on devices that support MPLS packet load balancing, such as aggregation switches and core switches.

Command	**mpls field { [top-label] [2nd-label] [3rd-label] [src-ip] [dst-ip] [vlan] [src-port] [dst-port] [src-mac] [dst-mac] [protocol] [l4-src-port] [l4-dst-port] [l2-etype] }**
Parameter Description	**src-ip**: Indicates that load is distributed based on the source IP addresses of incoming MPLS packets. **dst-ip**: Indicates that load is distributed based on the destination IP addresses of incoming MPLS packets. **top-label**: Indicates that load is distributed based on the top labels of incoming MPLS packets. **2nd-label**: Indicates that load is distributed based on the second labels of incoming MPLS packets. **3rd-label**: Indicates that load is distributed based on the third labels of incoming MPLS packets. **vlan**: Indicates that load is distributed based on the VLAN IDs of incoming MPLS packets. **src-port**: Indicates that load is distributed based on the source port numbers of incoming MPLS packets. **dst-port**: Indicates that load is distributed based on the panel port for outgoing MPLS packets. **src-mac**: Indicates that load is distributed based on the source MAC addresses of incoming MPLS packets. **dst-mac**: Indicates that load is distributed based on the destination MAC addresses of incoming MPLS packets. **protocol**: Indicates that load is distributed based on the protocol types of incoming MPLS packets.

	l4-src-port: Indicates that load is distributed based on the Layer-4 source port numbers of incoming MPLS packets. **l4-dst-port**: Indicates that load is distributed based on the Layer-4 destination port numbers of incoming MPLS packets. **l2-etype**: Indicates that load is distributed based on the Ethernet types of MPLS packets.
Defaults	By default, the load balancing mode of MPLS packets is **top-label** and **2nd-label**.
Command Mode	Profile configuration mode
Usage Guide	To restore the default settings, run **no mpls field** in profile configuration mode.

The MPLS load balancing algorithm takes effect only for MPLS Layer-3 VPN packets.

Configuring the TRILL Packet Load Balancing Mode

- Optional.
- Perform this configuration to specify the TRILL packet load balancing mode.
- Perform this configuration on devices that support TRILL packet load balancing, such as aggregation switches and core switches.

Command	**trill field { [vlan] [src-ip] [dst-ip] [src-port] [dst-port] [src-mac] [dst-mac] [l4-src-port] [l4-dst-port] [l2-etype] [protocol] [ing-nick] [egr-nick] }**
Parameter Description	**vlan**: Indicates that load is distributed based on the VLAN IDs of incoming TRILL packets. **src-ip**: Indicates that load is distributed based on the source IP addresses of incoming TRILL packets. **dst-ip**: Indicates that load is distributed based on the destination IP addresses of incoming TRILL packets. **src-port**: Traffic is distributed according to the source port numbers of the incoming TRILL packets. **src-mac**: Indicates that load is distributed based on the source MAC addresses of incoming TRILL packets. **dst-mac**: Indicates that load is distributed based on the destination MAC addresses of incoming TRILL packets.

	l4-src-port: Indicates that load is distributed based on the Layer-4 source port numbers of incoming TRILL packets. **l4-dst-port**: Indicates that load is distributed based on the Layer-4 destination port numbers of incoming TRILL packets. **l2-etype**: Indicates that load is distributed based on the Ethernet types of TRILL packets. **protocol**: Indicates that load is distributed based on the protocol types of incoming TRILL packets. **Ing-nick**: Indicates that load is distributed based on the Ingress Rbridge Nicknames of incoming TRILL packets. **egr-nick**: Indicates that load is distributed based on the Egress Rbridge Nicknames of incoming TRILL packets.
Defaults	By default, the load balancing mode of TRILL packets is **src-mac**, **dst-mac**, and **vlan**.
Command Mode	Profile configuration mode
Usage Guide	To restore the default settings, run **no trill field** in profile configuration mode. TRILL Transit RBridge packet flows are balanced based on the following fields: **ing-nick**, **egr-nick**, **src-mac**, **dst-mac**, **vlan**, and **l2-etype**. TRILL Egress RBridge packet flows are balanced based on the following fields: Layer-2 packets: **src-mac**, **dst-mac**, **vlan**, and **l2- protocol**. Layer-3 packets: **src-ip**, **dst-ip**, **l4-src-port**, **l4-dst-port**, **protocol**, and **vlan**. The **src-port** and **dst-port** fields can be used to balance all TRILL Transit RBridge and TRILL Egress RBridge packet flows.

Configuring the FCoE Packet Load Balancing Mode

- Optional.
- Perform this configuration to specify the FCoE packet load balancing mode.
- Perform this configuration on devices that support FCoE packet load balancing, such as aggregation switches and core switches.

Command	fcoe field {[vlan] [src-port] [dst-port] [src-id] [dst-id] [rx-id] [ox-id] [fabric-id]}

Parameter Description	**vlan**: Indicates that load is distributed based on the VLAN IDs of incoming FCoE packets. **src-port**: Indicates that load is distributed based on the source port numbers of incoming FCoE packets. **src-id**: Indicates that load is distributed based on the source IDs of FCoE packets. **dst-id**: Indicates that load is distributed based on the destination IDs of FCoE packets. **rx-id:** Indicates that load is distributed based on the Responder Exchange IDs of FCoE packets. **ox-id**: Indicates that load is distributed based on the Originator Exchange IDs of FCoE packets. **fabric-id**: Indicates that load is distributed based on the FC network fabric IDs of FCoE packets.
Defaults	By default, the load balancing mode of FCoE packets is **src-id**, **dst-id**, and **ox-id**.
Command Mode	Profile configuration mode
Usage Guide	To restore the default settings, run **no fcoe field** in profile configuration mode.

Configuring the Hash Disturbance Factor

- Optional
- Perform this operation to balance packets of the same type over the AP port for devices of the same type.

Command	**hash-disturb** ***string***
Parameter Description	**String**: Indicates the character string used to calculate the hash disturbance factor.
Defaults	By default, no hash disturbance factor is set.
Command Mode	Profile configuration mode
Usage Guide	To restore the default settings, run **no hash-disturb** in profile configuration mode.

Enabling or Disabling Hash Synchronization

- Optional
- Perform this operation to ensure that uplink and downlink streams of the same packet type are transmitted over the same path.

Command	**hash-disturb {ipv4 | ipv6 | fcoe| on }**
Parameter Description	**ipv4**: Indicates that hash synchronization is enabled for IPv4 packets. **ipv6**: Indicates that hash synchronization is enabled for IPv6 packets. **fcoe**: Indicates that hash synchronization is enabled for FCoE packets. on: Indicates that hash synchronization is enabled for packets on a module. Different modules support different packets type.
Defaults	Set it as required.
Command Mode	Profile configuration mode
Usage Guide	When hash synchronization is enabled for IPv4, IPv6, and FCoE packets as required, if uplink and downlink streams of the same packet type do not need to be transmitted over the same path, run the **no** form of this command in profile configuration mode.

Configuring Global Traffic Balance Algorithm Mode on AP

- Optional
- Perform this operation when traffic changes to keep traffic balance.

Command	**aggregateport algorithm mode *number***
Parameter Description	*Number*: Indicates algorithm mode.
Defaults	The default mode varies from product. Run command ***show aggregateport load-balance*** to check the default setting.
Command Mode	Global configuration mode
Usage Guide	Run command ***no aggregateport algorithm mode*** in global configuration mode to restore the default setting. Run command ***show running*** and ***show aggregateport load-balance*** to check whether it takes effect.

Configuring the Balancing Factor Acquisition Mode for Tunnel Packets

- Optional. When performing load balancing, use this command to specify the balancing factor acquisition mode for specific tunnel packets, to optimize traffic balancing.

Command	**aggregateport hash-header {inner | outer | inner-outer}**
Parameter Description	**inner**: Specifies the inner layer in the header of tunnel packets as the source for acquiring the balancing factor. **outer**: Specifies the outer layer in the header of tunnel packets as the source for acquiring the balancing factor. **Inner-outer**: Specifies both the inner and outer layers in the header of tunnel packets as the source for acquiring the balancing factor.
Defaults	The default configuration varies with products.
Command Mode	Global configuration mode
Usage Guide	Use the **default** form of this command to restore the default acquisition mode. After configuration, if the **show running** command does not display the configuration, the configured mode is the same as the default value. The supported configuration options and types of tunnel packets vary with products.

Verification

- Run **show running** to display the configuration.
- Run **show aggregateport load-balance** to display the load balancing configuration. If a device supports load balancing configuration on a specific AP port, run **show aggregateport summary** to display the configuration.
- Run **show load-balance-profile** to display the enhanced load balancing profile.

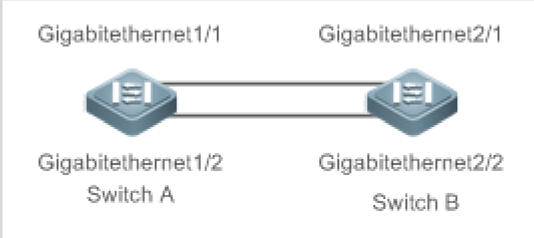
Command	**show aggregateport** ***aggregate-port-number*** **[load-balance | summary]**
Parameter Description	*aggregate-port-number*: Indicates the number of an AP port. **load-balance**: Displays the load balancing algorithm. **summary**: Displays the summary of each link.
Command Mode	Any mode

Usage Guide	The information on All AP ports is displayed if you do not specify the AP port number.
	QTECH# show aggregateport 1 summary AggregatePort MaxPorts SwitchPort Mode Load balance Ports ------------- --------------- ---------- ------ ---------------------------- ------------------------ **Ag1** 8 Enabled ACCESS **dst-mac** **Gi0/2**

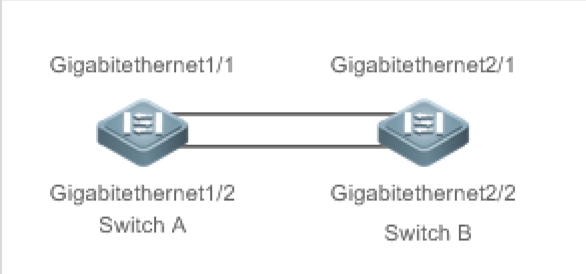
Command	**show load-balance-profile [*profile-name*]**
Parameter Description	*profile-name*: Indicates the profile name.
Command Mode	Any mode
Usage Guide	All enhanced profiles are displayed if you do not specify the profile number.
	QTECH# show load-balance-profile module0 Load-balance-profile: module0 Packet Hash Field: IPv4: src-ip dst-ip IPv6: src-ip dst-ip L2 : src-mac dst-mac vlan MPLS: top-labe l2nd-label

Configuration Example

Configuring a Load Balancing Mode

Scenario **Figure 3-4**	
Configuration Steps	▪ Add the GigabitEthernet 1/1 and GigabitEthernet 1/2 ports on Switch A to static AP port 3. ▪ Add the GigabitEthernet 2/1 and GigabitEthernet 2/2 ports on Switch B to static AP port 3. ▪ On Switch A, configure source MAC address-based load balancing for AP port 3 in global configuration mode. ▪ On Switch B, configure destination MAC address-based load balancing for AP port 3 in global configuration mode.
Switch A	SwitchA# configure terminal SwitchA(config)# interface range GigabitEthernet 1/1-2 SwitchA(config-if-range)# port-group 3 SwitchA(config-if-range)# exit SwitchA(config)# aggregateport load-balance src-mac
Switch B	SwitchB# configure terminal SwitchB(config)# interface range GigabitEthernet 2/1-2 SwitchB(config-if-range)# port-group 3 SwitchB(config-if-range)# exit SwitchB(config)# aggregateport load-balance dst-mac
Verification	▪ Run **show aggregateport load-balance** to check the load balancing algorithm configuration.
Switch A	SwitchA# show aggregatePort load-balance Load-balance : **Source MAC**
Switch B	SwitchB# show aggregatePort load-balance Load-balance : **Destination MAC**

Configuring Hash Load Balancing Control

Scenario Figure 1-7	
Configuration Steps	▪ Add the GigabitEthernet 1/1 and GigabitEthernet 1/2 ports on Switch A to static AP port 3. ▪ Add the GigabitEthernet 2/1 and GigabitEthernet 2/2 ports on Switch B to static AP port 3. ▪ On Switch A, disable hash synchronization for FCoE packets. ▪ On Switch B, disable hash synchronization for FCoE packets. ▪ On Switch A, configure the hash disturbance factor A. ▪ On Switch B, configure the hash disturbance factor B. ▪ On Switch A, enable flexible hash. ▪ On Switch B, enable flexible hash.
Switch A	SwitchA# configure terminal SwitchA(config)# interface range GigabitEthernet 1/1-2 SwitchA(config-if-range)# port-group 3 SwitchA(config-if-range)# exit SwitchA(config)#load-balance-profile SwitchA(config-load-balance-profile)#no hash-symmetrical fcoe SwitchA(config-load-balance-profile)#hash-disturb A SwitchA(config-load-balance-profile)#exit SwitchA(config)#aggregateport hash-elasticity enable
Switch B	SwitchB# configure terminal SwitchB(config)# interface range GigabitEthernet 2/1-2 SwitchB(config-if-range)# port-group 3 SwitchB(config-if-range)# exit SwitchB(config)#load-balance-profile SwitchB(config-load-balance-profile)# no hash-symmetrical fcoe SwitchA(config-load-balance-profile)#hash-disturb B SwitchB(config-load-balance-profile)#exit

	SwitchB(config)#aggregateport hash-elasticity enable
Verification	▪ Run **show running** to check whether the configuration is correct.

Common Errors

A user enables hash synchronization for IPv4, IPv6, FCoE and On packets. However, no configuration is displayed when the user runs **show running**. This is because hash synchronization for IPv4, IPv6, and FCoE packets is enabled by default. After the user disables the function, the configuration is displayed.

3.5.5 Configuring an AP Capacity Mode

Configuration Effect

- Change the maximum number of configurable AP ports and the maximum number of member ports in each AP port.

Notes

- The system has a default AP capacity mode. You can run **show aggregateport capacity** to display the current capacity mode.
- If the current configuration (maximum number of AP ports or the number of member ports in each AP port) exceeds the capacity to be configured, the capacity mode configuration will fail.

Configuration Steps

Configuring an AP Capacity Mode

- (Optional) Perform this configuration to change the AP capacity.
- Perform this configuration on devices that support AP capacity change, such as core switches.

Command	aggregateport capacity mode *capacity-mode*
Parameter Description	*capacity-mode*: Indicates a capacity mode.
Defaults	By default, AP capacity modes vary with devices. For example, 256 x 16 indicates that the device has a maximum of 256 AP ports and 16 member ports in each AP port.
Command Mode	Global configuration mode

Usage Guide	The system provides several capacity modes for devices that support capacity mode configuration. To restore the default settings, run **no aggregateport capacity mode** in global configuration mode.

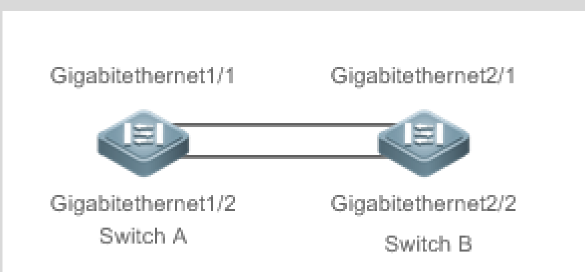
Verification

- Run **show running** to display the configuration.
- Run **show aggregateport capacity** to display the current AP capacity mode and AP capacity usage.

Command	**show aggregateport capacity**
Parameter Description	N/A
Command Mode	Any mode
Usage Guide	N/A
	QTECH# show aggregateport capacity AggregatePort Capacity Information: Configuration Capacity Mode: 128*16. Effective Capacity Mode : 256*8. Available Capacity : 128*8. Total Number: 128, Used: 1, Available: 127.

Configuration Example

Configuring an AP Capacity Mode

Scenario Figure 3-6	

Configuration Steps	▪ Add the GigabitEthernet 1/1 and GigabitEthernet 1/2 ports on Switch A to static AP port 3. ▪ Add the GigabitEthernet 2/1 and GigabitEthernet 2/2 ports on Switch B to static AP port 3. ▪ On Switch A, configure the 128 x128 AP capacity mode. ▪ On Switch B, configure the 256 x 64 AP capacity mode.
Switch A	SwitchA# configure terminal SwitchA(config)# interface range GigabitEthernet 1/1-2 SwitchA(config-if-range)# port-group 3 SwitchA(config-if-range)# exit SwitchA(config)# aggregateport capacity mode 128*128
Switch B	SwitchB# configure terminal SwitchB(config)# interface range GigabitEthernet 2/1-2 SwitchB(config-if-range)# port-group 3 SwitchB(config-if-range)# exit SwitchB(config)# aggregateport capacity mode 256*64
Verification	▪ Run **show aggregateport capacity** to check the AP capacity mode configuration.
Switch A	SwitchA# show aggregatePort capacity AggregatePort Capacity Information: Configuration Capacity Mode: 128*128. Effective Capacity Mode : 128*128. Available Capacity Mode : 128*128. Total Number : 128, Used: 1, Available: 127.
Switch B	SwitchB# show aggregatePort capacity AggregatePort Capacity Information: Configuration Capacity Mode: 256*64. Effective Capacity Mode : 256*64. Available Capacity Mode : 256*64. Total Number : 256, Used: 1, Available: 255.

3.5.6 Enabling BFD for AP Member Ports

Configuration Effect

- Enable BFD for all the member ports of a specified AP port.
- After BFD is enabled for an AP port, each member port performs BFD to determine whether the packets should be distributed to the member port to realize load balancing. When BFD detects a member port Down, the packets are not distributed to the port. When BFD detects that the member port is restored to Up, the packets are distributed to the port again.

Notes

- After BFD is enabled for an AP port, BFD sessions are set up. To make the sessions take effect, you need to configure BFD parameters. For details, see *Configuring BFD*.
- Enabling or disabling BFD for a single AP member port is not supported. You must enable or disable BFD for the entire AP group.
- Only member ports in the forwarding state are enabled with BFD. If a member port is not in the forwarding state because the link or LACP is down, the BFD session on the member port is automatically deleted.
- If only one member port is available (in the forwarding state), all packets are distributed to this port. In this case, BFD fails. When there are more than one available member port, BFD takes effect again.

Configuration Steps

Enabling BFD for AP Member Ports

- (Optional) Enable BFD when you need to detect path failure on member ports in milliseconds. Traffic on the faulty link will be switched to other member links in case of a link failure.
- Perform this configuration on devices that support AP-BFD correlation.

Command	**aggregate bfd-detect {ipv4 | ipv6}** ***src_ip dst_ip***
Parameter Description	**ipv4**: Enables IPv4 BFD if the AP port is configured with an IPv4 address. **ipv6**: Enables IPv6 BFD if the AP port is configured with an IPv6 address. *src_ip*: Indicates the source IP address, that is, the IP address configured on the AP port. *dst_ip*: Indicates the destination IP address, that is, the IP address configured on the peer AP port.
Defaults	By default, BFD is disabled.

Command Mode	Interface configuration mode of the specified AP port
Usage Guide	1. To make BFD sessions take effect, you need to configure BFD parameters. For details, see *Configuring BFD*. 2. Different products may support different IPv4/IPv6 BFD. 3. Both IPv4 BFD and IPv6 BFD can be enabled for an AP port if both are supported. 4. After BFD is enabled for an AP port, BFD sessions are automatically set up on its member ports in the forwarding state.

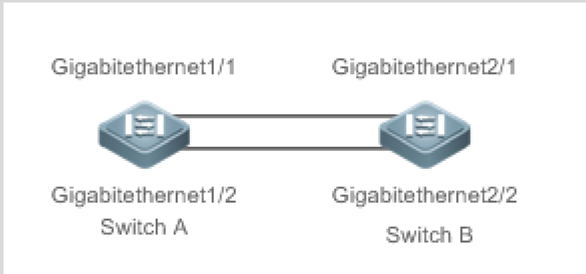
Verification

- Run **show running** to display the configuration.
- Run **show interface aggregateport** to display the BFD state of the AP member ports.

Command	**show interface aggregateport *ap-num***
Parameter Description	*ap-num:* Indicates the number of an AP port.
Command Mode	Any mode
Usage Guide	N/A
	QTECH# show interface aggregateport 11 … Aggregate Port Informations: Aggregate Number: 11 Name: "AggregatePort 11" Members: (count=2) GigabitEthernet 0/1 Link Status: Up Lacp Status: bndl BFD Status: UP GigabitEthernet 0/2 Link Status: Up Lacp Status: susp BFD Status: Invalid …

Configuration Example

Enabling IPv4 BFD for AP Member Ports

Scenario **Figure 3-9**	
Configuration Steps	▪ Enable LACP for the GigabitEthernet 1/1 and GigabitEthernet 1/2 ports on Switch A and add the ports to LACP AP port 3. ▪ Enable LACP for the GigabitEthernet 2/1 and GigabitEthernet 2/2 ports on Switch B and add the ports to LACP AP port 3. ▪ Configure IP address 1.0.0.1 for AP port 3 on Switch A and enable IPv4 BFD. ▪ Configure IP address 1.0.0.2 for AP port 3 on Switch B and enable IPv4 BFD.
Switch A	SwitchA# configure terminal SwitchA(config)# interface range GigabitEthernet 1/1-2 SwitchA(config-if-range)# no switchport SwitchA(config-if-range)# port-group 3 mode active SwitchA(config-if-range)# exit SwitchA(config)# interface aggregateport 3 SwitchA(config-if-Aggregateport 3)# ip address 1.0.0.1 SwitchA(config-if-Aggregateport 3)# aggregate bfd-detect ipv4 1.0.0.1 1.0.0.2 SwitchA(config-if-Aggregateport 3)# bfd interval 50 min_rx 50 multiplier 3
Switch B	SwitchB# configure terminal SwitchB(config)# interface range GigabitEthernet 1/1-2 SwitchB(config-if-range)# no switchport SwitchB(config-if-range)# port-group 3 mode active SwitchB(config-if-range)# exit SwitchB(config)# interface aggregateport 3 SwitchB(config-if-Aggregateport 3)# ip address 1.0.0.2 SwitchB(config-if-Aggregateport 3)# aggregate bfd-detect ipv4 1.0.0.2 1.0.0.1

	SwitchB(config-if-Aggregateport 3)# bfd interval 50 min_rx 50 multiplier 3
Verification	▪ Run **show run** to check whether the configuration takes effect. ▪ Run **show interface aggregateport** to display the BFD state of the AP member ports.
Switch A	SwitchA# show run | include AggregatePort 3 Building configuration... Current configuration: 54 bytes interface AggregatePort 3 no switchport ip address 1.0.0.1 aggregate bfd-detect ipv4 1.0.0.1 1.0.0.2 bfd interval 50 min_rx 50 multiplier 3 SwitchA# show interface aggregateport 3 … Aggregate Port Informations: Aggregate Number: 3 Name: "AggregatePort 3" Members: (count=2) GigabitEthernet 1/1 Link Status: Up Lacp Status: bndl BFD Status: UP GigabitEthernet 1/2 Link Status: Up Lacp Status: bndl BFD Status: UP …
Switch B	SwitchB# show run | include AggregatePort 3 Building configuration... Current configuration: 54 bytes interface AggregatePort 3 no switchport ip address 1.0.0.2 aggregate bfd-detect ipv4 1.0.0.2 1.0.0.1 bfd interval 50 min_rx 50 multiplier 3 SwitchB# show interface aggregateport 3 …

	Aggregate Port Informations: Aggregate Number: 3 Name: "AggregatePort 3" Members: (count=2) GigabitEthernet 1/1 Link Status: Up Lacp Status: bndl BFD Status: UP GigabitEthernet 1/2 Link Status: Up Lacp Status: bndl BFD Status: UP ...

Common Errors

1. If BFD is enabled for an AP port without BFD parameters, BFD does not take effect.
2. After BFD is enabled for an AP port, the BFD neighbor must be a directly connected AP port enabled with BFD.

3.5.7 Configuring a Preferred AP Member Port

Configuration Effect

- Configure a member port as the preferred AP member port.
- After the preferred member port is configured, the management VLAN packets on the AP port are forwarded by this port.

Notes

- For details about management VLAN configuration, see *Configuring MAC*.
- Only one preferred member port can be configured for one AP port.
- After an LACP AP member port is configured as the preferred AP member port, if the LACP negotiation on all AP member ports fails, the preferred port is automatically downgraded to a static AP member port.

Configuration Steps

Configuring a Preferred AP Member Port

- (Optional) Perform this configuration to specify an AP member port dedicated to forwarding management VLAN packets.
- The configuration is applicable to dual-system servers. Configure the port connected to the management NIC of the server as the preferred AP member port.

Command	aggregateport primary-port
Parameter Description	N/A
Defaults	By default, No AP member port is a preferred port.
Command Mode	Interface configuration mode of an AP member port
Usage Guide	N/A

Verification

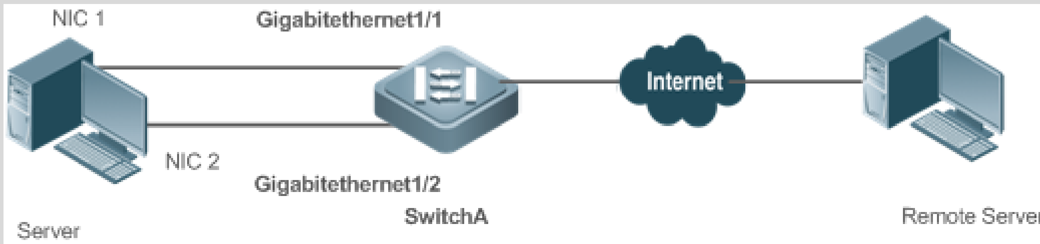
- Run **show running** to display the configuration.
- Run **show interface aggregateport** to display the preferred AP member port.

Command	**show interface aggregateport** ***ap-num***
Parameter Description	*ap-num:* Indicates the number of an AP port.
Command Mode	Any mode
Usage Guide	N/A
	QTECH# show interface aggregateport 11 … Aggregate Port Informations: Aggregate Number: 11 Name: "AggregatePort 11" Members: (count=2) Primary Port: GigabitEthernet 0/1 GigabitEthernet 0/1 Link Status: Up Lacp Status: bndl GigabitEthernet 0/2 Link Status: Up Lacp Status: bndl

	...

Configuration Example

Configuring a Preferred AP Member Port

Scenario **Figure 3-7**	
Configuration Steps	▪ Enable LACP for the GigabitEthernet 1/1 and GigabitEthernet 1/2 ports on Switch A and add the ports to LACP AP port 3. ▪ Configure the GigabitEthernet 1/1 port on Switch A as a preferred port. ▪ Configure VLAN 10 on Switch A as the management VLAN.
Switch A	SwitchA# configure terminal SwitchA(config)# interface range GigabitEthernet 1/1-2 SwitchA(config-if-range)# port-group 3 mode active SwitchA(config-if-range)# exit SwitchA(config)# interface gigabitEthernet 1/1 SwitchA(config-if-GigabitEthernet 1/1) aggregateport primary-port SwitchA(config-if-GigabitEthernet 1/1)# exit SwitchA(config)# aggregateport-admin vlan 10 SwitchA(config)# interface aggregateport 3 SwitchA(config-if-Aggregateport 3)# switchport mode trunk SwitchA(config-if-Aggregateport 3)#
Verification	▪ Run **show run** to check whether the configuration takes effect. ▪ Run **show interface aggregateport** to display the preferred AP member port.
Switch A	SwitchA# show run | include GigabitEthernet 1/1 Building configuration... Current configuration: 54 bytes interface GigabitEthernet 1/1

	aggregateport primary-port portgroup 3 mode active SwitchA# show interface aggregateport 3 … Aggregate Port Informations: Aggregate Number: 3 Name: "AggregatePort 3" Members: (count=2) Primary Port: GigabitEthernet 1/1 GigabitEthernet 1/1 Link Status: Up Lacp Status: bndl GigabitEthernet 1/2 Link Status: Up Lacp Status: bndl …

3.5.8 Configuring the Minimum Number of LACP AP Member Ports

Configuration Effect

- After the minimum number of AP member ports is configured, the aggregation group takes effect only when the number of member ports is greater than the minimum number.

Notes

- If the number of LACP AP member ports for an LACP aggregation group is less than the minimum number of AP member ports configured, all AP member ports are in the unbinding state.
- After the minimum number of static AP member ports is configured, if the number of static AP member ports in the Up state is less than the minimum number, the static AP member ports in the Up state cannot forward data and the corresponding AP is down. However, the state of the peer is not affected. Therefore, corresponding functions must be configured on the peer.

Configuration Steps

Configuring the Minimum Number of AP Member Ports

- (Optional) Perform this configuration to specify the minimum number of AP member ports.

Command	**aggregateport member minimum *number***

Parameter Description	*number*: Indicates the minimum number of member ports.
Defaults	By default, the minimum number of member ports is 1.
Command Mode	Interface configuration mode of the specified AP port
Usage Guide	N/A

Configuring the Minimum Number of AP Member Ports (Action)

- (Optional) Perform this configuration when the number of AP member ports in the Up state is less than the minimum number of the AP member ports.

Command	**aggregateport member minimum action [shutdown]**
Parameter Description	*Shutdown*: shuts down the aggregated port when the number of AP member ports in the Up state is less than the minimum number of the AP member ports.
Defaults	By default, no action is triggered.
Command Mode	Interface configuration mode of the specified AP port
Usage Guide	N/A

Verification

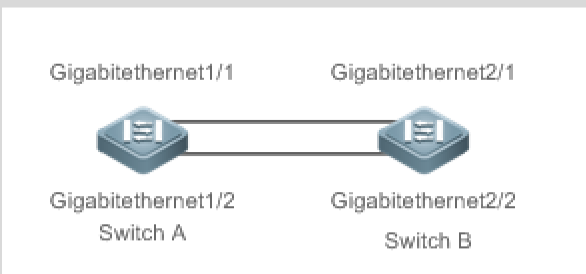
- Run **show running** to display the configuration.
- Run **show interface aggregateport** to display the state of the AP member ports.

Command	**show interface aggregateport *ap-num***
Parameter Description	*ap-num:* Indicates the number of an AP port.
Command Mode	Any mode

Usage Guide	N/A
	QTECH# show interface aggregateport 3 … Aggregate Port Informations: Aggregate Number: 3 Name: "AggregatePort 3" Members: (count=2) GigabitEthernet 0/1 Link Status: Up Lacp Status: bndl GigabitEthernet 0/2 Link Status: Up Lacp Status: bndl …

Configuration Example

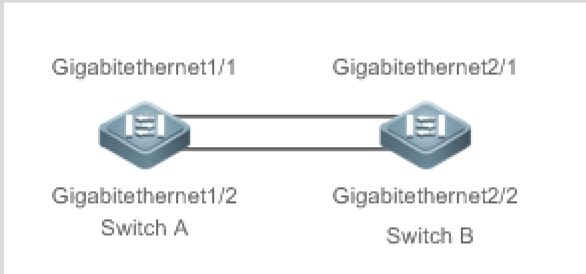
- Configuring the Minimum Number of LACP AP Member Ports, with the Number of LACP AP Member Ports Less Than the Minimum Number of LACP AP Member Ports

Scenario **Figure 3-12**	
Configuration Steps	▪ Enable LACP for the GigabitEthernet 1/1 and GigabitEthernet 1/2 ports on Switch A and add the ports to LACP AP port 3. ▪ Enable LACP for the GigabitEthernet 2/1 and GigabitEthernet 2/2 ports on Switch B and add the ports to LACP AP port 3. ▪ On Switch A, set the minimum number of the member ports of AP port 3 to 3.
Switch A	SwitchA# configure terminal SwitchA(config)# interface range GigabitEthernet 1/1-2 SwitchA(config-if-range)# no switchport

	SwitchA(config-if-range)# port-group 3 mode active SwitchA(config-if-range)# exit SwitchA(config)# interface aggregateport 3 SwitchA(config-if-Aggregateport 3)# aggregateport minimum member 3
Switch B	SwitchB# configure terminal SwitchB(config)# interface range GigabitEthernet 2/1-2 SwitchB(config-if-range)# no switchport SwitchB(config-if-range)# port-group 3 mode active SwitchB(config-if-range)# exit SwitchB(config)# interface aggregateport 3 SwitchB(config-if-Aggregateport 3)# aggregateport minimum member 3
Verification	▪ Run **show run** to check whether the configuration takes effect. ▪ Run **show lacp summery** to display the aggregation state of each AP member port.
Switch A	SwitchA# show LACP summary 3 System Id:32768, 08c6.b3.0001 Flags: S - Device is requesting Slow LACPDUs F - Device is requesting Fast LACPDUs. A - Device is in active mode. P - Device is in passive mode. Aggregate port 3: Local information: LACP port Oper Port Port Port Flags State Priority Key Number State -- Gi1/1 SA bndl 32768 0x3 0x1 0x3d Gi1/2 SA bndl 32768 0x3 0x2 0x3d Partner information: LACP port Oper Port Port Port Flags Priority Dev ID Key Number State --

	Gi1/1 SA 32768 08c6.b3.0002 0x3 0x1 0x3d Gi1/2 SA 32768 08c6.b3.0002 0x3 0x2 0x3d

- Configuring the Minimum Number of LACP AP Member Ports, with the Number of LACP AP Member Ports Not Less Than the Minimum Number of LACP AP Member Ports

Scenario **Figure 1-13**	
Configuration Steps	▪ Enable LACP for the GigabitEthernet 1/1, GigabitEthernet 1/2 and GigabitEthernet 1/3 ports on Switch A and add the ports to LACP AP port 3. ▪ Enable LACP for the GigabitEthernet 2/1, GigabitEthernet2/2 and GigabitEthernet 2/3 ports on Switch B and add the ports to LACP AP port 3. ▪ Set the minimum number of member ports of LACP AP port 3 to 2.
Switch A	SwitchA# configure terminal SwitchA(config)# interface range GigabitEthernet 1/1-3 SwitchA(config-if-range)# no switchport SwitchA(config-if-range)# port-group 3 mode active SwitchA(config-if-range)# exit SwitchA(config)# interface aggregateport 3 SwitchA(config-if-Aggregateport 3)# aggregateport member minimum 2
Switch B	SwitchB# configure terminal SwitchB(config)# interface range GigabitEthernet 2/1-3 SwitchB(config-if-range)# no switchport SwitchB(config-if-range)# port-group 3 mode active SwitchB(config-if-range)# exit SwitchB(config)# interface aggregateport 3 SwitchB(config-if-Aggregateport 3)# aggregateport member minimum 2
Verification	▪ Run **show run** to check whether the configuration is correct. ▪ Run **show lacp summery** to query the status of each member port of the AP port.

Switch A	SwitchA# show LACP summary 3 **System Id:32768, 08c6.b3.0001** Flags: S - Device is requesting Slow LACPDUs F - Device is requesting Fast LACPDUs. A - Device is in active mode. P - Device is in passive mode. **Aggregate port 3:** **Local information:** LACP port Oper Port Port Port Flags State Priority Key Number State -- **Gi1/1 SA bndl 32768 0x3 0x1 0x3d** **Gi1/2 SA bndl 32768 0x3 0x2 0x3d** **Gi1/3 SA bndl 32768 0x3 0x3 0x3d** Partner information: LACP port Oper Port Port Port Flags Priority Dev ID Key Number State --- **Gi1/1 SA 32768 08c6.b3.0002 0x3 0x1 0x3d** **Gi1/2 SA 32768 08c6.b3.0002 0x3 0x2 0x3d** **Gi1/3 SA 32768 08c6.b3.0002 0x3 0x3 0x3d**

Common Errors

The number of LACP AP member ports of an LACP aggregation group is less than the minimum number of AP member ports configured, the LACP aggregation group is not in the binding state.

3.5.9 Enabling the LACP Independent Port Function

Configuration Effect

- After the independent LACP port function is enabled, an LACP member port automatically changes to a common physical port if the LACP member port does not receive LACP packets within the set time-out period. The LACP member port state is changed to **individual** and the LACP member port can forward packets properly.

- After the LACP member port receives LACP packets, it changes to an LACP independent port again to perform LACP packet negotiation.
- The time-out period of an independent port can be adjusted by configuration.

Notes

- After the LACP independent port function is enabled, an LACP member port will not change to a common physical port immediately. An LACP member port changes to an independent port (a common physical port) only if it does not receive LACP packets within the set time-out period,
- The time-out period configuration of LACP independent port only affects LACP member ports that have not turned into independent ports. After the time-out period is configured, the period calculation will restart.
- In the long time-out mode, the LACP packet is sent every 30s. The time-out period should be longer than 30s so as not to affect the normal LACP negotiation. It is recommended to configure the time-out period at least twice the period of LACP packet sending. In the short time-out period, there is no limit.

Configuration Steps

Enabling the LACP Independent Port Function

- Optional
- Perform this operation so that an member port of LACP aggregate group can forward packets normally when the LACP member port cannot perform LACP negotiation.

Command	**lacp individual-port enable**
Parameter Description	N/A
Defaults	By default, the LACP independent port function is disabled.
Command Mode	Interface configuration mode
Usage Guide	N/A

- Configuring the Time-out Period of LACP Independent Port
- Optional
- Perform this operation when an LACP independent port needs to adjust the time-out period.

Command	**lacp individual-timeout period *time***
Parameter Description	*Time:* Time-out period. The range is 10-90, and the unit is second.
Defaults	The time-out period of LACP independent port is 90s by default.
Command Mode	Global configuration mode

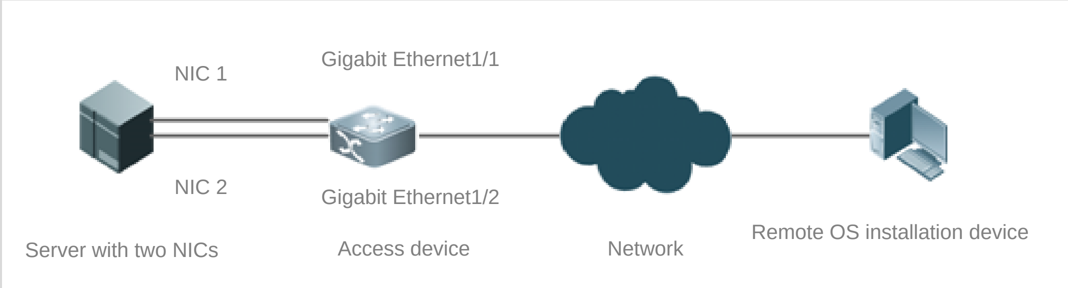
Verification

- Run **show running** to query the corresponding configuration.
- Run **show interface aggregateport** to query the AP member port status.

Command	**show interface aggregateport *ap-num***
Parameter Description	**ap-num**: Indicates the AP number.
Command Mode	All modes
Usage Guide	N/A
Command Presentation	QTECH# show interface aggregateport 3 … Aggregate Port Informations: Aggregate Number: 3 Name: "AggregatePort 3" Members: (count=2) **GigabitEthernet 0/1 Link Status: Up Lacp Status: individual** **GigabitEthernet 0/2 Link Status: Up Lacp Status: individual** …

Configuration Example

- Enabling the LACP Independent Port Function

Scenario **Figure 1-14**	
Description	As shown in Figure 1-14, the server uses NIC 1 and NIC 2 as the communication ports to access to the Gigabitethernet1/1 and Gigabitethernet1/2 ports of the access device. The Gigabitethernet1/1 and Gigabitethernet1/2 ports are added to the LACP aggregation group, for example, AP port 3. A specific VLAN, for example, VLAN 10 is allocated. The LACP independent port function is enabled for the Gigabitethernet1/1 and Gigabitethernet1/2 ports. When the OS is not installed on the server, LACP negotiation between the server and the access device fails. In this case, the Gigabitethernet1/1 and Gigabitethernet1/2 ports of the access device change to common physical ports and are allocated to VLAN 10 automatically. The server uses NIC 1 or NIC 2 to communicate with the remote OS installation device. After the OS is installed, the server connects to the access device in LACP mode.
Configuration Steps	▪ Enable LACP for the GigabitEthernet 1/1 and GigabitEthernet 1/2 ports on the access device and add the ports to LACP AP port 3. ▪ Enable the LACP independent port function for the GigabitEthernet 1/1 and GigabitEthernet 1/2 ports on the access device. ▪ Allocate AP port 3 on the access device to VLAN 10.
Switch A	SwitchA# configure terminal SwitchA(config)# interface range GigabitEthernet 1/1-2 SwitchA(config-if-range)# port-group 3 mode active SwitchA(config-if-range)# lacp individual-port enable SwitchA(config-if-range)# exit SwitchA(config)# interface aggregateport 3 SwitchA(config-if-Aggregateport 3)#switch access vlan 10 SwitchA(config-if-Aggregateport 3)#
Verification	▪ Run **show run** to check whether the configuration is correct. ▪ Run **show lacp summery** to query the status of each member port of the AP port.

Switch A	SwitchA# show LACP summary 3 **System Id:32768, 08c6.b3.0001** Flags: S - Device is requesting Slow LACPDUs F - Device is requesting Fast LACPDUs. A - Device is in active mode. P - Device is in passive mode. **Aggregate port 3:** **Local information:** LACP port Oper Port Port Port Flags State Priority Key Number State -- **Gi1/1 SA individual 32768 0x3 0x1 0x3d** **Gi1/2 SA individual 32768 0x3 0x2 0x3d** Partner information: LACP port Oper Port Port Port Flags Priority Dev ID Key Number State --- **Gi1/1 SA 32768 08c6.b3.0002 0x3 0x1 0x3d** **Gi1/2 SA 32768 08c6.b3.0002 0x3 0x2 0x3d**

3.6 Monitoring

Clearing

Description	**Command**
Clears the statistics of LACP packets on a LACP member port.	clear lacp counters [*key-number* | *interface-type interface-number*]

Displaying

Description	**Command**

Displays the configuration of an enhanced load balancing profile.	**show load-balance-profile** [*profile-name*]
Displays the LACP aggregation state. You can display the information on a specified LACP AP port by specifying *key-number*.	**show lacp summary [*key-numebr*]**
Displays the statistics of LACP packets on LACP member ports. You can display the information on a specified LACP AP port by specifying *key-number*.	**show lacp counters** [*key-numebr*]
Displays the summary or load balancing algorithm of an AP port.	**show aggregateport** [*ap-number*] { **load-balance** | summary }
Displays the capacity mode and usage of an AP port.	**show aggregateport capacity**

Debugging

System resources are occupied when debugging information is output. Therefore, disable debugging immediately after use.

Description	Command
Debugs an AP port.	**debug lsm ap**
Debugs LACP.	**debug lacp { packet | event | database | ha | realtime | stm | timer | all}**

4 CONFIGURING VLAN

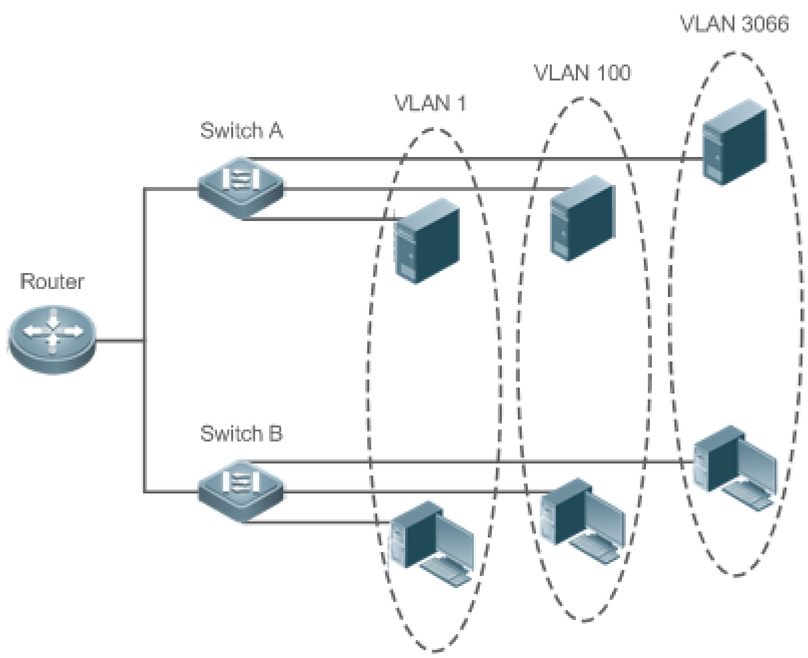
4.1 Overview

A Virtual Local Area Network (VLAN) is a logical network created based on a physical network. A VLAN can be categorized into Layer-2 networks of the OSI model.

A VLAN has the same properties as a common LAN, except for physical location limitation. Unicast, broadcast and multicast frames of Layer 2 are forwarded and transmitted within a VLAN, keeping traffic segregated.

We may define a port as a member of a VLAN, and all terminals connected to this port are parts of a virtual network that supports multiple VLANs. You do not need to adjust the network physically when adding, removing and modifying users. Communication among VLANs is realized through Layer-3 devices, as shown in the following figure.

Figure 5-1



Protocols and Standards

IEEE 802.1Q

4. 2 Applications

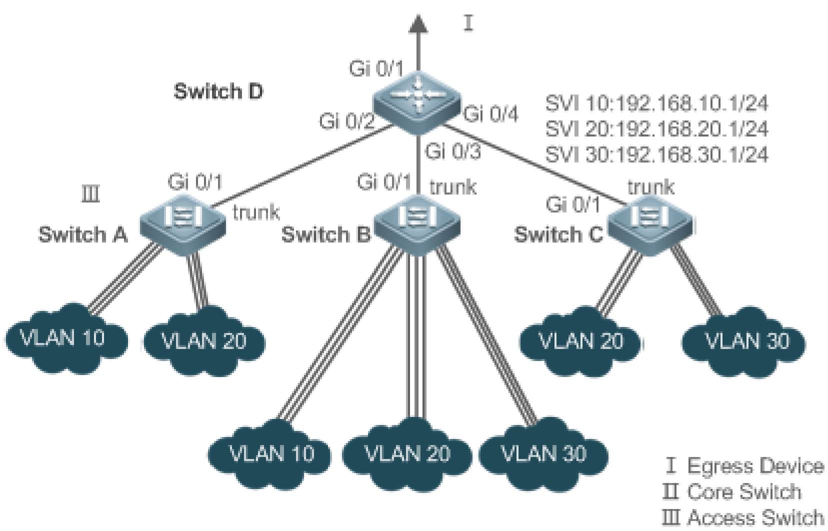
Application	Description
Isolating VLANs at Layer 2 and Interconnecting VLANs at Layer 3	An intranet is divided into multiple VLANs, realizing Layer-2 isolation and Layer-3 interconnection with each other through IP forwarding by core switches.

4.2.1 Isolating VLANs at Layer 2 and Interconnecting VLANs at Layer 3

Scenario

An intranet is divided into VLAN 10, VLAN 20 and VLAN 30, realizing Layer-2 isolation from each other. The three VLANs correspond respectively to the IP sub-networks 192.168.10.0/24, 192.168.20.0/24, and 192.168.30.0/24, realizing interconnection with each other through IP forwarding by Layer-3 core switches.

Figure 5-2



Remarks:	**Switch A, Switch B and Switch C are access switches.** **Configure three VLANs on a core switch and the port connected to the access switches as a Trunk port, and specify a list of allowed-VLANs to realize Layer-2 isolation;** **Configure three SVIs on the core switch, which are the gateway interfaces of the IP sub-networks corresponding to the three VLANs, and configure the IP addresses for these interfaces.**

	Create VLANs respectively on the three access switches, assign Access ports for the VLANs, and specify Trunk ports of the core switch.

Deployment

- Divide an intranet into multiple VLANs to realize Layer-2 isolation among them.
- Configure SVIs on a Layer-3 switch to realize Layer-3 communication among VLANs.

4.3 Features

Basic Concepts

VLAN

A VLAN is a logical network created based on a physical network. A VLAN has the same properties as a common LAN, except for physical location limitation. Unicast, broadcast and multicast frames of Layer 2 are forwarded and transmitted within a VLAN, keeping traffic segregated.

- The VLANs supported by QTECH products comply with the IEEE802.1Q standard. A maximum of 4094 VLANs (VLAN ID 1-4094) are supported, among which VLAN 1 cannot be deleted.
- The configurable VLAN IDs are from 1 to 4094.
- In case of insufficient hardware resources, the system returns information on VLAN creation failure.

Port Mode

You can determine the frames allowed to pass a port and the VLANs which the port belongs to by configuring the port mode. See the following table for details.

Port Mode	Description
Access port	An Access port belongs to only one VLAN, which is specified manually.
Trunk port (802.1Q)	A Trunk port belongs to all the VLANs of an access switch by default, and it can forward the frames of all the VLANs or the frames of allowed-VLANs.
Uplink port	An Uplink port belongs to all the VLANs of an access switch by default, and it can forward the frames of all the VLANs and tag the native VLAN egress traffic.

Hybrid port	A Hybrid port belongs to all the VLANs of an access switch by default, and it can forward the frames of all the VLANs and send frames of VLANs untagged. It can also transmit frames of allowed-VLANs.
Servicechain Port	A service chain port does not learn MAC addresses and can forward packets from any VLAN by default. In addition, no other configuration is allowed.

Overview

Feature	Description
VLAN	VLAN helps realize Layer-2 isolation.

4.3.1 VLAN

Every VLAN has an independent broadcast domain, and different VLANs are isolated on Layer 2.

Working Principle

Every VLAN has an independent broadcast domain, and different VLANs are isolated on Layer 2.

Layer-2 isolation: If no SVIs are configured for VLANs, VLANs are isolated on Layer 2. This means users in these VLANs cannot communicate with each other.

Layer-3 interconnection: If SVIs are configured on a Layer-3 switch for VLANs, these VLANs can communicate with each other on Layer 3.

4.4 Configuration

Configuration	Description and Command	
Configuring Basic VLAN	⚠ (Mandatory) It is used to create a VLAN.	
	vlan	Enters a VLAN ID.
	⚠ (Optional) It is used to configure an Access port to transmit the flows from a single VLAN.	
	switchport mode access	Defines a port as a Layer-2 Access port.

	switchport access vlan	Assigns a port to a VLAN.
	add interface	Adds one Access port or a group of such ports to the current VLAN.
	(Optional) It is used to rename a VLAN.	
	name	Names a VLAN.
[Configuring a Trunk Port]()	(Mandatory) It is used to configure the port as a Trunk port.	
	switchport mode trunk	Defines a port as a Layer-2 Trunk port.
	(Optional) It is used to configure Trunk ports to transmit flows from multiple VLANs.	
	switchport trunk allowed vlan	Configures allowed-VLANs for a Trunk port.
	switchport trunk native vlan	Specifies a native VLAN for a Trunk port.
[Configuring an Uplink Port]()	(Mandatory) It is used to configure the port as an Uplink port.	
	switchport mode uplink	Configures a port as an Uplink port.
	(Optional) It is used to restore the port mode.	
	no switchport mode	Restores the port mode.
[Configuring a Hybrid Port]()	(Mandatory) It is used to configure a port as a Hybrid port.	
	switchport mode hybrid	Configures a port as a Hybrid port.
	(Optional) It is used to transmit the frames of multiple VLANs untagged.	
	no switchport mode	Restores the port mode.
	switchport hybrid allowed vlan	Configures allowed-VLANs for a Hybrid port.
	switchport hybrid native vlan	Configures a default VLAN for a Hybrid port.

Configuring a Service Chain Port	(Mandatory) It is used to configure a port as a service chain port.	
	switchport mode servicechain	Configures a port as a service chain port.
Configuring an Inherited VLAN for an Independent Port	(Mandatory) After a port is configured as an AP, if its member port is changed to independent port, then the independent port uses the inherited VLAN configured on the AP as its allowed VLAN list. If AP does not configure the inherited VLAN for the independent port, the member port inherits the allowed VLAN list of AP as its allowed VLAN list.	
	switchport mode servicechain	Configures a port as a service chain port.

4.4.1 Configuring Basic VLAN

Configuration Effect

- A VLAN is identified by a VLAN ID. You may add, delete, modify VLANs 2 to 4094, but VLAN 1 is created automatically and cannot be deleted. You may configure the port mode, and add or remove a VLAN.

Notes

- N/A

Configuration Steps

Creating and Modifying a VLAN

- Mandatory.
- In case of insufficient hardware resources, the system returns information on VLAN creation failure.
- Use the **vlan** *vlan-id* command to create a VLAN or enter VLAN mode.
- Configuration:

Command	**vlan *vlan-id***
Parameter Description	vlan-id: indicates VLAN ID ranging from 1 to 4094.
Defaults	VLAN 1 is created automatically and is not deletable.

Command Mode	Global configuration mode
Usage Guide	If you enter a new VLAN ID, the corresponding VLAN will be created. If you enter an existing VLAN ID, the corresponding VLAN will be modified. You may use the no vlan *vlan-id* command to delete a VLAN. The undeletable VLANs include VLAN1, the VLANs configured with SVIs, and SubVLANs.

Renaming a VLAN

- Optional.
- You cannot rename a VLAN the same as the default name of another VLAN.
- Configuration:

Command	**name vlan-name**
Parameter Description	vlan-name: indicates a VLAN name.
Defaults	By default, the name of a VLAN is its VLAN ID. For example, the default name of the VLAN 4 is VLAN 0004.
Command Mode	VLAN configuration mode
Usage Guide	To restore the VLAN name to defaults, use the **no name** command.

Assigning Current Access port to a Specified VLAN

- Optional.
- Use the **switchport mode access** command to specify Layer-2 ports (switch ports) as Access ports.
- Use the **switchport access vlan** *vlan-id* command to add an Access port to a specific VLAN so that the flows from the VLAN can be transmitted through the port.

Command	**switchport mode access**
Parameter Description	N/A

Defaults	A switch port is an Access port by default.
Command Mode	Interface configuration mode
Usage Guide	N/A

Command	**switchport access vlan *vlan-id***
Parameter Description	*vlan-id*: indicates a VLAN ID.
Defaults	An Access port is added to VLAN 1 by default.
Command Mode	Interface configuration mode
Usage Guide	If a port is assigned to a non-existent VLAN, the VLAN will be created automatically.

Adding an Access Port to Current VLAN

- Optional.
- This command takes effect only on an Access port. After an Access port is added to a VLAN, the flows of the VLAN can be transmitted through the port.
- Configuration:

Command	**add interface { *interface-id* | range *interface-range* }**
Parameter Description	*interface-id*: indicates a single port. *interface-id*: indicates multiple ports.
Defaults	By default, all Layer-2 Ethernet ports belong to VLAN 1.
Command Mode	VLAN configuration mode

Usage Guide	In VLAN configuration mode, add a specific Access port to a VLAN. This command takes the same effect as command **switchport access vlan** *vlan-id*.

For the two commands of adding a port to a VLAN, the command configured later will overwrite the other one.

Verification

- Send untagged packets to an Access port, and they are broadcast within the VLAN.
- Use commands **show vlan** and **show interface switchport** to check whether the configuration takes effect.

Command	**show vlan [id *vlan-id*]**
Parameter Description	*vlan-id* **:** indicates a VLAN ID.
Command Mode	Any mode
Usage Guide	N/A
Command Display	QTECH(config-vlan)#show vlan id 20 VLAN Name Status Ports ---- -------------------------------- --------- ----------------------------------- **20 VLAN0020 STATIC Gi0/1**

Configuration Example

- Configuring Basic VLAN and Access Port

Configuration Steps	▪ **Create a VLAN and rename it.** ▪ **Add an Access port to the VLAN. There are two approaches. One is:**
	QTECH# configure terminal QTECH(config)# vlan 888

	QTECH(config-vlan)# name test888 QTECH# (config-vlan)# exit QTECH(config)# interface GigabitEthernet 0/3 QTECH(config-if-GigabitEthernet 0/3)# switchport mode access QTECH(config-if-GigabitEthernet 0/3)# switchport access vlan 20 The other approach is adding an Access port (GigabitEthernet 0/3) to VLAN20: QTECH# configure terminal SwitchA(config)#vlan 20 SwitchA(config-vlan)#add interface GigabitEthernet 0/3
Verification	Check whether the configuration is correct.
	QTECH(config-vlan)#show vlan VLAN Name Status Ports ---- ------------------------------- --------- ----------------------------------- 1 VLAN0001 STATIC **20 VLAN0020 STATIC Gi0/3** **888 test888 STATIC** QTECH(config-vlan)# QTECH# show interface GigabitEthernet 0/3 switchport Interface Switchport Mode Access Native Protected VLAN lists ------------------------------- ---------- --------- ------ ------ --------- ------------- GigabitEthernet 0/3 **enabled ACCESS 20 1 Disabled ALL** QTECH# show run !

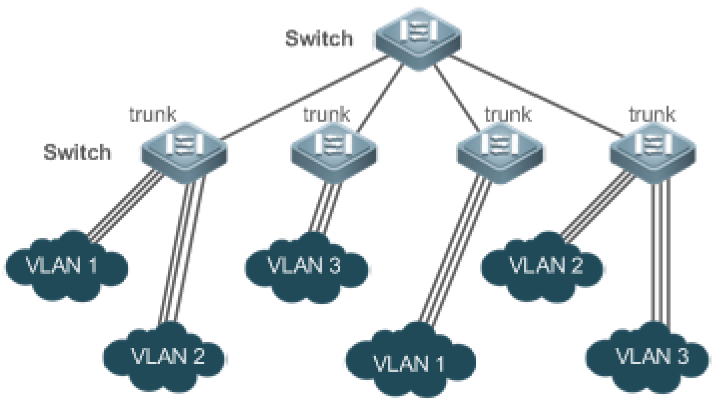
4.4.2 Configuring a Trunk Port

Configuration Effect

A Trunk is a point-to-point link connecting one Ethernet interface or multiple ones to other network devices (for example, a router or switch) and it may transmit the flows from multiple VLANs.

The Trunk of Qtech devices adopts the 802.1Q encapsulation standard. The following figure displays a network adopting a Trunk connection.

Figure 5-3



You may configure an Ethernet port or Aggregate Port (See *Configuring Aggregate Port* for details) as a Trunk port.

You should specify a native VLAN for a Trunk port. The untagged packets received by and sent from the Trunk port are considered to belong to the native VLAN. The default VLAN ID (PVID in the IEEE 802.1Q) of this Trunk port is the native VLAN ID. Meanwhile, frames of the native VLAN sent via the Trunk are untagged. The default native VLAN of a Trunk port is VLAN 1.

When configuring a Trunk link, make sure the Trunk ports at the two ends of the link adopt the same native VLAN.

Configuration Steps

Configuring a Trunk Port

- Mandatory.
- Configure a Trunk port to transmit the flows from multiple VLANs.
- Configuration:

Command	**switchport mode trunk**
Parameter Description	N/A
Defaults	The default mode is Access, which can be modified to Trunk.
Command Mode	Interface configuration mode

Usage Guide	To restore all properties of a Trunk port to defaults, use the **no switchport mode** command.

Defining Allowed-VLANs for a Trunk Port

- Optional.
- By default, a trunk port transmits the flows from all the VLANs (1 to 4094). You may configure a list of allowed-VLANs to prohibit flows of some VLANs from passing through a Trunk port.
- Configuration:

Command	**switchport trunk allowed vlan {all | [add | remove | except | only] }** ***vlan-list***
Parameter Description	The parameter vlan-list can be a VLAN or some VLANs, and the VLAN IDs are connected by "-" in order. For example: 10–20. **all** indicates allowed-VLANs include all VLANs; **add** indicates adding a specific VLAN to the list of allowed-VLANs; **remove** indicates removing a specific VLAN from the list of allowed-VLANs; **except** indicates adding all VLANs except those in the listed VLAN to the list of allowed-VLANs. **only** indicates adding the listed VLANs to the list of allowed-VLANs, and removing the other VLANs from the list.
Defaults	The Trunk port and the Uplink port belong to all VLANs.
Command Mode	Interface configuration mode
Usage Guide	To restore the configuration on a Trunk port to defaults (**all**), use the **no switchport trunk allowed vlan** command.

Configuring a Native VLAN

- Optional.
- A Trunk port receives and sends tagged or untagged 802.1Q frames. Untagged frames transmit the flows from the native VLAN. The default native VLAN is VLAN 1.
- If a frame carries the VLAN ID of a native VLAN, its tag will be stripped automatically when it passes a Trunk port.
- Configuration:

Command	**switchport trunk native vlan** ***vlan-id***

Parameter Description	*vlan-id*: indicates a VLAN ID.
Defaults	The default VALN for a Trunk/Uplink port is VLAN 1.
Command Mode	Interface configuration mode
Usage Guide	To restore the native VLAN of a Trunk port back to defaults, use the **no switchport trunk native vlan** command.

When you set the native VLAN of a port to a non-existent VLAN, this VLAN will not be created automatically. Besides, the native VLAN can be out of the list of allowed-VLANs for this port. In this case, the flows from the native VLAN cannot pass through the port.

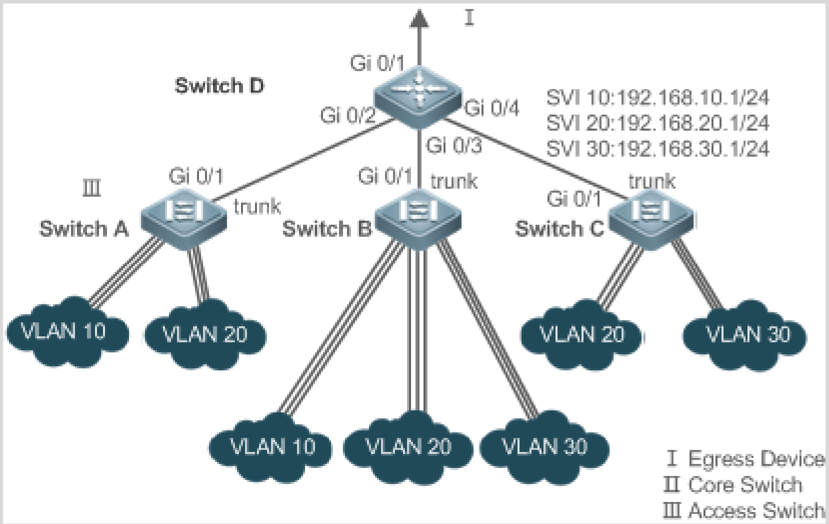
Verification

- Send tag packets to a Trunk port, and they are broadcast within the specified VLANs.
- Use commands **show vlan** and **show interface switchport** to check whether the configuration takes effect.

Command	show vlan [id *vlan-id*]
Parameter Description	*vlan-id* : indicates a VLAN ID.
Command Mode	Any mode
Usage Guide	N/A
Command Display	QTECH(config-vlan)#show vlan id 20 VLAN Name Status Ports ---- ------------------------------- --------- ----------------------------------- **20 VLAN0020 STATIC Gi0/1**

Configuration Example

- Configuring Basic VLAN to Realize Layer-2 Isolation and Layer-3 Interconnection

Scenario **Figure 5-4**	
Configuration Steps	Networking Requirements: As shown in the figure above, an intranet is divided into VLAN 10, VLAN 20 and VLAN 30, realizing Layer-2 isolation from each other. The three VLANs correspond respectively to the IP sub-networks 192.168.10.0/24, 192.168.20.0/24, and 192.168.30.0/24, realizing interconnection with each other through IP forwarding by Layer-3 core switches. Key Points: The following example describes the configuration steps on a core switch and an access switch. ▪ Configure three VLANs on a core switch and the port connected to the access switches as a Trunk port, and specify a list of allowed-VLANs to realize Layer-2 isolation. ▪ Configure three SVIs on the core switch, which are the gateway interfaces of the IP sub-networks corresponding to the three VLANs, and configure the IP addresses for these interfaces. ▪ Create VLANs respectively on the three access switches, assign Access ports for the VLANs, and specify Trunk ports of the core switch. The following example describes the configuration steps on Switch A.
D	D#configure terminal D(config)#vlan 10 D(config-vlan)#vlan 20 D(config-vlan)#vlan 30

	D(config-vlan)#exit D(config)#interface range GigabitEthernet 0/2-4 D(config-if-range)#switchport mode trunk D(config-if-range)#exit D(config)#interface GigabitEthernet 0/2 D(config-if-GigabitEthernet 0/2)#switchport trunk allowed vlan remove 1-4094 D(config-if-GigabitEthernet 0/2)#switchport trunk allowed vlan add 10,20 D(config-if-GigabitEthernet 0/2)#interface GigabitEthernet 0/3 D(config-if-GigabitEthernet 0/3)#switchport trunk allowed vlan remove 1-4094 D(config-if-GigabitEthernet 0/3)#switchport trunk allowed vlan add 10,20,30 D(config-if-GigabitEthernet 0/3)#interface GigabitEthernet 0/4 D(config-if-GigabitEthernet 0/4)#switchport trunk allowed vlan remove 1-4094 D(config-if-GigabitEthernet 0/4)#switchport trunk allowed vlan add 20,30 D#configure terminal D(config)#interface vlan 10 D(config-if-VLAN 10)#ip address 192.168.10.1 255.255.255.0 D(config-if-VLAN 10)#interface vlan 20 D(config-if-VLAN 20)#ip address 192.168.20.1 255.255.255.0 D(config-if-VLAN 20)#interface vlan 30 D(config-if-VLAN 30)#ip address 192.168.30.1 255.255.255.0 D(config-if-VLAN 30)#exit
A	A#configure terminal A(config)#vlan 10 A(config-vlan)#vlan 20 A(config-vlan)#exit A(config)#interface range GigabitEthernet 0/2-12 A(config-if-range)#switchport mode access A(config-if-range)#switchport access vlan 10 A(config-if-range)#interface range GigabitEthernet 0/13-24 A(config-if-range)#switchport mode access A(config-if-range)#switchport access vlan 20 A(config-if-range)#exit

	A(config)#interface GigabitEthernet 0/1 A(config-if-GigabitEthernet 0/1)#switchport mode trunk
Verification	Display the VLAN configuration on the core switch. ▪ Display VLAN information including VLAN IDs, VLAN names, status and involved ports. ▪ Display the status of ports Gi 0/2, Gi 0/3 and Gi 0/4.
D	D#show vlan VLAN Name Status Ports ---- -------- -------- ------------------------------- 1 VLAN0001 STATIC Gi0/1, Gi0/5, Gi0/6, Gi0/7 Gi0/8, Gi0/9, Gi0/10, Gi0/11 Gi0/12, Gi0/13, Gi0/14, Gi0/15 Gi0/16, Gi0/17, Gi0/18, Gi0/19 Gi0/20, Gi0/21, Gi0/22, Gi0/23 Gi0/24 10 VLAN0010 STATIC Gi0/2, Gi0/3 20 VLAN0020 STATIC Gi0/2, Gi0/3, Gi0/4 30 VLAN0030 STATIC Gi0/3, Gi0/4 D#show interface GigabitEthernet 0/2 switchport Interface Switchport Mode Access Native Protected VLAN lists ------------------------------- ---------- --------- ------ ------ --------- -------------- GigabitEthernet 0/2 enabled TRUNK 1 1 Disabled 10,20 D#show interface GigabitEthernet 0/3 switchport Interface Switchport Mode Access Native Protected VLAN lists ------------------------------- ---------- --------- ------ ------ --------- -------------- GigabitEthernet 0/3 enabled TRUNK 1 1 Disabled 10,20,30 D#show interface GigabitEthernet 0/4 switchport Interface Switchport Mode Access Native Protected VLAN lists ------------------------------- ---------- --------- ------ ------ --------- -------------- GigabitEthernet 0/4 enabled TRUNK 1 1 Disabled 20,30

Common Errors

N/A

4.4.3 Configuring an Uplink Port

Configuration Effect

- An Uplink port is usually used in QinQ (the IEEE 802.1ad standard) environment, and is similar to a Trunk port. Their difference is that an Uplink port only transmits tagged frames while a Trunk port sends untagged frames of the native VLAN.

Configuration Steps

Configuring an Uplink Port

- Mandatory.
- Configure an Uplink port to transmit the flows from multiple VLANS, but only tagged frames can be transmitted.
- Configuration:

Command	**switchport mode uplink**
Parameter Description	N/A
Defaults	The default mode is Access, which can be modified to Uplink.
Command Mode	Interface configuration mode
Usage Guide	To restore all properties of an Uplink port to defaults, use the **no switchport mode** command.

Defining Allowed-VLANs for a Trunk Port

- Optional.
- You may configure a list of allowed-VLANs to prohibit flows of some VLANs from passing through an Uplink port.
- Configuration:

Command	**switchport trunk allowed vlan { all | [add | remove | except | only] }** ***vlan-list***

Parameter Description	The parameter *vlan-list* can be a VLAN or some VLANs, and the VLAN IDs are connected by "-" in order. For example: 10–20. **all** indicates allowed-VLANs include all VLANs; **add** indicates adding a specific VLAN to the list of allowed-VLANs; **remove** indicates removing a specific VLAN from the list of allowed-VLANs; **except** indicates adding all VLANs except those in the listed VLAN to the list of allowed-VLANs; and **only** indicates adding the listed VLANs to the list of allowed-VLANs, and removing the other VLANs from the list.
Command Mode	Interface configuration mode
Usage Guide	To restore the allowed-VLANs to defaults (**all**), use the **no switchport trunk allowed vlan** command.

Configuring a Native VLAN

- Optional.
- If a frame carries the VLAN ID of a native VLAN, its tag will not be stripped when it passes an Uplink port. This is contrary to a Trunk port.
- Configuration:

Command	**switchport trunk native vlan *vlan-id***
Parameter Description	*vlan-id*: indicates a VLAN ID.
Command Mode	Interface configuration mode
Usage Guide	To restore the native VLAN of an Uplink to defaults, use the **no switchport trunk native vlan** command.

Verification

- Send tag packets to an Uplink port, and they are broadcast within the specified VLANs.

- Use commands **show vlan** and **show interface switchport** to check whether the configuration takes effect.

Command	**show vlan [id *vlan-id*]**
Parameter Description	*vlan-id* : indicates a VLAN ID.
Command Mode	Any mode
Usage Guide	N/A
Command Display	QTECH(config-vlan)#show vlan id 20 VLAN Name Status Ports ---- -------------------------------- --------- ----------------------------------- 20 VLAN0020 STATIC Gi0/1

Configuration Example

Configuring an Uplink Port

Configuration Steps	**The following is an example of configuring Gi0/1 as an Uplink port.**
	QTECH# configure terminal QTECH(config)# interface gi 0/1 QTECH(config-if-GigabitEthernet 0/1)# switchport mode uplink QTECH(config-if-GigabitEthernet 0/1)# end
Verification	Check whether the configuration is correct.
	QTECH# show interfaces GigabitEthernet 0/1 switchport Interface Switchport Mode Access Native Protected VLAN lists -------------------------------- ---------- --------- ------ ------ --------- -----------------

	GigabitEthernet 0/1 enabled **UPLINK** 1 1 disabled ALL

4.4.4 Configuring a Hybrid Port

Configuration Effect

- A Hybrid port is usually used in SHARE VLAN environment. By default, a Hybrid port is the same as a Trunk port. Their difference is that a Hybrid port can send the frames from the VLANs except the default VLAN in the untagged format.

Configuration Steps

Configuring a Hybrid Port

- Mandatory.
- Configure a Hybrid port to transmit the flows from multiple VLANs.
- Configuration:

Command	**switchport mode hybrid**
Parameter Description	N/A
Defaults	The default mode is Access, which can be modified to Hybrid.
Command Mode	Interface configuration mode
Usage Guide	To restore all properties of a Hybrid port to defaults, use the **no switchport mode** command.

Defining Allowed-VLANs for a Hybrid Port

- Optional.
- By default, a Hybrid port transmits the flows from all the VLANs (1 to 4094). You may configure a list of allowed-VLANs to prohibit flows of some VLANs from passing through a Hybrid port.
- Configuration:

Command	**switchport hybrid allowed vlan [[add | only] tagged | [add] untaged | remove] *vlan_list***
Parameter Description	*vlan-id*: indicates a VLAN ID.
Defaults	By default a Hybrid port belongs to all VLANs. The port is added to the default VLAN in untagged form and to the other VLANs in the tagged form.
Command Mode	Interface configuration mode
Usage Guide	N/A

Configuring a Native VLAN

- Optional.
- If a frame carries the VLAN ID of a native VLAN, its tag will be stripped automatically when it passes a Hybrid port.
- Configuration:

Command	**switchport hybrid native vlan *vlan_id***
Parameter Description	*vlan-id*: indicates a VLAN ID.
Defaults	The default native VLAN is VLAN 1.
Command Mode	Interface configuration mode
Usage Guide	To restore the native VLAN of a Hybrid port to defaults, use the no switchport hybrid native vlan command.

Verification

- Send tagged packets to an Hybrid port, and they are broadcast within the specified VLANs.
- Use commands **show vlan** and **show interface switchport** to check whether the configuration takes effect.

Command	show vlan [id *vlan-id*]
Parameter Description	*vlan-id* **:** indicates a VLAN ID.
Command Mode	Any mode
Usage Guide	N/A
Command Display	QTECH(config-vlan)#show vlan id 20 VLAN Name Status Ports ---- -------------------------------- --------- ----------------------------------- **20 VLAN0020 STATIC Gi0/1**

Configuration Example

Configuring a Hybrid Port

Configuration Steps	**The following is an example of configuring Gi0/1 as a Hybrid port.**
	QTECH# configure terminal QTECH(config)# interface gigabitEthernet 0/1 QTECH(config-if-GigabitEthernet 0/1)# switchport mode hybrid QTECH(config-if-GigabitEthernet 0/1)# switchport hybrid native vlan 3 QTECH(config-if-GigabitEthernet 0/1)# switchport hybrid allowed vlan untagged 20-30 QTECH(config-if-GigabitEthernet 0/1)# end
Verification	Check whether the configuration is correct.
	QTECH(config-if-GigabitEthernet 0/1)#show run interface gigabitEthernet 0/1 Building configuration...

	Current configuration : 166 bytes interface GigabitEthernet 0/1 switchport switchport mode hybrid switchport hybrid native vlan 3 switchport hybrid allowed vlan add untagged 20-30

4.4.5 Configuring a Service Chain Port

Configuration Effect

- In normal cases, the service chain port is used at layer 2 diversion environment. By default, the service chain port does not learn MAC addresses and can forward packets from any VLAN. In addition, it is deployed in transparent mode to divert layer-2 and layer-3 packets.

Configuration Steps

Configuring a Service Chain Port

- Mandatory.
- Perform this operation to configure a port as a service chain port.
- Perform this operation on the switch.

Command	**switchport mode servicechain**
Parameter Description	N/A
Defaults	The default mode is **ACCESS**.
Command Mode	Interface configuration model
Usage Guide	Before changing a port from an access, trunk, hybrid, uplink, or 802.1Q tunnel port to a service chain port, clear other configurations on the port and changes the port to an access port first. To restore the default settings, run **no switchport mode** in interface configuration mode.

Verification

- The service chain port does not learn the MAC address when packets with tags are sent over the service chain port. In addition, packets are transmitted regardless of the carried tag and whether the VLAN is created.

Configuration Example

- Configuring a Service Chain Port

Only configuration related to the service chain port is described.

Configuration Steps	Configure the Gi0/1 port as a service chain port.
	QTECH# configure terminal QTECH(config)# interface gigabitEthernet 0/1 QTECH(config-if-GigabitEthernet 0/1)# switchport mode servicechain QTECH(config-if-GigabitEthernet 0/1)# end
Verification	Run **show run** to check whether the configuration is correct.
	QTECH(config-if-GigabitEthernet 0/1)#show run interface gigabitEthernet 0/1 Building configuration... Current configuration : 166 bytes interface GigabitEthernet 0/1 switchport switchport mode **servicechain**

4.4.6 Configuring an Inherited VLAN for an Independent Port

Configuration Effect

- Only trunk, uplink, and hybrid ports support this configuration. After the extend VLAN list of a trunk or uplink port is specified, when this port is an AP and a member port of the AP is changed to an independent port, the member port uses the extend VLAN list configured on the AP as the allowed VLAN list. Likewise, after the extend VLAN list of a hybrid port is specified, the extend VLAN list is used as the allowed VLAN list of a member hybrid port, and a member hybrid port that is changed to an independent port will also inherit the tag VLAN list of the AP.

Configuration Steps

- Configuring an Inherited VLAN for an Independent Port
- Mandatory.
- Perform this operation on the switch. In PXE OS installation scenarios, perform this operation on an AP.

Command	**switchport individual-port extend-vlan *vlan-list***
Parameter Description	N/A
Defaults	No inherited VLAN is configured by default.
Command Mode	Interface configuration mode of a switch port
Usage Guide	To disable this function, use the **no switchport individual-port extend-vlan** or **default switchport individual-port extend-vlan** command. Only trunk, uplink, and hybrid ports support this configuration.

Verification

- Run the **show run** command to check whether the **switchport individual-port extend-vlan** command exists on the interface.

Configuration Example

- Configuring an Inherited VLAN for an Independent Port

Only the configuration related to inherited VLANs of independent ports is described.

Configuration Steps	**The following is an example of this command:**
	QTECH# configure terminal QTECH(config)# interface gigabitEthernet 0/1 QTECH(config-if-GigabitEthernet 0/1) switchport mode trunk QTECH(config-if-GigabitEthernet 0/1) switchport individual-port extend-vlan 10
Verification	Run the **show run** command to check whether the configuration is correct.
	QTECH(config-if-GigabitEthernet 0/1)#show run Building configuration...

	Current configuration : 166 bytes interface GigabitEthernet 0/1 switchport individual-port extend-vlan 10

4.5 Monitoring

Displaying

Description	Command
Displays VLAN configuration.	show vlan
Displays configuration of switch ports.	**show interface switchport**

Debugging

⚠ System resources are occupied when debugging information is output. Disable the debugging switch immediately after use.

Description	Command
Debugs VLANs.	debug bridge vlan

5 CONFIGURING MAC VLAN

5.1 Overview

The MAC VLAN function refers to assigning VLANs based on MAC addresses, which is a new method of VLAN assignment. This function is often used with 802.1Xdynamic VLAN assignment to implement secure and flexible access of 802.1Xterminals. After an 802.1Xuser passes authentication, the access switch automatically generates a MAC VLAN entry based on the VLAN and user MAC address pushed by the authentication server. A network administrator can also configure the association between a MAC address and a VLAN on the switch in advance.

Protocols

IEEE 802.1Q: Virtual Bridged Local Area Networks and Standards

5.2 Applications

Application	Description
Configuring MAC VLAN	Configures the MAC VLAN function to assign VLANs based on users' MAC addresses. When the physical location of a user changes, i.e. switching from one switch to another, it is unnecessary to re-configure the VLAN of the port used by the user.

5.2.1 Configuring MAC VLAN

Scenario

With popularization of mobile office, terminal devices usually do not use fixed ports for network access. A terminal device may use port A to access the network this time, but use port B to access the network next time. If the VLAN configurations of ports A and B are different, the terminal device will be assigned to a different VLAN in the second access, and fail to use the resources of the previous VLAN. If the VLAN configurations of ports A and B are the same, security issues may be introduced when port B is assigned to other terminal devices. How to allow hosts of different VLANs to access the network on the same port? The MAC VLAN function is hereby introduced.

The biggest advantage of MAC VLAN lies in that when the physical location of a user changes, i.e. switching from one switch to another, it is unnecessary to re-configure the VLAN of the port used by the user. Therefore, MAC address-based VLAN assignment can be regarded as user-based.

Deployment

- Configure or push MAC VLAN entries on a layer-2 switch or wireless device to assign VLANs based on users' MAC addresses.

5.3 Overview

Feature

Feature	Description

Configuring MAC VLAN	Configures the MAC VLAN function to assign VLANs based on users' MAC addresses.

5.3.1 Configuring MAC VLAN

Working Principle

When a switch receives a packet, the switch compare the source MAC address of the packet with the MAC address specified in a MAC VLAN entry. If they match, the switch forwards the packet to the VLAN specified in the MAC VLAN entry. If they don't match, the VLAN to which the data stream belongs is still determined by the VLAN assignment rule of the port.

To ensure that a PC is assigned to a specified VLAN no matter which switch it is connected to, you can perform configuration by using the following approaches:

- Static configuration by using commands. You can configure the association between a MAC address and a VLAN on a local switch by using commands.
- Automatic configuration by using an authentication server (802.1Xdynamic VLAN assignment). After a user passes authentication, a switch dynamically creates an association between the MAC address and a VLAN based on the information provided by the authentication server. When the user goes offline, the switch automatically deletes the association. This approach requires that the MAC-VLAN association be configured on the authentication server. For details about 802.1Xdynamic VLAN assignment, refer to the Configuring 802.1X.

MAC VLAN entries support both of the two approaches, that is, the entries can be configured on both a local switch and an authentication server. The configurations can take effect only if they are consistent. If the configurations are different, the configuration performed earlier takes effect.

- The MAC VLAN function can be configured on hybrid ports only.
- MAC VLAN entries are effective only for untagged packets, but not effective for tagged packets.
- For MAC VLAN entries statically configured or dynamically generated, the specified VLANs must exist.
- VLANs specified in MAC VLAN entries cannot be Super VLANs (but can be Sub VLANs), Remote VLANs, or Primary VLANs (but can be Secondary VLANs).
- MAC addresses specified in MAC VLAN entries must be unicast addresses.
- MAC VLANs are effective for all hybrid ports that are enabled with the MAC VLAN function.

5.4 Configuration

Configuration	Description and Command	
Enabling MAC VLAN on a Port	⚠ (Mandatory) It is used to enable the MAC VLAN function on a port.	
	mac-vlan enable	Enables MAC VLAN on a port.
Adding a Static MAC VLAN Entry Globally	⚠ (Optional) It is used to bind MAC addresses with VLANs.	
	mac-vlan mac-address	Configures a static MAC VLAN entry.

5.4.1 Enabling MAC VLAN on a Port

Configuration Effect

Enable the MAC VLAN function on a port so that MAC VLAN entries can take effect on the port.

Notes

N/A

Configuration Steps

Enabling MAC VLAN on a Port

- Mandatory.
- By default, the MAC VLAN function is disabled on ports and all MAC VLAN entries are ineffective on the ports.
- Enable MAC VLAN on a switch.

Command	mac-vlan enable
Parameter Description	N/A
Defaults	The MAC VLAN function is disabled on a port.

Command Mode	Interface configuration mode
Usage Guide	N/A

Verification

Run the **show mac-vlan interface** command to display information about the ports enabled with the MAC VLAN function.

Command	**show mac-vlan interface**
Parameter Description	N/A
Command Mode	Privileged configuration mode/Global configuration mode/Interface configuration mode
Usage Guide	N/A
Command Display	QTECH# show mac-vlan interface MAC VLAN is enabled on following interface: --------------------------------------- **FastEthernet 0/1**

Configuration Example

Enabling MAC VLAN on a Port

Configuration Steps	▪ **Enable the MAC VLAN function on the Fast Ethernet 0/10 port.**
	QTECH# configure terminal QTECH(config)# interface FastEthernet0/10 QTECH(config-if-FastEthernet 0/10)# mac-vlan enable

Verification	▪ Check the information about the port enabled with the MAC VLAN function.
	QTECH# show mac-vlan interface MAC VLAN is enabled on following interface: -------------------------------------- **FastEthernet 0/10**

Common Errors

When the MAC VLAN function is enabled on a port, the port is not configured as a layer-2 port (such as switch port or AP port) in advance.

5.4.2 Adding a Static MAC VLAN Entry Globally

Configuration Effect

- Configure a static MAC VLAN entry to bind a MAC addresses with a VLAN. The 802.1p priority can be configured, which is 0 by default.

Notes

N/A

Configuration Steps

Adding a Static MAC VLAN Entry

- Optional.
- To bind a MAC addresses with a VLAN, you should perform this configuration. The 802.1p priority can be configured, which is 0 by default.
- Add a static MAC VLAN entry on a switch.

Command	**mac-vlan mac-address** ***mac-address*** **[mask** ***mac-mask*****] vlan** ***vlan-id*** **[priority** ***pri_val*** **]**
Parameter Description	**mac-address** *mac-address*: Indicates a MAC address. **mask** *mac-mask*: Indicates a mask. **vlan** *vlan-id*: Indicates the associated VLAN. **priority** *pri_val*: Indicates the priority.

Defaults	No static MAC VLAN entry is configured by default.
Command Mode	Global configuration mode
Usage Guide	N/A

- If an untagged packet is matched with a MAC VLAN entry, the packet is modified to the VLAN specified by the MAC VLAN entry once arriving at the switch since the MAC VLAN entry has the highest priority. Subsequent functions and protocols are implemented based on the modified VLAN. Possible influences are as follows:
- If an 802.1Xuser fails to be authenticated, the hybrid port jumps to VLAN 100 specified by the FAIL VLAN function; however, the MAC VLAN entry statically configured redirects all packets of this user to VLAN 200. Consequently, the user cannot implement normal communication in FAIL VLAN 100.
- After an untagged packet is matched with a MAC VLAN entry, the VLAN that triggers MAC address learning is the VLAN redirected based on the MAC VLAN entry.
- For a port that is enabled with the MAC VLAN function, if received packets are matched with both MAC VLAN entries with full F masks and those without full F masks, the packets are processed based on the MAC VLAN entries without full F masks.
- If an untagged packet is matched with both a MAC VLAN entry and a VOICE VLAN entry, the packet priority is modified simultaneously. The priority of the VOICE VLAN entry is used as that of the packet.
- If an untagged packet is matched with both a MAC VLAN entry and a PROTOCOL VLAN entry, the VLAN carried in the packet should be the MAC VLAN.
- The MAC VLAN function is applied only to untagged packets, but not applied to PRIORITY packets (packets whose VLAN tag is 0 and carrying COS PRIORITY information) and the processing actions are uncertain.
- The QoS packet trust model on a switch is disabled by default, which will change PRIORITY of all packets to 0 and overwrite the modification on packet priorities by the MAC VLAN function. Run the mls qos trust cos command in the interface configuration mode to enable the QoS trust model and trust packet priorities.

Deleting All Static MAC VLAN Entries

- Optional.
- To delete all static MAC VLAN entries, you should perform this configuration.

- Perform this configuration on a switch.

Command	no mac-vlan all
Parameter Description	N/A
Command Mode	Global configuration mode
Usage Guide	N/A

Deleting the Static MAC VLAN Entry of a Specified MAC Address

- Optional.
- To delete the MAC VLAN entry of a specified MAC address, you should perform this configuration.
- Perform this configuration on a switch.

Command	**no mac-vlan mac-address** ***mac-address*** **[mask** ***mac-mask*** **]**
Parameter Description	**mac-address** *mac-address*: Indicates a MAC address. **mask** *mac-mask*: Indicates a mask.
Command Mode	Global configuration mode
Usage Guide	N/A

Deleting the Static MAC VLAN Entry of a Specified VLAN

- Optional.
- To delete the MAC VLAN entry of a specified VLAN, you should perform this configuration.
- Perform this configuration on a switch.

Command	**no mac-vlan vlan** ***vlan-id***
Parameter Description	**vlan** *vlan-id*: Indicates a VLAN.

Command Mode	Global configuration mode
Usage Guide	N/A

Verification

- Run the **show mac-vlan static** command to check whether all static MAC VLAN entries are correct.
- Run the **show mac-vlan vlan** *vlan-id* command to check whether the MAC VLAN entry of a specified VLAN is correct.
- Run the **show mac-vlan mac-address** *mac-address* [**mask** *mac-mask*] command to display the MAC VLAN entry of a specified MAC address.

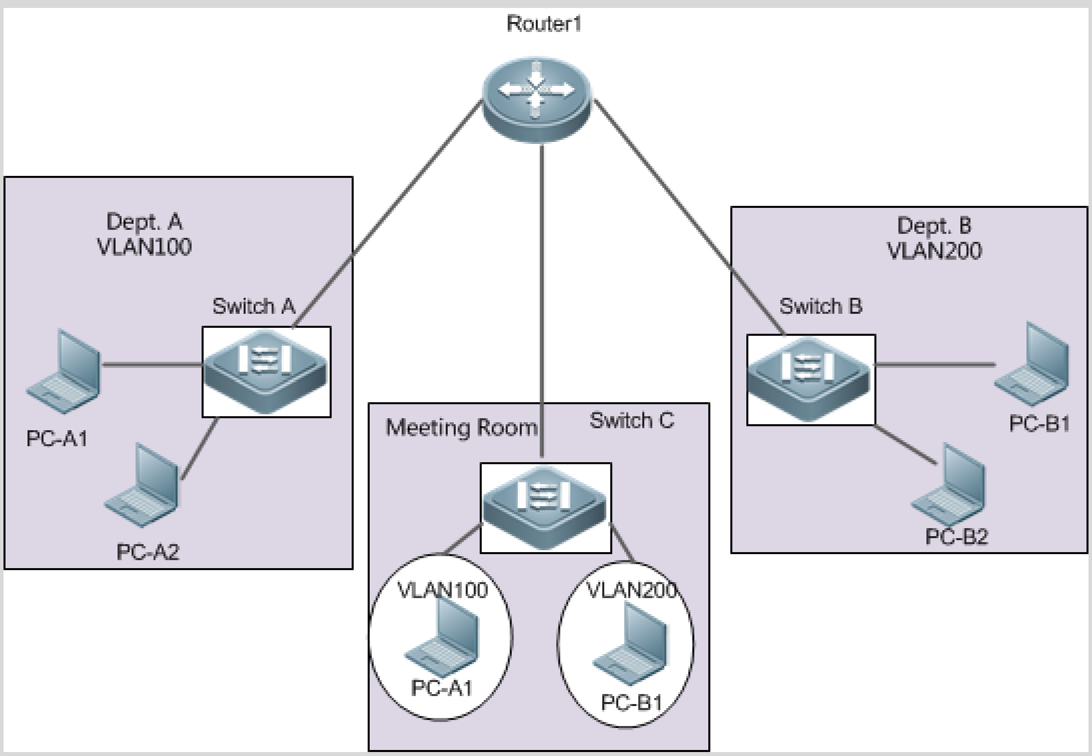
Command	**show mac-vlan static** **show mac-vlan vlan *vlan-id*** **show mac-vlan mac-address *mac-address* [mask *mac-mask*]**
Parameter Description	**vlan** *vlan-id*: Indicates a specified VLAN. **mac-address** *mac-address*: Indicates a specified MAC address. **mask** *mac-mask*: Indicates a specified mask.
Command Mode	Privileged configuration mode/Global configuration mode/Interface configuration mode
Usage Guide	N/A
Command Display	QTECH# show mac-vlan all The following MAC VLAN address exist: S: Static D: Dynamic MAC ADDR MASK VLAN ID PRIO STATE --- **0000.0000.0001 ffff.ffff.ffff 2 0 D** **0000.0000.0002 ffff.ffff.ffff 3 3 S** **0000.0000.0003 ffff.ffff.ffff 3 3 S&D** **Total MAC VLAN address count: 3**

Configuration Example

Adding a Static MAC VLAN Entry Globally

As shown in Figure 6-1,PC-A1 and PC-A2 belong to department A and are assigned to VLAN 100. PC-B1 and PC-B2 belong to department B and are assigned to VLAN 200. Due to employee mobility, the company provides a temporary office at the meeting room but requires that accessed employees be assigned to the VLANs of their own departments. For example, PC-A1 must be assigned to VLAN 100 and PC-B1 must be assigned to VLAN 200 after access.

Since the access ports for PCs at the meeting room are not fixed, the MAC VLAN function can be used to associate the PC MAC addresses with the VLANs of their departments. No matter which ports the employees use for access, the MAC VLAN function automatically assigns the VLANs of their departments.

Scenario **Figure 6-1**	
Configuration Steps	▪ Configure the port connecting Switch C and Router 1 as a Trunk port. ▪ Configure all ports connecting PCs on Switch C as hybrid ports, enable the MAC VLAN function and modify the default untagged VLAN list. ▪ Configure MAC VLAN entries on Switch C.
A	A# configure terminal A(config)# interface interface_name A(config-if)# switchport mode trunk

	A(config-if)# exit A(config)# interface interface_name A(config-if)# switchport mode hybrid A(config-if)# switchport hybrid allowed vlan add untagged 100,200 A(config-if)# mac-vlan enable A(config-if)# exit A(config)# mac-vlan mac-address PC-A1-mac vlan 100 A(config)# mac-vlan mac-address PC-B1-mac vlan 200
Verification	Check the configured static MAC VLAN entries on Switch C.
A	A# QTECH# show mac-vlan static The following MAC VLAN address exist: S: Static D: Dynamic MAC ADDR MASK VLAN ID PRIO STATE --- **PC-A1-macffff.ffff.ffff 100 0 S** **PC-B1-macffff.ffff.ffff 200 3 S** **Total MAC VLAN address count: 2**

5.5 Monitoring

Displaying

Description	Command
Displays all the MAC VLAN entries, including static and dynamic.	**show mac-vlan all**
Displays the dynamic MAC VLAN entries.	**show mac-vlan dynamic**
Displays the static MAC VLAN entries.	**show mac-vlan static**

Displays the MAC VLAN entries of a specified VLAN.	**show mac-vlan vlan** *vlan-id*
Displays the MAC VLAN entries of a specified MAC address.	**show mac-vlan mac-address** *mac-address* [**mask** *mac-mask*]

Debugging

System resources are occupied when debugging information is output. Therefore, disable debugging immediately after use.

Description	Command
Debugs the MAC VLAN function.	**debug bridge mvlan**

6 CONFIGURING SUPER VLAN

6.1 Overview

Super virtual local area network (VLAN) is an approach to dividing VLANs.Super VLAN is also called VLAN aggregation, and is a management technology tailored for IP address optimization.

Using super VLAN can greatly save IP addresses. Only one IP address needs to be assigned to the super VLAN that consists of multiple sub VLANs, which greatly saves IP addresses and facilitates network management.

6.2 Application

Application	Description
Sharing One IP Gateway Among Multiple VLANs	VLANs are divided to implement layer-2 (L2) isolation of access users. All VLAN users share one IP gateway to implement layer-3 (L3) communication and communication with external networks.

6.2.1 Sharing One IP Gateway Among Multiple VLANs

Scenario

Multiple VLANs are isolated at L2 on a L3 device, but users of these VLANs can perform L3 communication with each other in the same network segment.

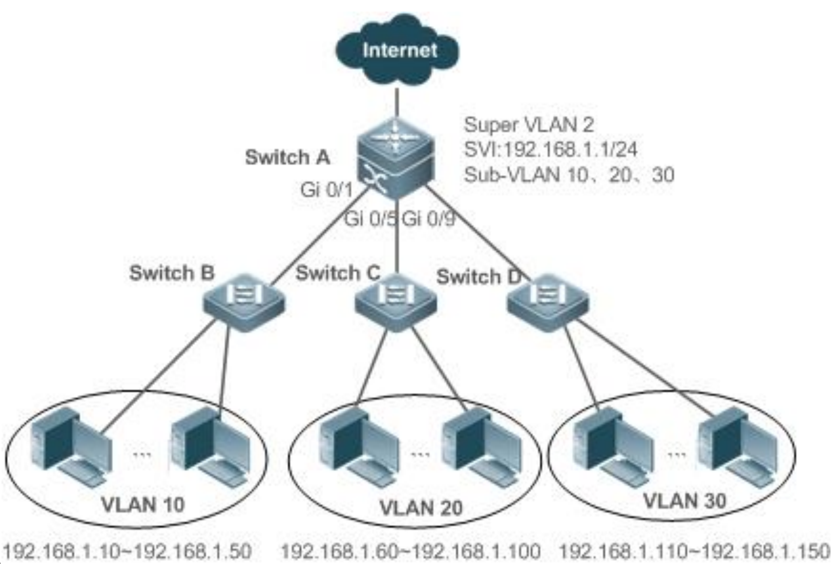


Figure7-1

Remarks	**Switch A is a gateway or core switch.** **Switch B, Switch C, and Switch D are access switches.** **On Switch A, a super VLAN and multiple sub VLANs are configured, and a L3 interface and the IP address of the L3 interface are configured for the super VLAN.** **VLAN 10 is configured on Switch B, VLAN 20 is configured on Switch C, and VLAN 30 is configured on Switch D. Different departments of the company reside in different VLANs.**

Deployment

On the intranet, use the super VLAN so that multiple sub VLANs can share one IP gateway and meanwhile VLANs are mutually isolated at L2.

Users in sub VLANs can perform L3 communication through the gateway of the super VLAN.

6.3 Features

Basic Concepts

Super VLAN

Super VLAN is also called VLAN aggregation, and is a management technology tailored for IP address optimization. It aggregates multiple VLANs to one IP network segment. No physical port can be added to a super VLAN. The switch virtual interface (SVI) is used to manage the cross-VLAN communication of sub VLANs. The super VLAN cannot be used as a common 802.1Q VLAN, but can be treated as the primary VLAN of sub VLANs.

Sub VLAN

A sub VLAN is an independent broadcast domain. Sub VLANs are mutually isolated at L2. Users of sub VLANs of the same or different super VLANs communicate with each other through the L3 SVIs of their own super VLANs.

ARP Proxy

A L3 SVI can be created only for a super VLAN. Users in a sub VLAN communicates with users in other sub VLANs of the same super VLAN or users in other network segments through the ARP proxy and the L3 SVI of the super VLAN. When a user of a sub VLAN sends an ARP request to a user of another sub VLAN, the gateway of the super VLAN uses its own MAC addressto send or respond to the ARP requests. The process is called ARP proxy.

IP Address Range of the Sub VLAN

Based on the gateway IP address configured for the super VLAN, an IP address range can be configured for each sub VLAN.

Overview

Feature	Description
Super VLAN	Create a L3 interface as anSVI to allow all sub VLANs to share the same IP network segment through the ARP proxy.

6.3.1 Super VLAN

Users of all sub VLANs of a super VLAN can be allocated IP addresses in the same IP address range, and share the same IP gateway. Users can implement cross-VLAN communication through this gateway. It is unnecessary to allocate a gateway for every VLAN, which saves the IP addresses.

Working Principle

IP addresses in a network segment are allocated to different sub VLANs that belong to the same super VLAN. Each sub VLAN has an independent broadcast domain of the VLAN, and different sub VLANs are isolated from each other at L2. When users in sub VLANs need to perform L3 communication, the IP address of the SVI of the super VLAN is used as the gateway address. In this way, multiple VLANs share the same IP gateway, and it is unnecessary to configure a gateway for every VLAN. In addition, to implement L3 communication between sub VLANs and between sub VLANs and other network segments, the ARP proxy function is used to forward and process the ARP requests and responses.

L2 communication of sub VLANs: If the SVI is not configured for the super VLAN, sub VLANs of super VLAN are mutually isolated at L2, that is, users in different sub VLANs cannot communicate with each other. If the SVI is configured for the super VLAN, and the gateway of the super VLAN can function as the ARP proxy, users in different sub VLANs of the same super VLAN can communicate with each other. This is because IP addresses of users in different sub VLANs belong to the same network segment, and communication between these users is still treated as L2 communication.

L3 communication of sub VLANs: If users in sub VLANs of a super VLAN need to perform L3 communication across network segments, the gateway of this super VLAN functions as the ARP proxy to respond to the ARP requests in place of sub VLANs.

6.4 Configuration

Configuration Item	Description and Command
	⚠ Mandatory.

[Configuring Basic Functions of the Super VLAN]()	**supervlan**	Configures a super VLAN.
	subvlan*vlan-id-list*	Configures a sub VLAN.
	proxy-arp	Enables the ARP proxy function.
	interface vlan*vlan-id*	Creates a virtual interface for a super VLAN.
	ip address*ip mask*	Configures the IP address of the virtual interface of a super VLAN.
	Optional.	
	subvlan-address-range *start-ip end-ip*	Specifies the IP address range in a sub VLAN.

6.4.1 Configuring Basic Functions of the Super VLAN

Configuration Effect

Enable the super VLAN function and configure an SVI for the super VLAN to implement L2/L3 communication between sub VLANs across VLANs.

Users in all sub VLANs of a super VLAN share the same IP gateway. It is unnecessary to specify a network segment for every VLAN, which saves the IP addresses.

Notes

A super VLAN does not belong to any physical port. Therefore, the device configured with the super VLAN cannot process packets that contain the super VLAN tag.

Both the super VLAN function and the ARP proxy function of each sub VLAN must be enabled.

An SVI and an IP address must be configured for a super VLAN. The SVI is a virtual interface used for communication of users in all sub VLANs.

Configuration Steps

Configuring a Super VLAN

- Mandatory.
- No physical port exists in a super VLAN.

- The ARP proxy function must be enabled. This function is enabled by default.
- You can run the **supervlan** command to change a common VLAN into a super VLAN.
- After a common VLAN becomes a super VLAN, ports added to this VLAN will be deleted from this VLAN because no physical port exists in a super VLAN.

A super VLAN is valid only after you configure sub VLANs for this super VLAN.

VLAN 1 cannot be configured as a super VLAN.

A super VLAN cannot be configured as a sub VLAN of another super VLAN. A sub VLAN of a super VLAN cannot be configured as a super VLAN.

Command	**supervlan**
Parameter Description	N/A
Defaults	By default, a VLAN is a common VLAN.
Command Mode	VLAN configuration mode
Usage Guide	By default, the super VLAN function is disabled. No physical port can be added to a super VLAN. Once a VLAN is not a super VLAN, all its sub VLANs become common static VLANs.

Configuring a Virtual Interface for a Super VLAN

- Mandatory.
- No physical port can be added to a super VLAN. You can configure the L3 SVI for a VLAN.

When a super VLAN is configure with an SVI, it allocates a L3 interface i to each sub VLANs. If a sub VLAN is not allocated a L3 interfacedue to resource deficiency, the sub VLAN becomes a common VLAN again.

Command	**interface vlan*vlan-id***
Parameter Description	*vlan-id*: Indicates the ID of the super VLAN.
Defaults	By default, no super VLAN is configured.
Command Mode	Global configuration mode

Usage Guide	A L3 interface must be configured as the virtual interface of a super VLAN.

Configuring the Gateway of a Super VLAN

- Mandatory.
- The IP gateway on the L3 SVI is configured as the proxy for all users in sub VLANs to respond to ARP requests.

Command	**ip address*ip mask***
Parameter Description	*ip*: Indicates the IP address of the gateway on the virtual interface of a super VLAN. *Mask*: Indicates the mask.
Defaults	By default, no gateway is configured for a super VLAN.
Command Mode	Interface configuration mode
Usage Guide	Run this command to configure the gateway for a super VLAN. Users of all sub VLANs of the super VLAN share this gateway.

Configuring a Sub VLAN

- Mandatory.
- Physical ports can be added to sub VLANs. Sub VLANs of a super VLAN share the gateway address of the super VLAN and reside in the same network segment.
- The ARP proxy function must be enabled. This function is enabled by default.
- You can run the **subvlan***vlan-id-list* command to change a common VLAN into a sub VLAN of a super VLAN. Physical ports can be added to sub VLANs.
- Communication of users in a sub VLAN is managed by the super VLAN.

⚠ You must change a sub VLAN into a common VLAN before you can delete this sub VLAN by running the **no vlan** command.

⚠ One sub VLAN belongs to only one super VLAN.

Command	**subvlan*vlan-id-list***
Parameter Description	*vlan-id-list* : Specifies multiple VLANs as sub VLANs of a super VLAN.

Defaults	By default, a VLAN is a common VLAN.
Command Mode	VLAN configuration mode
Usage Guide	Connection interfaces can be added to a sub VLAN. You must change a sub VLAN into a common VLAN before you can delete this sub VLAN by running the **no vlan** [*id*]command. You cannot configure a L3 SVI of the VLAN for a sub VLAN. If you have configured a L3 SVI for a super VLAN, the attempt of adding more sub VLANs may fail due to resource deficiency. If you configure sub VLANs to a super VLAN, and then configure a L3 SVI of the VLAN for a super VLAN, some sub VLANs may become common VLANs again due to resource deficiency.

Configuring the ARP Proxy

- (Mandatory) The ARP proxy function is enabled by default.
- Users in sub VLANs can implement L2/L3 communication across VLANs through the gateway proxy only after the ARP proxy function is enabled on both the super VLAN and sub VLANs.
- Users in sub VLANs can communicate with users of other VLANs only after the ARP proxy function is enabled on both the super VLAN and sub VLANs.

The ARP proxy function must be enabled on both the super VLAN and sub VLANs.Otherwise, this function does not take effect.

Command	**proxy-arp**
Parameter Description	N/A
Defaults	By default, the ARP proxy function is enabled.
Command Mode	VLAN configuration mode
Usage Guide	By default, the ARP proxy function is enabled. Run this command to enable the ARP proxy function on both the super VLAN and sub VLANs.

	Users in sub VLANs can implement L2/L3 communication across VLANs only after the ARP proxy function is enabled on both the super VLAN and sub VLANs.

Configuring the IP Address Range of the Sub VLAN

- You can allocate an IP address range to each sub VLAN. Users in a sub VLAN can communicate with users of other VLANs only when their IP addresses are in the specified range.
- Unless otherwise specified, you do not need to configure the IP address range.

IP addresses dynamically allocated to users through DHCP may not be in the allocated IP address range. If the IP addresses allocated through DCHP are not in the specified range, users in a sub VLAN cannot communicate with users of other VLANs. Therefore, be cautious in using the **subvlan-address-range** *start-ip end-ip*command.

The IP address range of a sub VLAN must be within the IP address range of the super VLAN to which the sub VLAN belongs.Otherwise, users in sub VLANs cannot communicate with each other.

IP addresses of users in a sub VLAN must be within the IP address range of the sub VLAN.Otherwise, users in the sub VLAN cannot communicate with each other.

Command	**subvlan-address-range** ***start-ip end-ip***
Parameter Description	*start-ip*: Indicates the start IP address of a sub VLAN. *end-ip*: Indicates the end IP address of a sub VLAN.
Defaults	By default, no IP address range is configured.
Command Mode	VLAN configuration mode
Usage Guide	Optional. Run this command to configure the IP address range of users in a sub VLAN. IP address ranges of different sub VLANs of a super VLAN cannot overlap with each other. The IP address range of a sub VLAN must be within the IP address range of the super VLAN to which the sub VLAN belongs. Otherwise, users in sub VLANs cannot communicate with each other. Users in a sub VLAN can communicate with users of other VLANs only when their IP addresses (either dynamically allocated through DHCP or statically configured) are in the configured IP address range.

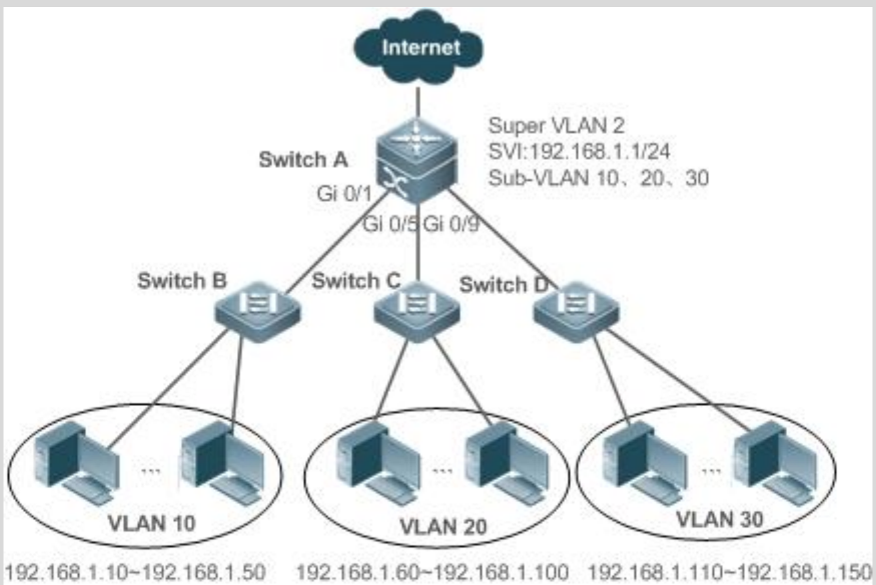
	⚠ IP addresses allocated through DHCP may not be in the configured IP address range. In this case, users in a sub VLAN cannot communicate with users of other VLANs. Therefore, be cautious when using this command.

Verification

After each sub VLAN is correlated with the gateway of the super VLAN, users in sub VLANs can ping each other.

Configuration Example

- Configuring a Super VLAN on the Network so That Users in its Sub VLANs Use the Same Network Segment and Share the Same IP Gateway to Save IP Addresses

Scenario **Figure 7-2**	
Configuration Steps	Perform the related super VLAN configuration on the core switch. On the access switches, configure the common VLANs corresponding to the sub VLANs on the core switch.
A	SwitchA#configure terminal Enter configuration commands, one per line. End with CNTL/Z. SwitchA(config)#vlan 2 SwitchA(config-vlan)#exit SwitchA(config)#vlan 10 SwitchA(config-vlan)#exit

	SwitchA(config)#vlan 20 SwitchA(config-vlan)#exit SwitchA(config)#vlan 30 SwitchA(config-vlan)#exit SwitchA(config)#vlan 2 SwitchA(config-vlan)#supervlan SwitchA(config-vlan)#subvlan 10,20,30 SwitchA(config-vlan)#exit SwitchA(config)#interface vlan 2 SwitchA(config-if-VLAN 2)#ip address 192.168.1.1 255.255.255.0 SwitchA(config)#vlan 10 SwitchA(config-vlan)#subvlan-address-range 192.168.1.10 192.168.1.50 SwitchA(config-vlan)#exit SwitchA(config)#vlan 20 SwitchA(config-vlan)#subvlan-address-range 192.168.1.60 192.168.1.100 SwitchA(config-vlan)#exit SwitchA(config)#vlan 30 SwitchA(config-vlan)#subvlan-address-range 192.168.1.110 192.168.1.150 SwitchA(config)#interface range gigabitEthernet 0/1,0/5,0/9 SwitchA(config-if-range)#switchport mode trunk
Verification	Verify that the source host (192.168.1.10) and the destination host (192.168.1.60) can ping each other.
A	SwitchA(config-if-range)#show supervlan supervlan id supervlan arp-proxy subvlan id subvlan arp-proxy subvlan ip range ------------ ------------------- ---------- ----------------- --------- 2 ON 10 ON192.168.1.10 - 192.168.1.50 20 ON 192.168.1.60 - 192.168.1.100 30 ON 192.168.1.110 - 192.168.1.150

Common Errors

The SVI and IP gateway are not configured for the super VLAN. Consequently, communication fails between sub VLANs and between sub VLANs and other VLANs.

The ARP proxy function is disabled on the super VLAN or sub VLANs. Consequently, users in sub VLANs cannot communicate with users of other VLANs.

The IP address range of the sub VLAN is configured, but IP addresses allocated to users are not in this range.

6.5 Monitoring

Displaying

Description	Command
Displays the super VLAN configuration.	**show supervlan**

Debugging

System resources are occupied when debugging information is output. Therefore, disable debugging immediately after use.

Description	Command
Debugs the super VLAN.	**debug bridge svlan**

7 CONFIGURING PROTOCOL VLAN

7.1 Overview

The protocol VLAN technology is a VLAN distribution technology based on the packet protocol type. It can distribute packets of a certain protocol type with a null VLAN ID to the same VLAN. That is, the switch, based on the protocol type and encapsulation format of packets received by ports, matches the received untagged packets with protocol profiles. If the matching is successful, the switch automatically distributes the packets to a relevant VLAN for transmission. There are two types of protocol VLANs: IP address-based protocol VLAN and protocol VLAN based on the packet type and Ethernet type on ports. The protocol VLAN based on the packet type and Ethernet type on ports is called protocol VLAN for short and the IP address-based protocol VLAN is called subnet VLAN for short.

The protocol VLAN is applicable only to Trunk ports and Hybrid ports.

Protocols and Standards

IEEE standard 802.1Q

7.2 Applications

Application	Description
Configuration and Application of Protocol VLAN	Implements Layer-2 communication isolation of user hosts that use different protocol packets for communication to reduce the network traffic.
Configuration and Application of Subnet VLAN	Specifies the VLAN range based on the IP network segment to which user packets belong.

7.2.1 Configuration and Application of Protocol VLAN

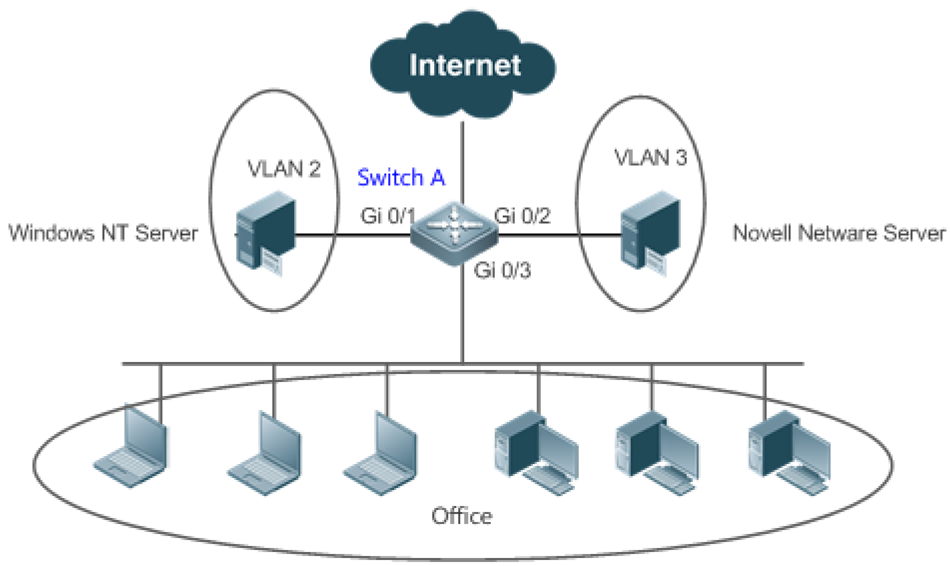
Scenario

As shown in the following figure, the network architecture is composed of the interconnected Windows NT server and Novell Netware server and the office area is connected to the Layer-3 device Switch A through a hub. There are different PCs in the office area. Some PCs use the Windows NT operating system (OS) and support the IP protocol, and some PCs use the Novell Netware OS and support the IPX protocol. PCs in the office area communicate with the external network and servers through the uplink port Gi 0/3.

The main requirements are as follows:

- The Layer-2 communication of PCs using the Windows NT OS is isolated from that of PCs using the Novell Netware OS, so as to reduce the network traffic.

Figure 8-1



Remarks	**Switch A is a switch and Port Gi 0/3 is a Hybrid port. Port Gi 0/1 is an Access port and belongs to VLAN 2. Port Gi 0/2 is also an Access port and belongs to VLAN 3.**

Deployment

- Configure profiles of the packet type and Ethernet type (in this example, configure Profile 1 for IP protocol packets and configure Profile 2 for IPX protocol packets).
- Apply the profiles to the uplink port (Port Gi 0/3 in this example) and associate them with VLANs (in this example, associate Profile 1 with VLAN 2 and associate Profile 2 with VLAN 3).

⚠ The configured protocol VLANs take effect only on the Trunk ports and Hybrid ports.

7.2.2 Configuration and Application of Subnet VLAN

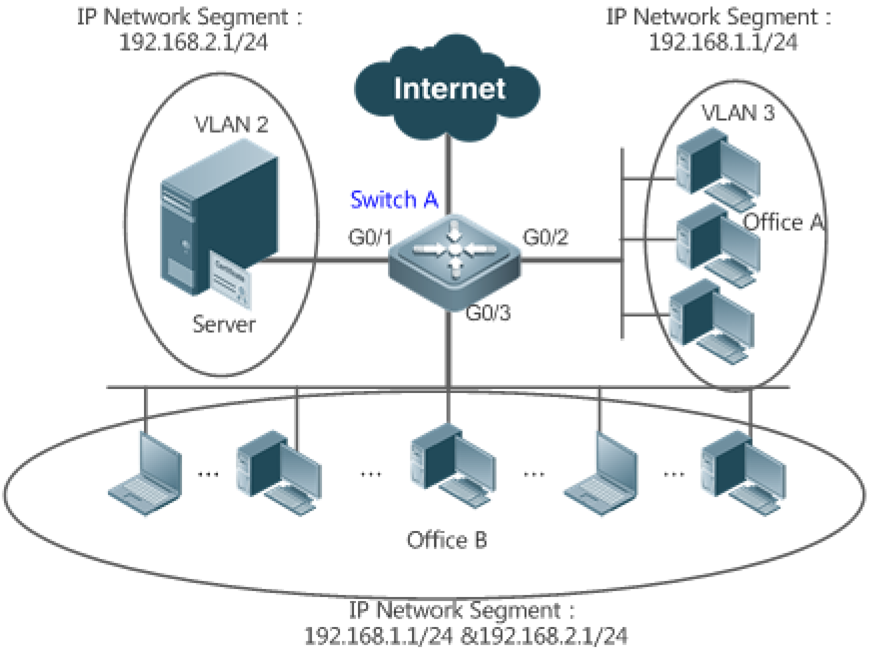
Scenario

As shown in the following figure, PCs in Office A and Office B are connected to the Layer-3 device Switch A through hubs. In Office A, the PCs belong to a fixed network segment and they are distributed to the same VLAN by port. In Office B, the PCs belong to two network segments, but they cannot be distributed to VLANs by fixed port.

The main requirements are as follows:

For PCs in Office B, Switch A can determine the VLAN range of the PCs based on the IP network segment to which their packets belong.

Figure 8-2



Remarks	Switch A is a switch. Port G0/1 is an Access port and belongs to VLAN 2. Port G0/2 is also an Access port and belongs to VLAN 3. Port G0/3 is a Hybrid port.

Deployment

- Globally configure subnet VLANs (in this example, allocate the IP network segment 192.168.1.1/24 to VLAN 3 and the IP network segment 192.168.2.1/24 to VLAN 2) and enable the subnet VLAN function on the uplink port (Port Gi 0/3 in this example).

⚠ The configured subnet VLANs take effect only on the Trunk ports and Hybrid ports.

7.3 Features

Basic Concepts

Protocol VLAN

The protocol VLAN technology is a VLAN distribution technology based on the packet protocol type. It can distribute packets of a certain protocol type with a null VLAN ID to the same VLAN.

VLANs need to be specified for packets received by device ports so that a packet belongs to a unique VLAN. There are three possible cases:

- If a packet contains a null VLAN ID (untagged or priority packet) and the device supports only port-based VLAN distribution, the VLAN ID in the tag added to the packet is the PVID of the input port.
- If a packet contains a null VLAN ID (untagged or priority packet) and the device supports VLAN distribution based on the packet protocol type, the VLAN ID in the tag added to the packet is selected from the VLAN IDs mapped to the protocol suite configuration of the input port. If the protocol type of the packet does not match all protocol suite configuration of the input port, a VLAN ID is allocated according to the port-based VLAN distribution.
- If a packet is a tagged packet, the VLAN to which the packet belongs is determined by the VLAN ID in the tag.

Subnet VLANs can be configured only globally that is, only the protocol VLAN function can be enabled or disabled on ports. The matching configuration is globally performed for the protocol VLAN, the matching configuration is selected on ports and the VLAN IDs are specified for packets that are matched successfully.

- If an input packet contains a null VLAN ID and the IP address of the input packet matches an IP address, the packet is distributed to the subnet VLAN.
- If an input packet contains a null VLAN ID and the packet type and Ethernet type of the input packet match the packet type and Ethernet type of an input port, the packet is allocated to the protocol VLAN.

Protocol VLAN Priority

The priority of a subnet VLAN is higher than that of a protocol VLAN. That is, if a subnet VLAN and protocol VLAN are configured at the same time and an input packet conforms to both the subnet VLAN and protocol VLAN, the subnet VLAN prevails.

Overview

Feature	Description
Automatic VLAN Distribution Based on Packet Type	The service types supported on a network are bound with VLANs or packets from a specified IP network segment are transmitted in a specified VLAN to facilitate management and maintenance.

7.3.1 Automatic VLAN Distribution Based on Packet Type

Working Principle

Set rules on the hardware and enable the rules on ports. The rules take effect only after they are enabled on ports. The rules include the packet type and IP address of packets. When a port receives untagged data packets that meet the rules, the port automatically distributes them to the VLAN specified in the rules for transmission. When the rules are disabled on ports, untagged data packets are distributed to the Native VLAN according to the port configuration.

Related Configuration

7.4 Configuration

Configuration	Description and Command	
Configuring the Protocol VLAN Function	⚠ (Mandatory) It is used to enable the VLAN distribution function based on the packet type and Ethernet type of the protocol VLAN.	
	protocol-vlan profile *num* frame-**type** [*type*] **ether-type** [*type*]	Configures the profile of the packet type and Ethernet type.
	protocol-vlan profile *num* ether-**type** [*type*]	Configures the profile of the Ethernet type (some models do not support frame identification).
	protocol-vlan profile *num* **vlan** *vid*	(Interface configuration mode) Applies the protocol VLAN on a port.
Configuring the Subnet VLAN Function	⚠ (Mandatory) It is used to enable IP address-based VLAN distribution function of the protocol VLAN.	
	protocol-vlan ipv4 *address* **mask** *address* **vlan** *vid*	Configures an IP address, subnet mask, and VLAN distribution.
	protocol-vlan ipv4	(Interface configuration mode) Enables the subnet VLAN on a port.

7.4.1 Configuring the Protocol VLAN Function

Configuration Effect

Bind service types supported in a network with VLANs to facilitate management and maintenance.

Notes

- It is recommended that the protocol VLAN be configured after VLANs, and the Trunk, Hybrid, Access, and AP attributes of ports are configured.
- If protocol VLAN is configured on a Trunk port or Hybrid port, all VLANs relevant to the protocol VLAN need to be contained in the permitted VLAN list of the Trunk port or Hybrid port.

Configuration Steps

Configuring the Protocol VLAN Globally

- Mandatory.
- The protocol VLAN can be applied on an interface only in global configuration mode.

Command	**protocol-vlan profile *num* frame-type [*type]* ether-type [*type]***
Parameter Description	*num:* Indicates the profile index. *type*: Indicates the packet type and Ethernet type.
Defaults	The protocol VLAN is disabled by default.
Command Mode	Global configuration mode
Usage Guide	The protocol VLAN can be configured on an interface only when the protocol VLAN is globally configured. When the global configuration of a protocol VLAN profile is deleted, the protocol VLAN configuration is deleted from all interfaces corresponding to the profile of the protocol VLAN.

Switching the Port Mode to Trunk/Hybrid Mode

- Mandatory. The protocol VLAN function takes effect only on ports that are in Trunk/Hybrid mode.

Enabling the Protocol VLAN on a Port

- Mandatory. The protocol VLAN is disabled by default.
- The protocol VLAN is truly enabled only when it is applied on interfaces.

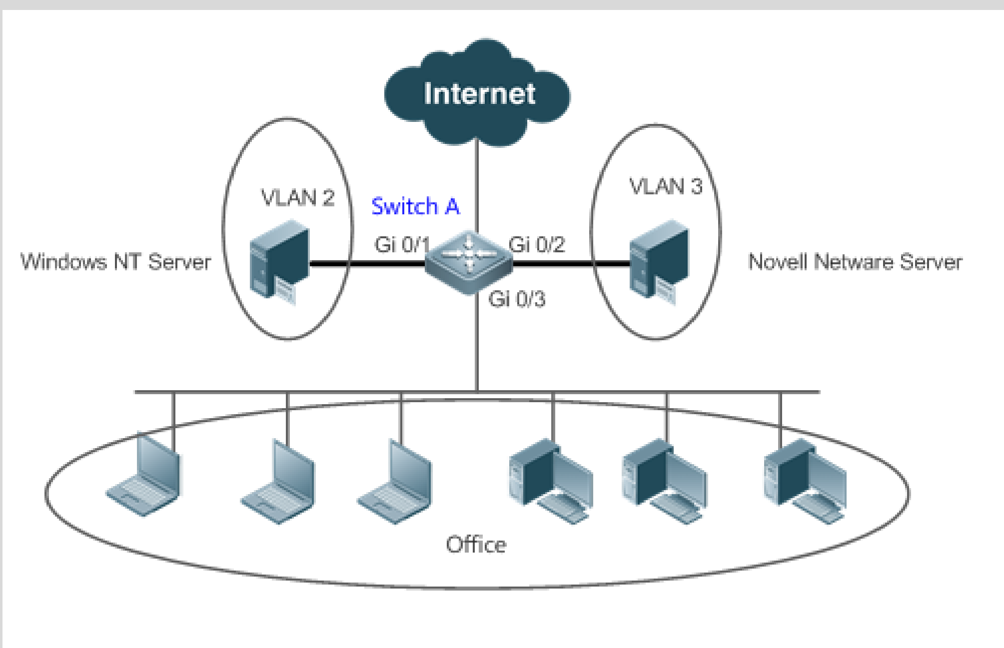
Command	**protocol-vlan profile *num* vlan *vid***
Parameter Description	*num:* Indicates the profile index. *vid*: Indicates the VLAN ID. The value 1 indicates the maximum VLAN ID supported by the product.
Defaults	The protocol VLAN is disabled by default.
Command Mode	Interface configuration mode
Usage Guide	An interface must work in Trunk/Hybrid mode.

Verification

Run the **show protocol-vlan profile** command to check the configuration.

Configuration Example

Enabling the Protocol VLAN Function in the Topological Environment

Scenario **Figure 8-3**	

Configuration Steps	▪ Configure VLAN 2 and VLAN 3 for user communication on Switch A. ▪ Configure the protocol VLAN globally on Switch A (in this example, configure Profile 1 for IP protocol packets and configure Profile 2 for IPX protocol packets), enable the protocol VLAN function on the uplink port (Port Gi 0/3 in this example), and complete the protocol-VLAN association (in this example, associate Profile 1 with VLAN 2 and associate Profile 2 with VLAN 3). ▪ Port Gi 0/1 is an Access port and belongs to VLAN 2. Port Gi 0/2 is also an Access port and belongs to VLAN 3. Port Gi 0/3 is a Hybrid port. Ensure that the user communication VLANs are contained in the permitted untagged VLAN list of the Hybrid port.
A	1. Create VLAN 2 and VLAN 3 for user network communication. # configure terminal Enter configuration commands, one per line. End with CNTL/Z. A(config)# vlan range 2-3 2. Configure the port mode. A(config)#interface gigabitEthernet 0/1 A(config-if-GigabitEthernet 0/1)#switchport A(config-if-GigabitEthernet 0/1)#switchport access vlan 2 A(config-if-GigabitEthernet 0/1)#exit A(config)#interface gigabitEthernet 0/2 A(config-if-GigabitEthernet 0/2)#switchport A(config-if-GigabitEthernet 0/2)#switchport access vlan 3 A(config-if-GigabitEthernet 0/2)#exit A(config)# interface gigabitEthernet 0/3 A(config-if-GigabitEthernet 0/3)#switchport A(config-if-GigabitEthernet 0/3)# switchport mode hybrid A(config-if-GigabitEthernet 0/3)# switchport hybrid allowed vlan untagged 2-3 3. Configure the protocol VLAN globally. Configure Profile 1 for IP protocol packets and Profile 2 for IPX protocol packets (in this example, assume that packets are encapsulated using Ethernet II and the Ethernet types of IP protocol packets and IPX protocol packets are 0X0800 and 0X8137 respectively).

	A(config)#protocol-vlan profile 1 frame-type ETHERII ether-type 0x0800 A(config)#protocol-vlan profile 2 frame-type ETHERIIether-type 0x8137 4. Apply Profile 1 and Profile 2 to Port Gi 0/3 and allocate Profile 1to VLAN 2 and Profile 2 to VLAN 3. A(config)# interface gigabitEthernet 0/3 A(config-if-GigabitEthernet 0/3) #protocol-vlan profile 1 vlan 2 A(config-if-GigabitEthernet 0/3) #protocol-vlan profile 2 vlan 3
Verification	Check whether the protocol VLAN configuration on the device is correct.
A	A(config)#show protocol-vlan profile profile frame-type ether-type/DSAP+SSAP interface vlan ------- ---------------- ---------------------- --------------- ---- 1 ETHERII 0x0800 Gi0/3 2 2 ETHERII 0x8137 Gi0/3 3

Common Errors

- A port connected to the device is not in Trunk/Hybrid mode.
- The permitted VLAN list of the port connected to the device does not contain the user communication VLANs.
- The protocol VLAN function is disabled on a port.

7.4.2 Configuring the Subnet VLAN Function

Configuration Effect

Distribute packets from a specified network segment or IP address to a specified VLAN for transmission.

Notes

- It is recommended that the protocol VLAN be configured after VLANs, and the Trunk, Hybrid, Access, and AP attributes of ports are configured.
- If protocol VLAN is configured on a Trunk port or Hybrid port, all VLANs relevant to the protocol VLAN need to be contained in the permitted VLAN list of the Trunk port or Hybrid port.

Configuration Steps

Configuring the Subnet VLAN Globally

- Mandatory.
- The subnet VLAN can be applied on an interface only in global configuration mode.

Command	**protocol-vlan ipv4 *address* mask *address* vlan *vid***
Parameter Description	*address*: Indicates the IP address. *vid*: Indicates the VLAN ID. The value **1** indicates the maximum VLAN ID supported by the product.
Defaults	The subnet VLAN is disabled by default.
Command Mode	Global configuration mode
Usage Guide	The subnet VLAN can be enabled on an interface even if the protocol VLAN is not enabled globally. Nevertheless, the subnet VLAN takes effect only when the protocol VLAN is configured globally.

Switching the Port Mode to Trunk/Hybrid Mode

- Mandatory. The subnet VLAN function takes effect only on ports that are in Trunk/Hybrid mode.

Enabling the Subnet VLAN on a Port

- Mandatory. The subnet VLAN is disabled by default.
- The subnet VLAN is truly enabled only when it is applied on interfaces.

Command	**protocol-vlan ipv4**
Parameter Description	N/A
Defaults	The subnet VLAN is disabled by default.
Command Mode	Interface configuration mode

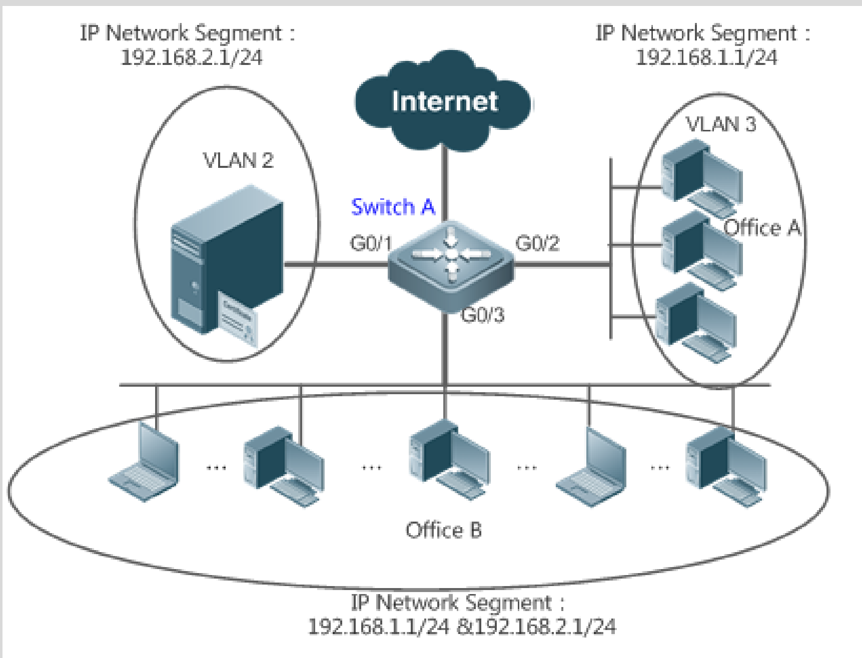
Usage Guide	An interface must work in Trunk/Hybrid mode.

Verification

Run the **show protocol-vlan ipv4** command to check the configuration.

Configuration Example

Enabling the Subnet VLAN Function in the Topological Environment

Scenario **Figure 8-4**	
Configuration Steps	▪ Configure VLAN 2 and VLAN 3 for user communication on Switch A. ▪ Globally configure subnet VLANs on Switch A (in this example, allocate the IP network segment 192.168.1.1/24 to VLAN 3 and the IP network segment 192.168.2.1/24 to VLAN 2) and enable the subnet VLAN function on the uplink port (Port Gi 0/3 in this example). ▪ Port Gi 0/1 is an Access port and belongs to VLAN 2. Port Gi 0/2 is also an Access port and belongs to VLAN 3. Port Gi 0/3 is a Hybrid port. Ensure that the user communication VLANs are contained in the permitted untagged VLAN list of the Hybrid port.
A	1. Create VLAN 2 and VLAN 3 for user network communication. A# configure terminal

	Enter configuration commands, one per line. End with CNTL/Z. A(config)# vlan range 2-3 2. Configure the port mode. A(config)#interface gigabitEthernet 0/1 A(config-if-GigabitEthernet 0/1)#switchport A(config-if-GigabitEthernet 0/1)#switchport access vlan 2 A(config-if-GigabitEthernet 0/1)#exit A(config)#interface gigabitEthernet 0/2 A(config-if-GigabitEthernet 0/2)#switchport A(config-if-GigabitEthernet 0/2)#switchport access vlan 3 A(config-if-GigabitEthernet 0/2)#exit A(config)# interface gigabitEthernet 0/3 A(config-if-GigabitEthernet 0/3)#switchport A(config-if-GigabitEthernet 0/3)# switchport mode hybrid A(config-if-GigabitEthernet 0/3)# switchport hybrid allowed vlan untagged 2-3 3. Configure the subnet VLAN globally. A(config)# protocol-vlan ipv4 192.168.1.0 mask 255.255.255.0 vlan 3 A(config)# protocol-vlan ipv4 192.168.2.0 mask 255.255.255.0 vlan 2 4. Enable the subnet VLAN on interfaces. The subnet VLAN is disabled by default. (config-if-GigabitEthernet 0/3)# protocol-vlan ipv4
Verification	Check whether the subnet VLAN configuration on the device is correct.
A	A# show protocol-vlan ipv4 ip mask vlan --------------- --------------- ---- 192.168.1.0 255.255.255.0 3 192.168.2.0 255.255.255.0 2

	interface ipv4 status -------------------- ----------- Gi0/3 enable

Common Errors

- A port connected to the device is not in Trunk/Hybrid mode.
- The permitted VLAN list of the port connected to the device does not contain the user communication VLANs.
- The subnet VLAN is disabled on a port.

7.5 Monitoring

Displaying

Description	Command
Displays the protocol VLAN content.	show protocol-vlan

Debugging

⚠ System resources are occupied when debugging information is output. Therefore, disable debugging immediately after use.

Description	Command
Debugs the protocol VLAN.	**debug bridge protvlan**

8 CONFIGURING PRIVATE VLAN

8.1 Overview

Private VLAN divides the Layer-2 broadcast domain of a VLAN into multiple subdomains. Each subdomain is composed of one private VLAN pair: primary VLAN and secondary VLAN.

One private VLAN domain may consist of multiple private VLAN pairs and each private VLAN pair represents one subdomain. In a private VLAN domain, all private VLAN pairs share the same primary VLAN. The secondary VLAN IDs of subdomains are different.

If a service provider allocates one VLAN to each user, the number of users that can be supported by the service provider is restricted because one device supports a maximum of 4,096 VLANs. On a Layer-3 device, one subnet address or a series of addresses are allocated to each VLAN, which results in the waste of IP addresses. The private VLAN technology properly solves the preceding two problems. Private VLAN is hereinafter called PVLAN for short.

8.2 Applications

Application	Description
Cross-Device Layer-2 Application of PVLAN	Users of an enterprise can communicate with each other but the user communication between enterprises is isolated.
Layer-3 Application of PVLAN on a Single Device	All enterprise users share the same gateway address and can communicate with the external network.

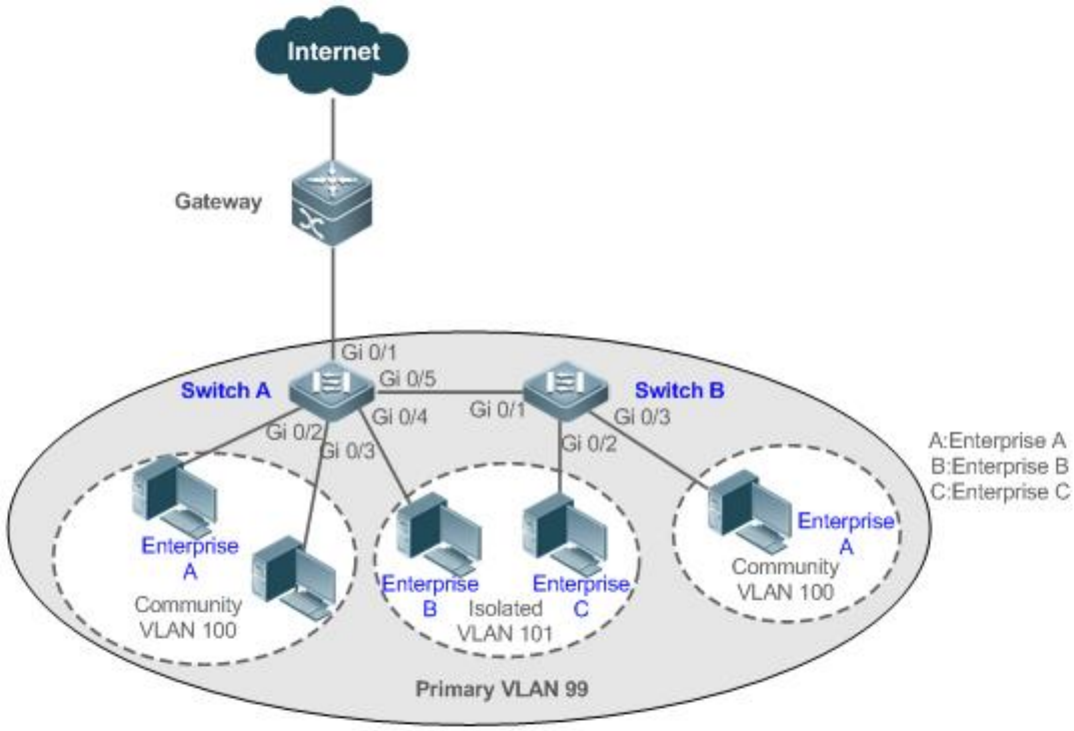
8.2.1 Cross-Device Layer-2 Application of PVLAN

Scenario

As shown in the following figure, in the hosting service operation network, enterprise user hosts are connected to the network through Switch A or Switch B. The main requirements are as follows:

- Users of an enterprise can communicate with each other but the user communication between enterprises is isolated.
- All enterprise users share the same gateway address and can communicate with the external network.

Figure 9-1



Remarks	**Switch A and Switch B are access switches.** **PVLAN runs across devices. The ports for connecting the devices need to be configured as Trunk ports, that is, Port Gi 0/5 of Switch A and Port Gi 0/1 of Switch B are configured as Trunk ports.** **Port Gi 0/1 for connecting Switch A to the gateway needs to be configured as a promiscuous port.** **Port Gi 0/1 of the gateway can be configured as a Trunk port or Hybrid port and the Native VLAN is the primary VLAN of PVLAN.**

Deployment

- Configure all enterprises to be in the same PVLAN (primary VLAN 99 in this example). All enterprise users share the same Layer-3 interface through this VLAN to communicate with the external network.
- If an enterprise has multiple user hosts, allocate the user hosts of different enterprises to different community VLANs. That is, configure the ports connected to the enterprise user hosts as the host ports of a community VLAN, so as to implement user communication inside an enterprise but isolate the user communication between enterprises.

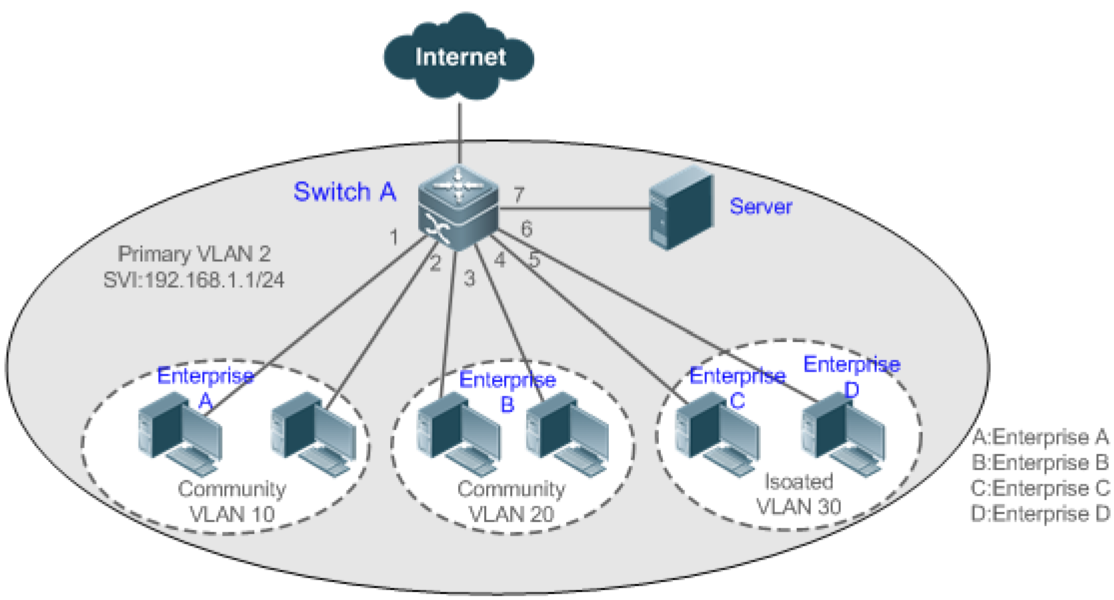
- If an enterprise has only one user host, configure the ports connected to the user hosts of such enterprises as the host ports of an isolated VLAN so as to implement isolation of user communication between the enterprises.

8.2.2 Layer-3 Application of PVLAN on a Single Device

As shown in the following figure, in the hosting service operation network, enterprise user hosts are connected to the network through the Layer-3 device Switch A. The main requirements are as follows:

- Users of an enterprise can communicate with each other but the user communication between enterprises is isolated.
- All enterprise users can access the server.
- All enterprise users share the same gateway address and can communicate with the external network.

Figure 9-2



Remarks	**Switch A is a gateway switch.** **When user hosts are connected to a single device, Port Gi 0/7 for connecting to the server is configured as a promiscuous port so that enterprise users can communicate with the server.** **Layer-3 mapping needs to be performed on the primary VLAN and secondary VLANs so that the users can communicate with the external network.**

Deployment

- Configure the port that is directly connected to the server as a promiscuous port. Then, all enterprise users can communicate with the server through the promiscuous port.
- Configure the gateway address of PVLAN on the Layer-3 device (Switch A in this example) (in this example, set the SVI address of VLAN 2 to 192.168.1.1/24) and configure the mapping between the primary VLAN and secondary VLANs on the Layer-3 interface. Then, all enterprise users can communicate with the external network through the gateway address.

8.3 Features

Basic Concepts

PVLAN

PVLAN supports three types of VLANs: primary VLANs, isolated VLANs, and community VLANs.

A PVLAN domain has only one primary VLAN. Secondary VLANs implement Layer-2 isolation in the same PVLAN domain. There are two types of secondary VLANs.

Isolated VLAN

Ports in the same isolated VLAN cannot mutually make Layer-2 communication. A PVLAN domain has only one isolated VLAN.

Community VLAN

Ports in the same community VLAN can make Layer-2 communication with each other but cannot make Layer-2 communication with ports in other community VLANs. A PVLAN domain can have multiple community VLANs.

Layer-2 Association of PVLAN

PVLAN pairs exist only after Layer-2 association is performed among the three types of VLANs of PVLAN. Then, a primary VLAN has a specified secondary VLAN and a secondary VLAN has a specified primary VLAN. A primary VLAN and secondary VLANs are in the one-to-many relationship.

Layer-3 Association of PVLAN

In PVLAN, Layer-3 interfaces, that is, switched virtual interfaces (SVIs) can be created only in a primary VLAN. Users in a secondary VLAN can make Layer-3 communication only after Layer-3 association is performed between the secondary VLAN and the primary VLAN. Otherwise, the users can make only Layer-2 communication.

Community Port

Community ports are ports in a community VLAN. Community ports in the same community VLAN can communicate with each other and can communicate with promiscuous ports. They cannot communicate with community ports in other community VLANs or isolated ports in an isolated VLAN.

Promiscuous Port

Promiscuous ports are ports in a primary VLAN. They can communicate with any ports, including isolated ports and community ports in secondary VLANs of the same PVLAN domain.

In PVLAN, SVIs can be created only in a primary VLAN and SVIs cannot be created in secondary VLANs.

Ports in PVLAN can be used as mirroring source ports but cannot be used as mirroring destination ports.

Overview

Feature	Description
PVLAN Layer-2 Isolation and IP Address Saving	Ports of different PVLAN types can be configured to implement interworking and isolation of VLAN intermediate user hosts.
	After Layer-2 mapping is performed between a primary VLAN and secondary VLANs, only Layer-2 communication is supported. If Layer-3 communication is required, users in a secondary VLAN need to use SVIs of the primary VLAN to make Layer-3 communication.

8.3.1 PVLAN Layer-2 Isolation and IP Address Saving

Add users to subdomains of PVLAN to isolate communication between enterprises and between enterprise users.

Working Principle

Configure PVLAN, configure Layer-2 association and Layer-3 association between a primary VLAN and SubVLANs of PVLAN, and configure ports connected to user hosts, external network devices, and servers as different types of PVLAN ports. In this way, subdomain division and communication of users in subdomains with the external network and servers can be implemented.

Packet Forwarding Relationship Between Ports of Different Types

Output Port	Promiscuous Port	Isolated Port	Community Port	Isolated Trunk Port	Promiscuous Trunk Port	Trunk Port

Input Port				**(in the Same VLAN)**	**(in the Same VLAN)**	**(in the Same VLAN)**
Promiscuous Port	Supported	Supported	Supported	Supported	Supported	Supported
Isolated Port	Supported	Unsupported	Unsupported	Unsupported	Supported	Supported
Community Port	Supported	Unsupported	Supported	Supported	Supported	Supported

VLAN Tag Changes After Packet Forwarding Between Ports of Different Types

Output Port **Input Port**	**Promiscuous Port**	**Isolated Port**	**Community Port**	**Isolated Trunk Port** **(in the Same VLAN)**	**Promiscuous Trunk Port** **(in the Same VLAN)**	**Trunk Port** **(in the Same VLAN)**
Promiscuous Port	Unchanged	Unchanged	Unchanged	A secondary VLAN ID is added.	A primary VLAN ID tag is added and the VLAN tag keeps unchanged in the non-PVLAN.	A primary VLAN ID tag is added.
Isolated Port	Unchanged	NA	NA	NA	A primary VLAN ID tag is added and the VLAN tag keeps unchanged in the non-PVLAN.	An isolated VLAN ID tag is added.

Community Port	Unchanged	NA	Unchanged	A community VLAN ID tag is added.	A primary VLAN ID tag is added and the VLAN tag keeps unchanged in the non-PVLAN.	A community VLAN ID tag is added.
Switch CPU	Untag	Untag	Untag	A secondary VLAN ID tag is added.	A primary VLAN ID tag is added and the VLAN tag keeps unchanged in the non-PVLAN.	A primary VLAN ID tag is added.

8.4 Configuration

<table>
<tr><th>Configuration</th><th colspan="2">Description and Command</th></tr>
<tr><td rowspan="5">Configuring Basic Functions of PVLAN</td><td colspan="2">⚠ (Mandatory) It is used to configure a primary VLAN and secondary VLANs.</td></tr>
<tr><td>private-vlan {community | isolated | primary}</td><td>Configures the PVLAN type.</td></tr>
<tr><td colspan="2">⚠ (Mandatory) It is used to configure Layer-2 association between a primary VLAN and secondary VLANs of PVLAN to form PVLAN pairs.</td></tr>
<tr><td>private-vlan association {svlist | add svlist | remove svlist}</td><td>Configures Layer-2 association between a primary VLAN and secondary VLANs to form PVLAN pairs.</td></tr>
<tr><td colspan="2">⚠ (Optional) It is used to allocate users to an isolated VLAN or community VLAN.</td></tr>
</table>

	switchport mode private-vlan host	Configures a PVLAN host port.
	switchport private-vlan host-association ***p_vid s_vid***	Associates Layer-2 ports with PVLAN and allocates ports to subdomains.
	⚠ (Optional) It is used to configure a port as a promiscuous port.	
	Switchport mode private-vlan promiscuous	Configures a PVLAN promiscuous port.
	switchport private-vlan mapping ***p_vid*** **{** ***svlist*** **| add** ***svlist*** **| remove** ***svlist*** **}**	Configures the primary VLAN to which a PVLAN promiscuous port belongs and a list of secondary VLANs. PVLAN packets can be transmitted or received through this port only after the configuration is performed.
	⚠ (Optional) It is used to configure Layer-3 communication for users in a secondary VLAN.	
	private-vlan mapping { ***svlist*** **| add** ***svlist*** **| remove** ***svlist*** **}**	Configures the SVI of the primary VLAN and configures Layer-3 association between the primary VLAN and secondary VLANs after PVLAN is created and Layer-2 association is performed. Users in a SubVLAN can make Layer-3 communication through the SVI of the primary VLAN.

8.4.1 Configuring Basic Functions of PVLAN

Configuration Effect

- Enable PVLAN subdomains to form to implement isolation between enterprises and between enterprise users.
- Implement Layer-3 mapping between multiple secondary VLANs and the primary VLAN so that and multiple VLANs uses the same IP gateway, thereby helping save IP addresses.

Notes

- After a primary VLAN and a secondary VLAN are configured, a PVLAN subdomain exist only after Layer-2 association is performed between them.
- A port connected to a use host must be configured as a specific PVLAN port so that the user host joins a subdomain to implement the real user isolation.
- The port connected to the external network and the port connected to a server must be configured as promiscuous ports so that upstream and downstream packets are forwarded normally.
- Users in a secondary VLAN can make Layer-3 communication through the SVI of the primary VLAN only after Layer-3 mapping is performed between the secondary VLAN and the primary VLAN.

Configuration Steps

Configuring PVLAN

- Mandatory.
- A primary VLAN and a secondary VLAN must be configured. The two types of VLANs cannot exist independently.
- Run the **private-vlan** { **community** | **isolated** | **primary** } command to configure a VLAN as the primary VLAN of PVLAN and other VLANs as secondary VLANs.

Command	**private-vlan { community | isolated | primary }**
Parameter Description	**community**: Specifies that the VLAN type is community VLAN. **isolated**: Specifies that the VLAN type is isolated VLAN. **primary**: Specifies that the VLAN type is the primary VLAN of a PVLAN pair.
Defaults	VLANs are common VLANs and do not have the attributes of PVLAN.
Command Mode	VLAN mode
Usage Guide	This command is used to specify the primary VLAN and secondary VLANs of PVLAN.

Configuring Layer-2 Association of PVLAN

- Mandatory.
- PVLAN subdomains form, and isolated ports, community ports, and Layer-3 association can be configured only after Layer-2 association is performed between the primary VLAN and secondary VLANs of PVLAN.

- By default, after various PVLANs are configured, the primary VLANs and secondary VLANs are independent of each other. A primary VLAN has a secondary VLAN and a secondary VLAN has a primary VLAN only after Layer-2 association is performed.
- Run the **private-vlan association** { *svlist* | **add** *svlist* | **remove** *svlist* } command to configure or cancel the Layer-2 association between the primary VLAN and secondary VLANs of PVLAN. A PVLAN subdomain forms only after Layer-2 association is configured,. The PVLAN subdomain does not exist after Layer-2 association is cancelled. If Layer-2 association is not performed, when isolated ports and promiscuous ports are used to configure associated PVLAN pairs, the configuration will fail or the association between ports and VLANs will be cancelled.

Command	**private-vlan association { *svlist* | add *svlist* | remove *svlist* }**
Parameter Description	*svlist*: Specifies the list of secondary VLANs to be associated or disassociated. add *svlist*: Adds the secondary VLANs to be associated. remove *svlist*: Cancels the association between *svlist* and the primary VLAN.
Defaults	By default, the primary VLAN and secondary VLANs are not associated.
Command Mode	Primary VLAN mode of PVLAN
Usage Guide	This command is used to configure Layer-2 association between a primary VLAN and secondary VLANs to form PVLAN pairs. Each primary VLAN can be associated with only one isolated VLAN but can be associated with multiple community VLANs.

Configuring Layer-3 Association of PVLAN

- If users in a secondary VLAN domain needs to make Layer-3 communication, configure a Layer-3 interface SVI for the primary VLAN and then configure Layer-3 association between the primary VLAN and secondary VLANs on the SVI.
- By default, SVIs can be configured only in a primary VLAN. Secondary VLANs do not support Layer-3 communication.
- If users in a secondary VLAN of PVLAN need to make Layer-3 communication, the SVI of the primary VLAN needs to be used to transmit and receive packets.
- Run the **private-vlan mapping** { *svlist* | **add** *svlist* | **remove** *svlist* } command to configure or cancel the Layer-3 association between the primary VLAN and secondary VLANs of PVLAN. Users in a secondary VLAN can make Layer-3 communication with the external network only after Layer-3

association is configured. After Layer-3 association is cancelled, users in a secondary VLAN cannot make Layer-3 communication.

Command	**private-vlan mapping { *svlist* | add *svlist* | remove *svlist* }**
Parameter Description	*svlist*: Indicates the list of secondary VLANs, for which Layer-3 mapping needs to be configured. add *svlist*: Adds the secondary VLANs to be associated with a Layer-3 interface. remove *svlist:* Cancels the secondary VLANs associated with a Layer-3 interface.
Defaults	By default, the primary VLAN and secondary VLANs are not associated.
Command Mode	Interface configuration mode of the primary VLAN
Usage Guide	A Layer-3 SVI must be configured for the primary VLAN first. Layer-3 interfaces can be configured only in a primary VLAN. Layer-2 association must be performed between associated secondary VLANs and the primary VLAN.

Configuring Isolated Ports and Community Ports

- After the primary VLAN and secondary VLANs of PVLAN as well as Layer-2 association are configured, allocate the device ports connected to user hosts so as to specify the subdomains to which the user hosts belong.
- If an enterprise has only one user host, set the port connected to the user host as an isolated port.
- If an enterprise has multiple user hosts, set the ports connected to the user hosts as community ports.

Command	**switchport mode private-vlan host** **switchport private-vlan host-association *p_vid s_vid***
Parameter Description	*p_vid*: Indicates the primary VLAN ID in a PVLAN pair. *s_vid*: Indicates the secondary VLAN ID in a PVLAN pair. The port is an associated port if the VLAN is an isolated VLAN and the port is a community port if the VLAN is a community VLAN.

Defaults	By default, the interface works in Access mode; no private VLAN pairs are associated.
Command Mode	Both commands run in interface configuration mode.
Usage Guide	Both the preceding commands need to be configured. Before a port is configured as an isolated port or promiscuous port, and the port mode must be configured as the host port mode. Whether a port is configured as an isolated port or community port depends on the *s_vid* parameter. *p_vid* and *s_vid* must be respectively the IDs of the primary VLAN and secondary VLAN in a PVLAN pair, on which Layer-2 association is performed. One host port can be associated with only one PVLAN pair.

Configuring a Promiscuous Port

- According to the table listing port packet transmission and receiving rules in section "Features", the single port type of PVLAN cannot ensure symmetric forwarding of upstream and downstream packets. Ports for connecting to the external network or server need to be configured as promiscuous ports to ensure that users can successfully access the external network or server.

Command	**switchport mode private-vlan promiscuous** **switchport private-vlan mapping *p_vid*{ *svlist* | add *svlist* | remove *svlist* }**
Parameter Description	*p_vid*: Indicates the primary VLAN ID in a PVLAN pair. *svlist*: Indicates the secondary VLAN associated with a promiscuous port. Layer-2 association must be performed between it and *p_vid*. add *svlist*: Adds a secondary VLAN to be associated with a port. remove *svlist:* Cancels the secondary VLAN associated with a port.
Defaults	By default, an interface works in Access mode; a promiscuous port is not associated with a secondary VLAN.
Command Mode	Interface configuration mode
Usage Guide	The port mode must be configured as the promiscuous mode.

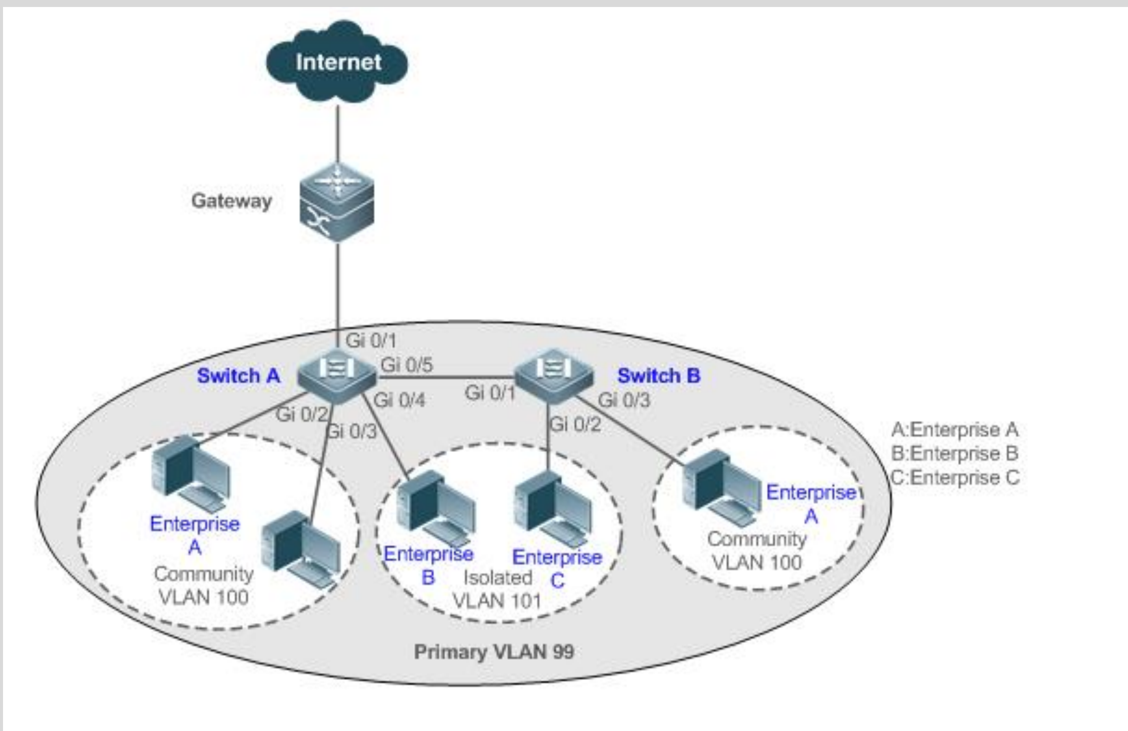
	If a port is configured as a promiscuous port, it must be associated with PVLN pairs. Otherwise, the port cannot bear or forward services. One promiscuous port can be associated with multiple PVLAN pairs within one primary VLAN but cannot be associated with multiple primary VLANs.

Verification

Make user hosts connected to PVLAN ports transmit and receive packets as per PVLAN port forwarding rules to implement isolation. Configure Layer-3 association to make users in the primary VLAN and secondary VLANs of the same PVLAN to share the same gateway IP address and make Layer-3 communication.

Configuration Example

Cross-Device Layer-2 Application of PVLAN

Figure 9-3	
Configuration Steps	▪ Configure all enterprises to be in the same PVLAN (primary VLAN 99 in this example). All enterprise users share the same Layer-3 interface through this VLAN to communicate with the external network. ▪ If an enterprise has multiple user hosts, allocate each enterprise to a different community VLAN (in this example, allocate Enterprise A to Community VLAN 100) to

	implement user communication inside an enterprise and isolate user communication between enterprises. ▪ If an enterprise has only one user host, allocate such enterprises to the same isolated VLAN (in this example, allocate Enterprise B and Enterprise C to Isolated VLAN 101) to isolate user communication between enterprises.
A	SwitchA#configure terminal Enter configuration commands, one per line. End with CNTL/Z. SwitchA(config)#vlan 99 SwitchA(config-vlan)#private-vlan primary SwitchA(config-vlan)#exit SwitchA(config)#vlan 100 SwitchA(config-vlan)#private-vlan community SwitchA(config-vlan)#exit SwitchA(config)#vlan 101 SwitchA(config-vlan)#private-vlan isolated SwitchA(config-vlan)#exit SwitchA(config)#vlan 99 SwitchA(config-vlan)#private-vlan association 100-101 SwitchA(config-vlan)#exit SwitchA(config)#interface range gigabitEthernet 0/2-3 SwitchA(config-if-range)#switchport mode private-vlan host SwitchA(config-if-range)#switchport private-vlan host-association 99 100 SwitchA(config-if-range)#exit SwitchA(config)#interface gigabitEthernet 0/4 SwitchA(config-if-GigabitEthernet 0/4)#switchport mode private-vlan host SwitchA(config-if-GigabitEthernet 0/4)#switchport private-vlan host-association 99 101
B	SwitchB#configure terminal Enter configuration commands, one per line. End with CNTL/Z. SwitchB(config)#vlan 99 SwitchB(config-vlan)#private-vlan primary SwitchB(config-vlan)#exit SwitchB(config)#vlan 100

	SwitchB(config-vlan)#private-vlan community SwitchB(config-vlan)#exit SwitchB(config)#vlan 101 SwitchB(config-vlan)#private-vlan isolated SwitchB(config-vlan)#exit SwitchB(config)#vlan 99 SwitchB(config-vlan)#private-vlan association 100-101 SwitchB(config-vlan)#exit SwitchB(config)#interface gigabitEthernet 0/2 SwitchB(config-if-GigabitEthernet 0/2)#switchport mode private-vlan host SwitchB(config-if-GigabitEthernet 0/2)# switchport private-vlan host-association 99 101 SwitchB(config-if-GigabitEthernet 0/2)#exit SwitchB(config)#interface gigabitEthernet 0/3 SwitchB(config-if-GigabitEthernet 0/3)#switchport mode private-vlan host SwitchB(config-if-GigabitEthernet 0/3)# switchport private-vlan host-association 99 100 SwitchB(config-if-GigabitEthernet 0/3)#exit
Verification	Check whether VLANs and ports are correctly configured, and check whether packet forwarding is correct according to packet forwarding rules in section "Features".
A	SwitchA#show running-config ! vlan 99 private-vlan primary private-vlan association add 100-101 ! vlan 100 private-vlan community ! vlan 101 private-vlan isolated

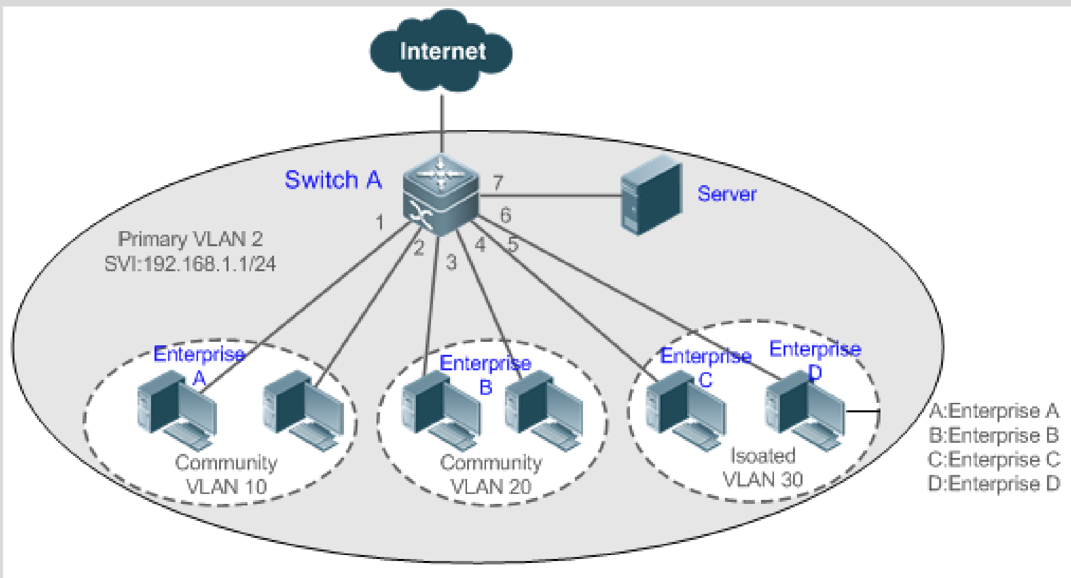
	! interface GigabitEthernet 0/1 switchport mode private-vlan promiscuous switchport private-vlan mapping 99 add 100-101 ! interface GigabitEthernet 0/2 switchport mode private-vlan host switchport private-vlan host-association 99 100 ! interface GigabitEthernet 0/3 switchport mode private-vlan host switchport private-vlan host-association 99 100 ! interface GigabitEthernet 0/4 switchport mode private-vlan host switchport private-vlan host-association 99 101 !
B	SwitchB#show running-config ! vlan 99 private-vlan primary private-vlan association add 100-101 ! vlan 100 private-vlan community ! vlan 101 private-vlan isolated !

Common Errors

- Layer-2 association is not performed between the primary VLAN and secondary VLANs of PVLAN, and a port VLAN list fails to be added when isolated ports, promiscuous ports, and community ports are configured.
- One host port fails to be associated with multiple PVLAN pairs.

Configuration Example

Layer-3 Application of PVLAN on a Single Device

<table>
<tr><td>Figure 9-4</td><td>
</td></tr>
<tr><td>Configuration Steps</td><td>Configure the PVLAN function on the device (Switch A in this example). For details about the configuration, see configuration tips in "Cross-Device Layer-2 Application of PVLAN."
Set the port that is directly connected to the server (Port Gi 0/7 in this example) as a promiscuous port. Then, all enterprise users can communicate with the server through the promiscuous port.
Configure the gateway address of PVLAN on the Layer-3 device (Switch A in this example) (in this example, set the SVI address of VLAN 2 to 192.168.1.1/24) and configure the Layer-3 interface mapping between the primary VLAN (VLAN 2 in this example) and secondary VLANs (VLAN 10, VLAN 20, and VLAN 30 in this example). Then, all enterprise users can communicate with the external network through the gateway address.</td></tr>
<tr><td>A</td><td>SwitchA#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.</td></tr>
</table>

	SwitchA(config)#vlan 2 SwitchA(config-vlan)#private-vlan primary SwitchA(config-vlan)#exit SwitchA(config)#vlan 10 SwitchA(config-vlan)#private-vlan community SwitchA(config-vlan)#exit SwitchA(config)#vlan 20 SwitchA(config-vlan)#private-vlan community SwitchA(config-vlan)#exit SwitchA(config)#vlan 30 SwitchA(config-vlan)#private-vlan isolated SwitchA(config-vlan)#exit SwitchA(config)#vlan 2 SwitchA(config-vlan)#private-vlan association 10,20,30 SwitchA(config-vlan)#exit SwitchA(config)#interface range gigabitEthernet 0/1-2 SwitchA(config-if-range)#switchport mode private-vlan host SwitchA(config-if-range)#switchport private-vlan host-association 2 10 SwitchA(config-if-range)#exit SwitchA(config)#interface range gigabitEthernet 0/3-4 SwitchA(config-if-range)#switchport mode private-vlan host SwitchA(config-if-range)#switchport private-vlan host-association 2 20 SwitchA(config-if-range)#exit SwitchA(config)#interface range gigabitEthernet 0/5-6 SwitchA(config-if-range)#switchport mode private-vlan host SwitchA(config-if-range)#switchport private-vlan host-association 2 30 SwitchA(config-if-range)#exit SwitchA(config)#interface gigabitEthernet 0/7 SwitchA(config-if-GigabitEthernet 0/7)#switchport mode private-vlan promiscuous SwitchA(config-if-GigabitEthernet 0/7)#switchport private-vlan maping 2 10,20,30 SwitchA(config-if-GigabitEthernet 0/7)#exit SwitchA(config)#interface vlan 2 SwitchA(config-if-VLAN 2)#ip address 192.168.1.1 255.255.255.0

	SwitchA(config-if-VLAN 2)#private-vlan mapping 10,20,30 SwitchA(config-if-VLAN 2)#exit
Verification	Ping the gateway address 192.168.1.1 from user hosts in different subdomains. The ping operation is successful.
A	SwitchA#show running-config ! vlan 2 private-vlan primary private-vlan association add 10,20,30 ! vlan 10 private-vlan community ! vlan 20 private-vlan community ! vlan 30 private-vlan isolated ! interface GigabitEthernet 0/1 switchport mode private-vlan host switchport private-vlan host-association 2 10 ! interface GigabitEthernet 0/2 switchport mode private-vlan host switchport private-vlan host-association 2 10 ! interface GigabitEthernet 0/3 switchport mode private-vlan host switchport private-vlan host-association 2 20

```
!
interface GigabitEthernet 0/4
 switchport mode private-vlan host
 switchport private-vlan host-association 2 20
!
interface GigabitEthernet 0/5
 switchport mode private-vlan host
 switchport private-vlan host-association 2 30
!
interface GigabitEthernet 0/6
 switchport mode private-vlan host
 switchport private-vlan host-association 2 30
!
interface GigabitEthernet 0/7
 switchport mode private-vlan promiscuous
 switchport private-vlan mapping 2 add 10,20,30
!
interface VLAN 2
 no ip proxy-arp
 ip address 192.168.1.1 255.255.255.0
 private-vlan mapping add 10,20,30
!
SwitchA#show vlan private-vlan
VLAN  Type   Status   Routed   Ports  Associated VLANs
----------------------------- ------------------
2    primary    active   Enabled  Gi0/7        10,20,30
10   community  active   Enabled  Gi0/1, Gi0/2    2
20   community  active   Enabled  Gi0/3, Gi0/4    2
30   isolated   active   Enabled  Gi0/5, Gi0/6    2
```

Common Errors

- No Layer-2 association is performed on the primary VLAN and secondary VLANs of PVLAN and the Layer-3 association fails to be configured.

- The device is connected to the external network before Layer-3 association is configured. As a result, the device cannot communicate with the external network.
- The interfaces for connecting to the server and the external network are not configured as promiscuous interfaces, which results in asymmetric forwarding of upstream and downstream packets.

8.5 Monitoring

Displaying

Description	Command
Displays PVLAN configuration.	**show vlan private-vlan**

Debugging

System resources are occupied when debugging information is output. Therefore, disable debugging immediately after use.

Description	Command
Debugs PVLAN.	**debug bridge pvlan**

9 CONFIGURING MSTP

9.1 Overview

Spanning Tree Protocol (STP) is a Layer-2 management protocol. It cannot only selectively block redundant links to eliminate Layer-2 loops but also can back up links.

Similar to many protocols, STP is continuously updated from Rapid Spanning Tree Protocol (RSTP) to Multiple Spanning Tree Protocol (MSTP) as the network develops.

For the Layer-2 Ethernet, only one active link can exist between two local area networks (LANs). Otherwise, a broadcast storm will occur. To enhance the reliability of a LAN, it is necessary to establish a redundant link and keep some paths in backup state. If the network is faulty and a link fails, you must switch the redundant link to the active state. STP can automatically activate the redundant link without any manual operations. STP enables devices on a LAN to:

- Discover and start the best tree topology on the LAN.
- Troubleshoot a fault and automatically update the network topology so that the possible best tree topology is always selected.

The LAN topology is automatically calculated based on a set of bridge parameters configured by the administrator. The best topology tree can be obtained by properly configuring these parameters.

RSTP is completely compatible with 802.1D STP. Similar to traditional STP, RSTP provides loop-free and redundancy services. It is characterized by rapid speed. If all bridges in a LAN support RSTP and are properly configured by the administrator, it takes less than 1 second (about 50 seconds if traditional STP is used) to re-generate a topology tree after the network topology changes.

STP and RSTP have the following defects:

- STP migration is slow. Even on point-to-point links or edge ports, it still takes two times of the forward delay for ports to switch to the forwarding state.
- RSTP can rapidly converge but has the same defect with STP: Since all VLANs in a LAN share the same spanning tree, packets of all VLANs are forwarded along this spanning tree. Therefore, redundant links cannot be blocked according to specific VLANs and data traffic cannot be balanced among VLANs.

MSTP, defined by the IEEE in 802.1s, resolves defects of STP and RSTP. It cannot only rapidly converge but also can enable traffic of different VLANs to be forwarded along respective paths, thereby providing a better load balancing mechanism for redundant links.

In general, STP/RSTP works based on ports while MSTP works based on instances. An instance is a set of multiple VLANs. Binding multiple VLANs to one instance can reduce the communication overhead and resource utilization.

QTECH devices support STP, RSTP, and MSTP, and comply with IEEE 802.1D, IEEE 802.1w, and IEEE 802.1s.

Protocols and Standards

- IEEE 802.1D: Media Access Control (MAC) Bridges
- IEEE 802.1w: Part 3: Media Access Control (MAC) Bridges—Amendment 2: Rapid Reconfiguration
- IEEE 802.1s: Virtual Bridged Local Area Networks—Amendment 3: Multiple Spanning Trees

9.2 Applications

Application	Description
MSTP+VRRP Dual-Core Topology	With a hierarchical network architecture model, the MSTP+VRRP mode is used to implement redundancy and load balancing to improve system availability of the network.
BPDU Tunnel	In QinQ network environment, Bridge Protocol Data Unit (BPDU) Tunnel is used to implement tunnel-based transparent transmission of STP packets.

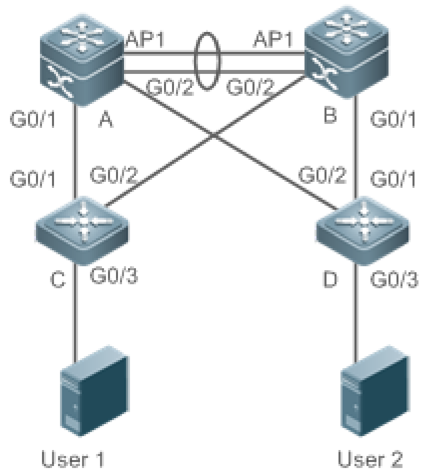
9.2.1 MSTP+VRRP Dual-Core Topology

Scenario

The typical application of MSTP is the MSTP+VRRP dual-core solution. This solution is an excellent solution to improve system availability of the network. Using a hierarchical network architecture model, it is generally divided into three layers (core layer, convergence layer, and access layer) or two layers (core layer and access layer). They form the core network system to provide data exchange service.

The main advantage of this architecture is its hierarchical structure. In the hierarchical network architecture, all capacity indicators, characteristics, and functions of network devices at each layer are optimized based on their network locations and roles, enhancing their stability and availability.

Figure 10-1 MSTP+VRRP Dual-Core Topology



Remarks	**The topology is divided into two layers: core layer (Devices A and B) and access layer (Devices C and D).**

Deployment

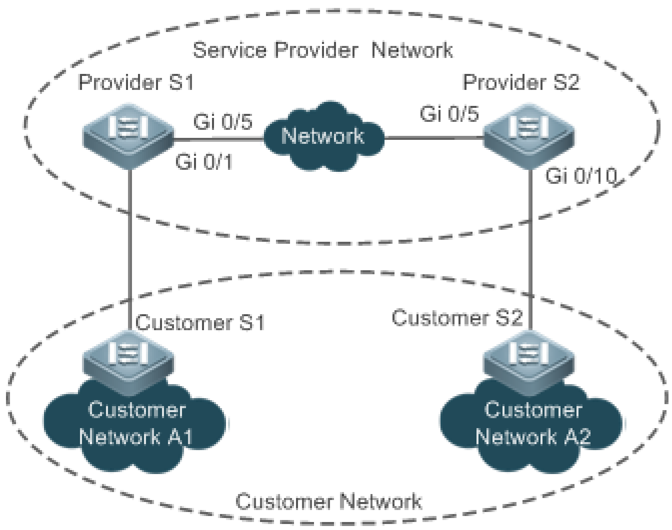
- Core layer: Multiple MSTP instances are configured to realize load balancing. For example, two instances are created: Instance 1 and Instance 2. Instance 1 maps VLAN 10 while Instance 2 maps VLAN 20. Device A is the root bridge of Instances 0 and 1 (Instance 0 is CIST, which exists by default). Device B is the root bridge of Instance 2.
- Core layer: Devices A and B are the active VRRP devices respectively on VLAN 10 and VLAN 20.
- Access layer: Configure the port directly connected to the terminal (PC or server) as a PortFast port, and enable BPDU guard to prevent unauthorized users from accessing illegal devices.

9.2.2 BPDU Tunnel

Scenario

The QinQ network is generally divided into two parts:customer network and service provider (SP) network. You can enable BPDU Tunnel to calculate STP packets of the customer network independently of the SP network, thereby preventing STP packets between the customer network from affecting the SP network.

Figure 10-2 BPDU Tunnel Topology



Remarks	**As shown in the above figure, the upper part is the SP network and the lower part is the customer network. The SP network consists of two provider edges (PEs): Provider S1 and Provider S2. Customer Network A1 and Customer Network A2 are a user's two sites in different regions. Customer S1 and Customer S2, access devices from the customer network to the SP network, access the SP network respectively through Provider S1 and Provider S2.** **Using BPDU Tunnel, Customer Network A1 and Customer Network A2 in different regions can perform unified spanning tree calculation across the SP network, not affecting the spanning tree calculation of the SP network.**

Deployment

- Enable basic QinQ on the PEs (Provider S1/Provider S2 in this example) so that data packets of the customer network are transmitted within the specified VLAN on the SP network.
- Enable STP transparent transmission on the PEs (Provider S1/Provider S2 in this example) so that the SP network can transmit STP packets of the customer network through BPDU Tunnel.

9.3 Features

Basic Concepts

BPDU

To generate a stable tree topology network, the following conditions must be met:

- Each bridge has a unique ID consisting of the bridge priority and MAC address.
- The overhead of the path from the bridge to the root bridge is called root path cost.
- A port ID consists of the port priority and port number.

Bridges exchange BPDU packets to obtain information required for establishing the best tree topology. These packets use the multicast address 01-80-C2-00-00-00 (hexadecimal) as the destination address.

A BPDU consists of the following elements:

- Root bridge ID assumed by the local bridge
- Root path cost of the local bridge
- Bridge ID (ID of the local bridge)
- Message age (age of a packet)
- Port ID (ID of the port sending this packet)
- **Forward-Delay Time**, **Hello Time**, **Max-Age Time** are time parameters specified in the MSTP.
- Other flags, such as flags indicating network topology changes and local port status.

If a bridge receives a BPDU with a higher priority (smaller bridge ID and lower root path cost) at a port, it saves the BPDU information at this port and transmits the information to all other ports. If the bridge receives a BPDU with a lower priority, it discards the information.

Such a mechanism allows information with higher priorities to be transmitted across the entire network. BPDU exchange results are as follows:

- A bridge is selected as the root bridge.
- Except the root bridge, each bridge has a root port, that is, a port providing the shortest path to the root bridge.
- Each bridge calculates the shortest path to the root bridge.
- Each LAN has a designated bridge located in the shortest path between the LAN and the root bridge. A port designated to connect the bridge and the LAN is called designated port.
- The root port and designated port enter the forwarding status.

Bridge ID

According to IEEE 802.1W, each bridge has a unique ID. The spanning tree algorithm selects the root bridge based on the bridge ID. The bridge ID consists of eight bytes, of which the last six bytes are the MAC address of the bridge. In its first two bytes (as listed in the following table), the first four bits indicate the priority; the last eight bits indicate the system ID for use in extended protocol. In RSTP, the system ID is 0. Therefore, the bridge priority should be a integral multiple of 4,096.

	Bit	**Value**
Priority value	16	32,768

	15	16,384
	14	8,192
	13	4,096
System ID	12	2,048
	11	1,024
	10	512
	9	256
	8	128
	7	64
	6	32
	5	16
	4	8
	3	4
	2	2
	1	1

Spanning-Tree Timers

The following three timers affect the performance of the entire spanning tree:

- Hello timer: Interval for periodically sending a BPDU packet.
- Forward-Delay timer: Interval for changing the port status, that is, interval for a port to change from the listening state to the learning state or from the learning state to the forwarding state when RSTP runs in STP-compatible mode.
- Max-Age timer: The longest time-to-live (TTL) of a BPDU packet. When this timer elapses, the packet is discarded.

Port Roles and Port States

Each port plays a role on a network to reflect different functions in the network topology.

- Root port: Port providing the shortest path to the root bridge.
- Designated port: Port used by each LAN to connect the root bridge.
- Alternate port: Alternative port of the root port. Once the root port loses effect, the alternate port immediately changes to the root port.
- Backup port: Backup port of the designated port. When a bridge has two ports connected to a LAN, the port with the higher priority is the designated port while the port with the lower priority is the backup port.
- Disabled port: Inactive port. All ports with the operation state being down play this role.

The following figures show the roles of different ports:

R = Root port   D = Designated port   A = Alternate port   B = Backup port

Unless otherwise specified, port priorities decrease from left to right.

Figure 10-3

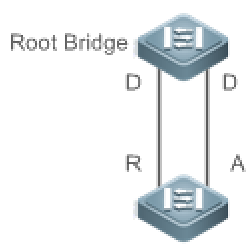


Figure 10-4

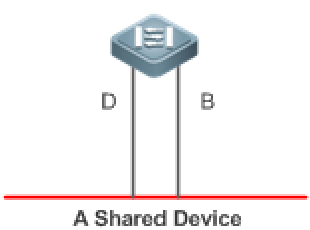
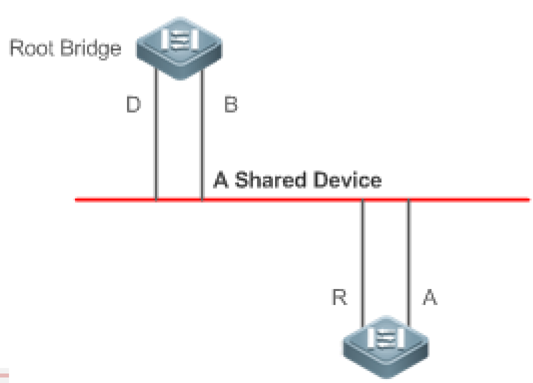


Figure 10-5



Each port has three states indicating whether to forward data packets so as to control the entire spanning tree topology.

- Discarding: Neither forwards received packets nor learns the source MAC address.
- Learning: Does not forward received packets but learns the source MAC address, which is a transitive state.
- Forwarding: Forwards received packets and learns the source MAC address.

For a stable network topology, only the root port and designated port can enter the forwarding state while other ports are always in discarding state.

Hop Count

Internal spanning trees (ISTs) and multiple spanning tree instances (MSTIs) calculate whether the BPDU packet time expires based on an IP TTL-alike mechanism Hop Count, instead of Message Age and Max Age.

It is recommended to run the **spanning-tree max-hops** command in global configuration mode to configure the hop count. In a region, every time a BPDU packet passes through a device from the root bridge, the hop count decreases by 1. When the hop count becomes 0, the BPDU packet time expires and the device discards the packet.

To be compatible with STP and RSTP outside the region, MSTP also retains the Message Age and Max Age mechanisms.

Overview

Feature	Description
STP	STP, defined by the IEEE in 802.1D, is used to eliminate physical loops at the data link layer in a LAN.
RSTP	RSTP, defined by the IEEE in 802.1w, is optimized based on STP to rapidly converge the network topology.
MSTP	MSTP, defined by the IEEE in 802.1s, resolves defects of STP, RSTP, and Per-VLAN Spanning Tree (PVST). It cannot only rapidly converge but also can forward traffic of different VLANs along respective paths, thereby providing a better load balancing mechanism for redundant links.

MSTP Optical Features	MSTP includes the following features: PortFast, BPDU guard, BPDU filter, TC protection, TC guard, TC filter, BPDU check based on the source MAC address, BPDU filter based on the illegal length, Auto Edge, root guard, and loop guard.

9.3.1 STP

STP is used to prevent broadcast storms incurred by loops and provide link redundancy.

Working Principle

For the Layer-2 Ethernet, only one active link can exist between two LANs. Otherwise, a broadcast storm will occur. To enhance the reliability of a LAN, it is necessary to establish a redundant link and keep some paths in backup state. If the network is faulty and a link fails, you must switch the redundant link to the active state. STP can automatically activate the redundant link without any manual operations. STP enables devices on a LAN to:

- Discover and start the best tree topology on the LAN.
- Troubleshoot a fault and automatically update the network topology so that the possible best tree topology is always selected.

The LAN topology is automatically calculated based on a set of bridge parameters configured by the administrator. The best topology tree can be obtained by properly configuring these parameters.

Related Configuration

Enabling spanning-tree

- By default, the spanning-tree function is disabled.
- Run the **spanning-tree** [**forward-time** *seconds* | **hello-time** *seconds* | **max-age** *seconds*] command to enable STP and configure basic attributes.
- The forward-time ranges from 4 to 30. The hello-time ranges from 1 to 10. The max-age ranges from 6 to 40.

Running the **clear** commands may lose vital information and thus interrupt services. The value ranges of forward-time, hello-time, and max-age are related. If one of them is modified, the other two ranges are affected. The three values must meet the following condition: 2 x (Hello Time + 1 second) <= Max-Age Time <= 2 x (Forward-Delay Time –1 second). Otherwise, the configuration will fail.

9.3.2 RSTP

RSTP is completely compatible with 802.1D STP. Similar to traditional STP, RSTP provides loop-free and redundancy services. It is characterized by rapid speed. If all bridges in a LAN support RSTP and are properly configured by the administrator, it takes less than 1 second (about 50 seconds if traditional STP is used) to re-generate a topology tree after the network topology changes.

Working Principle

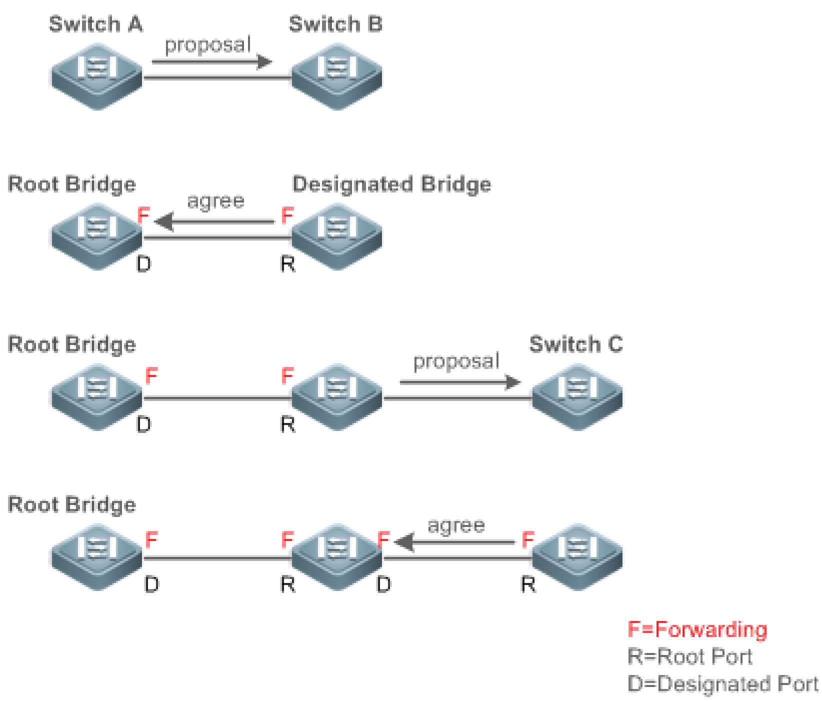
Fast RSTP Convergence

RSTP has a special feature, that is, to make ports quickly enter the forwarding state.

STP enables a port to enter the forwarding state 30 seconds (two times of the Forward-Delay Time; the Forward-Delay Time can be configured, with a default value of 15 seconds) after selecting a port role. Every time the topology changes, the root port and designated port reselected by each bridge enter the forwarding state 30 seconds later. Therefore, it takes about 50 seconds for the entire network topology to become a tree.

RSTP differs greatly from STP in the forwarding process. As shown in Figure 10-6, Switch A sends an RSTP Proposal packet to Switch B. If Switch B finds the priority of Switch A higher, it selects Switch A as the root bridge and the port receiving the packet as the root port, enters the forwarding state, and then sends an Agree packet from the root port to Switch A. If the designated port of Switch A is agreed, the port enters the forwarding state. Switch B's designated port resends a Proposal packet to extend the spanning tree by sequence. Theoretically, RSTP can recover the network tree topology to rapidly converge once the network topology changes.

Figure 10-6



The above handshake process is implemented only when the connection between ports is in point-to-point mode. To give the devices their full play, it is recommended not to enable point-to-point connection between devices.

Figure 10-7 and Figure 10-8 show the examples of non point-to-point connection.

Example of non point-to-point connection:

Figure 10-7

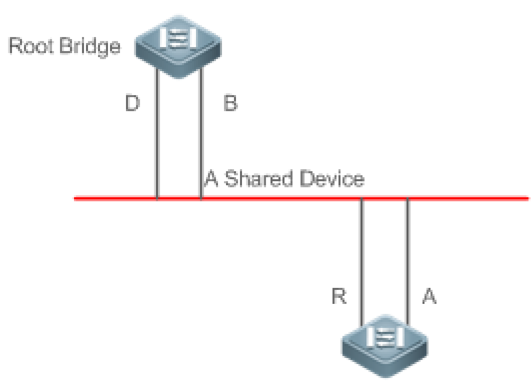


Figure 10-8

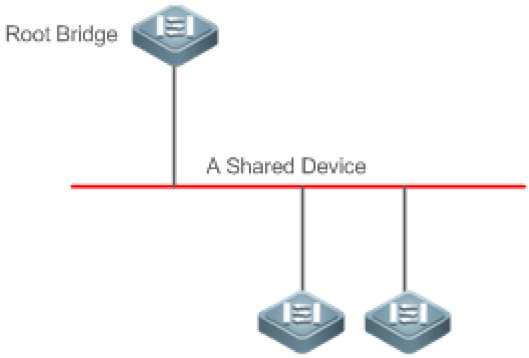
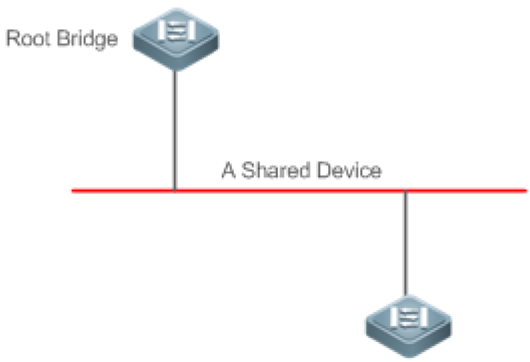


Figure 10-9 shows an example of point-to-point connection.

Figure 10-9



Compatibility Between RSTP and STP

RSTP is completely compatible with STP. RSTP automatically checks whether the connected bridge supports STP or RSTP based on the received BPDU version number. If the port connects to an STP bridge, the port enters the forwarding state 30 seconds later, which cannot give RSTP its full play.

Another problem may occur when RSTP and STP are used together. As shown in the following figures, Switch A (RSTP) connects to Switch B (STP). If Switch A finds itself connected to an STP bridge, it sends an STP BPDU packet. However, if Switch B is replaced with Switch C (RSTP) but Switch A still sends STP BPDU packets, Switch C will assume itself connected to the STP bridge. As a result, two RSTP devices work under STP, greatly reducing the efficiency.

RSTP provides the protocol migration feature to forcibly send RSTP BPDU packets (the peer bridge must support RSTP). In this case, Switch A is enforced to send an RSTP BPDU and Switch C then finds itself connected to the RSTP bridge. As a result, two RSTP devices work under RSTP, as shown in Figure 10-11.

Figure 10-10

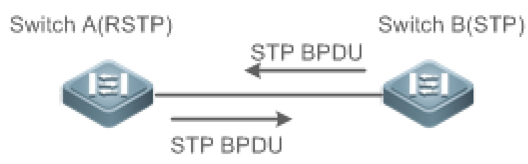
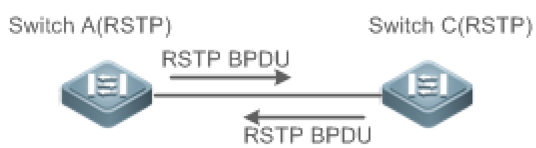


Figure 10-11



Related Configuration

- Configuring Protocol Migration
- Run the clear spanning-tree detected-protocols [interface *interface-id*] command to enforce version check on a port. For details, see "Compatibility Between RSTP and STP".

9.3.3 MSTP

MSTP resolves defects of STP and RSTP. It cannot only rapidly converge but also can forward traffic of different VLANs along respective paths, thereby providing a better load balancing mechanism for redundant links.

Working Principle

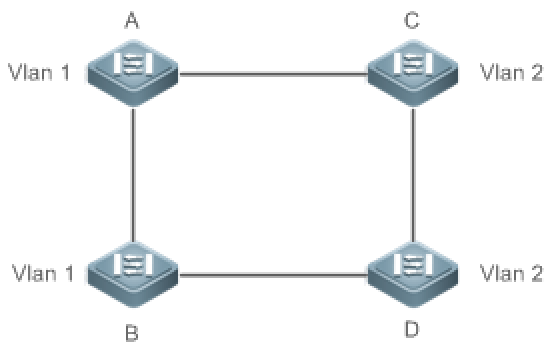
QTECH devices support MSTP. MSTP is a new spanning tree protocol developed from traditional STP and RSTP and includes the fast RSTP forwarding mechanism.

Since traditional spanning tree protocols are irrelevant to VLANs, problems may occur in specific network topologies:

As shown in

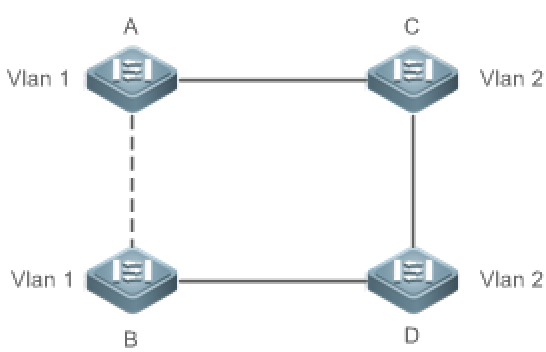
Figure 10-12, Devices A and B are in VLAN 1 while Devices C and D are in VLAN 2, forming a loop.

Figure 10-12



If the link from Device A to Device B through Devices C and D costs less than the link from Device A direct to Device B, the link between Device A and Device B enters the discarding state (as shown in Figure 10-13). Since Devices C and D do not include VLAN 1 and cannot forward data packets of VLAN 1, VLAN 1 of Device A fails to communicate with VLAN 1 of Device B.

Figure 10-13

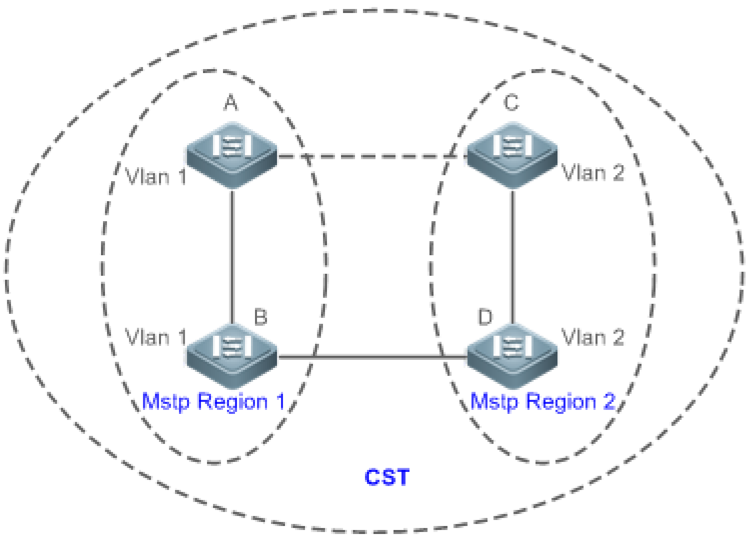


MSTP is developed to resolve this problem. It divides one or multiple VLANs of a device into an instance. Devices configured with the same instance form an MST region to run an independent spanning tree (called IST). This MST region, like a big device, implements the spanning tree algorithm with other MST regions to generate a complete spanning tree called common spanning tree (CST).

Based on this algorithm, the above network can form the topology shown in

Figure 10-14 under the MSTP algorithm: Devices A and B are in MSTP region 1 in which no loop occurs, and therefore no link enters the discarding state. This also applies to MSTP Region 2. Region 1 and Region 2, like two big devices having loops, select a link to enter the discarding state based on related configuration.

Figure 10-14



This prevents loops to ensure proper communication between devices in the same VLAN.

MSTP Region Division

To give MSTP its due play, properly divide MSTP regions and configure the same MST configuration information for devices in the same MSTP region.

MST configuration information include:

- MST configuration name: Consists of at most 32 bytes to identify an MSTP region.
- MST Revision Number: Consists of 16 bits to identify an MSTP region.
- MST instance-VLAN mapping table: A maximum number of 64 instances (with their IDs ranging from 1 to 64) are created for each device and Instance 0 exists mandatorily. Therefore, the system supports a maximum number of 65 instances. Users can assign 1 to 4,994 VLANs belonging to different instances (ranging from 0 to 64) as required. Unassigned VLANs belong to Instance 0 by default. In this case, each MSTI is a VLAN group and implements the spanning tree algorithm of the MSTI specified in the BPDU packet, not affected by CIST and other MSTIs.

Run the **spanning-tree mst configuration** command in global configuration mode to enter the MST configuration mode to configure the above information.

MSTP BPDUs carry the above information. If the BPDU received by a device carries the same MST configuration information with the information on the device, it regards that the connected device belongs to the same MST region with itself. Otherwise, it regards the connected device originated from another MST region.

It is recommended to configure the instance-VLAN mapping table after disabling MSTP. After the configuration, re-enable MSTP to ensure stability and convergence of the network topology.

IST (Spanning Tree in an MSTP Region)

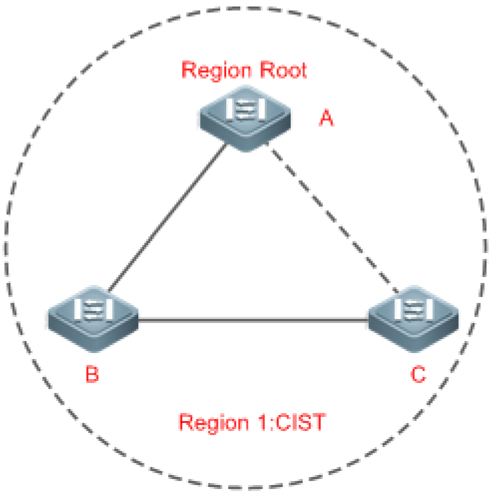
After MSTP regions are divided, each region selects an independent root bridge for each instance based on the corresponding parameters such as bridge priority and port priority, assigns roles to each port on each device, and specifies whether the port is in forwarding or discarding state in the instance based on the port role.

Through MSTP BPDU exchange, an IST is generated and each instance has their own spanning trees (MSTIs), in which the spanning tree corresponding to Instance 0 and CST are uniformly called Common Instance Spanning Tree (CIST). That is, each instance provides a single and loop-free network topology for their own VLAN groups.

As shown in Figure 90-15, Devices A, B, and C form a loop in Region 1.

As shown in Figure 90-15, Device A has the highest priority in the CIST (Instance 0) and thereby is selected as the region root. Then MSTP enables the link between A and C to enter the discarding state based on other parameters. Therefore, for the VLAN group of Instance 0, only links from A to B and from B to C are available, interrupting the loop of this VLAN group.

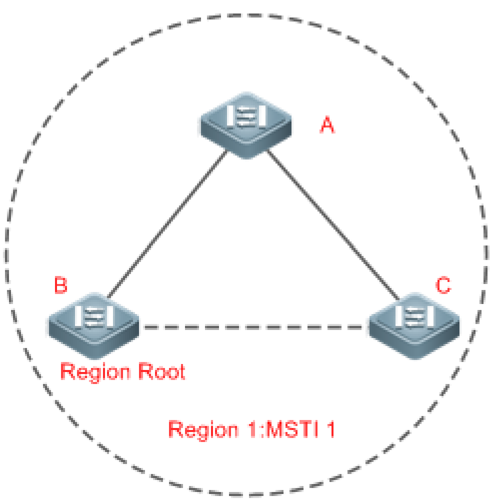
Figure 90-15



As shown in

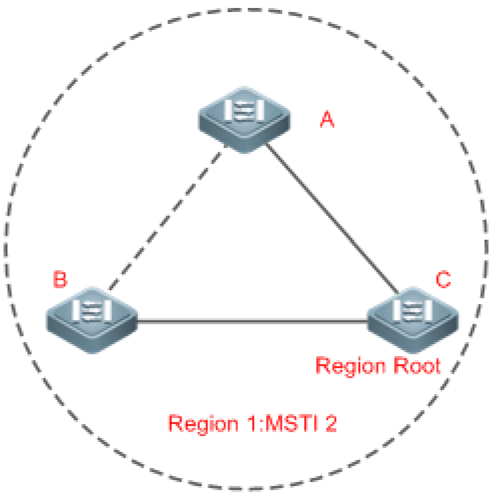
Figure 10-16, Device B has the highest priority in the MSTI 1 (Instance 1) and thereby is selected as the region root. Then MSTP enables the link between B and C to enter the discarding state based on other parameters. Therefore, for the VLAN group of Instance 1, only links from A to B and from A to C are available, interrupting the loop of this VLAN group.

Figure 10-16



As shown in Figure 10-17, Device C has the highest priority in the MSTI 2 (Instance 2) and thereby is selected as the region root. Then MSTP enables the link between B and C to enter the discarding state based on other parameters. Therefore, for the VLAN group of Instance 2, only links from B to C and from A to C are available, interrupting the loop of this VLAN group.

Figure 10-17

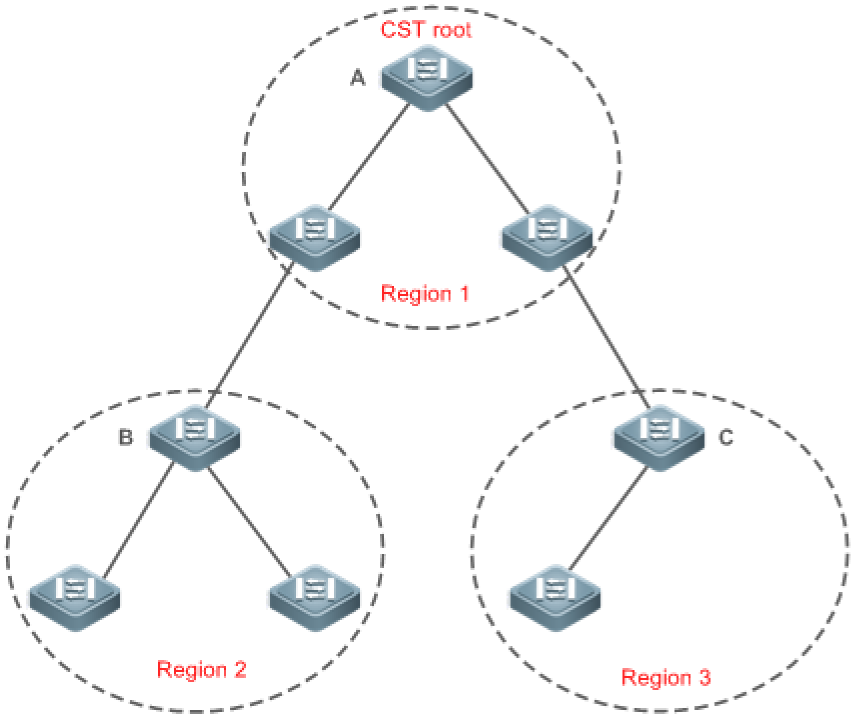


Note that MSTP does not care which VLAN a port belongs to. Therefore, users should configure the path cost and priority of a related port based on the actual VLAN configuration to prevent MSTP from interrupting wrong loops.

CST (Spanning Tree Between MSTP Regions)

Each MSTP region is like a big device for the CST. Different MSTP regions form a bit network topology tree called CST. As shown in Figure 10-18, Device A, of which the bridge ID is the smallest, is selected as the root in the entire CST and the CIST regional root in this region. In Region 2, since the root path cost from Device B to the CST root is lowest, Device B is selected as the CIST regional root in this region. For the same reason, Device C is selected as the CIST regional root.

Figure 10-18



The CIST regional root may not be the device of which the bridge ID is the smallest in the region but indicates the device of which the root path cost from this region to the CST root is the smallest.

For the MSTI, the root port of the CIST regional root has a new role "master port". The master port acts as the outbound port of all instances and is in forwarding state for all instances. To make the topology more stable, we suggest that the master port of each region to the CST root be on the same device of the region if possible.

Compatibility Among MSTP, RSTP, and STP

Similar to RSTP, MSTP sends STP BPDUs to be compatible with STP. For details, see "Compatibility Between RSTP and STP".

Since RSTP processes MSTP BPDUs of the CIST, MSTP does not need to send RSTP BPDUs to be compatible with it.

Each STP or RSTP device is a single region and does not form the same region with any devices.

Related Configuration

Configuring STP

- By default, the STP mode is MSTP mode.
- Run **spanning-tree mode** [**stp | rstp | mstp**] to modify the STP mode.

9.3.4 MSTP Optional Features

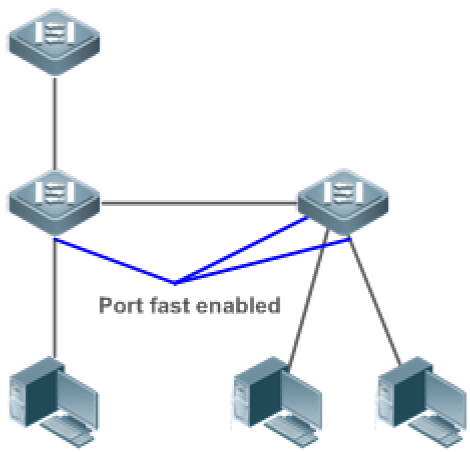
MSTP optional features mainly include PortFast port, BPDU guard, BPDU filter, TC guard, and guard. The optional features are mainly used to deploy MSTP configurations based on the network topology and application characteristics in the MSTP network. This enhances the stability, robustness, and anti-attack capability of MSTP, meeting application requirements of MSTP in different customer scenarios.

Working Principle

- PortFast

If a port of a device connects directly to the network terminal, this port is configured as a PortFast port to directly enter the forwarding state. If the PortFast port is not configured, the port needs to wait for 30 seconds to enter the forwarding state. Figure 10-19 shows which ports of a device can be configured as PortFast ports.

Figure 10-19



If a PortFast port still receives BPDUs, its Port Fast Operational State is Disabled and the port enters the forwarding state according to the normal STP algorithm.

- BPDU Guard

BPDU guard can be enabled globally or enabled on an interface.

It is recommended to run the **spanning-tree portfast bpduguard default** command in global configuration mode to enable global BPDU guard. If PortFast is enabled on a port or this port is automatically identified as an edge port, this port enters the error-disabled state to indicate the configuration error immediately after receiving a BPDU. At the same time, the port is disabled, indicating that a network device may be added by an unauthorized user to change the network topology.

It is also recommended to run the **spanning-tree bpduguard enable** command in interface configuration mode to enable BPDU guard on a port (whether PortFast is enabled or not on the port). In this case, the port enters the error-disabled state immediately after receiving a BPDU.

- BPDU Filter

BPDU filter can be enabled globally or enabled on an interface.

It is recommended to run the **spanning-tree portfast bpdufilter default** command in global configuration mode to enable global BPDU filter. In this case, the PortFast port neither receives nor sends BPDUs and therefore the host connecting directly to the PortFast port receives no BPDUs. If the port changes its Port Fast Operational State to Disabled after receiving a BPDU, BPDU filter automatically loses effect.

It is also recommended to run the **spanning-tree bpdufilter enable** command in interface configuration mode to enable BPDU filter on a port (whether PortFast is enabled or not on the port). In this case, the port neither receives nor sends BPDUs but directly enters the forwarding state.

- TC Protection

TC BPDUs are BPDU packets carrying the TC. If a switch receives such packets, it indicates the network topology changes and the switch will delete the MAC address table. For Layer-3 switches in this case, the forwarding module is re-enabled and the port status in the ARP entry changes. When a switch is attacked by forged TC BPDUs, it will frequently perform the above operations, causing heavy load and affecting network stability. To prevent this problem, you can enable TC protection.

TC protection can only be globally enabled or disabled. This function is disabled by default.

When TC protection is enabled, the switch deletes TC BPDUs within a specified period (generally 4 seconds) after receiving them and monitors whether any TC BPDU packet is received during the period. If a device receives TC BPDU packets during this period, it deletes them when the period expires. This can prevent the device from frequently deleting MAC address entries and ARP entries.

TC Guard

TC protection ensures less dynamic MAC addresses and ARP entries removed when a large number of TC packets are generated on the network. However, a device receiving TC attack packets still performs many removal operations and TC packets can be spread, affecting the entire network. Users can enable TC guard to prevent TC packets from spreading globally or on a port. If TC guard is enabled globally or on a port, a port receiving TC packets filters these TC packets or TC packets generated by itself so that TC packets will not be spread to other ports. This can effectively control possible TC attacks in the network to ensure network stability. Particularly on Layer-3 devices, this function can effectively prevent the access-layer device from flapping and interrupting the core route.

⚠ If TC guard is used incorrectly, the communication between networks is interrupted.

⚠ It is recommended to enable this function only when illegal TC attack packets are received in the network.

⚠ If TC guard is enabled globally, no port spreads TC packets to others. This function can be enabled only on laptop access devices.

⚠ If TC guard is enabled on a port, the topology changes incurred and TC packets received on the port will not be spread to other ports. This function can be enabled only on uplink ports, particularly on ports of the convergence core.

TC Filter

If TC guard is enabled on a port, the port does not forward TC packets received and generated by the port to other ports performing spanning tree calculation on the device. When the status of a port changes (for example, from blocking to forwarding), the port generates TC packets, indicating that the topology may have changed.

In this case, since TC guard prevents TC packets from spreading, the device may not clear the MAC addresses of the port when the network topology changes, causing a data forwarding error.

To resolve this problem, TC filter is introduced. TC filter does not process TC packets received by ports but processes TC packets in case of normal topology changes. If TC filter is enabled, the address removal problem will be avoided and the core route will not be interrupted when ports not enabled with PortFast frequently go up or down, and the core routing entries can be updated in a timely manner when the topology changes.

⚠ TC filter is disabled by default.

BPDU Source MAC Address Check

BPDU source MAC address check prevents BPDU packets from maliciously attacking switches and causing MSTP abnormal. When the switch connected to a port on a point-to-point link is determined, you can enable BPDU source MAC address check to receive BPDU packets sent only by the peer switch and discard all other BPDU packets, thereby preventing malicious attacks. You can enable the BPDU source MAC address check in interface configuration mode for a specific port. One port can only filter one MAC address. If you run the **no bpdu src-mac-check** command to disable BPDU source MAC address check on a port, the port receives all BPDU packets.

BPDU Filter

If the Ethernet length of a BPDU exceeds 1,500, this BPDU will be discarded, preventing receipt of illegal BPDU packets.

Auto Edge

If the designated port of a device does not receive a BPDU from the downlink port within a specific period (3 seconds), the device regards a network device connected to the designated port, configures the port as an edge port, and switches the port directly into the forwarding state. The edge port will be automatically identified as a non-edge port after receiving a BPDU.

You can run the **spanning-tree autoedge disabled** command to disable Auto Edge.

This function is enabled by default.

- If Auto Edge conflicts with the manually configured PortFast, the manual configuration prevails.
- Since this function is used for rapid negotiation and forwarding between the designated port and the downlink port, STP does not support this function. If the designated port is in forwarding state, the Auto Edge configuration does not take effect on this port. It takes only when rapid negotiation is re-performed, for example, when the network cable is removed and plugged.
- If BPDU filter has been enabled on a port, the port directly enters the forwarding state and is not automatically identified as an edge port.
- This function applies only to the designated port.

Root Guard

In the network design, the root bridge and backup root bridge are usually divided into the same region. Due to incorrect configuration of maintenance personnel or malicious attacks in the network, the root bridge may receive configuration information with a higher priority and thereby switches to the backup root bridge, causing incorrect changes in the network topology. Root guard is to resolve this problem.

If root guard is enabled on a port, its roles on all instances are enforced as the designated port. Once the port receives configuration information with a higher priority, it enters the root-inconsistent (blocking) state. If the port does not receive configuration information with a higher priority within a period, it returns to its original state.

If a port enters the blocking state due to root guard, you can manually restore the port to the normal state by disabling root guard on this port or disabling spanning tree guard (running **spanning-tree guard none** in interface configuration mode).

- If root guard is used incorrectly, the network link will be interrupted.
- If root guard is enabled on a non-designated port, this port will be enforced as a designated port and enter the BKN state. This indicates that the port enters the blocking state due to root inconsistency.
- If a port enters the BKN state due to receipt of configuration information with a higher priority in MST0, this port will be enforced in the BKN state in all other instances.
- Root guard and loop guard cannot take effect on a port at the same time.

Loop Guard

Due to the unidirectional link failure, the root port or backup port becomes the designated port and enters the forwarding state if it does not receive BPDUs, causing a network loop. Loop guard is to prevent this problem.

If a port enabled with loop guard does not receive BPDUs, the port switches its role but stays in discarding state till it receives BPDUs and recalculates the spanning tree.

- You can enable loop guard globally or on a port.
- Root guard and loop guard cannot take effect on a port at the same time.
- Before MSTP is restarted on a port, the port enters the blocking state in loop guard. If the port still receives no BPDU after MSTP is restarted, the port will become a designated port and enter the forwarding state. Therefore, it is recommended to identify the cause why a port enters the blocking state in loop protection and rectify the fault as soon as possible before restarting MSTP. Otherwise, the spanning tree topology will still become abnormal after MSTP is restarted.

BPDU Transparent Transmission

In IEEE 802.1Q, the destination MAC address 01-80-C2-00-00-00 of the BPDU is used as a reserved address. That is, devices compliant with IEEE 802.1Q do not forward the BPDU packets received. However, devices may need to transparently transmit BPDU packets in actual network deployment. For example, if STP is disabled on a device, the device needs to transparently transmit BPDU packets so that the spanning tree between devices is properly calculated.

- BPDU transparent transmission is disabled by default.
- BPDU transparent transmission takes effect only when STP is disabled. If STP is enabled on a device, the device does not transparently transmit BPDU packets.

BPDU Tunnel

The QinQ network is generally divided into two parts: customer network and SP network. Before a user packet enters the SP network, it is encapsulated with the VLAN tag of an SP network and also retains the original VLAN tag as data. As a result, the packet carries two VLAN tags to pass through the SP network. In the SP network, packets are transmitted only based on the outer-layer VLAN tag. When packets leave the SP network, the outer-layer VLAN tag is removed.

The STP packet transparent transmission feature, namely BPDU Tunnel, can be used to realize the transmission of STP packets between the customer network without any impact on the SP network. If an STP packet sent from the customer network enters a PE, the PE changes the destination MAC address of the packet to a private address before the packet is forwarded by the SP network. When the packet reaches the PE at the peer end, the PE changes the destination MAC address to a public address and returns the packet to the customer network at the peer end, realizing transparent transmission across the SP network. In this case, STP on the customer network is calculated independently of that on the SP network.

Related Configuration

Configuring PortFast

- PortFast is disabled by default.
- In global configuration mode, run the **spanning-tree portfast default** command to enable PortFast on all ports and the **no spanning-tree portfast default** command to disable PortFast on all ports.
- In interface configuration mode, run the **spanning-tree portfast** command to enable PortFast on a port and the **spanning-tree portfast disabled** command to disable PortFast on a port.

Configuring BPDU Guard

- BPDU guard is disabled by default.
- In global configuration mode, run the **spanning-tree portfast bpduguard default** command to enable BPDU guard on all ports and the **no spanning-tree portfast bpduguard default** command to disable BPDU guard on all ports.
- In interface configuration mode, run the **spanning-tree bpduguard enabled** command to enable BPDU guard on a port and the **spanning-tree bpduguard disabled** command to disable BPDU guard on a port.

Configuring BPDU Filter

- BPDU Filter is disabled by default.
- In global configuration mode, run the **spanning-tree portfast bpdufilter default** command to enable BPDU filter on all ports and the **no spanning-tree portfast bpdufilter default** command to disable BPDU filter on all ports.
- In interface configuration mode, run the **spanning-tree bpdufilter enabled** command to enable BPDU filter on a port and the **spanning-tree bpdufilter disabled** command to disable BPDU filter on a port.

Configuring TC Protection

- TC protection is disabled by default.
- In global configuration mode, run the **spanning-tree tc-protection** command to enable TC protection on all ports and the **no spanning-tree tc-protection** command to disable TC protection on all ports.
- TC protection can only be enabled or disabled globally.

Enabling TC Guard

- TC guard is disabled by default.
- In global configuration mode, run the **spanning-tree tc-protection tc-guard** command to enable TC guard on all ports and the **no spanning-tree tc-protection tc-guard** command to disable TC guard on all ports.
- In interface configuration mode, run the **spanning-tree tc-guard** command to enable TC guard on a port and the **no spanning-tree tc-guard** command to disable TC guard on a port.

Configuring TC Filter

- TC filter is disabled by default.

- In interface configuration mode, run the **spanning-tree ignore tc** command to enable TC filter on a port and the **no spanning-tree ignore tc** command to disable it on a port.

Enabling BPDU Source MAC Address Check

- BPDU Source MAC Address Check is disabled by default.
- In interface configuration mode, run the **bpdu src-mac-check** *H.H.H* command to enable BPDU source MAC address check on a port and the **no bpdu src-mac-check** command to disable it on a port.

Configuring Auto Edge

- Auto Edge is disabled by default.
- In interface configuration mode, run the **spanning-tree autoedge** command to enable Auto Edge on a port and the **spanning-tree autoedge disabled** command to disable it on a port.

Configuring Root Guard

- Root Guard is disabled by default.
- In interface configuration mode, run the **spanning-tree guard root** command to enable root guard on a port and the **no spanning-tree guard root** command to disable it on a port.

Configuring Loop Guard

- Loop Guard is disabled by default.
- In global configuration mode, run the **spanning-tree loopguard default** command to enable loop guard on all ports and the **no spanning-tree loopguard default** command to disable it on all ports.
- In interface configuration mode, run the **spanning-tree guard loop** command to enable loop guard on a port and the **no spanning-tree guard loop** command to disable it on a port.

Configuring BPDU Transparent Transmission

- BPDU Transparent Transmission is disabled by default.
- In global configuration mode, run the **bridge-frame forwarding protocol bpdu** command to enable BPDU transparent transmission and the **no bridge-frame forwarding protocol bpdu** command to disable it.
- BPDU transparent transmission takes effect only when STP is disabled. If STP is enabled on a device, the device does not transparently transmit BPDU packets.

Configuring BPDU Tunnel

- BPDU Tunnel is disabled by default.
- In global configuration mode, run the **l2protocol-tunnel stp** command to globally enable BPDU Tunnel and the **no l2protocol-tunnel stp** command to globally disable it.
- In interface configuration mode, run the **l2protocol-tunnel stp enable** command to enable BPDU Tunnel on a port and the **no l2protocol-tunnel stp enable** command to disable it on a port.
- BPDU Tunnel takes effect only when it is enabled in both global configuration mode and interface configuration mode.

9.4 Configuration

Configuration	Description and Command	
Enabling STP	(Mandatory) It is used to enable STP.	
	spanning-tree	Enables STP and configures basic attributes.
	spanning-tree mode	Configures the STP mode.
Configuring STP Compatibility	(Optional) It is used to be compatible with competitor devices.	
	spanning-tree compatible enable	Enables the compatibility mode of a port.
	clear spanning-tree detected-protocols	Performs mandatory version check for BPDUs.
Configuring an MSTP Region	(Optional) It is used to configure an MSTP region.	
	spanning-tree mst configuration	Enters the MST configuration mode.
Enabling Fast RSTP Convergence	(Optional) It is used to configure whether the link type of a port is point-to-point connection.	
	spanning-tree link-type	Configures the link type.
Configuring Priorities	(Optional) It is used to configure the switch priority or port priority.	
	spanning-tree priority	Configures the switch priority.
	spanning-tree port-priority	Configures the port priority.
Configuring the Port Path Cost	(Optional) It is used to configure the path cost of a port or the default path cost calculation method.	
	spanning-tree cost	Configures the port path cost.

	spanning-tree pathcost method	Configures the default path cost calculation method.
Configuring the Maximum Hop Count of a BPDU Packet	(Optional) It is used to configure the maximum hop count of a BPDU packet.	
	spanning-tree max-hops	Configures the maximum hop count of a BPDU packet.
Enabling PortFast-related Features	(Optional) It is used to enable PortFast-related features.	
	spanning-tree portfast	Enables PortFast.
	spanning-tree portfast bpduguard default	Enables BPDU guard on all ports.
	spanning-tree bpduguard enabled	Enables BPDU guard on a port.
	spanning-tree portfast bpdufilter default	Enables BPDU filter on all ports.
	spanning-tree bpdufilter enabled	Enables BPDU filter on a port.
Enabling TC-related Features	(Optional) It is used to enable TC-related features.	
	spanning-tree tc-protection	Enables TC protection.
	spanning-tree tc-protection tc-guard	Enables TC guard on all ports.
	spanning-tree tc-guard	Enables TC guard on a port.
	spanning-tree ignore tc	Enables TC filter on a port.
Enabling BPDU Source MAC Address Check	(Optional) It is used to enable BPDU source MAC address check.	
	bpdu src-mac-check	Enables BPDU source MAC address check on a port.
Configuring Auto Edge	(Optional) It is used to configure Auto Edge.	

	spanning-tree autoedge	Enables Auto Edge on a port. This function is enabled by default.
Enabling Guard-related Features	(Optional) It is used to enable port guard features.	
	spanning-tree guard root	Enables root guard on a port.
	spanning-tree loopguard default	Enables loop guard on all ports.
	spanning-tree guard loop	Enables loop guard on a port.
	spanning-tree guard none	Disables the guard feature on a port.
Enabling BPDU Transparent Transmission	(Optional) It is used to enable BPDU transparent transmission	
	bridge-frame forwarding protocol bpdu	Enables BPDU transparent transmission.
Enabling BPDU Tunnel	(Optional) It is used to enable BPDU Tunnel.	
	l2protocol-tunnel stp	Enables BPDU Tunnel globally.
	l2protocol-tunnel stp enable	Enables BPDU Tunnel on a port.
	l2protocol-tunnel stp tunnel-dmac	Configures the transparent transmission address of BPDU Tunnel.

9.4.1 Enabling STP

Configuration Effect

- Enable STP globally and configure the basic attributes.
- Configure the STP mode.

Notes

- STP is disabled by default. Once STP is enabled, the device starts to run STP. The device runs MSTP by default.

- The default STP mode is MSTP mode.
- STP and Transparent Interconnection of Lots of Links (TRILL) of the data center cannot be enabled at the same time.
- STP timer parameters take effect only when the device is selected as the root bridge of the spanning tree. That is, the timer parameters of a non-root bridge should use the timer values of the root bridge.

Configuration Steps

Enabling STP

- Mandatory.
- Unless otherwise specified, enable STP on each device.
- Run the **spanning-tree** [**forward-time** *seconds* | **hello-time** *seconds* | **max-age** *seconds*] command to enable STP and configure basic attributes.

Running the **clear** commands may lose vital information and thus interrupt services. The value ranges of forward-time, hello-time, and max-age are related. If one of them is modified, the other two ranges are affected. The three values must meet the following condition: 2 x (Hello Time + 1 second) <= Max-Age Time <= 2 x (Forward-Delay Time –1 second). Otherwise, the topology may become unstable.

Command	**spanning-tree [forward-time *seconds* | hello-time *seconds* | max-age *seconds* | tx-hold-count *numbers*]**
Parameter Description	**forward-time** *seconds*: Indicates the interval when the port status changes. The value ranges from 4 to 30 seconds. The default value is 15 seconds. **hello-time** *seconds*: Indicates the interval when a device sends a BPDU packet. The value ranges from 1 to 10 seconds. The default value is 2 seconds. **max-age** *second*: Indicates the longest TTL of a BPDU packet. The value ranges from 6 to 40 seconds. The default value is 20 seconds. **tx-hold-count** *numbers*: Indicates the maximum number of BPDUs sent per second. The value ranges from 1 to 10. The default value is 3.
Defaults	STP is disabled by default.
Command Mode	Global configuration mode

Usage Guide	The value ranges of forward-time, hello-time, and max-age are related. If one of them is modified, the other two ranges are affected. The three values must meet the following condition: 2 x (Hello Time + 1 second) <= Max-Age Time <= 2 x (Forward-Delay Time – 1 second) Otherwise, the topology may become unstable.

Configuring the STP Mode

- Optional.
- According to related 802.1 protocol standards, STP, RSTP, and MSTP are mutually compatible, without any configuration by the administrator. However, some vendors' devices do not work according to 802.1 protocol standards, possibly causing incompatibility. Therefore, QTECH provides a command for the administrator to switch the STP mode to a lower version if other vendors' devices are incompatible with QTECH devices.
- Run the **spanning-tree mode** [**stp** | **rstp** | **mstp**] command to modify the STP mode.

Command	**spanning-tree mode [stp | rstp | mstp]**
Parameter Description	stp: Spanning Tree Protocol (IEEE 802.1d) rstp: Rapid Spanning Tree Protocol (IEEE 802.1w) mstp: Multiple Spanning Tree Protocol (IEEE 802.1s)
Defaults	The default value is mstp.
Command Mode	Global configuration mode
Usage Guide	However, some vendors' devices do not work according to 802.1 protocol standards, possibly causing incompatibility. If other vendors' devices are incompatible with QTECH devices, run this command to switch the STP mode to a lower version.

Verification

Display the configuration.

Related Commands

Configuring STP

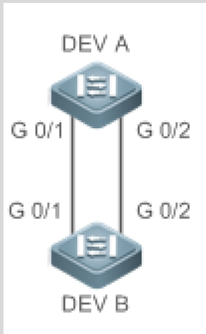
Command	**spanning-tree [forward-time *seconds* | hello-time *seconds* | max-age *seconds* | tx-hold-count *numbers*]**
Parameter Description	**forward-time** *seconds*: Indicates the interval when the port status changes. The value ranges from 4 to 30 seconds. The default value is 15 seconds. **hello-time** *seconds*: Indicates the interval when a device sends a BPDU packet. The value ranges from 1 to 10 seconds. The default value is 2 seconds. **max-age** *second*: Indicates the longest TTL of a BPDU packet. The value ranges from 6 to 40 seconds. The default value is 20 seconds. **tx-hold-count** *numbers*: Indicates the maximum number of BPDUs sent per second. The value ranges from 1 to 10. The default value is 3.
Command Mode	Global configuration mode
Usage Guide	The value ranges of forward-time, hello-time, and max-age are related. If one of them is modified, the other two ranges are affected. The three values must meet the following condition: 2 x (Hello Time + 1 second) <= Max-Age Time <= 2 x (Forward-Delay Time – 1 second) Otherwise, the topology may become unstable and the configuration will fail.

Configuring the STP Mode

Command	**spanning-tree mode [stp | rstp | mstp]**
Parameter Description	**stp**: Spanning Tree Protocol (IEEE 802.1d) **rstp**: Rapid Spanning Tree Protocol (IEEE 802.1w) **mstp**: Multiple Spanning Tree Protocol (IEEE 802.1s)
Command Mode	Global configuration mode
Usage Guide	However, some vendors' devices do not work according to 802.1 protocol standards, possibly causing incompatibility. If other vendors' devices are incompatible with QTECH devices, run this command to switch the STP mode to a lower version.

Configuration Example

Enabling STP and Configuring Timer Parameters

Scenario Figure 10-20	
Configuration Steps	▪ Enable STP and set the STP mode to STP on the devices. ▪ Configure the timer parameters of root bridge DEV A as follows: Hello Time=4s, Max Age=25s, Forward Delay=18s.
DEV A	Step 1: Enable STP and set the STP mode to STP. QTECH#configure terminal Enter configuration commands, one per line. End with CNTL/Z. QTECH(config)#spanning-tree QTECH(config)#spanning-tree mode stp Step 2: Configure the timer parameters of root bridge DEV A. QTECH(config)#spanning-tree hello-time 4 QTECH(config)#spanning-tree max-age 25 QTECH(config)#spanning-tree forward-time 18
DEV B	Enable STP and set the STP mode to STP. QTECH#configure terminal Enter configuration commands, one per line. End with CNTL/Z. QTECH(config)#spanning-tree QTECH(config)#spanning-tree mode stp
Verification	▪ Run the **show spanning-tree summary** command to display the spanning tree topology and protocol configuration parameters.
DEV A	QTECH#show spanning-tree summary

	Spanning tree enabled protocol stp Root ID Priority 0 Address 08c6.b3.3344 this bridge is root Hello Time 4 sec Forward Delay 18 sec Max Age 25 sec Bridge ID Priority 0 Address 08c6.b3.3344 Hello Time 4 sec Forward Delay 18 sec Max Age 25 sec Interface Role Sts Cost Prio OperEdge Type ---------------- ---- --- ---------- -------- -------- ---------------- Gi0/2 Desg FWD 20000 128 False P2p Gi0/1 Desg FWD 20000 128 False P2p
DEV B	QTECH#show spanning-tree summary Spanning tree enabled protocol stp Root ID Priority 0 Address 08c6.b3.3344 this bridge is root Hello Time 4 sec Forward Delay 18 sec Max Age 25 sec Bridge ID Priority 32768 Address 08c6.b3.78cc Hello Time 2 sec Forward Delay 15 sec Max Age 20 sec Interface Role Sts Cost Prio OperEdge Type ---------------- ---- --- ---------- -------- -------- ---------------- Gi0/2 Altn BLK 20000 128 False P2p Bound(STP) Gi0/1 Root FWD 20000 128 False P2p Bound(STP)

Common Errors

N/A

9.4.2 Configuring STP Compatibility

Configuration Effect

- Enable the compatibility mode of a port to realize interconnection between QTECH devices and other SPs' devices.
- Enable protocol migration to perform forcible version check to affect the compatibility between RSTP and STP.

Notes

- If the compatibility mode is enabled on a port, this port will add different MSTI information into the to-be-sent BPDU based on the current port to realize interconnection between QTECH devices and other SPs' devices.
- When enabling compatibility on a port, ensure correct VLAN trimming information of the port. It is recommended to configure consistent VLAN lists for ports at both ends of the link.

Configuration Steps

Enabling the Compatibility Mode on a Port

- Optional.
- Configuring Protocol Migration
- Optional.
- If the peer device supports RSTP, you can enforce version check on the local device to force the two devices to run RSTP.

Verification

Display the configuration.

Related Commands

Enabling the Compatibility Mode on a Port

Command	spanning-tree compatible enable
Parameter Description	N/A

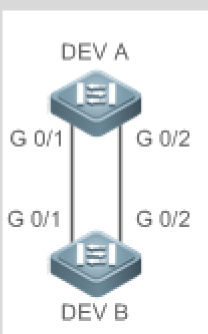
Defaults	The compatibility mode is disabled on a port by default.
Command Mode	Interface configuration mode
Usage Guide	If the compatibility mode is enabled on a port, this port will add different MSTI information into the to-be-sent BPDU based on the current port to realize interconnection between QTECH devices and other SPs' devices.

Enabling Protocol Migration

Command	**clear spanning-tree detected-protocols [interface *interface-id*]**
Parameter Description	**interface** *interface-id*: Indicates a port.
Command Mode	Privileged EXEC mode
Usage Guide	This command is used to enforce a port to send RSTP BPDU packets and perform forcible check on them.

Configuration Example

Enabling STP Compatibility

Scenario Figure 10-21	
Configuration Steps	▪ Configure Instances 1 and 2 on Devices A and B, and map Instance 1 with VLAN 10 and Instance 2 with VLAN 20. ▪ Configure Gi0/1 and Gi0/2 to respectively belong to VLAN 10 and VLAN 20, and enable STP compatibility.

DEV A	Step 1: Configure Instances 1 and 2, and map Instances 1 and 2 respectively with VLANs 10 and 20. QTECH#configure terminal Enter configuration commands, one per line. End with CNTL/Z. QTECH(config)#spanning-tree mst configuration QTECH(config-mst)#instance 1 vlan 10 QTECH(config-mst)#instance 2 vlan 20 Step 2: Configure the VLAN the port belongs to, and enable STP compatibility on the port. QTECH(config)#int gi 0/1 QTECH(config-if-GigabitEthernet 0/1)#switchport access vlan 10 QTECH(config-if-GigabitEthernet 0/1)#spanning-tree compatible enable QTECH(config-if-GigabitEthernet 0/1)#int gi 0/2 QTECH(config-if-GigabitEthernet 0/2)#switchport access vlan 20 QTECH(config-if-GigabitEthernet 0/2)#spanning-tree compatible enable
DEV B	Perform the same steps as DEV A.
Verification	▪ Run the **show spanning-tree summary** command to check whether the spanning tree topology is correctly calculated.
DEV A	QTECH#show spanning-tree summary Spanning tree enabled protocol mstp MST 0 vlans map : 1-9, 11-19, 21-4094 Root ID Priority 32768 Address 08c6.b3.78cc this bridge is root Hello Time 2 sec Forward Delay 15 sec Max Age 20 sec Bridge ID Priority 32768 Address 08c6.b3.78cc Hello Time 2 sec Forward Delay 15 sec Max Age 20 sec

	Interface Role Sts Cost Prio OperEdge Type ---------------- ---- --- ---------- -------- -------- ---------------- Gi0/2 Desg FWD 20000 128 False P2p Gi0/1 Desg FWD 20000 128 False P2p MST 1 vlans map : 10 Region Root Priority 32768 Address 08c6.b3.78cc this bridge is region root Bridge ID Priority 32768 Address 08c6.b3.78cc Interface Role Sts Cost Prio OperEdge Type ---------------- ---- --- ---------- -------- -------- ---------------- Gi0/1 Desg FWD 20000 128 False P2p MST 2 vlans map : 20 Region Root Priority 32768 Address 08c6.b3.78cc this bridge is region root Bridge ID Priority 32768 Address 08c6.b3.78cc Interface Role Sts Cost Prio OperEdge Type ---------------- ---- --- ---------- -------- -------- ---------------- Gi0/2 Desg FWD 20000 128 False P2p
DEV B	QTECH#show spanning-tree summary Spanning tree enabled protocol mstp MST 0 vlans map : 1-9, 11-19, 21-4094

```
 Root ID    Priority    32768
            Address     08c6.b3.78cc
            this bridge is root
            Hello Time   2 sec  Forward Delay 15 sec  Max Age 20 sec

 Bridge ID  Priority    32768
            Address     08c6.b3.3344
            Hello Time   4 sec  Forward Delay 18 sec  Max Age 25 sec

Interface        Role Sts Cost       Prio     OperEdge Type
---------------- ---- --- ---------- -------- -------- ----------------
Gi0/2            Altn BLK 20000      128      False    P2p
Gi0/1            Root FWD 20000      128      False    P2p

MST 1 vlans map : 10
 Region Root Priority   32768
            Address     08c6.b3.78cc
            this bridge is region root

 Bridge ID  Priority    32768
            Address     08c6.b3.3344

Interface        Role Sts Cost       Prio     OperEdge Type
---------------- ---- --- ---------- -------- -------- ----------------
Gi0/1            Root FWD 20000      128      False    P2p

MST 2 vlans map : 20
 Region Root Priority   32768
            Address     08c6.b3.78cc
            this bridge is region root

 Bridge ID  Priority    32768
            Address     08c6.b3.3344
```

```
Interface       Role Sts Cost       Prio     OperEdge Type
---------------- ---- --- ---------- -------- -------- ----------------
Gi0/2          Root FWD 20000      128      False    P2p
```

Common Errors

N/A

9.4.3 Configuring an MSTP Region

Configuration Effect

Configure an MSTP region to adjust which devices belong to the same MSTP region and thereby affect the network topology.

Notes

- To make multiple devices belong to the same MSTP region, configure the same name, revision number, and instance-VLAN mapping table for them.
- You can configure VLANs for Instances 0 to 64, and then the remaining VLANs are automatically allocated to Instance 0. One VLAN belongs to only one instance.
- It is recommended to configure the instance-VLAN mapping table after disabling STP. After the configuration, re-enable MSTP to ensure stability and convergence of the network topology.

Configuration Steps

Configuring an MSTP Region

- Optional.
- Configure an MSTP region when multiple devices need to belong to the same MSTP region.

Verification

Display the configuration.

Related Commands

Entering MSTP Region Configuration Mode

- Optional.
- Configure an MSTP region when multiple devices need to belong to the same MSTP region.

- Run the **spanning-tree mst configuration** command to enter the MST configuration mode.
- Run the **instance** *instance-id* **vlan** *vlan-range* command to configure the MSTI-VLAN mapping.
- Run the **name** *name* command to configure the MST name.
- Run the **revision** *version* command to configure the MST version number.

Command	**spanning-tree mst configuration**
Parameter Description	N/A
Command Mode	Global configuration mode
Usage Guide	Run this command to enter the MST configuration mode.

Configuring Instance-VLAN Mapping

Command	**instance *instance-id* vlan *vlan-range***
Parameter Description	*instance-id*: Indicates the MSTI ID, ranging from 0 to 64. *vlan-range*: Indicates the VLAN ID, ranging from 1 to 4,094.
Defaults	The default instance-VLAN mapping is that all VLANs are in Instance 0.
Command Mode	MST configuration mode
Usage Guide	To add a VLAN group to an MSTI, run this command. For example, instance 1 vlan 2-200: Adds VLANs 2 to 200 to Instance 1. instance 1 vlan 2,20,200: Adds VLANs 2, 20, and 200 to Instance 1. You can use the no form of this command to remove VLANs from an instance. Removed VLANs are automatically forwarded to Instance 0.

Configuring MST Version Name

Command	**name** *name*
Parameter Description	*name*: Indicates the MST name. It consists of a maximum of 32 bytes.
Defaults	The default name is an empty character string.
Command Mode	MST configuration mode
Usage Guide	N/A

Configuring MST Version Number

Command	**revision** *version*
Parameter Description	*version*: Indicates the MST revision number, ranging from 0 to 65,535.
Defaults	The default revision number is 0.
Command Mode	MST configuration mode
Usage Guide	N/A

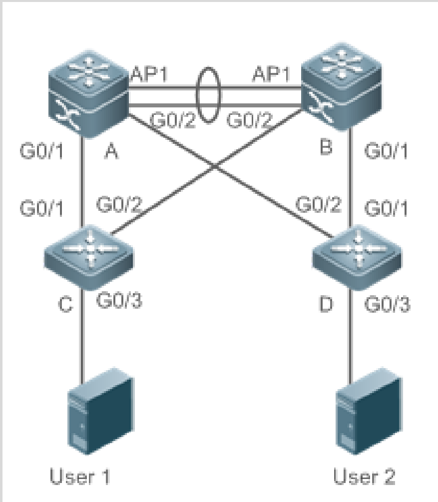
Verification

Display the configuration.

- Run the **show spanning-tree mst configuration** command to display the MSTP region configuration.

Configuration Example

Enabling MSTP to Achieve VLAN Load Balancing in the MSTP+VRRP Topology

Scenario **Figure 10-22**	
Configuration Steps	▪ Enable MSTP and create Instances 1 and 2 on Switches A, B, C, and D. ▪ Configure Switch A as the root bridge of Instances 0 and 1 and Switch B as the root bridge of Instance 2. ▪ Configure Switch A as the VRRP master device of VLANs 1 and 10 and Switch B as the VRRP master device of VLAN 20.
A	Step 1: Configure VLANs 10 and 20, and configure ports as Trunk ports. A(config)#vlan 10 A(config-vlan)#vlan 20 A(config-vlan)#exit A(config)#int range gi 0/1-2 A(config-if-range)#switchport mode trunk A(config-if-range)#int ag 1 A(config-if-AggregatePort 1)# switchport mode trunk Step 2: Enable MSTP and create Instances 1 and 2. A(config)#spanning-tree A(config)# spanning-tree mst configuration A(config-mst)#instance 1 vlan 10 A(config-mst)#instance 2 vlan 20 A(config-mst)#exit Step 3: Configure Switch A as the root bridge of Instances 0 and 1. A(config)#spanning-tree mst 0 priority 4096

	A(config)#spanning-tree mst 1 priority 4096 A(config)#spanning-tree mst 2 priority 8192 Step 4: Configure VRRP priorities to enable Switch A to act as the VRRP master device of VLAN 10, and configure the virtual gateway IP address of VRRP. A(config)#interface vlan 10 A(config-if-VLAN 10)ip address 192.168.10.2 255.255.255.0 A(config-if-VLAN 10) vrrp 1 priority 120 A(config-if-VLAN 10) vrrp 1 ip 192.168.10.1 Step 5 Set the VRRP priority to the default value 100 to enable Switch A to act as the VRRP backup device of VLAN 20. A(config)#interface vlan 20 A(config-if-VLAN 20)ip address 192.168.20.2 255.255.255.0 A(config-if-VLAN 20) vrrp 1 ip 192.168.20.1
B	Step 1: Configure VLANs 10 and 20, and configure ports as Trunk ports. B(config)#vlan 10 B(config-vlan)#vlan 20 B(config-vlan)#exit B(config)#int range gi 0/1-2 B(config-if-range)#switchport mode trunk B(config-if-range)#int ag 1 B(config-if-AggregatePort 1)# switchport mode trunk Step 2: Enable MSTP and create Instances 1 and 2. B(config)#spanning-tree B(config)# spanning-tree mst configuration B(config-mst)#instance 1 vlan 10 B(config-mst)#instance 2 vlan 20 B(config-mst)#exit Step 3: Configure Switch A as the root bridge of Instance 2. B(config)#spanning-tree mst 0 priority 8192

	B(config)#spanning-tree mst 1 priority 8192 B(config)#spanning-tree mst 2 priority 4096 Step 4: Configure the virtual gateway IP address of VRRP. B(config)#interface vlan 10 B(config-if-VLAN 10)ip address 192.168.10.3 255.255.255.0 B(config-if-VLAN 10) vrrp 1 ip 192.168.10.1 Step 5 Set the VRRP priority to 120 to enable Switch B to act as the VRRP backup device of VLAN 20. B(config)#interface vlan 20 B(config-if-VLAN 20)vrrp 1 priority 120 B(config-if-VLAN 20)ip address 192.168.20.3 255.255.255.0 B(config-if-VLAN 20) vrrp 1 ip 192.168.20.1
C	Step 1: Configure VLANs 10 and 20, and configure ports as Trunk ports. C(config)#vlan 10 C(config-vlan)#vlan 20 C(config-vlan)#exit C(config)#int range gi 0/1-2 C(config-if-range)#switchport mode trunk Step 2: Enable MSTP and create Instances 1 and 2. C(config)#spanning-tree C(config)# spanning-tree mst configuration C(config-mst)#instance 1 vlan 10 C(config-mst)#instance 2 vlan 20 C(config-mst)#exit Step 3: Configure the port connecting Device C directly to users as a PortFast port and enable BPDU guard. C(config)#int gi 0/3 C(config-if-GigabitEthernet 0/3)#spanning-tree portfast C(config-if-GigabitEthernet 0/3)#spanning-tree bpduguard enable

D	Perform the same steps as Device C.
Verification	▪ Run the **show spanning-tree summary** command to check whether the spanning tree topology is correctly calculated. ▪ Run the **show vrrp brief** command to check whether the VRRP master/backup devices are successfully created.
A	QTECH#show spanning-tree summary Spanning tree enabled protocol mstp MST 0 vlans map : 1-9, 11-19, 21-4094 Root ID Priority 4096 Address 08c6.b3.3344 this bridge is root Hello Time 4 sec Forward Delay 18 sec Max Age 25 sec Bridge ID Priority 4096 Address 08c6.b3.3344 Hello Time 4 sec Forward Delay 18 sec Max Age 25 sec Interface Role Sts Cost Prio OperEdge Type ---------------- ---- --- ---------- -------- -------- ---------------- Ag1 Desg FWD 19000 128 False P2p Gi0/1 Desg FWD 200000 128 False P2p Gi0/2 Desg FWD 200000 128 False P2p MST 1 vlans map : 10 Region Root Priority 4096 Address 08c6.b3.3344 this bridge is region root Bridge ID Priority 4096 Address 08c6.b3.3344 Interface Role Sts Cost Prio OperEdge Type ---------------- ---- --- ---------- -------- -------- ---------------- Ag1 Desg FWD 19000 128 False P2p Gi0/1 Desg FWD 200000 128 False P2p Gi0/2 Desg FWD 200000 128 False P2p

<table>
<tr><td></td><td><pre>
MST 2 vlans map : 20
  Region Root Priority   4096
          Address   08c6.b3.78cc
          this bridge is region root

  Bridge ID Priority   8192
          Address   08c6.b3.3344

Interface   Role Sts Cost   Prio   OperEdge Type
---------------- ---- --- ---------- -------- -------- ----------------
Ag1   Root FWD 19000   128   False   P2p
Gi0/1   Desg FWD 200000   128   False   P2p
Gi0/2   Desg FWD 200000   128   False   P2p
</pre></td></tr>
<tr><td>B</td><td><pre>
QTECH#show spanning-tree summary

Spanning tree enabled protocol mstp
MST 0 vlans map : 1-9, 11-19, 21-4094
  Root ID   Priority   4096
          Address   08c6.b3.3344
          this bridge is root
          Hello Time   4 sec Forward Delay 18 sec Max Age 25 sec

  Bridge ID Priority   8192
          Address   08c6.b3.78cc
          Hello Time   2 sec Forward Delay 15 sec Max Age 20 sec
Interface   Role Sts Cost   Prio   OperEdge Type
---------------- ---- --- ---------- -------- -------- ----------------
Ag1   Root FWD 19000   128   False   P2p
Gi0/1   Desg FWD 200000   128   False   P2p
Gi0/2   Desg FWD 200000   128   False   P2p
MST 1 vlans map : 10
  Region Root Priority   4096
</pre></td></tr>
</table>

	Address 08c6.b3.3344 this bridge is region root Bridge ID Priority 8192 Address 08c6.b3.78cc Interface Role Sts Cost Prio OperEdge Type ---------------- ---- --- ---------- -------- -------- ---------------- Ag1 Root FWD 19000 128 False P2p Gi0/1 Desg FWD 200000 128 False P2p Gi0/2 Desg FWD 200000 128 False P2p MST 2 vlans map : 20 Region Root Priority 4096 Address 08c6.b3.78cc this bridge is region root Bridge ID Priority 4096 Address 08c6.b3.78cc Interface Role Sts Cost Prio OperEdge Type ---------------- ---- --- ---------- -------- -------- ---------------- Ag1 Desg FWD 19000 128 False P2p Gi0/1 Desg FWD 200000 128 False P2p Gi0/2 Desg FWD 200000 128 False P2p
C	QTECH#show spanning-tree summary Spanning tree enabled protocol mstp MST 0 vlans map : 1-9, 11-19, 21-4094 Root ID Priority 4096 Address 08c6.b3.3344 this bridge is root Hello Time 4 sec Forward Delay 18 sec Max Age 25 sec Bridge ID Priority 32768 Address 08c6.b3.00ea

```
          Hello Time   2 sec  Forward Delay 15 sec  Max Age 20 sec

Interface        Role Sts Cost       Prio     Type  OperEdge
---------------- ---- --- ---------- -------- ----- ---------------
Fa0/2            Altn BLK 200000     128      P2p   False
Fa0/1            Root FWD 200000     128      P2p   False

MST 1 vlans map : 10
  Region Root Priority   4096
          Address     08c6.b3.3344
          this bridge is region root

  Bridge ID  Priority    32768
          Address     08c6.b3.00ea

Interface        Role Sts Cost       Prio     Type  OperEdge
---------------- ---- --- ---------- -------- ----- ---------------
Fa0/2            Altn BLK 200000     128      P2p   False
Fa0/1            Root FWD 200000     128      P2p   False

MST 2 vlans map : 20
  Region Root Priority   4096
          Address     08c6.b3.78cc
          this bridge is region root

  Bridge ID  Priority    32768
          Address     08c6.b3.00ea

Interface        Role Sts Cost       Prio     Type  OperEdge
---------------- ---- --- ---------- -------- ----- ---------------
Fa0/2            Root FWD 200000     128      P2p   False
Fa0/1            Altn BLK 200000     128      P2p   False
```

D	Omitted.

Common Errors

- MST region configurations are inconsistent in the MSTP topology.
- VLANs are not created before you configure the mapping between the instance and VLAN.
- A device runs STP or RSTP in the MSTP+VRRP topology, but calculates the spanning tree according to the algorithms of different MST regions.

9.4.4 Enabling Fast RSTP Convergence

Configuration Effect

Configure the link type to make RSTP rapidly converge.

Notes

- If the link type of a port is point-to-point connection, RSTP can rapidly converge. For details, see "Fast RSTP Convergence". If the link type is not configured, the device automatically sets the link type based on the duplex mode of the port. If a port is in full duplex mode, the device sets the link type to point-to-point. If a port is in half duplex mode, the device sets the link type to shared. You can also forcibly configure the link type to determine whether the port connection is point-to-point connection.
- The link type of a port is related to the rate and duplex mode. If the port is in half duplex mode, the link type is shared.

Configuration Steps

Configuring the Link Type

- Optional.

Verification

Display the configuration.

- Run the **show spanning-tree** [**mst** *instance-id*] **interface** *interface-id* command to display the spanning tree configuration of the port.

Related Commands

Configuring the Link Type

Command	**spanning-tree link-type [point-to-point | shared]**
Parameter Description	**point-to-point**: Forcibly configures the link type of a port to be point-to-point. **shared**: Forcibly configures the link type of a port to be shared.
Defaults	If a port is in full duplex mode, the link type of the port is point-to-point. If a port is in half duplex mode, the link type of the port is shared.
Command Mode	Interface configuration mode
Usage Guide	If the link type of a port is point-to-point connection, RSTP can rapidly converge. If the link type is not configured, the device automatically sets the link type based on the duplex mode of the port.

Configuration Example

Enabling Fast RSTP Convergence

Configuration Steps	**Set the link type of a port to point-to-point.**
	QTECH(config)#int gi 0/1 QTECH(config-if-GigabitEthernet 0/1)#spanning-tree link-type point-to-point
Verification	▪ Run the **show spanning-tree summary** command to display the link type of the port.
	QTECH#show spanning-tree summary Spanning tree enabled protocol mstp MST 0 vlans map : ALL Root ID Priority 32768 Address 08c6.b3.78cc this bridge is root Hello Time 2 sec Forward Delay 15 sec Max Age 20 sec

```
Bridge ID  Priority    32768
           Address     08c6.b3.3344
           Hello Time   2 sec  Forward Delay 15 sec  Max Age 20 sec

Interface       Role Sts Cost       Prio     OperEdge Type
---------------- ---- --- ---------- -------- -------- ----------------
Gi0/1           Root FWD 20000      128      False    P2p
```

Common Errors

N/A

9.4.5 Configuring Priorities

Configuration Effect

- Configure the switch priority to determine a device as the root of the entire network and to determine the topology of the entire network.
- Configure the port priority to determine which port enters the forwarding state.

Notes

- It is recommended to set the priority of the core device higher (to a smaller value) to ensure stability of the entire network. You can assign different switch priorities to different instances so that each instance runs an independent STP based on the assigned priorities. Devices in different regions use the priority only of the CIST (Instance 0). As described in bridge ID, the switch priority has 16 optional values: 0, 4,096, 8,192, 12,288, 16,384, 20,480, 24,576, 28,672, 32,768, 36,864, 40,960, 45,056, 49,152, 53,248, 57,344, 61,440. They are integral multiples of 4,096. The default value is 32,768.
- If two ports are connected to a shared device, the device selects a port with a higher priority (smaller value) to enter the forwarding state and a port with a lower priority (larger value) to enter the discarding state. If the two ports have the same priority, the device selects the port with a smaller port ID to enter the forwarding state. You can assign different port priorities to different instances on a port so that each instance runs an independent STP based on the assigned priorities.
- Similar to the switch priority, the port priority also has 16 optional values: 0, 16, 32, 48, 64, 80, 96, 112, 128, 144, 160, 176, 192, 208, 224, 240. They are integral multiples of 16. The default value is 128.
- The modified port priority takes effect only on the designated port.

Configuration Steps

Configuring the Switch Priority

- Optional.
- To change the root or topology of a network, configure the switch priority.
- Configuring the Port Priority
- Optional.
- To change the preferred port entering the forwarding state, configure the port priority.

Verification

Display the configuration.

- Run the **show spanning-tree** [**mst** *instance-id*] **interface** *interface-id* command to display the spanning tree configuration of the port.

Related Commands

Configuring the Switch Priority

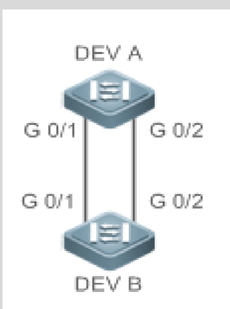
Command	spanning-tree [mst *instance-id*] priority *priority*
Parameter Description	**mst** *instance-id*: Indicates the instance ID, ranging from 0 to 64. **priority** *priority*: Indicates the switch priority. There are 16 optional values: 0, 4,096, 8,192, 12,288, 16,384, 20,480, 24,576, 28,672, 32,768, 36,864, 40,960, 45,056, 49,152, 53,248, 57,344, 61,440. They are integral multiples of 4,096.
Defaults	The default value of *instance-id* is 0 while that of *priority* is 32,768.
Command Mode	Global configuration mode
Usage Guide	Configure the switch priority to determine a device as the root of the entire network and to determine the topology of the entire network.

Configuring the Port Priority

Command	spanning-tree [mst *instance-id*] port-priority *priority*
Parameter Description	**mst** *instance-id*: Indicates the instance ID, ranging from 0 to 64. **port-priority** *priority*: Indicates the port priority. There are 16 optional values: 0, 16, 32, 48, 64, 80, 96, 112, 128, 144, 160, 176, 192, 208, 224, 240. They are integral multiples of 4,096.
Defaults	The default value of *instance-id* is 0. The default value of *priority* is 128.
Command Mode	Interface configuration mode
Usage Guide	If a loop occurs in a region, the port with a higher priority is preferred to enter the forwarding state. If two ports have the same priority, the port with a smaller port ID is selected to enter the forwarding state. Run this command to determine which port in the loop of a region enters the forwarding state.

Configuration Example

Configuring the Port Priority

Scenario Figure 10-23	
Configuration Steps	▪ Configure the bridge priority so that DEV A becomes the root bridge of the spanning tree. ▪ Configure the priority of Gi0/2 on DEV A is 16 so that Gi0/2 on DEV B can be selected as the root port.
DEV A	Step 1: Enable STP and configure the bridge priority. `QTECH(config)#spanning-tree`

	QTECH(config)#spanning-tree mst 0 priority 0 Step 2: Configure the priority of Gi 0/2. QTECH(config)# int gi 0/2 QTECH(config-if-GigabitEthernet 0/2)#spanning-tree mst 0 port-priority 16
DEV B	QTECH(config)#spanning-tree
Verification	▪ Run the **show spanning-tree summary** command to display the topology calculation result of the spanning tree.
DEV A	QTECH# QTECH#show spanning-tree summary Spanning tree enabled protocol mstp MST 0 vlans map : ALL Root ID Priority 0 Address 08c6.b3.3344 this bridge is root Hello Time 2 sec Forward Delay 15 sec Max Age 20 sec Bridge ID Priority 0 Address 08c6.b3.3344 Hello Time 2 sec Forward Delay 15 sec Max Age 20 sec Interface Role Sts Cost Prio OperEdge Type ---------------- ---- --- ---------- -------- -------- ---------------- Gi0/2 Desg FWD 20000 16 False P2p Gi0/1 Desg FWD 20000 128 False P2p
DEV B	QTECH#show spanning-tree summary Spanning tree enabled protocol mstp MST 0 vlans map : ALL Root ID Priority 0 Address 08c6.b3.3344 this bridge is root Hello Time 2 sec Forward Delay 15 sec Max Age 20 sec

```
 Bridge ID  Priority    32768
            Address     08c6.b3.78cc
            Hello Time   2 sec  Forward Delay 15 sec  Max Age 20 sec

Interface       Role Sts Cost       Prio     OperEdge Type
---------------- ---- --- ---------- -------- -------- ----------------
Gi0/2           Root FWD 20000      128      False    P2p
Gi0/1           Altn BLK 20000      128      False    P2p
```

Common Errors

N/A

9.4.6 Configuring the Port Path Cost

Configuration Effect

- Configure the path cost of a port to determine the forwarding state of the port and the topology of the entire network.
- If the path cost of a port uses its default value, configure the path cost calculation method to affect the calculation result.

Notes

- A device selects a port as the root port if the path cost from this port to the root bridge is the lowest. Therefore, the port path cost determines the root port of the local device. The default port path cost is automatically calculated based on the port rate (Media Speed). A port with a higher rate will have a low path cost. Since this method can calculate the most scientific path cost, do not change the path cost unless required. You can assign different path costs to different instances on a port so that each instance runs an independent STP based on the assigned path costs.
- If the port path cost uses the default value, the device automatically calculates the port path cost based on the port rate. However, IEEE 802.1d-1998 and IEEE 802.1t define different path costs for the same link rate. The value is a short integer ranging from 1 to 65,535 in 802.1d-1998 while is a long integer ranging from 1 to 200,000,000 in IEEE 802.1t. The path cost of an aggregate port (AP) has two solutions: 1. QTECH solution: Port Path Cost x 95%; 2. Solution recommended in standards: 20,000,000,000/Actual link bandwidth of the AP, in which Actual link bandwidth of the AP = Bandwidth of a member port x Number of active member ports. The administrator must unify the

path cost calculation method in the entire network. The default standard is the private long integer standard.

- The following table lists path costs automatically configured for different link rate in two solutions.

Port Rate	Port	IEEE 802.1d (short)	IEEE 802.1t (long)	IEEE 802.1t (long standard)
10M	Common port	100	2000000	2000000
	AP	95	1900000	2000000÷linkupcnt
100M	Common port	19	200000	200000
	AP	18	190000	200000÷linkupcnt
1000M	Common port	4	20000	20000
	AP	3	19000	20000÷linkupcnt
10000M	Common port	2	2000	2000
	AP	1	1900	20000÷linkupcnt

- QTECH's long integer standard is used by default. After the solution is changed to the path cost solution recommended by the standards, the path cost of an AP changes with the number of member ports in UP state. If the port path cost changes, the network topology also will change.
- If an AP is static, linkupcnt in the table is the number of active member ports. If an AP is an LACP AP, linkupcnt in the table is the number of member ports forwarding AP data. If no member port in the AP goes up, linkupcnt is 1. For details about AP and LACP, see the *Configuring AP*.
- The modified port path cost takes effect only on the Rx port.

Configuration Steps

Configuring the Port Path Cost

- Optional.
- To determine which port or path data packets prefer to pass through, configure the port path cost.
- Configuring the Default Path Cost Calculation Method
- Optional.
- To change the path cost calculation method, configure the default path cost calculation method.

Verification

Display the configuration.

- Run the **show spanning-tree** [**mst** *instance-id*] **interface** *interface-id* command to display the spanning tree configuration of the port.

Related Commands

Configuring the Port Path Cost

Command	**spanning-tree [mst *instance-id*] cost *cost***
Parameter Description	mst *instance-id*: Indicates the instance ID, ranging from 0 to 64. cost *cost*: Indicates the path cost, ranging from 1 to 200,000,000.
Defaults	The default value of *instance-id* is 0. The default value is automatically calculated based on the port rate. 1000 Mbps—20000 100 Mbps—200000 10 Mbps—2000000
Command Mode	Interface configuration mode
Usage Guide	A larger value of *cost* indicates a higher path cost.

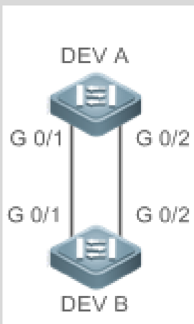
Configuring the Default Path Cost Calculation Method

Command	**spanning-tree pathcost method { *long* [*standard*] | *short* }**
Parameter Description	*long*: Uses the path cost specified in 802.1t. *standard*: Uses the cost calculated according to the standard. *short*: Uses the path cost specified in 802.1d.
Defaults	The path cost specified in 802.1t is used by default.

Command Mode	Global configuration mode
Usage Guide	If the port path cost uses the default value, the device automatically calculates the port path cost based on the port rate.

Configuration Example

Configuring the Port Path Cost

Scenario **Figure 10-24**	
Configuration Steps	▪ Configure the bridge priority so that DEV A becomes the root bridge of the spanning tree. ▪ Configure the path cost of Gi 0/2 on DEV B is 1 so that Gi 0/2 can be selected as the root port.
DEV A	QTECH(config)#spanning-tree QTECH(config)#spanning-tree mst 0 priority 0
DEV B	QTECH(config)#spanning-tree QTECH(config)# int gi 0/2 QTECH(config-if-GigabitEthernet 0/2)# spanning-tree cost 1
Verification	▪ Run the show spanning-tree summary command to display the topology calculation result of the spanning tree.
DEV A	QTECH# QTECH#show spanning-tree summary Spanning tree enabled protocol mstp MST 0 vlans map : ALL

<table>
<tr><td></td><td><pre>
 Root ID   Priority   0
            Address   08c6.b3.3344
            this bridge is root
            Hello Time   2 sec Forward Delay 15 sec Max Age 20 sec

 Bridge ID Priority   0
            Address   08c6.b3.3344
            Hello Time   2 sec Forward Delay 15 sec Max Age 20 sec

Interface   Role Sts Cost   Prio   OperEdge Type
---------------- ---- --- ---------- -------- -------- ----------------
Gi0/2   Desg FWD 20000   128   False   P2p
Gi0/1   Desg FWD 20000   128   False   P2p
</pre></td></tr>
<tr><td>DEV B</td><td><pre>
QTECH#show spanning-tree summary

Spanning tree enabled protocol mstp
MST 0 vlans map : ALL
 Root ID   Priority   0
            Address   08c6.b3.3344
            this bridge is root
            Hello Time   2 sec Forward Delay 15 sec Max Age 20 sec

 Bridge ID Priority   32768
            Address   08c6.b3.78cc
            Hello Time   2 sec Forward Delay 15 sec Max Age 20 sec

Interface   Role Sts Cost   Prio   OperEdge Type
---------------- ---- --- ---------- -------- -------- ----------------
Gi0/2   Root FWD 1   128   False   P2p
Gi0/1   Altn BLK 20000   128   False   P2p
</pre></td></tr>
</table>

Common Errors

N/A

9.4.7 Configuring the Maximum Hop Count of a BPDU Packet

Configuration Effect

- Configure the maximum hop count of a BPDU packet to change the BPDU TTL and thereby affect the network topology.

Notes

- The default maximum hop count of a BPDU packet is 20. Generally, it is not recommended to change the default value.

Configuration Steps

Configuring the Maximum Hop Count

- (Optional) If the network topology is so large that a BPDU packet exceeds the default 20 hops, it is recommended to change the maximum hop count.

Verification

Display the configuration.

Related Commands

Configuring the Maximum Hop Count

Command	**spanning-tree max-hops *hop-count***
Parameter Description	*hop-count*: Indicates the number of devices a BPDU passes through before being discarded. It ranges from 1 to 40.
Defaults	The default value of *hop-count* is 20.
Command Mode	Global configuration mode

Usage Guide	In a region, the BPDU sent by the root bridge includes a hop count. Every time a BPDU passes through a device from the root bridge, the hop count decreases by 1. When the hop count becomes 0, the BPDU times out and the device discards the packet. This command specifies the number of devices a BPDU passes through in a region before being discarded. Changing the maximum hop count will affect all instances.

Configuration Example

Configuring the Maximum Hop Count of a BPDU Packet

Configuration Steps	▪ **Set the maximum hop count of a BPDU packet to 25.**
	QTECH(config)# spanning-tree max-hops 25
Verification	▪ Run the show spanning-tree command to display the configuration.
	QTECH# show spanning-tree StpVersion : MSTP SysStpStatus : ENABLED MaxAge : 20 HelloTime : 2 ForwardDelay : 15 BridgeMaxAge : 20 BridgeHelloTime : 2 BridgeForwardDelay : 15 MaxHops: 25 TxHoldCount : 3 PathCostMethod : Long BPDUGuard : Disabled BPDUFilter : Disabled LoopGuardDef : Disabled ###### mst 0 vlans map : ALL BridgeAddr : 08c6.b3.3344

	Priority: 0 TimeSinceTopologyChange : 2d:0h:46m:4s TopologyChanges : 25 DesignatedRoot : 0.08c6.b3.78cc RootCost : 0 RootPort : GigabitEthernet 0/1 CistRegionRoot : 0.08c6.b3.78cc CistPathCost : 20000

9.4.8 Enabling PortFast-related Features

Configuration Effect

- After PortFast is enabled on a port, the port directly enters the forwarding state. However, since the Port Fast Operational State becomes disabled due to receipt of BPDUs, the port can properly run the STP algorithm and enter the forwarding state.
- If BPDU guard is enabled on a port, the port enters the error-disabled state after receiving a BPDU.
- If BPDU filter is enabled on a port, the port neither sends nor receives BPDUs.

Notes

- The global BPDU guard takes effect only when PortFast is enabled on a port.
- If BPDU filter is enabled globally, a PortFast-enabled port neither sends nor receives BPDUs. In this case, the host connecting directly to the PortFast-enabled port does not receive any BPDUs. If the port changes its Port Fast Operational State to Disabled after receiving a BPDU, BPDU filter automatically fails.
- The global BPDU filter takes effect only when PortFast is enabled on a port.

Configuration Steps

Enabling PortFast

- Optional.
- If a port connects directly to the network terminal, configure this port as a PortFast port.

Enabling BPDU Guard

- Optional.

- If device ports connect directly to network terminals, you can enable BPDU guard on these ports to prevent BPDU attacks from causing abnormality in the spanning tree topology. A port enabled with BPDU guard enters the error-disabled state after receiving a BPDU.
- If device ports connect directly to network terminals, you can enable BPDU guard to prevent loops on the ports. The prerequisite is that the downlink device (such as the hub) can forward BPDU packets.

Enabling BPDU Filter

- Optional.
- To prevent abnormal BPDU packets from affecting the spanning tree topology, you can enable BPDU filter on a port to filter abnormal BPDU packets.

Verification

Display the configuration.

- Run the show spanning-tree [mst *instance-id*] interface *interface-id* command to display the spanning tree configuration of the port.

Related Commands

Configuring PortFast

Command	**spanning-tree portfast**
Parameter Description	N/A
Defaults	PortFast is disabled on a port by default.
Command Mode	Interface configuration mode
Usage Guide	After PortFast is enabled on a port, the port directly enters the forwarding state. However, since the Port Fast Operational State becomes disabled due to receipt of BPDUs, the port can properly run the STP algorithm and enter the forwarding state.

Configuring BPDU Guard for all Ports

Command	**spanning-tree portfast bpduguard default**

Parameter Description	N/A
Defaults	BPDU guard is globally disabled by default.
Command Mode	Global configuration mode
Usage Guide	If BPDU guard is enabled on a port, the port enters the error-disabled state after receiving a BPDU. Run the show spanning-tree command to display the configuration.

Configuring BPDU Guard for a Port

Command	**spanning-tree bpduguard enabled**
Parameter Description	N/A
Defaults	BPDU guard is disabled on a port by default.
Command Mode	Interface configuration mode
Usage Guide	If BPDU guard is enabled on a port, the port enters the error-disabled state after receiving a BPDU.

Configuring BPDU Filter for all Ports

Command	**spanning-tree portfast bpdufilter default**
Parameter Description	N/A
Defaults	BPDU filter is globally disabled by default.
Command Mode	Global configuration mode

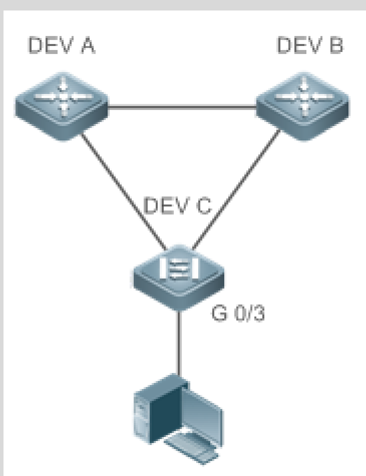
Usage Guide	If BPDU filter is enabled, corresponding ports neither send nor receive BPDUs.

Configuring BPDU Filter for a Port

Command	**spanning-tree bpdufilter enabled**
Parameter Description	N/A
Defaults	BPDU filter is disabled on a port by default.
Command Mode	Interface configuration mode
Usage Guide	If BPDU filter is enabled on a port, the port neither sends nor receives BPDUs.

Configuration Example

Enabling PortFast on a Port

Scenario **Figure 10-25**	
Configuration Steps	▪ Configure Gi 0/3 of DEV C as a PortFast port and enable BPDU guard.
DEV C	QTECH(config)# int gi 0/3

	QTECH(config-if-GigabitEthernet 0/3)# spanning-tree portfast %Warning: portfast should only be enabled on ports connected to a single host. Connecting hubs, switches, bridges to this interface when portfast is enabled,can cause temporary loops. QTECH(config-if-GigabitEthernet 0/3)#spanning-tree bpduguard enable
Verification	▪ Run the **show spanning-tree interface** command to display the port configuration.
DEV C	QTECH#show spanning-tree int gi 0/3 PortAdminPortFast : Enabled PortOperPortFast : Enabled PortAdminAutoEdge : Enabled PortOperAutoEdge : Enabled PortAdminLinkType : auto PortOperLinkType : point-to-point PortBPDUGuard : Enabled PortBPDUFilter : Disabled PortGuardmode : None ###### MST 0 vlans mapped :ALL PortState : forwarding PortPriority : 128 PortDesignatedRoot : 0.08c6.b3.3344 PortDesignatedCost : 0 PortDesignatedBridge :0.08c6.b3.3344 PortDesignatedPortPriority : 128 PortDesignatedPort : 4 PortForwardTransitions : 1 PortAdminPathCost : 20000 PortOperPathCost : 20000 Inconsistent states : normal PortRole : designatedPort

9.4.9 Enabling TC-related Features

Configuration Effect

- If TC protection is enabled on a port, the port deletes TC BPDU packets within a specified time (generally 4 seconds) after receiving them, preventing MAC and ARP entry from being removed.
- If TC guard is enabled, a port receiving TC packets filters TC packets received or generated by itself so that TC packets are not spread to other ports. In this way, possible TC attacks are efficiently prevented to keep the network stable.
- TC filter does not process TC packets received by ports but processes TC packets in case of normal topology changes.

Notes

- It is recommended to enable TC guard only when illegal TC attack packets are received in the network.

Configuration Steps

Enabling TC Protection

- Optional.
- TC protection is disabled by default.

Enabling TC Guard

- Optional.
- TC guard is disabled by default.
- To filter TC packets received or generated due to topology changes, you can enable TC guard.

Enabling TC Filter

- Optional.
- TC filter is disabled by default.
- To filter TC packets received on a port, you can enable TC filter on the port.

Verification

Display the configuration.

Related Commands

Enabling TC Protection

Command	spanning-tree tc-protection
Parameter Description	N/A
Defaults	TC protection is disabled by default.
Command Mode	Global configuration mode
Usage Guide	N/A

Configuring TC Guard for all Ports

Command	spanning-tree tc-protection tc-guard
Parameter Description	N/A
Defaults	TC guard is globally disabled by default.
Command Mode	Global configuration mode
Usage Guide	Enable TC guard to prevent TC packets from spreading.

Configuring TC Guard for a Port

Command	spanning-tree tc-guard
Parameter Description	N/A
Defaults	TC guard is disabled on a port by default.
Command Mode	Interface configuration mode

Usage Guide	Enable TC guard to prevent TC packets from spreading.

Configuring TC Filter for a Port

Command	**spanning-tree ignore tc**
Parameter Description	N/A
Defaults	TC filter is disabled by default.
Command Mode	Interface configuration mode
Usage Guide	If TC filter is enabled on a port, the port does not process received TC packets.

Configuration Example

Enabling TC Guard on a Port

Configuration Steps	**Enable TC guard on a port.**
	QTECH(config)#int gi 0/1 QTECH(config-if-GigabitEthernet 0/1)#spanning-tree tc-guard
Verification	▪ Run the **show run interface** command to display the TC guard configuration of the port.
	QTECH#show run int gi 0/1 Building configuration... Current configuration : 134 bytes interface GigabitEthernet 0/1

	switchport mode trunk spanning-tree tc-guard

Common Errors

- If TC guard or TC filter is incorrectly configured, an error may occur during packet forwarding of the network device. For example, when the topology changes, the device fails to clear MAC address in a timely manner, causing packet forwarding errors.

9.4.10 Enabling BPDU Source MAC Address Check

Configuration Effect

- Enable BPDU source MAC address check. After this, a device receives only BPDU packets with the source MAC address being the specified MAC address and discards other BPDU packets.

Notes

- When the switch connected to a port on a point-to-point link is determined, you can enable BPDU source MAC address check so that the switch receives the BPDU packets sent only by the peer switch.

Configuration Steps

Enabling BPDU Source MAC Address Check

- Optional.
- BPDU source MAC address check is disabled by default.
- To prevent malicious BPDU attacks, you can enable BPDU source MAC address check.

Verification

Display the configuration.

Related Commands

Enabling BPDU Source MAC Address Check

Command	**bpdu src-mac-check *H.H.H***

Parameter Description	*H.H.H*: Indicates an MAC address. The device receives only BPDU packets with this address being the source MAC address.
Defaults	BPDU source MAC address check is disabled by default.
Command Mode	Interface configuration mode
Usage Guide	BPDU source MAC address check prevents BPDU packets from maliciously attacking switches and causing MSTP abnormal. When the switch connected to a port on a point-to-point link is determined, you can enable BPDU source MAC address check to receive BPDU packets sent only by the peer switch and discard all other BPDU packets, thereby preventing malicious attacks. You can enable BPDU source MAC address check in interface configuration mode for a specific port. One port can only filter one MAC address.

Configuration Example

Enabling BPDU Source MAC Address Check on a Port

Configuration Steps	**Enable BPDU source MAC address check on a port.**
	QTECH(config)#int gi 0/1 QTECH(config-if-GigabitEthernet 0/1)#bpdu src-mac-check 08c6.b3.1234
Verification	▪ Run the **show run interface** command to display the spanning tree configuration of the port.
	QTECH#show run int gi 0/1 Building configuration... Current configuration : 170 bytes interface GigabitEthernet 0/1 switchport mode trunk

	bpdu src-mac-check 08c6.b3.1234 spanning-tree link-type point-to-point

Common Errors

- If BPDU source MAC address check is enabled on a port, the port receives only BPDU packets with the configured MAC address being the source MAC address and discards all other BPDU packets.

9.4.11 Configuring Auto Edge

Configuration Effect

- Enable Auto Edge. If a designated port does not receive any BPDUs within a specified time (3 seconds), it is automatically identified as an edge port. However, if the port receives BPDUs, its Port Fast Operational State will become Disabled.

Notes

Unless otherwise specified, do not disable Auto Edge.

- By default, the port is automatically identified as an edge port and enters the forwarding state if a designated port does not receive any BPDUs within 3 seconds. If packet loss or packet Tx/Rx delay occurs in the network, it is recommended to disable Auto Edge.

Configuration Steps

Configuring Auto Edge

- Optional.
- Auto Edge is enabled by default.

Verification

Display the configuration.

Related Commands

Configuring Auto Edge

Command	spanning-tree autoedge

Parameter Description	N/A
Defaults	Auto Edge is enabled by default.
Command Mode	Interface configuration mode
Usage Guide	If the designated port of a device does not receive a BPDU from the downlink port within a specific period (3 seconds), the device regards a network device connected to the designated port, configures the port as an edge port, and switches the port directly into the forwarding state. The edge port will be automatically identified as a non-edge port after receiving a BPDU. You can run the **spanning-tree autoedge disabled** command to disable Auto Edge.

Configuration Example

Disabling Auto Edge on a Port

	QTECH(config)#int gi 0/1 **QTECH(config-if-GigabitEthernet 0/1)#spanning-tree autoedge disabled**
Verification	▪ Run the **show spanning-tree interface** command to display the spanning tree configuration of the port.
	QTECH#show spanning-tree interface gi 0/1 PortAdminPortFast : Disabled PortOperPortFast : Disabled PortAdminAutoEdge : Disabled PortOperAutoEdge : Disabled PortAdminLinkType : point-to-point PortOperLinkType : point-to-point PortBPDUGuard : Disabled PortBPDUFilter : Disabled

	PortGuardmode : None ###### MST 0 vlans mapped :ALL PortState : forwarding PortPriority : 128 PortDesignatedRoot : 0.08c6.b3.3344 PortDesignatedCost : 0 PortDesignatedBridge :0.08c6.b3.3344 PortDesignatedPortPriority : 128 PortDesignatedPort : 2 PortForwardTransitions : 6 PortAdminPathCost : 20000 PortOperPathCost : 20000 Inconsistent states : normal PortRole : designatedPort

Common Errors

9.4.12 Enabling Guard-related Features

Configuration Effect

- If root guard is enabled on a port, its roles on all instances are enforced as the designated port. Once the port receives configuration information with a higher priority, it enters the root-inconsistent (blocking) state. If the port does not receive configuration information with a higher priority within a period, it returns to its original state.
- Due to the unidirectional link failure, the root port or backup port becomes the designated port and enters the forwarding state if it does not receive BPDUs, causing a network loop. Loop guard is to prevent this problem.

Notes

- Root guard and loop guard cannot take effect on a port at the same time.

Configuration Steps

Enabling Root Guard

- Optional.
- The root bridge may receive configuration with a higher priority due to incorrect configuration by maintenance personnel or malicious attacks in the network. As a result, the current root bridge may lose its role, causing incorrect topology changes. To prevent this problem, you can enable root guard on a designated port of a device.

Enabling Loop Guard

- Optional.
- You can enable loop guard on a port (root port, master port, or AP) to prevent it from failing to receive BPDUs sent by the designated bridge, increasing device stability. Otherwise, the network topology will change, possibly causing a loop.

Disabling Guard

- Optional.
- Guard is disabled by default.

Verification

Display the configuration.

Related Commands

Enabling Root Guard

Command	spanning-tree guard root
Parameter Description	N/A
Defaults	Root guard is disabled by default.
Command Mode	Interface configuration mode
Usage Guide	If root guard is enabled, the current root bridge will not change due to incorrect configuration or illegal packet attacks.

Enabling Loop Guard of all Ports

Command	**spanning-tree loopguard default**
Parameter Description	N/A
Defaults	Loop guard is disabled by default.
Command Mode	Global configuration mode
Usage Guide	Enabling loop guard on a root port or backup port will prevent possible loops caused by BPDU receipt failure.

Enabling Loop Guard of a Port

Command	**spanning-tree guard loop**
Parameter Description	N/A
Defaults	Loop guard is disabled by default.
Command Mode	Interface configuration mode
Usage Guide	Enabling loop guard on a root port or backup port will prevent possible loops caused by BPDU receipt failure.

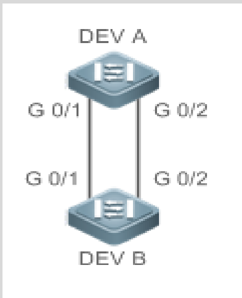
Disabling Guard

Command	**spanning-tree guard none**
Parameter Description	N/A
Defaults	Guard is disabled by default.
Command Mode	Interface configuration mode

Usage Guide	N/A

Configuration Example

Enabling Loop Guard on a Port

Scenario **Figure 10-26**	
Configuration Steps	▪ Configure DEV A as the root bridge and DEV B as a non-root bridge on a spanning tree. ▪ Enable loop guard on ports Gi 0/1 and Gi 0/2 of DEV B.
DEV A	QTECH(config)#spanning-tree QTECH(config)#spanning-tree mst 0 priority 0
DEV B	QTECH(config)#spanning-tree QTECH(config)# int range gi 0/1-2 QTECH(config-if-range)#spanning-tree guard loop
Verification	▪ Run the **show spanning-tree interface** command to display the spanning tree configuration of the port.
DEV A	Omitted.
DEV B	QTECH#show spanning-tree int gi 0/1 PortAdminPortFast : Disabled PortOperPortFast : Disabled PortAdminAutoEdge : Enabled PortOperAutoEdge : Disabled PortAdminLinkType : auto PortOperLinkType : point-to-point

	PortBPDUGuard : Disabled PortBPDUFilter : Disabled PortGuardmode : Guard loop ###### MST 0 vlans mapped :ALL PortState : forwarding PortPriority : 128 PortDesignatedRoot : 0.08c6.b3.78cc PortDesignatedCost : 0 PortDesignatedBridge :0.08c6.b3.78cc PortDesignatedPortPriority : 128 PortDesignatedPort : 17 PortForwardTransitions : 1 PortAdminPathCost : 20000 PortOperPathCost : 20000 Inconsistent states : normal PortRole : rootPort QTECH#show spanning-tree int gi 0/2 PortAdminPortFast : Disabled PortOperPortFast : Disabled PortAdminAutoEdge : Enabled PortOperAutoEdge : Disabled PortAdminLinkType : auto PortOperLinkType : point-to-point PortBPDUGuard : Disabled PortBPDUFilter : Disabled PortGuardmode : Guard loop ###### MST 0 vlans mapped :ALL PortState : discarding PortPriority : 128 PortDesignatedRoot : 0.08c6.b3.78cc PortDesignatedCost : 0 PortDesignatedBridge :0.08c6.b3.78cc PortDesignatedPortPriority : 128

	PortDesignatedPort : 18 PortForwardTransitions : 1 PortAdminPathCost : 20000 PortOperPathCost : 20000 Inconsistent states : normal PortRole : alternatePort

Common Errors

- If root guard is enabled on the root port, master port, or AP, the port may be incorrectly blocked.

9.4.13 Enabling BPDU Transparent Transmission

Configuration Effect

- If STP is disabled on a device, the device needs to transparently transmit BPDU packets so that the spanning tree between devices is properly calculated.

Notes

- BPDU transparent transmission takes effect only when STP is disabled. If STP is enabled on a device, the device does not transparently transmit BPDU packets.

Configuration Steps

Enabling BPDU Transparent Transmission

- Optional.
- If STP is disabled on a device that needs to transparently transmit BPDU packets, enable BPDU transparent transmission.

Verification

Display the configuration.

Related Commands

Enabling BPDU Transparent Transmission

Command	**bridge-frame forwarding protocol bpdu**

Parameter Description	N/A
Defaults	BPDU transparent transmission is disabled by default.
Command Mode	Global configuration mode
Usage Guide	In IEEE 802.1Q, the destination MAC address 01-80-C2-00-00-00 of the BPDU is used as a reserved address. That is, devices compliant with IEEE 802.1Q do not forward the BPDU packets received. However, devices may need to transparently transmit BPDU packets in actual network deployment. For example, if STP is disabled on a device, the device needs to transparently transmit BPDU packets so that the spanning tree between devices is properly calculated. BPDU transparent transmission takes effect only when STP is disabled. If STP is enabled on a device, the device does not transparently transmit BPDU packets.

Configuration Example

Enabling BPDU Transparent Transmission

Scenario **Figure 10-27**	
	STP is enabled on DEV A and DEV C while is disabled on DEV B.
Configuration Steps	▪ Enable BPDU transparent transmission on DEV B so that STP between DEV A and DEV C can be correctly calculated.
DEV B	`QTECH(config)#bridge-frame forwarding protocol bpdu`
Verification	▪ Run the **show run** command to check whether BPDU transparent transmission is enabled.
DEV B	`QTECH#show run`

	Building configuration... Current configuration : 694 bytes bridge-frame forwarding protocol bpdu

9.4.14 Enabling BPDU Tunnel

Configuration Effect

- Enable BPDU Tunnel so that STP packets from the customer network can be transparently transmitted across the SP network. STP packet transmission between the customer network does not affect the SP network, causing STP on the customer network to be calculated independently of that on the SP network.

Notes

- BPDU Tunnel takes effect only when it is enabled in both global configuration mode and interface configuration mode.

Configuration Steps

Enabling BPDU Tunnel

- (Optional) In a QinQ network, you can enable BPDU Tunnel if STP needs to be calculated separately between customer networks and SP networks.

Verification

Run the show l2protocol-tunnel stp command to display the BPDU Tunnel configuration.

Related Commands

Configuring BPDU Tunnel in Global Configuration Mode

Command	**l2protocol-tunnel stp**
Parameter Description	N/A
Defaults	BPDU Tunnel is disabled by default.

Command Mode	Global configuration mode
Usage Guide	BPDU Tunnel takes effect only when it is enabled in both global configuration mode and interface configuration mode.

Configuring BPDU Tunnel in Interface Configuration Mode

Command	**l2protocol-tunnel stp enable**
Parameter Description	N/A
Defaults	BPDU Tunnel is disabled by default.
Command Mode	Interface configuration mode
Usage Guide	BPDU Tunnel takes effect only when it is enabled in both global configuration mode and interface configuration mode.

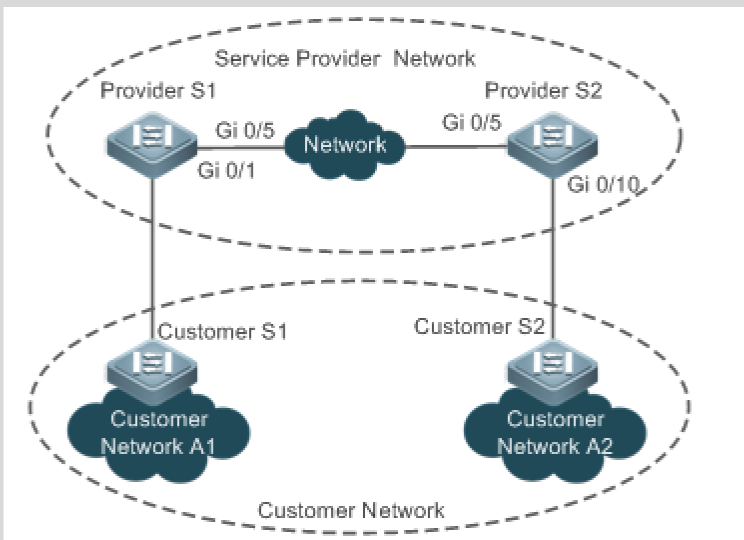
Configuring BPDU Tunnel Transparent Transmission Address

Command	**l2protocol-tunnel stp tunnel-dmac** ***mac-address***
Parameter Description	*mac-address*: Indicates the STP address for transparent transmission.
Defaults	The default MAC address is 01d0.f800.0005.
Command Mode	Global configuration mode
Usage Guide	If an STP packet sent from a customer network enters a PE, the PE changes the destination MAC address of the packet to a private address before the packet is forwarded by the SP network. When the packet reaches the PE at the peer end, the PE changes the destination MAC address to a public address and returns the packet to the customer network at the peer end, realizing transparent transmission across the SP network. This private address is the transparent transmission address of BPDU Tunnel.

	⚠ Optional transparent transmission addresses of STP packets include 01d0.f800.0005, 011a.a900.0005, 010f.e200.0003, 0100.0ccd.cdd0, 0100.0ccd.cdd1, and 0100.0ccd.cdd2. ⚠ If no transparent transmission address is configured, BPDU Tunnel uses the default address 01d0.f800.0005.

Configuration Example

Enabling BPDU Tunnel

Scenario **Figure 10-28**	
Configuration Steps	▪ Enable basic QinQ on the PEs (Provider S1/Provider S2 in this example) so that data packets of the customer network are transmitted within VLAN 200 on the SP network. ▪ Enable STP transparent transmission on the PEs (Provider S1/Provider S2 in this example) so that the SP network can transmit STP packets of the customer network through BPDU Tunnel.
Provider S1	Step 1: Create VLAN 200 on the SP network. QTECH#configure terminal Enter configuration commands, one per line. End with CNTL/Z. QTECH(config)#vlan 200 QTECH(config-vlan)#exit

	Step 2: Enable basic QinQ on the port connected to the customer network and use VLAN 20 for tunneling. QTECH(config)#interface gigabitEthernet 0/1 QTECH(config-if-GigabitEthernet 0/1)#switchport mode dot1q-tunnel QTECH(config-if-GigabitEthernet 0/1)#switchport dot1q-tunnel native vlan 200 QTECH(config-if-GigabitEthernet 0/1)#switchport dot1q-tunnel allowed vlan add untagged 200 Step 3: Enable STP transparent transmission on the port connected to the customer network. QTECH(config-if-GigabitEthernet 0/1)#l2protocol-tunnel stp enable QTECH(config-if-GigabitEthernet 0/1)#exit Step 4: Enable STP transparent transmission in global configuration mode. QTECH(config)#l2protocol-tunnel stp Step 5: Configure an Uplink port. QTECH(config)# interface gigabitEthernet 0/5 QTECH(config-if-GigabitEthernet 0/5)#switchport mode uplink
Provider S2	Configure Provider S2 by performing the same steps.
Verification	▪ Check whether the BPDU Tunnel configuration is correct. ▪ Verify the Tunnel port configuration by checking whether: 1. The port type is dot1q-tunnel; 2. The outer tag VLAN is consistent with the native VLAN and added to the VLAN list of the Tunnel port; 3. The port that accesses the SP network is configured as an Uplink port.
Provider S1	Step 1: Check whether the BPDU Tunnel configuration is correct. QTECH#show l2protocol-tunnel stp L2protocol-tunnel: stp Enable L2protocol-tunnel destination mac address: 01d0.f800.0005 GigabitEthernet 0/1 l2protocol-tunnel stp enable Step 2: Check whether the QinQ configuration is correct. QTECH#show running-config interface GigabitEthernet 0/1 switchport mode dot1q-tunnel

	switchport dot1q-tunnel allowed vlan add untagged 200 switchport dot1q-tunnel native vlan 200 l2protocol-tunnel stp enable spanning-tree bpdufilter enable ! interface GigabitEthernet 0/5 switchport mode uplink
Provider S2	Verify Provider S2 configuration by performing the same steps.

Common Errors

- In the SP network, BPDU packets can be correctly transparently transmitted only when the transparent transmission addresses of BPDU Tunnel are consistent.

9.5 Monitoring

Clearing

Running the **clear** commands may lose vital information and thus interrupt services.

Description	Command
Clears the statistics of packets sent and received on a port.	**clear spanning-tree counters [interface** ***interface-id*** **]**
Clears the STP topology change information.	**clear spanning-tree mst** ***instance-id*** **topochange record**

Displaying

Description	Command
Displays MSTP parameters and spanning tree topology information.	show spanning-tree
Displays the count of sent and received MSTP packets.	show spanning-tree counters [interface *interface-id*]

Displays MSTP instances and corresponding port forwarding status.	show spanning-tree summary
Displays the ports that are blocked by root guard or loop guard.	show spanning-tree inconsistentports
Displays the configuration of an MST region.	**show spanning-tree mst configuration**
Displays MSTP information of an instance.	**show spanning-tree mst *instance-id***
Displays MSTP information of the instance corresponding to a port.	**show spanning-tree mst *instance-id* interface *interface-id***
Displays topology changes of a port in an instance.	**show spanning-tree mst *instance-id* topochange record**
Displays MSTP information of all instances corresponding to a port.	**show spanning-tree interface *interface-id***
Displays the forwarding time.	**show spanning-tree forward-time**
Displays the hello time.	**show spanning-tree hello time**
Displays the maximum hop count.	**show spanning-tree max-hops**
Displays the maximum number of BPDU packets sent per second.	**show spanning-tree tx-hold-count**
Displays the path cost calculation method.	**show spanning-tree pathcost method**
Displays BPDU Tunnel information.	**show l2protocol-tunnel stp**

Debugging

System resources are occupied when debugging information is output. Therefore, disable the debugging switch immediately after use.

Description	Command
Debugs all STPs.	**debug mstp all**

Debugs MSTP Graceful Restart (GR).	**debug mstp gr**
Debugs BPDU packet receiving.	**debug mstp rx**
Debugs BPDU packet sending.	**debug mstp tx**
Debugs MSTP events.	**debug mstp event**
Debugs loop guard.	**debug mstp loopguard**
Debugs root guard.	**debug mstp rootguard**
Debugs the bridge detection state machine.	**debug mstp bridgedetect**
Debugs the port information state machine.	**debug mstp portinfo**
Debugs the port protocol migration state machine.	**debug mstp protomigrat**
Debugs MSTP topology changes.	**debug mstp topochange**
Debugs the MSTP receiving state machine.	**debug mstp receive**
Debugs the port role transition state machine.	**debug mstp roletran**
Debugs the port state transition state machine.	**debug mstp statetran**
Debugs the MSTP sending state machine.	**debug mstp transmit**

10 CONFIGURING GVRP

10.1 Overview

The GARP VLAN Registration Protocol (GVRP) is an application of the Generic Attribute Registration Protocol (GARP) used to dynamically configure and proliferate VLAN memberships.

GVRP simplifies VLAN configuration and management. It reduces the workload of manually configuring VLANs and adding ports to VLANs, and reduces the possibility of network disconnection due to inconsistent configuration. With GVRP, you can dynamically maintain VLANs and add/remove ports to/from VLANs to ensure VLAN connectivity in a topology.

Protocols and Standards

IEEE standard 802.1D

IEEE standard 802.1Q

10.2 Applications

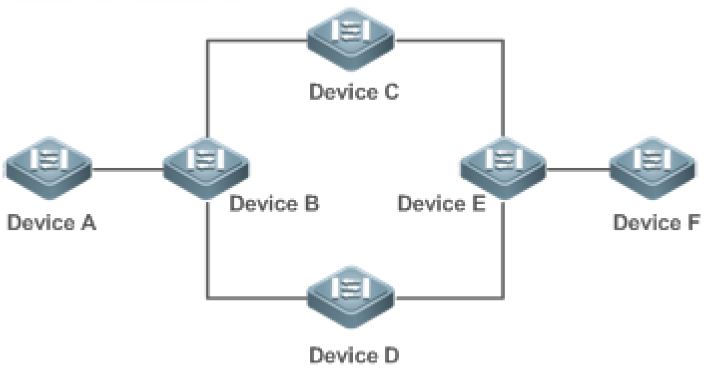
Application	Description
GVRP Configuration in a LAN	Connect two switches in a local area network (LAN) and realize VLAN synchronization.
GVRP PDUs Tunnel Application	Use the GVRP Protocol Data Units (PDUs) Tunnel feature to transparently transmit GVRP packets through a tunnel in a QinQ network environment.

10.2.1 GVRP Configuration in a LAN

Scenario

Enable GVRP and set the GVRP registration mode to Normal to register and deregister all dynamic and static VLANs between Device A and Device F.

Figure 11-1



Remarks	**Device A, Device B, Device C, Device D, Device E, and Device F are switches. The ports connected between two devices are Trunk ports.** **On Device A and Device F, configure static VLANs used for communication.** **Enable GVRP on all switches.**

Deployment

- On each device, enable the GVRP and dynamic VLAN creation features, and ensure that dynamic VLANs can be created on intermediate devices.
- On Device A and Device F, configure static VLANs used for communication. Device B, Device C, Device D, and Device E will dynamically learn the VLANs through GVRP.

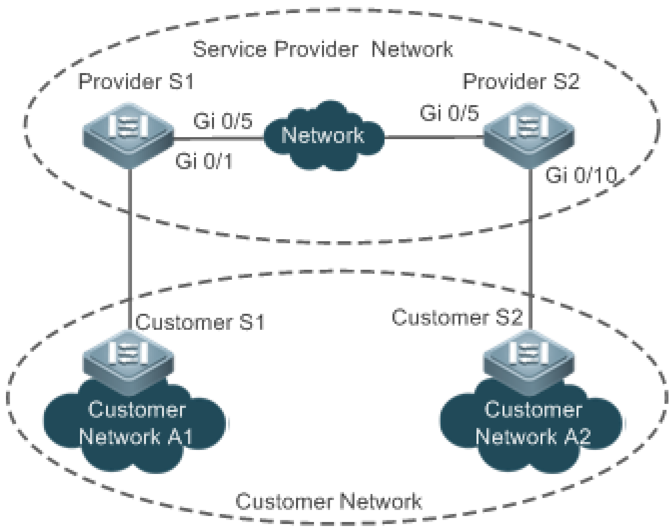
⚠ It is recommended that the Spanning Tree Protocol (STP) be enabled to avoid loops in the customer network topology.

10.2.2 GVRP PDUs Tunnel Application

Scenario

A QinQ network environment is generally divided into a customer network and a service provider (SP) network. The GVRP PDUs Tunnel feature allows GVRP packets to be transmitted between customer networks without impact on SP networks. The GVRP calculation in customer networks is separated from that in SP networks without interference.

Figure 11-2 GVRP PDUs Tunnel Application Topology



Remarks	**Figure 11-2 shows an SP network and a customer network. The SP network contains the provider edge (PE) devices Provider S1 and Provider S2. Customer Network A1 and Customer Network A2 are the same customer's two sites in different locations. Customer S1 and Customer S2 are the access devices in the customer network, which are connected to the SP network through Provider S1 and Provider S2 respectively.** **The GVRP PDUs Tunnel feature allows Customer Network A1 and Customer Network A2 to perform unified GVRP calculation across the SP network, without impact on the SP network's GVRP calculation.**

Deployment

- Enable basic QinQ on the PEs (Provider S1 and Provider S2) in the SP network to transmit data packets from the customer network through a specified VLAN in the SP network.
- Enable GVRP transparent transmission on the PEs (Provider S1 and Provider S2) in the SP network to allow the SP network to tunnel GVRP packets from the customer network via the GVRP PDUs Tunnel feature.

10.3 Features

Basic Concepts

- GVRP

GVRP is an application of GARP used to register and deregister VLAN attributes in the following modes:

- When a port receives a VLAN attribute declaration, the port will register the VLAN attributes contained in the declaration (that is, the port will join the VLAN).

- When a port receives a VLAN attribute revocation declaration, the port will deregister the VLAN attributes contained in the declaration (that is, the port will exit the VLAN).

Figure 11-3

Dynamic VLAN

A VLAN that can be dynamically created and deleted without the need for manual configuration is called a dynamic VLAN.

You can manually convert a dynamic VLAN to a static VLAN, but not the way around.

A protocol state machine controls the joining of ports to dynamic VLANs created through GVRP. Only the Trunk ports that receive GVRP VLAN attribute declaration can join these VLANs. You cannot manually add ports to dynamic VLANs.

Message Types

(1) Join message

When a GARP application entity hopes other GARP entities to register its attributes, it will send a Join message. When a GARP entity receives a Join message from another entity or requires other entities to register its static attributes, it will send a Join message. There are two types of Join message: JoinEmpty and JoinIn.

- JoinEmpty message: Used to declare an unregistered attribute
- JoinIn message: Used to declare a registered attribute

(2) Leave message

When a GARP application entity hopes other GARP entities to deregister its attributes, it will send a Leave message. When a GARP entity receives a Leave message from another entity or requires other entities to deregister its statically deregistered attributes, it will send a Leave message. There are two types of Leave message: LeaveEmpty and LeaveIn.

- LeaveEmpty message: Used to deregister an unregistered attribute
- LeaveIn message: Used to deregister a registered attribute

(3) LeaveAll message

Each GARP application entity starts its LeaveAll timer during startup. When the timer times out, the entity sends a LeaveAll message to deregister all attributes to enable other GARP entities to reregister attributes. When the GARP application entity receives a LeaveAll message from another entity, it also sends a LeaveAll message. The LeaveAll timer is restarted when a LeaveAll message is sent again to initiate a new cycle.

Timer Types

GARP defines four timers used to control GARP message sending.

(1) Hold timer

The Hold timer controls the sending of GARP messages (including Join and Leave messages). When a GARP application entity has its attributes changed or receives a GARP message from another entity, it starts the Hold timer. During the timeout period, the GARP application entity encapsulates all GARP messages to be sent into packets as few as possible, and sends the packets when the timer times out. This reduces the quantity of sent packets and saves bandwidth resources.

(2) Join timer

The Join timer controls the sending of Join messages. After a GARP application entity sends a Join message, it waits for one timeout interval of the Join timer to ensure that the Join message is reliably transmitted to another entity. If the GARP application entity receives a JoinIn message from another entity before the timer times out, it will not resend the Join message; otherwise, it will resend the Join message. Not each attribute has its own Join timer, but each GARP application entity has one Join timer.

(3) Leave timer

The Leave timer controls attribute deregistration. When a GARP application entity hopes other entities to deregister one of its attributes, it sends a Leave message. Other entities which receive the Leave message start the Leave timer. The attribute will be deregistered only if these entities receive no Join message mapped to the attribute during the timeout period.

(4) LeaveAll timer

Each GARP application entity starts its own LeaveAll timer upon startup. When the timer times out, the entity sends a LeaveAll message to enable other entities to reregister attributes. Then the LeaveAll timer is restarted to initiate a new cycle.

GVRP Advertising Modes

GVRP allows a switch to inform other interconnected devices of its VLANs and instruct the peer device to create specific VLANs and add the ports that transmit GVRP packets to corresponding VLANs.

Two GVRP advertising modes are available:

- Normal mode: A device externally advertises its VLAN information, including dynamic and static VLANs.
- Non-applicant mode: A device does not externally advertise its VLAN information.
- GVRP Registration Modes

A GVRP registration mode specifies whether the switch that receives a GVRP packet processes the VLAN information in the packet, such as dynamically creating a new VLAN and adding the port that receives the packet to the VLAN.

Two GVRP registration modes are available:

- Normal mode: Process the VLAN information in the received GVRP packet.
- Disabled mode: No to process the VLAN information in the received GVRP packet.

Overview

Feature	Description
Intra-Topology VLAN Information Synchronization	Dynamically creates VLANs and adds/removes ports to/from VLANs, which reduces the manual configuration workload and the probability of VLAN disconnection due to missing configuration.

10.3.1 Intra-Topology VLAN Information Synchronization

Working Principle

GVRP is an application of GARP based on the GARP working mechanism. GVRP maintains the dynamic registration information of VLANs on a device and propagates the information to other devices. A GVRP-enabled device receives VLAN registration information from other devices and dynamically updates the local VLAN registration information. The device also propagates the local VLAN registration information to other devices so that all devices in a LAN maintain consistent VLAN information. The VLAN registration information propagated by GVRP includes the manually-configured static registration information on the local device and the dynamic registration information from other devices.

External VLAN Information Advertising

The Trunk port on a GVRP-enabled device periodically collects VLAN information within the port, including the VLANs that the Trunk port joins or exits. The collected VLAN information is encapsulated in a GVRP packet to be sent to the peer device. After the Trunk port on the peer device receives the packet, it resolves the VLAN information. Then corresponding VLANs will be dynamically created, and the Trunk port will join the created VLANs or exit other VLANs. For details about the VLAN information, see the above description of GVRP message types.

Related Configurations

GVRP is disabled by default.

- Run [no] gvrp enable to enable or disable GVRP.

- After GVRP is enabled on a device, the device sends GVRP packets carrying VLAN information. If GVRP is disabled on the device, the device does not send GVRP packets carrying VLAN information or process received GVRP packets.

VLAN Registration and Deregistration

Upon receiving a GVRP packet, the switch determines whether to process the VLAN information in the packet according to the registration mode of the corresponding port. For details, see the above description of GVRP registration modes.

Related Configurations

- If GVRP is enabled, the port in Trunk mode is enabled with dynamic VLAN registration by default.
- To enable dynamic VLAN registration on a port, run the **gvrp registration mode normal** command. To disable dynamic VLAN registration on a port, run the **gvrp register mode disable** command.
- If dynamic VLAN registration is enabled, dynamic VLANs will be created on the local device when the port receives a GVRP packet carrying VLAN information from the peer end.
- If dynamic VLAN registration is disabled, no dynamic VLAN will be created on the local device when the port receives a GVRP packet from the peer end.Configuration

Configuration	Description and Command	
Configuring Basic GVRP Features and VLAN Information Synchronization	⚠ (Mandatory) It is used to enable GVRP and dynamic VLAN creation.	
	gvrp enable	Enables GVRP.
	gvrp dynamic-vlan-creation enable	Enables dynamic VLAN creation.
	switchport mode trunk	Switches to Trunk port mode. GVRP take effects only in Trunk mode.
	switchport trunk allowed vlan all	Allows the traffic from all VLANs to pass through.
	gvrp applicant state	Configures the advertising mode of a port. The Normal mode indicates to advertise VLAN information externally by sending a GVRP packet. The Non-applicant mode indicates not to advertise VLAN information externally.

	gvrp registration mode	Configures the registration mode of a port. The Normal mode indicates to process the VLAN information in the received GVRP packet, such as dynamically creating VLANs and adding ports to VLANs. The Disabled mode indicates not to process the VLAN information in the received GVRP packet.
	(Optional) It is used to configure timers and the registration mode and advertising mode of a port.	
	gvrp timer	Configures timers.
Configuring GVRP PDUs Transparent Transmission	(Optional) It is used to configure GVRP PDUs transparent transmission.	
	bridge-frame forwarding protocol gvrp	Enables GVRP PDUs transparent transmission.
Configuring the GVRP PDUs Tunnel Feature	(Optional) It is used to configure the GVRP PDUs Tunnel feature.	
	l2protocol-tunnel gvrp	Enables the GVRP PDUs Tunnel feature in global configuration mode.
	l2protocol-tunnel gvrp enable	Enables the GVRP PDUs Tunnel feature in interface configuration mode.
	l2protocol-tunnel gvrp tunnel-dmac	Configures the transparent transmission address used by the GVRP PDUs Tunnel feature.

10.4 Configuration

10.4.1 Configuring Basic GVRP Features and VLAN Information Synchronization

Configuration Effect

- Dynamically create/delete VLANs and add/remove ports to/from VLANs.
- Synchronize VLAN information between devices to ensure normal intra-topology communication.
- Reduce the manual configuration workload and simplify VLAN management.

Notes

- GVRP must be enabled on both connected devices. GVRP information is transmitted only by Trunk Links. The transmitted information contains the information of all VLANs on the current device, including dynamically learned VLANs and manually configured VLANs.
- If STP is enabled, only ports in Forwarding state participate in GVRP (such as receiving and sending GVRP PDUs) and have their VLAN information propagated by GVRP.
- All VLAN ports added by GVRP are tagged ports.
- The system does not save the VLAN information that is dynamically learned by GVRP. The information will be lost when the device is reset and cannot be saved manually.
- All devices that need to exchange GVRP information must maintain consistent GVRP timers (Join timer, Leave timer, and Leaveall timer).
- If STP is not enabled, all available ports can participate in GVRP. If Single Spanning Tree (SST) is enabled, only ports in Forwarding state in the SST Context participate in GVRP. If Multi Spanning Tree (MST) is enabled, GVRP can run in the Spanning Tree Context to which VLAN1 belongs. You cannot specify other Spanning Tree Context for GVRP.

Configuration Steps

Enabling GVRP

- Mandatory.
- Only GVRP-enabled devices can process GVRP packets.

Enabling Dynamic VLAN Creation

- Mandatory.
- After dynamic VLAN creation is enabled on a device, the device will dynamically create VLANs upon receiving GVRP Join messages.

Configuring Timers

- Optional.
- There are three GVRP timers: Join timer, Leave timer, and Leaveall timer, which are used to control message sending intervals.
- The timer interval relationships are as follows: The interval of the Leave timer must be three times or more greater than that of the Join timer; the interval of the Leaveall timer must be greater than that of the Leave timer.
- The three timers are controlled by the GVRP state machine and can be triggered by each other.

Configuring the Advertising Mode of a Port

- Optional.
- Two GVRP advertising modes are available: Normal (default) and Non-applicant.
- Normal mode: Indicates that a device externally advertises its VLAN information.
- Non-applicant mode: Indicates that a device does not externally advertise its VLAN information.

Configuring the Registration Mode of a Port

- Optional.
- Two GVRP registration modes are available: Normal and Disabled.

Switching to Trunk Port Mode

- Mandatory.
- GVRP takes effect only on ports in Trunk mode.

Verification

- Run the **show gvrp configuration** command to check the configuration.
- Check whether a dynamic VLAN is configured and the corresponding port joins the VLAN.

Related Commands

Enabling GVRP

Command	gvrp enable
Parameter Description	N/A
Defaults	By default, GVRP is disabled.
Command Mode	Global configuration mode
Usage Guide	GVRP can be enabled only in global configuration mode. If GVRP is not enabled globally, you can still set other GVRP parameters, but the parameter settings take effect only when GVRP starts running.

Enabling Dynamic VLAN Creation

Command	gvrp dynamic-vlan-creation enable
Parameter Description	N/A

Defaults	By default, dynamic VLAN creation is disabled.
Command Mode	Global configuration mode
Usage Guide	When a port receives a JoinIn or JoinEmpty message that indicates a non-existent VLAN on the local device, GVRP may create this VLAN, depending on the configuration of this command.

The parameters of a dynamic VLAN created through GVRP cannot be modified manually.

Configuring Timers

Command	gvrp timer { join *timer-value* | leave *timer-value* | leaveall *timer-value* }
Parameter Description	*timer-value* : 1–2,147,483,647 ms
Defaults	Join timer: 200ms, leave timer: 600ms, leaveall timer: 10,000ms
Command Mode	Global configuration mode
Usage Guide	The interval of the Leave timer must be three times or greater than that of the Join timer. The interval of the Leaveall timer must be greater than that of the Leave timer. The time unit is milliseconds. The following timer intervals are recommended in actual networking: Join timer: 6,000 ms (6s) Leave timer: 30,000 ms (30s) Leaveall timer: 120,000 ms (2 minutes) Ensure that the GVRP timer settings on all interconnected GVRP devices are consistent; otherwise, GVRP may work abnormally.

Configuring the Advertising Mode of a Port

Command	gvrp applicant state { normal | non-applicant }

Parameter Description	**normal:** Indicates that a port externally advertises VLAN information. **non-applicant:** Indicates that a port does not externally advertise VLAN information.
Defaults	By default, ports are allowed to send GVRP notification.
Command Mode	Interface configuration mode
Usage Guide	This command is used to configure the GVRP advertising mode of a port.

Configuring the Registration Mode of a Port

Command	**gvrp registration mode { normal | disabled }**
Parameter Description	**normal:** Indicates that the port is allowed to join a dynamic VLAN. **disabled:** Indicates that the port is not allowed to join a dynamic VLAN.
Defaults	If GVRP is enabled, the port in Trunk mode is enabled with dynamic VLAN registration by default.
Command Mode	Interface configuration mode
Usage Guide	This command is used to configure the GVRP registration mode of a port.

Configuration Example

- Enabling GVRP in a Topology and Dynamically Maintaining VLANs and the VLAN-Port Relationship

Scenario **Figure 11-4**	
Configuration Steps	▪ On Switch A and Switch C, configure VLANs used for communication in the customer network.

	▪ Enable the GVRP and dynamic VLAN creation features on Switch A, Switch B, and Switch C. ▪ Configure the ports connected between switches as Trunk ports, and ensure that the VLAN lists of Trunk ports include the communication VLANs. By default, a Trunk port allows the traffic from all VLANs to pass through. ▪ It is recommended that STP be enabled to avoid loops.
A	1. Create VLAN 1–200 used for communication in the customer network. A# configure terminal Enter configuration commands, one per line. End with CNTL/Z. A(config)# vlan range 1-200 2. Enable the GVRP and dynamic VLAN creation features. A(config)# gvrp enable A(config)# gvrp dynamic-vlan-creation enable 3. Configure the port connected to Switch B as a Trunk port. By default, a Trunk port allows the traffic from all VLANs to pass through. A(config)# interface gigabitEthernet 0/1 A(config-if-GigabitEthernet 0/1)# switchport mode trunk 4. Configure the advertising mode and registration mode of the Trunk port. The Normal mode is used by default and does not need to be configured manually. A(config-if-GigabitEthernet 0/1)# gvrp applicant state normal A(config-if-GigabitEthernet 0/1)# gvrp registration mode normal A(config-if-GigabitEthernet 0/1)# end
C	▪ The configuration on Switch C is the same as that on Switch A.
B	1. Enable the GVRP and dynamic VLAN creation features. B# configure terminal B(config)# gvrp enable B(config)# gvrp dynamic-vlan-creation enable 2. Configure the ports connected to Switch A and Switch C as Trunk ports. B(config)# interface range GigabitEthernet 0/2-3 B(config-if-GigabitEthernet 0/2)# switchport mode trunk

Verification	Check whether the GVRP configuration on each device is correct. Check whether VLAN 2–100 are dynamically created on Switch B and whether Port G 0/2 and Port G 0/3 on Switch B join the dynamic VLANs.
A	A# show gvrp configuration Global GVRP Configuration: GVRP Feature:enabled GVRP dynamic VLAN creation:enabled Join Timers(ms):200 Leave Timers(ms):600 Leaveall Timers(ms):1000 Port based GVRP Configuration: PORT Applicant Status Registration Mode ---------------------- -------------------- --------------------- GigabitEthernet 0/1 normal normal
B	B# show gvrp configuration Global GVRP Configuration: GVRP Feature:enabled GVRP dynamic VLAN creation:enabled Join Timers(ms):200 Leave Timers(ms):600 Leaveall Timers(ms):1000 Port based GVRP Configuration: PORT Applicant Status Registration Mode ---------------------- -------------------- --------------------- GigabitEthernet 0/2 normal normal GigabitEthernet 0/3 normal normal
C	C# show gvrp configuration Global GVRP Configuration: GVRP Feature:enabled GVRP dynamic VLAN creation:enabled Join Timers(ms):200

	Leave Timers(ms):600 Leaveall Timers(ms):1000 Port based GVRP Configuration: PORT Applicant Status Registration Mode ---------------------- -------------------- --------------------- GigabitEthernet 0/1 normal normal

Common Errors

- The ports connected between devices are not in Trunk mode.
- The VLAN lists of the ports connected between devices do not include the VLANs used for communication in the customer network.
- The GVRP advertising modes and registration modes of Trunk ports are not set to Normal.

10.4.2 Enabling GVRP PDUs Transparent Transmission

Configuration Effect

Enable devices to transparently transmit GVRP PDU frames to realize normal inter-device GVRP calculation when GVRP is not enabled.

Notes

GVRP PDUs transparent transmission takes effect only when GVRP is disabled. After GVRP is enabled, devices will not transparently transmit GVRP PDU frames.

Configuration Steps

Configuring GVRP PDUs Transparent Transmission

- Optional.
- Perform this configuration when you need to enable devices to transparently transmit GVRP PDU frames when GVRP is disabled.

Verification

Run the **show run** command to check whether GVRP PDUs transparent transmission is enabled.

Related Commands

Configuring GVRP PDUs Transparent Transmission

Command	**bridge-frame forwarding protocol gvrp**
Parameter Description	N/A
Command Mode	Global configuration mode
Defaults	The function is disabled by default.
Usage Guide	In the IEEE 802.1Q standard, the destination MAC address 01-80-C2-00-00-06 for GVRP PDUs is reserved. Devices compliant with IEEE 802.1Q do not forward received GVRP PDU frames. However, in actual network deployment, devices may need to transparently transmit GVRP PDU frames to realize normal inter-device GVRP calculation when GVRP is not enabled. GVRP PDUs transparent transmission takes effect only when GVRP is disabled. After GVRP is enabled, devices will not transparently transmit GVRP PDU frames.

Configuration Example

Configuring GVRP PDUs Transparent Transmission

Scenario **Figure 11-5**	
	Enable GVRP on DEV A and DEV C. (DEV B is not enabled with GVRP.)
Configuration Steps	Configure GVRP PDUs transparent transmission on DEV B to realize normal GVRP calculation between DEV A and DEV C.
DEV B	QTECH(config)#bridge-frame forwarding protocol gvrp
Verification	Run the **show run** command to check whether GVRP PDUs transparent transmission is enabled.
DEV B	QTECH#show run

	Building configuration... Current configuration : 694 bytes bridge-frame forwarding protocol gvrp

10.4.3 Configuring the GVRP PDUs Tunnel Feature

Configuration Effect

Transparently transmit GVRP packets between customer networks through tunnels in SP networks without impact on the SP networks, and thereby separate the GVRP calculation in customer networks from that in SP networks.

Notes

The GVRP PDUs Tunnel feature takes effect after it is enabled in global configuration mode and interface configuration mode.

Configuration Steps

Configuring the GVRP PDUs Tunnel Feature

- (Optional) Perform this configuration when you need to separate GVRP calculation between customer networks and SP networks in a QinQ environment.

Verification

Run the **show l2protocol-tunnel gvrp** command to check the GVRP PDUs Tunnel configuration.

Related Commands

Configuring the GVRP PDUs Tunnel Feature in Global Configuration Mode

Command	**l2protocol-tunnel gvrp**
Parameter Description	N/A

Defaults	The function is disabled by default.
Command Mode	Global configuration mode
Usage Guide	The GVRP PDUs Tunnel feature takes effect after it is enabled in global configuration mode and interface configuration mode.

Configuring the GVRP PDUs Tunnel Feature in Interface Configuration Mode

Command	**l2protocol-tunnel gvrp enable**
Parameter Description	N/A
Defaults	The function is disabled by default.
Command Mode	Interface configuration mode
Usage Guide	The GVRP PDUs Tunnel feature takes effect after it is enabled in global configuration mode and interface configuration mode.

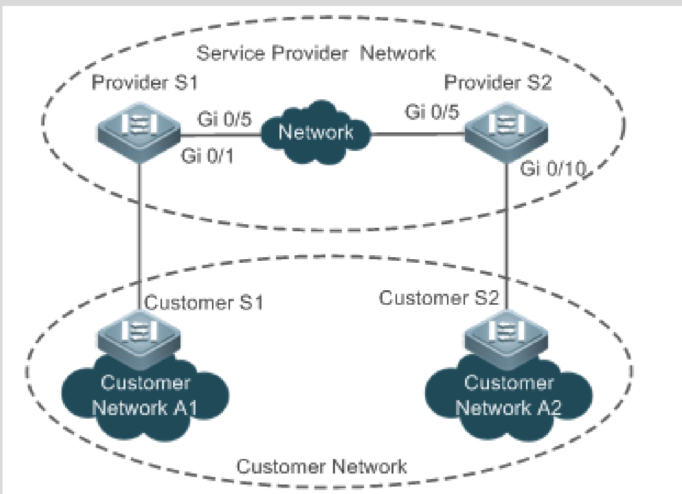
Configuring the GVRP PDUs Tunnel Transparent Transmission Address

Command	**l2protocol-tunnel gvrp tunnel-dmac *mac-address***
Parameter Description	*mac-address*: Indicates the GVRP address used by transparent transmission.
Defaults	The default address is 01d0.f800.0006.
Command Mode	Global configuration mode
Usage Guide	In GVRP PDUs Tunnel application, when a GVRP packet from a customer network enters the PE in an SP network, the destination MAC address of the packet is changed to a private address before the packet is forwarded in the SP network. When the packet reaches the peer PE, the destination MAC address is changed to a public address before the packet is sent to the customer network at the other end. In this way, the GVRP

	packet can be transparently transmitted across the SP network. The private address is the transparent transmission address used by the GVRP PDUs Tunnel feature. ⚠ Address range for transparent transmission of GVRP packets: 01d0.f800.0006, 011a.a900.0006 ⚠ When no transparent transmission address is configured, the default address 01d0.f800.0006 is used.

Configuration Example

Configuring the GVRP PDUs Tunnel Feature

Scenario **Figure 11-6**	
Configuration Steps	▪ Enable basic QinQ on the PEs (Provider S1 and Provider S2) in the SP network to transmit data packets from the customer network through VLAN 200 in the SP network. ▪ Enable GVRP transparent transmission on the PEs (Provider S1 and Provider S2) in the SP network to allow the SP network to tunnel GVRP packets from the customer network via the GVRP PDUs Tunnel feature.
Provider S1	Step 1: Create VLAN 200 of the SP network. QTECH#configure terminal Enter configuration commands, one per line. End with CNTL/Z. QTECH(config)#vlan 200 QTECH(config-vlan)#exit Step 2: Enable basic QinQ on the port connected to the customer network to tunnel data from the customer network through VLAN 200. QTECH(config)#interface gigabitEthernet 0/1

	QTECH(config-if-GigabitEthernet 0/1)#switchport mode dot1q-tunnel QTECH(config-if-GigabitEthernet 0/1)#switchport dot1q-tunnel native vlan 200 QTECH(config-if-GigabitEthernet 0/1)#switchport dot1q-tunnel allowed vlan add untagged 200 Step 3: Enable GVRP transparent transmission on the port connected to the customer network. QTECH(config-if-GigabitEthernet 0/1)#l2protocol-tunnel gvrp enable QTECH(config-if-GigabitEthernet 0/1)#exit Step 4: Enable GVRP transparent transmission globally. QTECH(config)#l2protocol-tunnel gvrp Step 5: Configure an uplink port. QTECH(config)# interface gigabitEthernet 0/5 QTECH(config-if-GigabitEthernet 0/5)#switchport mode uplink
Provider S2	The configuration on Provider S2 is similar to that on Provider S1.
Verification	▪ Check whether the GVRP PDUs Tunnel configuration is correct. ▪ Check whether the Tunnel port is configured correctly. Pay attention to the following: 1. The port type is dot1q-tunnel. 2. The outer tag VLAN is the Native VLAN and added to the VLAN list of the Tunnel port. 3. The ports on the PEs in the uplink direction are configured as Uplink ports.
Provider S1	1. Check whether the GVRP PDUs Tunnel configuration is correct. QTECH#show l2protocol-tunnel gvrp L2protocol-tunnel: Gvrp Enable L2protocol-tunnel destination mac address: 01d0.f800.0006 GigabitEthernet 0/1 l2protocol-tunnel gvrp enable 2. Check whether the QinQ configuration is correct. QTECH#show running-config interface GigabitEthernet 0/1 switchport mode dot1q-tunnel switchport dot1q-tunnel allowed vlan add untagged 200

	switchport dot1q-tunnel native vlan 200 l2protocol-tunnel gvrp enable ! interface GigabitEthernet 0/5 switchport mode uplink
Provider S2	The verification on Provider S2 is the same as that on Provider S1.

Common Errors

In an SP network, transparent transmission addresses are not configured consistently, which affects the transmission of GVRP PDU frames.

10.5 Monitoring

Clearing

Running the **clear** commands may lose vital information and thus interrupt services.

Description	Command
Clears port counters.	clear gvrp statistics { *interface-id* | all }

Displaying

Description	Command
Displays port counters.	**show gvrp statistics** { *interface-id* | **all** }
Displays the current GVRP status.	**show gvrp status**
Displays the current GVRP configuration.	**show gvrp configuration**
Displays the information of the GVRP PDUs Tunnel feature.	**show l2protocol-tunnel gvrp**

Debugging

System resources are occupied when debugging information is output. Therefore, disable debugging immediately after use.

Description	Command
Enables GVRP event debugging.	debug gvrp event
Enables GVRP timer debugging.	debug gvrp timer

11 CONFIGURING LLDP

11.1 Overview

The Link Layer Discovery Protocol (LLDP), defined in the IEEE 802.1AB standard, is used to discover the topology and identify topological changes. LLDP encapsulates local information of a device into LLDP data units (LLDPDUs) in the type/length/value (TLV) format and then sends the LLDPDUs to neighbors. It also stores LLDPDUs from neighbors in the management information base (MIB) to be accessed by the network management system (NMS).

With LLDP, the NMS can learn about topology, for example, which ports of a device are connected to other devices and whether the rates and duplex modes at both ends of a link are consistent. Administrators can quickly locate and rectify a fault based on the information.

A QTECH LLDP-compliant device is capable of discovering neighbors when the peer is either of the following:

- QTECH LLDP-compliant device
- Endpoint device that complies with the Link Layer Discovery Protocol-Media Endpoint Discovery (LLDP-MED)

Protocols and Standards

- IEEE 802.1AB 2005: Station and Media Access Control Connectivity Discovery
- ANSI/TIA-1057: Link Layer Discovery Protocol for Media Endpoint Devices

11.2 Applications

Application	Description
Displaying Topology	Multiple switches, a MED device, and an NMS are deployed in the network topology.
Conducting Error Detection	Two switches are directly connected and incorrect configuration will be displayed.

11.2.1 Displaying Topology

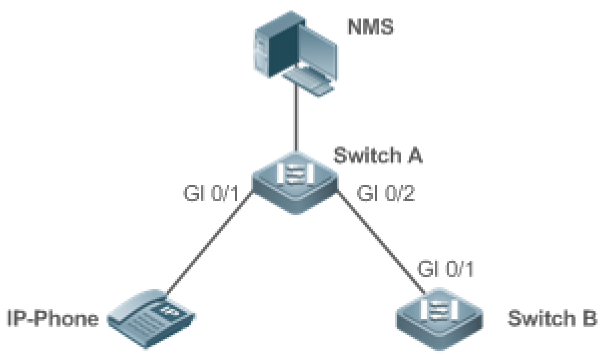
Scenario

Multiple switches, a MED device, and an NMS are deployed in the network topology.

As shown in the following figure, the LLDP function is enabled by default and no additional configuration is required.

- Switch A and Switch B discover that they are neighbors.
- Switch A discovers its neighbor MED device, that is, IP-Phone, through port GigabitEthernet 0/1.
- The NMS accesses MIB of switch A.

Figure 12-1



Remarks	**QTECH Switch A, Switch B, and IP-Phone support LLDP and LLDP-MED.** **LLDP on switch ports works in TxRx mode.** **The LLDP transmission interval is 30 seconds and transmission delay is 2 seconds by default.**

Deployment

- Run LLDP on a switch to implement neighbor discovery.
- Run the Simple Network Management Protocol (SNMP) on the switch so that the NMS acquires and sets LLDP-relevant information on the switch.

11.2.2 Conducting Error Detection

Scenario

Two switches are directly connected and incorrect configuration will be displayed.

As shown in the following figure, the LLDP function and LLDP error detection function are enabled by default, and no additional configuration is required.

- After you configure a virtual local area network (VLAN), port rate and duplex mode, link aggregation, and maximum transmission unit (MTU) of a port on Switch A, an error will be prompted if the configuration does not match that on Switch B, and vice versa.

Figure 12-2

Remarks	**QTECH Switch A and Switch B support LLDP.** **LLDP on switch ports works in TxRx mode.** **The LLDP transmission interval is 30 seconds and transmission delay is 2 seconds by default.**

Deployment

- Run LLDP on a switch to implement neighbor discovery and detect link fault.

11.3 Features

Basic Concepts

LLDPDU

LLDPDU is a protocol data unit encapsulated into an LLDP packet. Each LLDPDU is a sequence of TLV structures. The TLV collection consists of three mandatory TLVs, a series of optional TLVs, and one End Of TLV. The following figure shows the format of an LLDPDU.

Figure 12-3 LLDPDU Format

Chassis ID TLV	Port ID TLV	Time To Live TLV	Optional TLV	...	Optional TLV	End Of LLDPDU TLY
M	M	M				M

In the preceding figure:

- M indicates a mandatory TLV.
- In an LLDPDU, Chassis ID TLV, Port ID TLV, Time To Live TLV, and End Of LLDPDU TLV are mandatory and TLVs of other TLVs are optional.

LLDP Encapsulation Format

LLDP packets can be encapsulated in two formats: Ethernet II and Subnetwork Access Protocols (SNAP).

The following figure shows the format of LLDP packets encapsulated in the Ethernet II format.

Figure 12-4 Ethernet II Format

Destination Address	Source Address	Ethertype	LLDPDU	FCS

In the preceding figure:

- Destination Address: Indicates the destination MAC address, which is the LLDP multicast address 01-80-C2-00-00-0E.
- Source Address: Indicates the source MAC address, which is the port MAC address.
- Ethertype: Indicates the Ethernet type, which is 0x88CC.
- LLDPDU: Indicates the LLDP protocol data unit.
- FCS: Indicates the frame check sequence.

Figure 12-5 shows the format of LLDP packets encapsulated in the SNAP format.

Figure 12-5 SNAP Format

Destination Address	Source Address	SNAP-encoded Ethertype	LLDPDU	FCS

In the preceding figure:

- Destination Address: Indicates the destination MAC address, which is the LLDP multicast address 01-80-C2-00-00-0E.
- Source Address: Indicates the source MAC address, which is the port MAC address.
- SNAP-encoded Ethertype: Indicates the Ethernet type of the SNMP encapsulation, which is AA-AA-03-00-00-00-88-CC.
- LLDPDU: Indicates the LLDP protocol data unit.
- FCS: Indicates the frame check sequence.

TLV

TLVs encapsulated into an LLDPDU can be classified into two types:

- Basic management TLVs
- Organizationally specific TLVs

Basic management TLVs are a collection of basic TLVs used for network management. Organizationally specific TLVs are defined by standard organizations and other institutions, for example, the IEEE 802.1 organization and IEEE 802.3 organization define their own TLV collections.

4. Basic management TLVs

The basic management TLV collection consists of two types of TLVs: mandatory TLVs and optional TLVs. A mandatory TLV must be contained in an LLDPDU for advertisement and an optional TLV is contained selectively.

The following table describes basic management TLVs.

TLV Type	Description	Mandatory/Optional
End Of LLDPDU TLV	Indicates the end of an LLDPDU, occupying two bytes.	Mandatory
Chassis ID TLV	Identifies a device with a MAC address.	Mandatory

Port ID TLV	Identifies a port sending LLDPDUs.	Fixed
Time To Live TLV	Indicates the time to live (TTL) of local information on a neighbor. When a device receives a TLV containing TTL 0, it deletes the neighbor information.	Mandatory
Port Description TLV	Indicates the descriptor of the port sending LLDPDUs.	Optional
System Name TLV	Describes the device name.	Optional
System Description TLV	Indicates the device description, including the hardware version, software version, and operating system information.	Optional
System Capabilities TLV	Describes main functions of the device, such as the bridge, routing, and relay functions.	Optional
Management Address TLV	Indicates the management address, which contains the interface ID and object identifier (OID).	Optional

QTECH LLDP-compliant switches support advertisement of basic management TLVs.

5. Organizationally specific TLVs

Different organizations, such as the IEEE 802.1, IEEE 802.3, IETF and device suppliers, define specific TLVs to advertise specific information about devices. The organizationally unique identifier (OUI) field in a TLV is used to distinguish different organizations.

- Organizationally specific TLVs are optional and are advertised in an LLDPDU selectively. Currently, there are three types of common organizationally specific TLVs: IEEE 802.1 organizationally specific TLVs, IEEE 802.3 organizationally specific TLVs, and LLDP-MED TLVs.

The following table describes IEEE 802.1 organizationally specific TLVs.

TLV Type	**Description**
Port VLAN ID TLV	Indicates the VLAN identifier of a port.
Port And Protocol VLAN ID TLV	Indicates the protocol VLAN identifier of a port.

VLAN Name TLV	Indicates the VLAN name of a port.
Protocol Identity TLV	Indicates the protocol type supported by a port.

QTECH LLDP-compliant switches do not send the Protocol Identity TLV but receive this TLV.

IEEE 802.3 organizationally specific TLVs

The following table describes IEEE 802.3 organizationally specific TLVs.

TLV Type	Description
MAC/PHY Configuration//Status TLV	Indicates the rate and duplex mode of a port, and whether to support and enable auto-negotiation.
Power Via MDI TLV	Indicates the power supply capacity of a port.
Link Aggregation TLV	Indicates the link aggregation capacity of a port and the current aggregation state.
Maximum Frame Size TLV	Indicates the maximum size of the frame transmitted by a port.

QTECH LLDP-compliant devices support advertisement of IEEE 802.3 organizationally specific TLVs.

LLDP-MED TLV

LLDP-MED is an extension to LLDP based on IEEE 802.1AB LLDP. It enables users to conveniently deploy the Voice Over IP (VoIP) network and detect faults. It provides applications including the network configuration policies, device discovery, PoE management, and inventory management, meeting requirements for low cost, effective management, and easy deployment.

The following table describes LLDP-MED TLVs.

TLV Type	Description
LLDP-MED Capabilities TLV	Indicates the type of the LLDP-MED TLV encapsulated into an LLDPDU and device type (network connectivity device or endpoint device), and whether to support LLDP-MED,.

Network Policy TLV	Advertises the port VLAN configuration, supported application type (such as voice or video services), and Layer-2 priority information.
Location Identification TLV	Locates and identifies an endpoint device.
Extended Power-via-MDI TLV	Provides more advanced power supply management.
Inventory – Hardware Revision TLV	Indicates hardware version of a MED device.
Inventory – Firmware Revision TLV	Indicates the firmware version of the MED device.
Inventory – Software Revision TLV	Indicates the software version of the MED device.
Inventory – Serial Number TLV	Indicates the serial number of the MED device.
Inventory – Manufacturer Name TLV	Indicates the name of the manufacturer of the MED device.
Inventory – Model Name TLV	Indicates the module name of the MED device.
Inventory – Asset ID TLV	Indicates the asset identifier of the MED device, used for inventory management and asset tracking.

QTECH LLDP-compliant QTECH devices support advertisement of LLDP-MED TLVs.

Overview

Feature	Description
LLDP Work Mode	Configures the mode of transmitting and receiving LLDP packets.
LLDP Transmission Mechanism	Enables directly connected LLDP-compliant devices to send LLDP packets to the peer.

LLDP Reception Mechanism	Enables directly connected LLDP-compliant devices to receive LLDP packets from the peer.

11.3.1 LLDP Work Mode

Configure the LLDP work mode so as to specify the LLDP packet transmission and reception mode.

Working Principle

LLDP provides three work modes:

- TxRx: Transmits and receives LLDPDUs.
- Rx Only: Only receives LLDPDUs.
- Tx Only: Only transmits LLDPDUs.

When the LLDP work mode is changed, the port initializes the protocol state machine. You can set a port initialization delay to prevent repeated initialization of a port due to frequent changes of the LLDP work mode.

Related Configuration

Configuring the LLDP Work Mode

The default LLDP work mode is TxRx.

You can run the **lldp mode** command to configure the LLDP work mode.

If the work mode is set to TxRx, the device can both transmit and receive LLDP packets. If the work mode is set to Rx Only, the device can only receive LLDP packets. If the work mode is set to Tx Only, the device can only transmit LLDP packets. If the work mode is disabled, the device cannot transmit or receive LLDP packets.

11.3.2 LLDP Transmission Mechanism

LLDP packets inform peers of their neighbors. When the LLDP transmission mode is cancelled or disabled, LLDP packets cannot be transmitted to neighbors.

Working Principle

LLDP periodically transmits LLDP packets when working in TxRx or Tx Only mode. When information about the local device changes, LLDP immediately transmits LLDP packets. You can configure a delay time to avoid frequent transmission of LLDP packets caused by frequent changes of local information.

LLDP provides two types of packets:

- Standard LLDP packet, which contains management and configuration information about the local device.
- Shutdown packet: When the LLDP work mode is disabled or the port is shut down, LLDP Shutdown packets will be transmitted. A Shutdown packet consists of the Chassis ID TLV, Port ID TLV, Time To Live TLV, and End OF LLDP TLV. TTL in the Time to Live TLV is 0. When a device receives an LLDP Shutdown packet, it considers that the neighbor information is invalid and immediately deletes it.

When the LLDP work mode is changed from disabled or Rx to TxRx or Tx, or when LLDP discovers a new neighbor (that is, a device receives a new LLDP packet and the neighbor information is not stored locally), the fast transmission mechanism is started so that the neighbor quickly learns the device information. The fast transmission mechanism enables a device to transmit multiple LLDP packets at an interval of 1 second.

Related Configuration

Configuring the LLDP Work Mode

The default work mode is TxRx.

Run the **lldp mode txrx** or **lldp mode tx** command to enable the LLDP packet transmission function. Run the **lldp mode rx** or **no lldp mode** command to disable the LLDP packet transmission function.

In order to enable LLDP packet reception, set the work mode to TxRx or Rx Only. If the work mode is set to Rx Only, the device can only receive LLDP packets.

Configuring the LLDP Transmission Delay

The default LLDP transmission delay is 2 seconds.

Run the **lldp timer tx-delay** command to change the LLDP transmission delay.

If the delay is set to a very small value, the frequent change of local information will cause frequent transmission of LLDP packets. If the delay is set to a very large value, no LLDP packet may be transmitted even if local information is changed.

Configuring the LLDP Transmission Interval

The default LLDP transmission interval is 30 seconds.

Run the **lldp timer tx-interval** command to change the LLDP transmission interval.

If the interval is set to a very small value, LLDP packets may be transmitted frequently. If the interval is set to a very large value, the peer may not discover the local device in time.

Configuring the TLVs to Be Advertised

By default, an interface is allowed to advertise TLVs of all types except Location Identification TLV.

Run the **lldp tlv-enable** command to change the TLVs to be advertised.

Configuring the LLDP Fast Transmission Count

By default, three LLDP packets are fast transmitted.

Run the **lldp fast-count** command to change the number of LLDP packets that are fast transmitted.

11.3.3 LLDP Reception Mechanism

A device can discover the neighbor and determine whether to age the neighbor information according to received LLDP packets.

Working Principle

A device can receive LLDP packets when working in TxRx or Rx Only mode. After receiving an LLDP packet, a device conducts validity check. After the packet passes the check, the device checks whether the packet contains information about a new neighbor or about an existing neighbor and stores the neighbor information locally. The device sets the TTL of neighbor information according to the value of TTL TLV in the packet. If the value of TTL TLV is 0, the neighbor information is aged immediately.

Related Configuration

Configuring the LLDP Work Mode

The default LLDP work mode is TxRx.

Run the **lldp mode txrx** or **lldp mode rx** command to enable the LLDP packet reception function. Run the **lldp mode tx** or **no lldp mode** command to disable the LLDP packet reception function.

In order to enable LLDP packet reception, set the work mode to TxRx or Rx Only. If the work mode is set to Tx Only, the device can only transmit LLDP packets.

11.4 Configuration

Configuration	Description and Command	
Configuring the LLDP Function	⚠ (Optional) It is used to enable or disable the LLDP function in global or interface configuration mode.	
	lldp enable	Enables the LLDP function.
	no lldp enable	Disables the LLDP function.
	⚠ (Optional) It is used to configure the LLDP work mode.	

Configuring the LLDP Work Mode	**lldp mode {rx | tx | txrx }**	Configures the LLDP work mode.
	no lldp mode	Shuts down the LLDP work mode.
Configuring the TLVs to Be Advertised	⚠ (Optional) It is used to configure the TLVs to be advertised.	
	lldp tlv-enable	Configures the TLVs to be advertised.
	no lldp tlv-enable	Cancels TLVs.
Configures the Management Address to Be Advertised	⚠ (Optional) It is used to configure the management address to be advertised in LLDP packets.	
	lldp management-address-tlv [*ip-address*]	Configures the management address to be advertised in LLDP packets.
	no lldp management-address-tlv	Cancels the management address.
Configuring the LLDP Fast Transmission Count	⚠ (Optional) It is used to configure the number of LLDP packets that are fast transmitted.	
	lldp fast-count *value*	Configures the LLDP fast transmission count.
	no lldp fast-count	Restores the default LLDP fast transmission count.
Configuring the TTL Multiplier and Transmission Interval	⚠ (Optional) It is used to configure the TTL multiplier and transmission interval.	
	lldp hold-multiplier *value*	Configures the TTL multiplier.
	no lldp hold-multiplier	Restores the default TTL multiplier.
	lldp timer tx-interval *seconds*	Configures the transmission interval.

	no lldp timer tx-interval	Restores the default transmission interval.
Configuring the Transmission Delay	(Optional) It is used to configure the delay time for LLDP packet transmission.	
	lldp timer tx-delay *seconds*	Configures the transmission delay.
	no lldp timer tx-delay	Restores the default transmission delay.
Configuring the Initialization Delay	(Optional) It is used to configure the delay time for LLDP to initialize on any interface.	
	lldp timer reinit-delay *seconds*	Configures the initialization delay.
	no lldp timer reinit-delay	Restores the default initialization delay.
Configuring the LLDP Trap Function	(Optional) It is used to configure the LLDP Trap function.	
	lldp notification remote-change enable	Enables the LLDP Trap function.
	no lldp notification remote-change enable	Disables the LLDP Trap function.
	lldp timer notification-interval	Configures the LLDP Trap transmission interval.
	no lldp timer notification-interval	Restores the default LLDP Trap transmission interval.
Configuring the LLDP Error Detection Function	(Optional) It is used to configure the LLDP error detection function.	
	lldp error-detect	Enables the LLDP error detection function.
	no lldp error-detect	Disables the LLDP error detection function.

Configuring the LLDP Encapsulation Format	(Optional) It is used to configure the LLDP encapsulation format.	
	lldp encapsulation snap	Sets the LLDP encapsulation format to SNAP.
	no lldp encapsulation snap	Sets the LLDP encapsulation format to Ethernet II.
Configuring the LLDP Network Policy	(Optional) It is used to configure the LLDP Network Policy.	
	lldp network-policy profile *profile-num*	Configures an LLDP Network Policy.
	no lldp network-policy profile *profile-num*	Deletes an LLDP Network Policy.
Configuring the Civic Address	(Optional) It is used to configure the civic address of a device.	
	{ **country** | **state** | **county** | **city** | **division** | **neighborhood** | **street-group** | **leading-street-dir** | **trailing-street-suffix** | **street-suffix** | **number** | **street-number-suffix** | **landmark** | **additional-location-information** | **name** | **postal-code** | **building** | **unit** | **floor** | **room** | **type-of-place** | **postal-community-name** | **post-office-box** | **additional-code** } *ca-word*	Configures the civic address of a device.
	no { **country** | **state** | **county** | **city** | **division** | **neighborhood** | **street-group** | **leading-street-dir** | **trailing-street-suffix** | **street-suffix** | **number** | **street-number-suffix** | **landmark** | **additional-location-information** | **name** | **postal-code** | **building** | **unit** | **floor** | **room** | **type-of-place** | **postal-community-name** | **post-office-box** | **additional-code** } *ca-word*	Deletes civic address of a device.

Configuring the Emergency Telephone Number	(Optional) It is used to configure the emergency telephone number of a device.	
	lldp location elin identifier *id* **elin-location** *tel-number*	Configures the emergency telephone number of a device.
	no lldp location elin identifier *id*	Deletes the emergency telephone number of a device.
Configuring the Function of Ignoring PVID Detection	(Optional) It is used to ignore PVID detection.	
	lldp ignore pvid-error-detect	Enables the function of ignoring PVID detection.
	no lldp ignore pvid-error-detect	Disables the function of ignoring PVID detection.

11.4.1 Configuring the LLDP Function

Configuration Effect

Enable or disable the LLDP function.

Notes

- To make the LLDP function take effect on an interface, you need to enable the LLDP function globally and on the interface.

Configuration Steps

- Optional.
- Configure the LLDP function in global or interface configuration mode.

Verification

Display LLDP status

- Check whether the LLDP function is enabled in global configuration mode.
- Check whether the LLDP function is enabled in interface configuration mode.

Related Commands

Enabling the LLDP Function

Command	lldp enable
Parameter Description	N/A
Command Mode	Global configuration mode/Interface configuration mode
Usage Guide	The LLDP function takes effect on an interface only after it is enabled in global configuration mode and interface configuration mode.

Disabling the LLDP Function

Command	no lldp enable
Parameter Description	N/A
Command Mode	Global configuration mode/Interface configuration mode
Usage Guide	N/A

Configuration Example

Disabling the LLDP Function

Configuration Steps	Disable the LLDP function in global configuration mode.
	QTECH(config)#no lldp enable
Verification	Display global LLDP status.
	QTECH(config)#show lldp status Global status of LLDP: Disable

Common Errors

- If the LLDP function is enabled on an interface but disabled in global configuration mode, the LLDP function does not take effect on the interface.
- A port can learn a maximum of five neighbors.
- If a neighbor does not support LLDP but it is connected to an LLDP-supported device, a port may learn information about the device that is not directly connected to the port because the neighbor may forward LLDP packets.

11.4.2 Configuring the LLDP Work Mode

Configuration Effect

- If you set the LLDP work mode to TxRx, the interface can transmit and receive packets.
- If you set the LLDP work mode to Tx, the interface can only transmit packets but cannot receive packets.
- If you set the LLDP work mode to Rx, the interface can only receive packets but cannot transmit packets.
- If you disable the LLDP work mode, the interface can neither receive nor transmit packets.

Notes

- LLDP runs on physical ports (AP member ports for AP ports). Stacked ports and VSL ports do not support LLDP.

Configuration Steps

- Optional.
- Set the LLDP work mode to Tx or Rx as required.

Verification

Display LLDP status information on an interface

- Check whether the configuration takes effect.

Related Commands

Configuring the LLDP Work Mode

Command	**lldp mode { rx | tx | txrx }**

Parameter Description	**rx**: Only receives LLDPDUs. **tx**: Only transmits LLDPDUs. **txrx**: Transmits and receives LLDPDUs.
Command Mode	Interface configuration mode
Usage Guide	To make LLDP take effect on an interface, make sure to enable LLDP globally and set the LLDP work mode on the interface to Tx, Rx or TxRx.

Disabling the LLDP Work Mode

Command	**no lldp mode**
Parameter Description	N/A
Command Mode	Interface configuration mode
Usage Guide	After the LLDP work mode on an interface is disabled, the interface does not transmit or receive LLDP packets.

Configuration Example

Configuring the LLDP Work Mode

Configuration Steps	**Set the LLDP work mode to Tx in interface configuration mode.**
	QTECH(config)#interface gigabitethernet 0/1 QTECH(config-if-GigabitEthernet 0/1)#lldp mode tx
Verification	Display LLDP status information on the interface.
	QTECH(config-if-GigabitEthernet 0/1)#show lldp status interface gigabitethernet 0/1 Port [GigabitEthernet 0/1] Port status of LLDP : Enable

```
Port state                    : UP
Port encapsulation            : Ethernet II
Operational mode              : TxOnly
Notification enable           : NO
Error detect enable           : YES
Number of neighbors           : 0
Number of MED neighbors       : 0
```

11.4.3 Configuring the TLVs to Be Advertised

Configuration Effect

- Configure the type of TLVs to be advertised to specify the LLDPDUs in LLDP packets.

Notes

- If you configure the **all** parameter for the basic management TLVs, IEEE 802.1 organizationally specific TLVs, and IEEE 802.3 organizationally specific TLVs, all optional TLVs of these types are advertised.
- If you configure the **all** parameter for the LLDP-MED TLVs, all LLDP-MED TLVs except Location Identification TLV are advertised.
- If you want to configure the LLDP-MED Capability TLV, configure the LLDP 802.3 MAC/PHY TLV first; If you want to cancel the LLDP 802.3 MAC/PHY TLV, cancel the LLDP-MED Capability TLV first.
- If you want to configure LLDP-MED TLVs, configure the LLDP-MED Capability TLV before configuring other types of LLDP-MED TLVs. If you want to cancel LLDP-MED TLVs, cancel the LLDP-MED Capability TLV before canceling other types of LLDP-MED TLVs If a device is connected to an IP-Phone that supports LLDP-MED, you can configure the Network Policy TLV to push policy configuration to the IP-Phone.
- If a device supports the DCBX function by default, ports of the device are not allowed to advertise IEEE 802.3 organizationally specific TLVs and LLDP-MED TLVs by default.

Configuration Steps

- Optional.
- Configure the type of TLVs to be advertised on an interface.

Verification

Display the configuration of TLVs to be advertised on an interface

- Check whether the configuration takes effect.

Related Commands

Configuring TLVs to Be Advertised

Command	**lldp tlv-enable { basic-tlv { all | port-description | system-capability | system-description | system-name } |dot1-tlv { all | port-vlan-id | protocol-vlan-id [*vlan-id*] | vlan-name [*vlan-id*] } |dot3-tlv { all | link-aggregation | mac-physic | max-frame-size | power } | med-tlv { all | capability | inventory | location { civic-location | elin } identifier *id* | network-policy profile [*profile-num*] | power-over-ethernet } }**
Parameter Description	**basic-tlv**: Indicates the basic management TLV. **port-description**: Indicates the Port Description TLV. **system-capability**: Indicates the System Capabilities TLV. **system-description**: Indicates the System Description TLV. **system-name**: Indicates the System Name TLV. **dot1-tlv**: Indicates the IEEE 802.1 organizationally specific TLVs. **port-vlan-id**: Indicates the Port VLAN ID TLV. **protocol-vlan-id**: Indicates the Port And Protocol VLAN ID TLV. *vlan-id*: Indicates the Port Protocol VLAN ID, ranging from 1 to 4,094. **vlan-name**: Indicates the VLAN Name TLV. *vlan-id*: Indicates the VLAN name, ranging from 1 to 4,094. **dot3-tlv**: Indicates the IEEE 802.3 organizationally specific TLVs. **link-aggregation**: Indicates the Link Aggregation TLV. **mac-physic**: Indicates the MAC/PHY Configuration/Status TLV. **max-frame-size**: Indicates the Maximum Frame Size TLV. **power**: Indicates the Power Via MDI TLV. **med-tlv**: Indicates the LLDP MED TLV. **capability**: Indicates the LLDP-MED Capabilities TLV. **Inventory**: Indicates the inventory management TLV, which contains the hardware version, firmware version, software version, SN, manufacturer name, module name, and asset identifier. **location**: Indicates the Location Identification TLV. **civic-location**: Indicates the civic address information and postal information.

	elin: Indicates the emergency telephone number. *id*: Indicates the policy ID, ranging from 1 to 1,024. **network-policy**: Indicates the Network Policy TLV. *profile-num*: Indicates the Network Policy ID, ranging from 1 to 1,024. **power-over-ethernet**: Indicates the Extended Power-via-MDI TLV.
Command Mode	Interface configuration mode
Usage Guide	N/A

Canceling TLVs

Command	**no lldp tlv-enable {basic-tlv { all | port-description | system-capability | system-description | system-name } | dot1-tlv { all | port-vlan-id | protocol-vlan-id | vlan-name } | dot3-tlv { all | link-aggregation | mac-physic | max-frame-size | power } | med-tlv { all | capability | inventory | location { civic-location | elin } identifier *id* | network-policy profile [*profile-num*] | power-over-ethernet } }**
Parameter Description	**basic-tlv**: Indicates the basic management TLV. **port-description**: Indicates the Port Description TLV. **system-capability**: Indicates the System Capabilities TLV. **system-description**: Indicates the System Description TLV. **system-name**: Indicates the System Name TLV. **dot1-tlv**: Indicates the IEEE 802.1 organizationally specific TLVs. **port-vlan-id**: Indicates the Port VLAN ID TLV. **protocol-vlan-id**: Indicates the Port And Protocol VLAN ID TLV. **vlan-name**: Indicates the VLAN Name TLV. **dot3-tlv**: Indicates the IEEE 802.3 organizationally specific TLVs. **link-aggregation**: Indicates the Link Aggregation TLV. **mac-physic**: Indicates the MAC/PHY Configuration/Status TLV. **max-frame-size**: Indicates the Maximum Frame Size TLV. **power**: Indicates the Power Via MDI TLV. **med-tlv**: Indicates the LLDP MED TLV. **capability**: Indicates the LLDP-MED Capabilities TLV.

	Inventory: Indicates the inventory management TLV, which contains the hardware version, firmware version, software version, SN, manufacturer name, module name, and asset identifier. **location**: Indicates the Location Identification TLV. **civic-location**: Indicates the civic address information and postal information. **elin**: Indicates the emergency telephone number. *id*: Indicates the policy ID, ranging from 1 to 1,024. **network-policy**: Indicates the Network Policy TLV. *profile-num*: Indicates the Network Policy ID, ranging from 1 to 1,024. **power-over-ethernet**: Indicates the Extended Power-via-MDI TLV.
Command Mode	Interface configuration mode
Usage Guide	N/A

Configuration Example

Configuring TLVs to Be Advertised

Configuration Steps	**Cancel the advertisement of the IEEE 802.1 organizationally specific Port And Protocol VLAN ID TLV.**
	QTECH(config)#interface gigabitethernet 0/1 QTECH(config-if-GigabitEthernet 0/1)#no lldp tlv-enable dot1-tlv protocol-vlan-id
Verification	Display LLDP TLV configuration in interface configuration mode.
	QTECH(config-if-GigabitEthernet 0/1)#show lldp tlv-config interface gigabitethernet 0/1 LLDP tlv-config of port [GigabitEthernet 0/1] NAME STATUS DEFAULT ----------------------------- ------ -------

	Basic optional TLV: Port Description TLV YES YES System Name TLV YES YES System Description TLV YES YES System Capabilities TLV YES YES Management Address TLV YES YES IEEE 802.1 extend TLV: Port VLAN ID TLV YES YES Port And Protocol VLAN ID TLV NO YES VLAN Name TLV YES YES IEEE 802.3 extend TLV: MAC-Physic TLV YES YES Power via MDI TLV YES YES Link Aggregation TLV YES YES Maximum Frame Size TLV YES YES LLDP-MED extend TLV: Capabilities TLV YES YES Network Policy TLV YES YES Location Identification TLV NO NO Extended Power via MDI TLV YES YES Inventory TLV YES YES

11.4.4 Configures the Management Address to Be Advertised

Configuration Effect

- Configure the management address to be advertised in LLDP packets in interface configuration mode.
- After the management address to be advertised is cancelled, the management address in LLDP packets is subject to the default settings.

Notes

- LLDP runs on physical ports (AP member ports for AP ports). Stacked ports and VSL ports do not support LLDP.

Configuration Steps

- Optional.
- Configure the management address to be advertised in LLDP packets in interface configuration mode.

Verification

Display LLDP information on a local interface

- Check whether the configuration takes effect.

Related Commands

Configuring the Management Address to Be Advertised

Command	**lldp management-address-tlv [*ip-address*]**
Parameter Description	*ip-address*: Indicates the management address to be advertised in an LLDP packet.
Command Mode	Interface configuration mode
Usage Guide	A management address is advertised through LLDP packets by default. The management address is the IPv4 address of the minimum VLAN supported by the port. If no IPv4 address is configured for the VLAN, LLDP keeps searching for the qualified IP address. If no IPv4 address is found, LLDP searches for the IPv6 address of the minimum VLAN supported by the port. If no IPv6 address is found, the loopback address 127.0.0.1 is used as the management address.

Canceling the Management Address

Command	**no lldp management-address-tlv**
Parameter Description	N/A

Command Mode	Interface configuration mode
Usage Guide	A management address is advertised through LLDP packets by default. The management address is the IPv4 address of the minimum VLAN supported by the port. If no IPv4 address is configured for the VLAN, LLDP keeps searching for the qualified IP address. If no IPv4 address is found, LLDP searches for the IPv6 address of the minimum VLAN supported by the port. If no IPv6 address is found, the loopback address 127.0.0.1 is used as the management address.

Configuration Example

Configuring the Management Address to Be Advertised

Configuration Steps	Set the management address to 192.168.1.1 on an interface.
	QTECH(config)#interface gigabitethernet 0/1 QTECH(config-if-GigabitEthernet 0/1)#lldp management-address-tlv 192.168.1.1
	Display configuration on the interface.
	QTECH(config-if-GigabitEthernet 0/1)#show lldp local-information interface GigabitEthernet 0/1 Lldp local-information of port [GigabitEthernet 0/1] Port ID type : Interface name Port id : GigabitEthernet 0/1 Port description : GigabitEthernet 0/1 Management address subtype : ipv4 Management address : 192.168.1.1 Interface numbering subtype : ifIndex Interface number : 1 Object identifier :

	802.1 organizationally information Port VLAN ID : 1 Port and protocol VLAN ID(PPVID) : 1 PPVID Supported : YES PPVID Enabled : NO VLAN name of VLAN 1 : VLAN0001 Protocol Identity : 802.3 organizationally information Auto-negotiation supported : YES Auto-negotiation enabled : YES PMD auto-negotiation advertised : 1000BASE-T full duplex mode, 100BASE-TX full duplex mode, 100BASE-TX half duplex mode, 10BASE-T full duplex mode, 10BASE-T half duplex mode Operational MAU type : speed(100)/duplex(Full) PoE support : NO Link aggregation supported : YES Link aggregation enabled : NO Aggregation port ID : 0 Maximum frame Size : 1500 LLDP-MED organizationally information Power-via-MDI device type : PD Power-via-MDI power source : Local Power-via-MDI power priority : Power-via-MDI power value : Model name : Model name

11.4.5 Configuring the LLDP Fast Transmission Count

Configuration Effect

- Configure the number of LLDP packets that are fast transmitted.

Configuration Steps

- Optional.
- Configure the number of LLDP packets that are fast transmitted in global configuration mode.

Verification

Displaying the global LLDP status information

- Check whether the configuration takes effect.

Related Commands

Configuring the LLDP Fast Transmission Count

Command	lldp fast-count *value*
Parameter Description	*value*: Indicates the number of LLDP packets that are fast transmitted. The value ranges from 1 to 10. The default value is 3.
Command Mode	Global configuration mode
Usage Guide	N/A

Restoring the Default LLDP Fast Transmission Count

Command	no lldp fast-count
Parameter Description	N/A
Command Mode	Global configuration mode
Usage Guide	N/A

Configuration Example

Configuring the LLDP Fast Transmission Count

Configuration Steps	Set the LLDP fast transmission count to 5 in global configuration mode.
	QTECH(config)#lldp fast-count 5
Verification	Display the global LLDP status information.
	QTECH(config)#show lldp status Global status of LLDP : Enable Neighbor information last changed time : Transmit interval : 30s Hold multiplier : 4 Reinit delay : 2s Transmit delay : 2s Notification interval : 5s Fast start counts : 5

11.4.6 Configuring the TTL Multiplier and Transmission Interval

Configuration Effect

- Configure the TTL multiplier.
- Configure the LLDP packet transmission interval.

Configuration Steps

- Optional.
- Perform the configuration in global configuration mode.

Verification

Display LLDP status information on an interface

- Check whether the configuration takes effect.

Related Commands

Configuring the TTL Multiplier

Command	lldp hold-multiplier *value*
Parameter Description	*value*: Indicates the TLL multiplier. The value ranges from 2 to 10. The default value is 4.
Command Mode	Global configuration mode
Usage Guide	In an LLDP packet. the value of Time To Live TLV is calculated based on the following formula: Time to Live TLV= TTL multiplier x Packet transmission interval + 1. Therefore, you can modify the Time to Live TLV in LLDP packets by configuring the TTL multiplier.

Restoring the Default TTL Multiplier

Command	no lldp hold-multiplier
Parameter Description	N/A
Command Mode	Global configuration mode
Usage Guide	In an LLDP packet, the value of Time To Live TLV is calculated based on the following formula: Time to Live TLV = TTL multiplier x Packet transmission interval + 1. Therefore, you can modify the Time to Live TLV in LLDP packets by configuring the TTL multiplier.

Configuring the Transmission Interval

Command	lldp timer tx-interval *seconds*
Parameter Description	*seconds*: Indicates the LLDP packet transmission interval. The value ranges from 5 to 32,768.
Command Mode	Global configuration mode
Usage Guide	N/A

Restoring the Default Transmission Interval

Command	no lldp timer tx-interval
Parameter Description	N/A
Command Mode	Global configuration mode
Usage Guide	N/A

Configuration Example

Configuring the TTL Multiplier and Transmission Interval

Configuration Steps	Set the TTL multiplier to 3 and the transmission interval to 20 seconds. The TTL of local device information on neighbors is 61 seconds.
	QTECH(config)#lldp hold-multiplier 3 QTECH(config)#lldp timer tx-interval 20
Verification	Display the global LLDP status information.
	QTECH(config)#lldp hold-multiplier 3 QTECH(config)#lldp timer tx-interval 20 QTECH(config)#show lldp status Global status of LLDP : Enable Neighbor information last changed time : Transmit interval : 20s Hold multiplier : 3 Reinit delay : 2s Transmit delay : 2s Notification interval : 5s Fast start counts : 3

11.4.7 Configuring the Transmission Delay

Configuration Effect

- Configure the delay time for LLDP packet transmission.

Configuration Steps

- Optional.
- Perform the configuration in global configuration mode.

Verification

Displaying the global LLDP status information

- Check whether the configuration takes effect.

Related Commands

Configuring the Transmission Delay

Command	**lldp timer tx-delay *seconds***
Parameter Description	*seconds*: Indicates the transmission delay. The value ranges from 1 to 8,192.
Command Mode	Global configuration mode
Usage Guide	When local information of a device changes, the device immediately transmits LLDP packets to its neighbors. Configure the transmission delay to prevent frequent transmission of LLDP packets caused by frequent changes of local information.

Restoring the Default Transmission Delay

Command	**no lldp timer tx-delay**
Parameter Description	N/A
Command Mode	Global configuration mode

Usage Guide	When local information of a device changes, the device immediately transmits LLDP packets to its neighbors. Configure the transmission delay to prevent frequent transmission of LLDP packets caused by frequent changes of local information.

Configuration Example

Configuring the Transmission Delay

Configuration Steps	**Set the transmission delay to 3 seconds.**
	QTECH(config)#lldp timer tx-delay 3
Verification	Display the global LLDP status information.
	QTECH(config)#show lldp status Global status of LLDP : Enable Neighbor information last changed time : Transmit interval : 30s Hold multiplier : 4 Reinit delay : 2s Transmit delay : 3s Notification interval : 5s Fast start counts : 3

11.4.8 Configuring the Initialization Delay

Configuration Effect

- Configure the delay time for LLDP to initialize on any interface.

Configuration Steps

- Optional.
- Configure the delay time for LLDP to initialize on any interface.

Verification

Display the global LLDP status information

- Check whether the configuration takes effect.

Related Commands

Configuring the Initialization Delay

Command	**lldp timer reinit-delay *seconds***
Parameter Description	*seconds*: Indicates the initialization delay . The value ranges from 1 to 10 seconds.
Command Mode	Global configuration mode
Usage Guide	Configure the initialization delay to prevent frequent initialization of the state machine caused by frequent changes of the port work mode.

Restoring the Default Initialization Delay

Command	**no lldp timer reinit-delay**
Parameter Description	N/A
Command Mode	Global configuration mode
Usage Guide	Configure the initialization delay to prevent frequent initialization of the state machine caused by frequent changes of the port work mode.

Configuration Example

Configuring the Initialization Delay

Configuration Steps	**Set the initialization delay to 3 seconds.**

	QTECH(config)#lldp timer reinit-delay 3
Verification	Display the global LLDP status information.
	QTECH(config)#show lldp status Global status of LLDP : Enable Neighbor information last changed time : Transmit interval : 30s Hold multiplier : 4 Reinit delay : 3s Transmit delay : 2s Notification interval : 5s Fast start counts : 3

11.4.9 Configuring the LLDP Trap Function

Configuration Effect

- Configure the interval for transmitting LLDP Trap messages.

Configuration Steps

Enabling the LLDP Trap Function

- Optional.
- Perform the configuration in interface configuration mode.
- Configuring the LLDP Trap Transmission Interval
- Optional.
- Perform the configuration in global configuration mode.

Verification

Display LLDP status information

- Check whether the LLDP Trap function is enabled.
- Check whether the interval configuration takes effect.

Related Commands

Enabling the LLDP Trap Function

Command	lldp notification remote-change enable
Parameter Description	N/A
Command Mode	Interface configuration mode
Usage Guide	The LLDP Trap function enables a device to send its local LLDP information (such as neighbor discovery and communication link fault) to the NMS server so that administrators learn about the network performance

Disabling the LLDP Trap Function

Command	no lldp notification remote-change enable
Parameter Description	N/A
Command Mode	Interface configuration mode
Usage Guide	The LLDP Trap function enables a device to send its local LLDP information (such as neighbor discovery and communication link fault) to the NMS server so that administrators learn about the network performance.

Configuring the LLDP Trap Transmission Interval

Command	lldp timer notification-interval *seconds*
Parameter Description	*seconds*: Indicates the interval for transmitting LLDP Trap messages. The value ranges from 5 to 3,600 seconds. The default value is 5 seconds.
Command Mode	Global configuration mode
Usage Guide	Configure the LLDP Trap transmission interval to prevent frequent transmission of LLDP Trap messages. LLDP changes detected within this interval will be transmitted to the NMS server.

Restoring the LLDP Trap Transmission Interval

Command	no lldp timer notification-interval
Parameter Description	N/A
Command Mode	Global configuration mode
Usage Guide	Configure the LLDP Trap transmission interval to prevent frequent transmission of LLDP Trap messages. LLDP changes detected within this interval will be transmitted to the NMS server.

Configuration Example

Enabling the LLDP Trap Function and Configuring the LLDP Trap Transmission Interval

Configuration Steps	Enable the LLDP Trap function and set the LLDP Trap transmission interval to 10 seconds.
	QTECH(config)#lldp timer notification-interval 10 QTECH(config)#interface gigabitethernet 0/1 QTECH(config-if-GigabitEthernet 0/1)#lldp notification remote-change enable
Verification	Display LLDP status information.
	QTECH(config-if-GigabitEthernet 0/1)#show lldp status Global status of LLDP : Enable Neighbor information last changed time : Transmit interval : 30s Hold multiplier : 4 Reinit delay : 2s Transmit delay : 2s Notification interval : 10s

	Fast start counts : 3 -- Port [GigabitEthernet 0/1] -- Port status of LLDP : Enable Port state : UP Port encapsulation : Ethernet II Operational mode : RxAndTx Notification enable : YES Error detect enable : YES Number of neighbors : 0 Number of MED neighbors : 0

11.4.10 Configuring the LLDP Error Detection Function

Configuration Effect

- Enable the LLDP error detection function. When LLDP detects an error, the error is logged.
- Configure the LLDP error detection function to detect VLAN configuration at both ends of a link, port status, aggregate port configuration, MTU configuration, and loops.

Notes

N/A

Configuration Steps

- Optional.
- Enable or disable the LLDP error detection function in interface configuration mode.

Verification

Display LLDP status information on an interface

- Check whether the configuration takes effect.

Related Commands

Enabling the LLDP Error Detection Function

Command	**lldp error-detect**
Parameter Description	N/A
Command Mode	Interface configuration mode
Usage Guide	The LLDP error detection function relies on specific TLVs in LLDP packets exchanged between devices at both ends of a link. Therefore, a device needs to advertise correct TLVs to ensure the LLDP error detection function.

Disabling the LLDP Error Detection Function

Command	**no lldp error-detect**
Parameter Description	N/A
Command Mode	Interface configuration mode
Usage Guide	The LLDP error detection function relies on specific TLVs in LLDP packets exchanged between devices at both ends of a link. Therefore, a device needs to advertise correct TLVs to ensure the LLDP error detection function.

Configuration Example

Enabling the LLDP Error Detection Function

Configuration Steps	**Enable the LLDP error detection function on interface GigabitEthernet 0/1.**
	QTECH(config)#interface gigabitethernet 0/1 QTECH(config-if-GigabitEthernet 0/1)#lldp error-detect
Verification	Display LLDP status information on the interface.

	QTECH(config-if-GigabitEthernet 0/1)#show lldp status interface gigabitethernet 0/1 Port [GigabitEthernet 0/1] Port status of LLDP : Enable Port state : UP Port encapsulation : Ethernet II Operational mode : RxAndTx Notification enable : NO Error detect enable : YES Number of neighbors : 0 Number of MED neighbors : 0

11.4.11 Configuring the LLDP Encapsulation Format

Configuration Effect

- Configure the LLDP encapsulation format.

Configuration Steps

- Optional.
- Configure the LLDP encapsulation format on an interface.

Verification

Display LLDP status information of an interface

- Check whether the configuration takes effect.

Related Commands

- Setting the LLDP Encapsulation Format to SNAP

Command	**lldp encapsulation snap**
Parameter Description	N/A
Command Mode	Interface configuration mode

Usage Guide	⚠ The LLDP encapsulation format configuration on a device and its neighbors must be consistent.

- Restoring the Default LLDP Encapsulation Format (Ethernet II)

Command	**No lldp encapsulation snap**
Parameter Description	N/A
Command Mode	Interface configuration mode
Usage Guide	⚠ The LLDP encapsulation format configuration on a device and its neighbors must be consistent.

Configuration Example

Setting the LLDP Encapsulation Format to SNAP

Configuration Steps	**Set the LLDP encapsulation format to SNAP.**
	QTECH(config)#interface gigabitethernet 0/1 QTECH(config-if-GigabitEthernet 0/1)#lldp encapsulation snap
Verification	Display LLDP status information on the interface.
	QTECH(config-if-GigabitEthernet 0/1)#show lldp status interface gigabitethernet 0/1 Port [GigabitEthernet 0/1] Port status of LLDP : Enable Port state : UP Port encapsulation : Snap Operational mode : RxAndTx Notification enable : NO Error detect enable : YES Number of neighbors : 0

	Number of MED neighbors : 0

11.4.12 Configuring the LLDP Network Policy

Configuration Effect

- Configure the LLDP Network Policy.
- If a device is connected to an IP-Phone that supports LLDP-MED, you can configure the Network Policy TLV to push policy configuration to the IP-Phone, , which enables the IP-Phone to change the tag and QoS of voice streams. In addition to the LLDP Network Policy, perform the following steps on the device: 1. Enable the Voice VLAN function and add the port connected to the IP-Phone to the Voice VLAN. 2. Configure the port connected to the IP-Phone as a QoS trusted port (the trusted DSCP mode is recommended). 3. If 802.1X authentication is also enabled on the port, configure a secure channel for the packets from the Voice VLAN. If the IP-Phone does not support LLDP-MED, enable the voice VLAN function and add the MAC address of the IP-Phone to the Voice VLAN OUI list manually.
- For the configuration of the QoS trust mode, see *Configuring IP QoS*; for the configuration of the Voice VLAN, see *Configuring Voice VLAN*; for the configuration of the secure channel, see *Configuring ACL*.

Configuration Steps

- Optional.
- Configure the LLDP Network Policy.

Verification

- Displaying the LLDP network policy configuration.
- Check whether the configuration takes effect.

Related Commands

Configuring the LLDP Network Policy

Command	**lldp network-policy profile *profile-num***
Parameter Description	*profile-num*: Indicates the ID of an LLDP Network Policy. The value ranges from 1 to 1,024.

Command Mode	Global configuration mode
Usage Guide	Run this command to enter the LLDP network policy mode after specifying a policy ID. After entering the LLDP network policy mode, run the **{ voice | voice-signaling } vlan** command to configure a specific network policy.

Deleting the LLDP Network Policy

Command	**no lldp network-policy profile *profile-num***
Parameter Description	*profile-num*: Indicates the LLDP Network Policy ID. The value ranges from 1 to 1,024.
Command Mode	Interface configuration mode
Usage Guide	Run this command to enter the LLDP network policy mode after specifying a policy ID. After entering the LLDP network policy mode, run the **{ voice | voice-signaling } vlan** command to configure a specific network policy.

Configuration Example

Configuring the LLDP Network Policy

Configuration Steps	**Set the Network Policy TLV to 1 for LLDP packets to be advertised by port GigabitEthernet 0/1 and set the VLAN ID of the Voice application to 3, COS to 4, and DSCP to 6.**
	QTECH#config QTECH(config)#lldp network-policy profile 1 QTECH(config-lldp-network-policy)# voice vlan 3 cos 4 QTECH(config-lldp-network-policy)# voice vlan 3 dscp 6 QTECH(config-lldp-network-policy)#exit QTECH(config)# interface gigabitethernet 0/1

	QTECH(config-if-GigabitEthernet 0/1)# lldp tlv-enable med-tlv network-policy profile 1
Verification	Display the LLDP network policy configuration on the local device.
	network-policy information: -------------------------- network policy profile :1 voice vlan 3 cos 4 voice vlan 3 dscp 6

11.4.13 Configuring the Civic Address

Configuration Effect

- Configure the civic address of a device.

Configuration Steps

- Optional.
- Perform this configuration in LLDP Civic Address configuration mode.

Verification

Display the LLDP civic address of the local device

- Check whether the configuration takes effect.

Related Commands

Configuring the Civic Address of a Device

Command	**Configure the LLDP civic address. Use the no option to delete the address.** **{ country | state | county | city | division | neighborhood | street-group | leading-street-dir | trailing-street-suffix | street-suffix | number | street-number-suffix | landmark | additional-location-information | name | postal-code | building | unit | floor | room | type-of-place | postal-community-name | post-office-box | additional-code }** ***ca-word***

Parameter Description	**country**: Indicates the country code, with two characters. CH indicates China. **state**: Indicates the CA type is 1. **county**: Indicates that the CA type is 2. **city**: Indicates that the CA type is 3. **division**: Indicates that the CA type is 4. **neighborhood**: Indicates that the CA type is 5. **street-group**: Indicates that the CA type is 6. **leading-street-dir**: Indicates that the CA type is 16. **trailing-street-suffix**: Indicates that the CA type is 17. **street-suffix**: Indicates that the CA type is 18. **number**: Indicates that the CA type is 19. **street-number-suffix**: Indicates that the CA type is 20. **landmark**: Indicates that the CA type is 21. **additional-location-information**: Indicates that the CA type is 22. **name**: Indicates that the CA type is 23. **postal-code**: Indicates that the CA type is 24. **building**: Indicates that the CA type is 25. **unit**: Indicates that the CA type is 26. **floor**: Indicates that the CA type is 27. **room**: Indicates that the CA type is 28. **type-of-place**: Indicates that the CA type is 29. **postal-community-name**: Indicates that the CA type is 30. **post-office-box**: Indicates that the CA type is 31. **additional-code**: Indicates that the CA type is 32. *ca-word*: Indicates the address.
Command Mode	LLDP Civic Address configuration mode
Usage Guide	After entering the LLDP Civic Address configuration mode, configure the LLDP civic address.

Deleting the Civic Address of a Device

Command	**no { country | state | county | city | division | neighborhood | street-group | leading-street-dir | trailing-street-suffix | street-suffix | number | street-number-suffix | landmark | additional-location-information | name | postal-code | building | unit | floor | room | type-of-place | postal-community-name | post-office-box | additional-code }**
Parameter Description	N/A
Command Mode	LLDP Civic Address configuration mode
Usage Guide	After entering the LLDP Civic Address configuration mode, configure the LLDP civic address.

Configuring the Device Type

Command	**device-type *device-type***
Parameter Description	*device-type*: Indicates the device type. The value ranges from 0 to 2. The default value is 1. 0 indicates that the device type is DHCP server. 1 indicates that the device type is switch. 2 indicates that the device type is LLDP MED .
Command Mode	LLDP Civic Address configuration mode
Usage Guide	After entering the LLDP Civic Address configuration mode, configure the device type.

Restoring the Device Type

Command	**no device-type**
Parameter Description	N/A
Command Mode	LLDP Civic Address configuration mode

Usage Guide	After entering the LLDP Civic Address configuration mode, restore the default settings.

Configuration Example

Configuring the Civic Address of a Device

Configuration Steps	**Set the address of port GigabitEthernet 0/1 as follows: set country to CH, city to Fuzhou, and postal code to 350000.**
	QTECH#config QTECH(config)#lldp location civic-location identifier 1 QTECH(config-lldp-civic)# country CH QTECH(config-lldp-civic)# city Fuzhou QTECH(config-lldp-civic)# postal-code 350000
Verification	Display the LLDP civic address of port GigabitEthernet 0/1 1.
	civic location information: -------------------------- Identifier :1 country :CH device type :1 city :Fuzhou postal-code :350000

11.4.14 Configuring the Emergency Telephone Number

Configuration Effect

- Configure the emergency telephone number of a device.

Configuration Steps

- Optional.
- Perform this configuration in global configuration mode.

Verification

Display the emergency telephone number of the local device

- Check whether the configuration takes effect.

Related Commands

Configuring the Emergency Telephone Number of a Device

Command	**lldp location elin identifier *id* elin-location *tel-number***
Parameter Description	*id*: Indicates the identifier of an emergency telephone number. The value ranges from 1 to 1,024. *tel-number*: Indicates emergency telephone number, containing 10-25 characters.
Command Mode	Global configuration mode
Usage Guide	Run this command to configure the emergency telephone number.

Deleting the Emergency Telephone Number of a Device

Command	**no lldp location elin identifier *id***
Parameter Description	*id*: Indicates the identifier of an emergency telephone number. The value ranges from 1 to 1,024.
Command Mode	Global configuration mode
Usage Guide	N/A

Configuration Example

Configuring the Emergency Telephone Number of a Device

Configuration Steps	Set the emergency telephone number of port GigabitEthernet 0/1 to 085285555556.
	QTECH#config QTECH(config)#lldp location elin identifier 1 elin-location 085283671111
Verification	Display the emergency telephone number of port GigabitEthernet 0/1.
	elin location information: ------------------------- Identifier :1 elin number :085283671111

11.4.15 Configuring the Function of Ignoring PVID Detection

Configuration Effect

- Ignores the PVID detection.

Configuration Steps

- Optional.
- According to the real condition, select whether to enable the function..

Verification

Display the LLDP information.

- Check whether the status of PVID detection in global LLDP is the same as your configuration.

Related Commands

Ignoring PVID Detection

Command	lldp ignore pvid-error-detect
Parameter Description	N/A

Command Mode	Global configuration mode
Usage Guide	Use the command to ignore PVID detection.

Configuration Example

Configuring the Function of Ignoring PVID Detection

Configuration Steps	**Ignores PVID detection in global configuration mode.**
	QTECH#config QTECH(config)#lldp ignore pvid-error-detect
Verification	Display the global LLDP information.
	uijie(config)#show lldp status Global status of LLDP : Enable Neighbor information last changed time : Transmit interval : 30s Hold multiplier : 4 Reinit delay : 2s Transmit delay : 2s Notification interval : 5s Fast start counts : 5 Igore PVID error detect : YES

11.5 Monitoring

Clearing

Running the **clear** commands may lose vital information and thus interrupt services.

Description	Command
Clears LLDP statistics.	**clear lldp statistics** [**interface** *interface-name*]
Clears LLDP neighbor information.	**clear lldp table** [**interface** *interface-name*]

Displaying

Description	Command
Displays LLDP information on the local device, which will be organized as TLVs and sent to neighbors.	**show lldp local-information** [**global** | **interface** interface-name]
Displays the LLDP civic address or emergency telephone number of a local device.	**show lldp location** { **civic-location | elin-location** } { **identifier** *id* **| interface** *interface-name* **| static** }
Displays LLDP information on a neighbor.	**show lldp neighbors [interface** *interface-name*] [**detail**]
Displays the LLDP network policy configuration of the local device.	**show lldp network-policy** { **profile** [*profile-num*] | **interface** *interface-name* }
Displays LLDP statistics.	**show lldp statistics** [**global | interface** *interface-name*]
Displays LLDP status information.	**show lldp status** [**interface** *interface-name*]
Displays the configuration of TLVs to be advertised by a port.	**show lldp tlv-config** [**interface** *interface-name*]

Debugging

System resources are occupied when debugging information is output. Therefore, disable debugging immediately after use.

Description	Command
Debugs LLDP error processing.	**debug lldp error**
Debugs LLDP event processing.	**debug lldp event**
Debugs LLDP hot backup processing.	**debug lldp ha**
Debugs the LLDP packet reception.	**debug lldp packet**
Debugs the LLDP state machine.	**debug lldp stm**

12 CONFIGURING QINQ

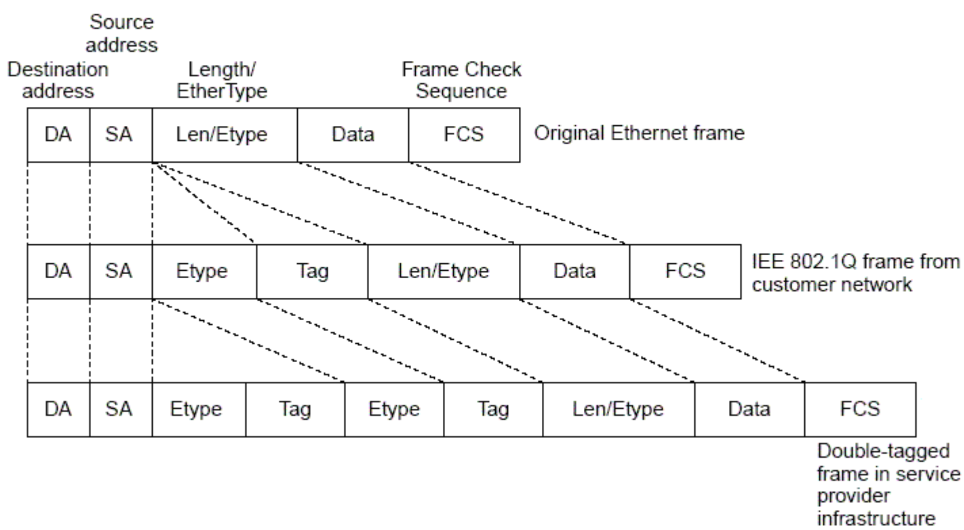
12.1 Overview

QinQ is used to insert a public virtual local area network (VLAN) tag into a packet with a private VLAN tag to allow the double-tagged packet to be transmitted over a service provider (SP) network.

Users on a metropolitan area network (MAN) must be separated by VLANs. IEEE 802.1Q supports only 4,094 VLANs, far from enough. Through the double-tag encapsulation provided by QinQ, a packet is transmitted over the SP network based on the unique outer VLAN tag assigned by the public network. In this way, private VLANs can be reused, which increases the number of available VLAN tags and provides a simple Layer-2 virtual private network (VPN) feature.

Figure 13-1 shows the double-tag insertion process. The entrance to an SP network is called a dot1q-tunnel port, or Tunnel port for short. All frames entering provider edges (PEs) are considered untagged. All tags, whether untagged frames or frames with customer VLAN tags, are encapsulated with the tags of the SP network. The VLAN ID of the SP network is the ID of the default VLAN for the Tunnel port.

Figure 13-1 Outer Tag Encapsulation



Protocols and Standards

IEEE 802.1ad

12.2 Applications

Application	Description
Implementing Layer-2 VPN Through Port-Based Basic QinQ	Data is transmitted from Customer A and Customer B to the peer end without conflict on the SP network even if the data comes from the same VLAN.
Implementing Layer-2 VPN and Service Flow Management Through C-TAG-Based Selective QinQ	Outer tags are inserted into frames flexibly based on different customer VLANs to achieve Layer-2 VPN, segregate service flows (e.g., broadband Internet access and IPTV), and implement various QoS policies. Customer tag (C-TAG)-based QinQ is more flexible than port-based QinQ.
Implementing Layer-2 VPN and Service Flow Management Through ACL-Based Selective QinQ	The different service flows, such as broadband Internet access and IPTV, are segregated based on access control lists (ACLs). Different QoS policies are applied to service flows through selective QinQ.
Implementing VLAN Aggregation for Different Services Through VLAN Mapping	Different service flows (PC, IPTV, and VoIP) are transmitted through different VLANs. The VLANs are aggregated on a campus network so that only one VLAN is used to carry the same service flows, thus saving VLAN resources.
Implementing QinQ-Based Layer-2 Transparent Transmission	Customer Network A and Customer Network B in different areas can perform unified Multiple Spanning Tree Protocol (MSTP) calculation or VLAN deployment across the SP network without affecting the SP network.

12.2.1 Implementing Layer-2 VPN Through Port-Based Basic QinQ

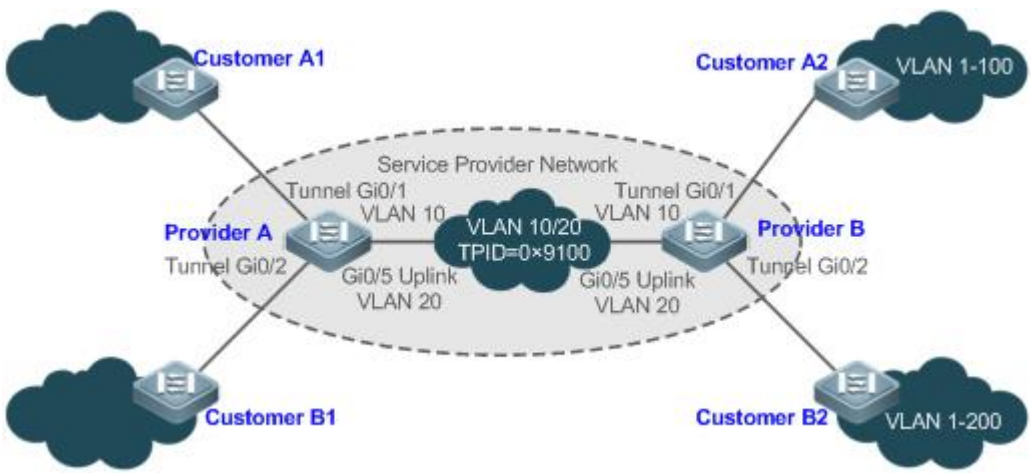
Scenario

An SP provides the VPN service to Customer A and Customer B.

- Customer A and Customer B belong to different VLANs on the SP network and achieve communication through respective SP VLANs.
- The VLANs of Customer A and Customer B are transparent to the SP network. The VLANs can be reused without conflicts.

- The Tunnel port encapsulates a native VLAN tag in each packet. Packets are transmitted through the native VLAN over the SP network without impact on the VLANs of Customer A and Customer B, thus implementing simple Layer-2 VPN.

Figure 13-2



Remarks	**Customer A1 and Customer A2 are the customer edges (CEs) for Customer A network. Customer B1 and Customer B2 are the CEs for Customer B network.** **Provider A and Provider B are the PEs on the SP network. Customer A and Customer B access the SP network through Provider A and Provider B.** **The VLAN of Customer A ranges from 1 to100.** **The VLAN of Customer B ranges from 1 to 200.**

Deployment

- Enable basic QinQ on PEs to implement Layer-2 VPN.
- The tag protocol identifiers (TPIDs) used by many switches (including QTECH switches) are set to 0x8100, but the switches of some vendors do not use 0x8100. In the latter case, you need to change the TPID value on the Uplink ports of PEs to the values of the TPIDs used by third-party switches.
- Configure priority replication and priority mapping for class of service (CoS) on the Tunnel ports of PEs, and configure different QoS policies for different service flows (for details, see *Configuring QoS*).

12.2.2 Implementing Layer-2 VPN and Service Flow Management Through C-TAG-Based Selective QinQ

Scenario

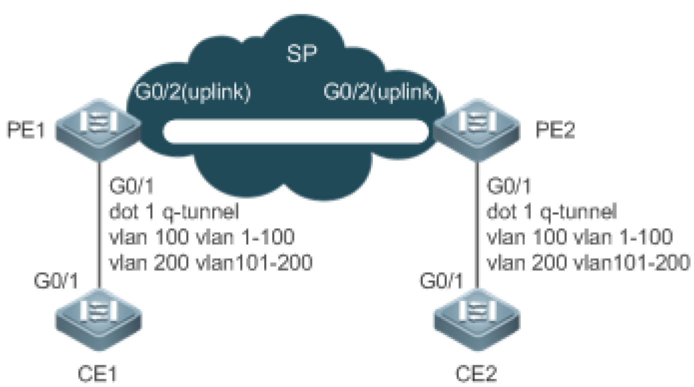
Basic QinQ encapsulates an outer tag of the native VLAN in a packet. That is, the encapsulation of outer tags depends on the native VLAN on Tunnel ports. Selective QinQ encapsulates an outer tag in a packet based on its inner tag to implement VPN transparent transmission and apply QoS policies flexibly.

- Broadband Internet access and IPTV are important services carried by MANs. The SPs manage different service flows through different VLANs and provides QoS policies for the VLANs or CoS. You can enable C-TAG-based QinQ on PEs to encapsulate outer VLAN tags in the service flows to achieve transparent transmission based on the QoS policies of the SP network.
- Important services and regular services are separated within different VLAN ranges. The customer can transmit service flows transparently over an SP network through C-TAG-based selective QinQ and ensure preferential transmission of important service flows by using the QoS policies of the SP network.

In Figure 13-3, the CEs are aggregated by the floor switches inside residential buildings. The broadband Internet access and IPTV services are segregated by VLANs with different QoS policies.

- The service flows of broadband Internet access and IPTV are transmitted transparently by different VLANs over the SP network.
- The SP network provides QoS policies based on VLANs or CoS. On the PEs, you can encapsulate an outer tag in the service flow based on its inner VLAN tag or set a CoS to ensure preferential transmission of service flows over the SP network.
- The CoS values of service packets can be changed through priority mapping or replication so that the QoS policies of the SP network are applied flexibly.

Figure 13-3



Remarks	**CE 1 and CE 2 access the SP network through PE1 and PE2.** **On CE 1 and CE 2, the broadband Internet access flows are transmitted through VLAN 1–100, and IPTV flows are transmitted through VLAN 101–200.** **PE 1 and PE 2 are configured with Tunnel ports and VLAN mappings to segregate service flows.**

Deployment

- Configure C-TAG-based selective QinQ on the ports (G0/1) of PE 1 and PE 2 connected to CE 1 and CE 2 respectively to realize the segregation and transparent transmission of service flows.

- If the SP network provides QoS policies based on VLANs or CoS, you can encapsulate an outer tag in the service flow based on its inner tag or set a CoS through priority replication or mapping on PE 1 and PE 2 to ensure preferential transmission of service flows over the SP network.

12.2.3 Implementing Layer-2 VPN and Service Flow Management Through ACL-Based Selective QinQ

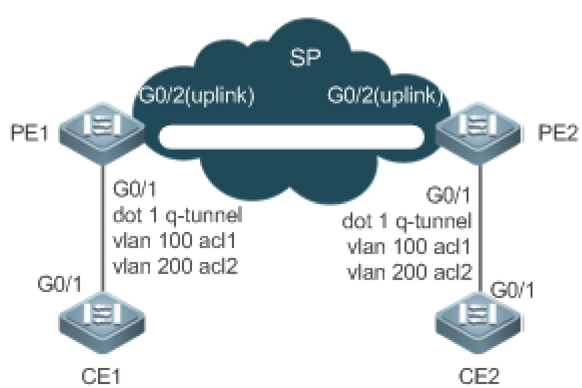
Scenario

The service flows from the customer network may be classified by MAC address, IP address, or protocol type, instead of by VLAN. The customer network may contain many low-end access devices unable to segregate service flows by VLAN IDs. In the preceding two situations, the packets from the customer network cannot be encapsulated with outer tags based on their inner tags to realize transparent transmission and implement QoS policies. Service flows may be classified by MAC address, IP address, or protocol type through ACLs. Selective QinQ uses ACLs to segregate service flows and add or modify outer tags in order to implement Layer-2 VPN and QoS policies based on different service flows.

In Figure 13-4, different VLANs are configured on PE 1 and PE 2 to transmit different service flows classified through ACLs. If the SP network provides QoS policies based on different services, certain services can be transmitted preferentially.

- Outer VLAN tags are encapsulated based on different service flows. The service flows of a customer network can be transmitted transparently, and its branch offices can access each other.
- The SP network provides QoS policies based on the VLAN tags or CoS values to ensure preferential transmission of certain service flows.

Figure 13-4



Remarks	**CE 1 and CE 2 access the SP network through PE1 and PE2.** **PE 1 and PE 2 classify flows based on ACLs: ACL 1 matches the Point-to-Point Protocol over Ethernet (PPPoE) flows, and ACL 2 matches the IPTV flows.**

	PE 1 and PE 2 are configured with Tunnel ports, as well as outer tag encapsulation policies applicable to service flows recognized by different ACLs.

Deployment

- Configure ACLs on PE 1 and PE 2 to segregate service flows.
- Configure ACL-based selective QinQ on the ports (G0/1) of PE 1 and PE 2 connected to CE 1 and CE 2 respectively to realize the segregation and transparent transmission of service flows.
- If the SP network provides QoS policies based on VLANs or CoS, you can encapsulate an outer tag in the service flow based on its inner tag or set a CoS through priority replication or mapping on PE 1 and PE 2 to ensure preferential transmission of service flows over the SP network.

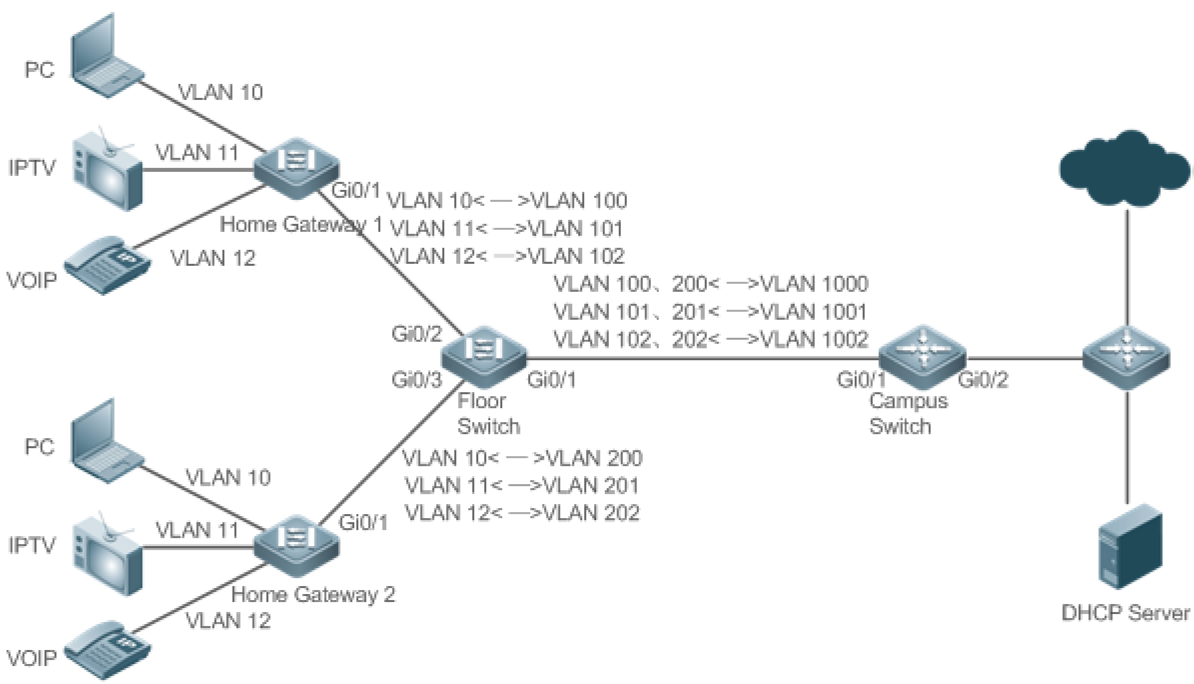
12.2.4 Implementing VLAN Aggregation for Different Services Through VLAN Mapping

Scenario

The different service flows of different users are segregated on a campus network.

- The different service flows are transmitted through different VLANs on the home gateway.
- The same service flows from different users are segregated on the floor switch.
- The same service flows from different users are sent by a campus switch through one single VLAN.

Figure 13-5



Remarks	**PC, IPTV, and VoIP are different user services.** **Switch A and Switch B are the gateway devices of different users.**

	Switch C is a floor switch. **Switch D is a campus switch.**

Deployment

- On the home gateway devices, configure VLANs for different services to segregate service flows. For example, configure VLAN 10 for the PC service, VLAN 11 for IPTV, and VLAN 12 for VoIP.
- On the ports of the floor switch (Switch D) connected to the home gateway devices, configure VLAN mapping to segregate the service flows of different users.
- On the campus switch, configure VLAN mapping to segregate the service flows.
- Through the preceding deployment, the different service flows of different users are segregated.

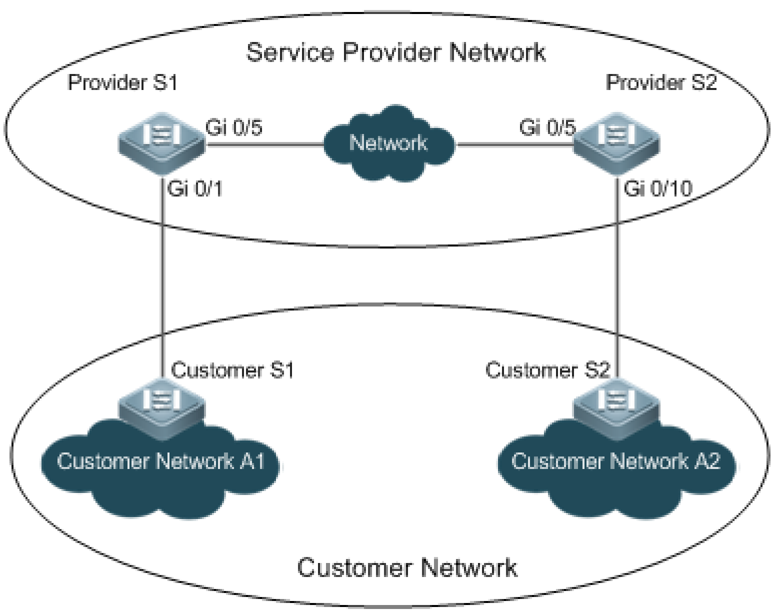
12.2.5 Implementing QinQ-Based Layer-2 Transparent Transmission

Scenario

The Layer-2 transparent transmission between customer networks has no impact on the SP network.

- The Layer-2 packets on customer networks are transparent to SP networks and can be transmitted between the customer networks without impact on the SP networks.

Figure 13-6



Remarks	**Customer S1 and Customer S2 access the SP network through Provider S1 and Provider S2.** **Provider S1 and Provider S2 are enabled with Layer-2 transparent transmission globally, and the Gi 0/1 and Gi 0/10 ports are enabled with Layer-2 transparent transmission.**

Deployment

- On the ports of the PEs (Provider S1 and Provider S2) connected to Customer S1 and Customer S2 respectively, configure Layer-2 transparent transmission between Customer Network A1 and Customer Network A2 without impact on the SP network.
- Configure STP transparent transmission based on user requirements to realize transparent transmission of bridge protocol data unit (BPDU) packets between Customer Network A1 and Customer Network A2 and to perform unified MSTP calculation across the SP network.
- Configure GARP VLAN Registration Protocol (GVRP) transparent transmission based on user requirements to realize transparent transmission of GVRP packets between Customer Network A1 and Customer Network A2 and dynamic VLAN configuration on the customer networks across the SP network.

12.3 Features

Basic Concepts

- Basic QinQ

Configure basic QinQ on a Tunnel port and configure a native VLAN for the port. Packets entering the port are encapsulated with outer tags containing the native VLAN ID. Basic QinQ does not segregate service flows and cannot encapsulate packets flexibly based on VLANs.

- Selective QinQ

Selective QinQ is classified into two types: selective QinQ based on C-TAGs and selective QinQ based on ACLs.

In C-TAG-based selective QinQ, outer tags are encapsulated in packets based on the inner tags to segregate service flows and realize transparent transmission.

In ACL-based selective QinQ, outer tags are encapsulated in packets based on the ACLs to segregate service flows.

- TPID

An Ethernet frame tag consists of four fields: TPID, User Priority, Canonical Format Indicator (CFI), and VLAN ID.

By default, the TPID is 0x8100 according to IEEE802.1Q. On the switches of some vendors, the TPID is set to 0x9100 or other values. The TPID configuration aims to ensure that the TPIDs of packets to be forwarded are compatible with the TPIDs supported by third-party switches.

Priority Mapping and Priority Replication

The default value of User Priority in Ethernet frame tags is 0, indicating regular flows. You can set this field to ensure preferential transmission of certain packets. You can specify User Priority by setting the value of CoS in a QoS policy.

Priority replication: If the SP network provides a QoS policy corresponding to a specified CoS in the inner tag, you can replicate the CoS of the inner tag to the outer tag to enable transparent transmission based on the QoS policy provided by the SP network.

Priority mapping: If the SP network provides various QoS policies corresponding to specified CoS values for different service flows, you can map the CoS value of the inner tag to the CoS value of the outer tag to ensure preferential transmission of service flows based on the QoS policies provided by the SP network.

Layer-2 Transparent Transmission

STP and GVRP packets may affect the topology of the SP network. If you want to unify the topology of two customer networks separated by the SP network without affecting the SP network topology, transmit the STP and GVRP packets from the customer networks over the SP network transparently.

Overview

Feature	Description
Basic QinQ	Configures the Tunnel port and specifies whether packets sent from the port are tagged.
Selective QinQ	Encapsulates different outer tags in data flows based on ACLs.
VLAN Mapping	Replaces the inner tags of packets with outer tags, and then restores the outer tags to inner tags based on the same rules.
TPID Configuration	By default, the TPID is 0x8100 according to IEEE802.1Q. On the switches of some vendors, the TPIDs of outer tags are set to 0x9100 or other values. The TPID configuration aims to ensure that the TPIDs of packets to be forwarded are compatible with the TPIDs supported by third-party switches.
MAC Address Replication	In ACL-based selective QinQ, the VLAN IDs for the MAC addresses that switches learn belong to the native VLAN. If VLAN conversion is implemented based on ACLs, upon receiving packets from the peer end, the local end may fail to query MAC addresses, causing a flood. To address this problem, MAC address replication is provided to replicate the MAC addresses of the native VLAN to the VLAN where the outer tag is located.
Layer-2 Transparent Transmission	Transmits Layer-2 packets between customer networks without impact on SP networks.

Priority Replication	If the SP network provides a QoS policy corresponding to a specified CoS value in the inner tag, you can replicate the CoS of the inner tag to the outer tag to enable transparent transmission based on the QoS policy provided by the SP network.
Priority Mapping	If the SP network provides various QoS policies corresponding to specified CoS values for different service flows, you can map the CoS value of the inner tag to the CoS value of the outer tag to ensure preferential transmission of service flows based on the QoS policies provided by the SP network.

12.3.1 Basic QinQ

Basic QinQ can be used to implement simple Layer-2 VPN, but it lacks flexibility in encapsulating outer tags.

Working Principle

After a Tunnel port receives a packet, the switch adds the outer tag containing the default VLAN ID to the packet. If the received packet already carries a VLAN tag, it is encapsulated as a double-tagged packet. If it does not have a VLAN tag, it is added with the VLAN tag containing the default VLAN ID.

12.3.2 Selective QinQ

Selective QinQ adds different outer tags to data flows flexibly.

Working Principle

Selective QinQ can be used to encapsulate different outer tags based on inner tags, MAC addresses, protocol numbers, source addresses, destination addresses, priorities, or the port numbers of applications. In this way, packets of different users, services, and priorities are encapsulated with different outer VLAN tags.

You can configure the following selective QinQ policies:

- Add an outer VLAN tag based on the inner VLAN tag.
- Modify an outer VLAN tag based on the outer VLAN tag.
- Modify an outer VLAN tag based on the inner VLAN tag.
- Modify an outer VLAN tag based on the inner and outer VLAN tags.
- Add an outer VLAN tag based on the ACL.
- Modify an outer VLAN tag based on the ACL.
- Modify an inner VLAN tag based on the ACL.

12.3.3 VLAN Mapping

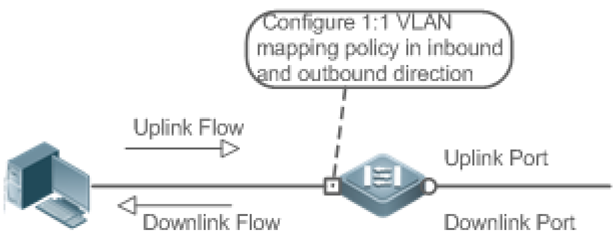
Working Principle

The inner tag of a packet is replaced by an outer tag to allow the packet to be transmitted based on the public network topology. When the packet is transmitted to the customer network, the outer tag is restored to the original inner tag based on the same rule. VLAN mapping supports the following mapping rule:

- 1:1 VLAN mapping: Changes a VLAN ID to the specified VLAN ID.
- 1:1 VLAN Mapping Mode 1

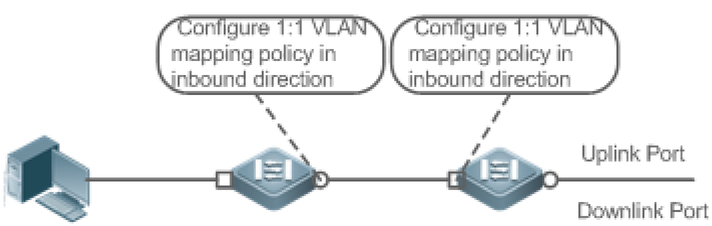
1:1 VLAN mapping is mainly applied on floor switches to use different VLANs to carry the same services from different users, as shown in Figure 13-7.

Figure 13-7



- Configure the Downlink port with a VLAN mapping policy in the inbound direction to map the inner tag of the uplink flow to an outer tag.
- Configure the Uplink port with a VLAN mapping policy in the outbound direction to map the outer tag of the downlink flow to the original inner tag.
- 1:1 VLAN Mapping Mode 2

Figure 13-8



- Configure the Downlink port with a VLAN mapping policy in the inbound direction to map the inner tag of the uplink flow to an outer tag.
- For downstream data flows, Configure the Uplink port with a VLAN mapping policy in the inbound direction to the outer tag of the downlink flow to the original inner tag.

12.3.4 TPID Configuration

Working Principle

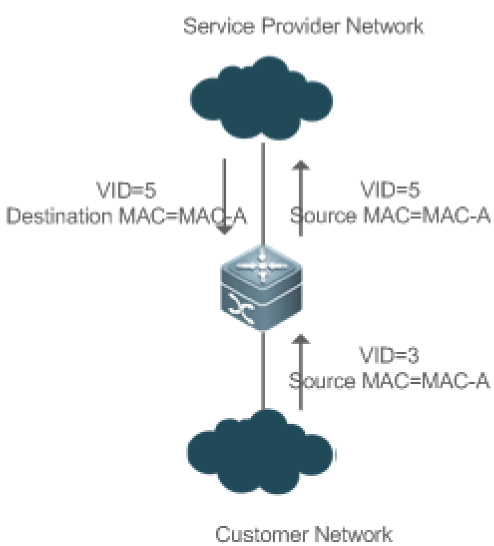
An Ethernet frame tag consists of four fields, namely, TPID, User Priority, CFI, and VLAN ID. By default, the TPID is 0x8100 according to IEEE802.1Q. On the switches of some vendors, the TPIDs of outer tags are set to 0x9100 or other values. The TPID configuration feature allows you to configure TPIDs on ports, which will replace the TPIDs of the outer VLAN tags in packets with the configured TPIDs to realize TPID compatibility.

12.3.5 MAC Address Replication

Working Principle

In ACL-based selective QinQ, the MAC address learned by a switch belongs to the native VLAN. The Tunnel port tags the packet with the specified outer VLAN ID based on the selective QinQ policy. Upon receiving a reply packet containing the same outer VLAN tag, the Tunnel port fails to find the MAC address in the outer VLAN as it is in the native VLAN, causing a flood.

Figure 13-9



As in Figure 13-9, the customer network is connected to the Tunnel port of the switch. Configured with native VLAN 4, the Tunnel port tags the packet whose source MAC address is A with outer VLAN 5. Upon receiving a packet with inner tag VLAN 3 and source MAC address A, the switch tags the packet with outer VLAN 5. Because the port is configured with native VLAN 4, MAC address A is learned by VLAN 4. Upon receiving the reply packet, the switch looks for MAC address A on VLAN 5 because the outer tag of the packet contains VLAN ID 5. However, MAC address A is not learned by VLAN 5, causing floods.

You can configure the Tunnel port to replicate the MAC address of the native VLAN to the outer VLAN to avoid continuous flooding of the packets from the SP network. You can also configure the Tunnel port to replicate the MAC address of the outer VLAN for the outer tag to the native VLAN to avoid continuous flooding of the packets from the customer network.

12.3.6 Layer-2 Transparent Transmission

Working Principle

The Layer-2 transparent transmission feature is designed to realize the transmission of Layer-2 packets between customer networks without impact on SP networks. When a Layer-2 packet from a customer network enters a PE, the PE changes the destination MAC address of the packet to a private address before forwarding the packet. The peer PE changes the destination MAC address to a public address to send the packet to the customer network at the other end, realizing transparent transmission on the SP network.

12.3.7 Priority Replication

Working Principle

If the SP network provides a QoS policy corresponding to a specified User Priority (CoS) in the inner tag, you can replicate the CoS of the inner tag to the outer tag to enable transparent transmission based on the QoS policy provided by the SP network.

12.3.8 Priority Mapping

Working Principle

If the SP network provides various QoS policies corresponding to specified CoS values for different service flows, you can map the CoS value of the inner tag to the CoS value of the outer tag to ensure preferential transmission of service flows based on the QoS policies provided by the SP network.

12.4 Limitations

- The QSW-6900 series products support four global Tag Protocol Identifier (TPID) values. One of the TPID values must be 0x8100, and the other three are random.

12.5 Configuration

Configuration	Description and Command	
Configuring QinQ	Mandatory.	
	switchport mode dot1q-tunnel	Configures a Tunnel port.

	switchport dot1q-tunnel allowed vlan { [**add**] **tagged** *vlist* | [**add**] **untagged** *vlist* | **remove** *vlist* }	Adds the VLANs to the Tunnel port in tagged or untagged mode.
	switchport dot1q-tunnel native vlan *VID*	Configures the default VLAN for the Tunnel port.
Configuring C-TAG-Based Selective QinQ	(Mandatory) It is used to configure C-TAG-based selective QinQ based on basic QinQ. Selective QinQ prevails over basic QinQ.	
	dot1q outer-vid *VID* **register inner-vid** *v_list*	Configures the policy to add the VLAN IDs of outer tags based on inner tags.
Configuring ACL-Based Selective QinQ	(Mandatory) It is used to configure ACL-based selective QinQ based on basic QinQ. Selective QinQ prevails over basic QinQ.	
	traffic-redirect access-group *acl* **nested-vlan** *VID* **in**	Configures the policy to add the VLAN IDs of outer tags based on ACLs.
Configuring VLAN Mapping	(Mandatory) It is used to enable VLAN mapping.	
	vlan-mapping-in vlan *cvlan* **remark** *svlan*	Configures 1:1 VLAN mapping in the inbound direction. This feature changes the inner VLAN ID of the packet entering a port to a specified outer VLAN ID.
	vlan-mapping-out vlan *svlan* **remark** *cvlan*	Configures 1:1 VLAN mapping in the outbound direction. This feature changes the outer VLAN ID of the packet exiting a port to a specified inner VLAN ID.
	vlan-mapping-in vlan *cvlan-list* **remark** *svlan*	Configures N:1 VLAN mapping in the inbound direction. This feature changes the inner VLAN ID of the packet entering a port to a specified outer VLAN ID.
	(Optional) It is used to realize TPID compatibility.	

Configuring TPIDs	**frame-tag tpid** *tpid*	Configures the TPID of a frame tag. If you want to set it to 0x9100, configure the **frame-tag tpid 9100** command. By default, the TPID is in hexadecimal format. You need to configure this feature on an egress port.
Configuring MAC Address Replication	(Optional) It is used to configure MAC address replication to prevent floods.	
	mac-address-mapping *x* **source-vlan** *src-vlan-list* **destination-vlan** *dst-vlan-id*	Replicates the dynamic MAC address of the source VLAN to the destination VLAN.
Configuring an Inner/Outer VLAN Tag Modification Policy	(Optional) It is used to adjust the outer and inner VLAN tags of the packets transmitted over SP networks based on network topologies.	
	dot1q relay-vid *VID* **translate local-vid** *v_list*	Configures the policy to change the VLAN IDs of outer tags based on the outer tags.
	dot1q relay-vid *VID* **translate inner-vid** *v_list*	Configures the policy to change the VLAN IDs of outer tags based on inner tags.
	dot1q new-outer-vlan *VID* **translate old-outer-vlan vid inner-vlan** *v_list*	Configures the policy to change the VLAN IDs of outer tags based on outer and inner tags.
	traffic-redirect access-group *acl* **outer-vlan** *VID* **in**	Configures the policy to change the VLAN IDs of outer tags based on an ACL.
	traffic-redirect access-group *acl* **inner-vlan** *VID* **out**	Configures the policy to change the VLAN IDs of inner tags based on an ACL.
Configuring Priority Mapping and Priority Replication	(Optional) It is used to apply the QoS policy provided by the SP network by priority replication.	
	inner-priority-trust enable	Replicates the value of the User Priority field in the inner tag (C-

		TAG) to the User Priority field of the outer tag (S-TAG).
	(Optional) It is used to apply the QoS policy provided by the SP network by priority mapping.	
	dot1q-Tunnel cos *inner-cos-value* **remark-cos** *outer-cos-value*	Sets the value of the User Priority field in the outer tag (S-TAG) based on the User Priority field of the inner tag (C-TAG).
Configuring Layer-2 Transparent Transmission	(Optional) It is used to transmit MSTP and GVRP packets transparently based on the customer network topology without affecting the SP network topology.	
	l2protocol-tunnel stp	Enables STP transparent transmission in global configuration mode.
	l2protocol-tunnel stp enable	Enables STP transparent transmission in interface configuration mode.
	l2protocol-tunnel gvrp	Enables GVRP transparent transmission in global configuration mode.
	l2protocol-tunnel gvrp enable	Enables GVRP transparent transmission in interface configuration mode.
	l2protocol-tunnel{**STP**|**GVRP**}**tunnel-dmac** *mac-address*	Configures a transparent transmission address.

- Pay attention to the following limitations when you configure QinQ:
- Do not configure a routed port as the Tunnel port.
- Do not enable 802.1X on the Tunnel port.
- Do not enable the port security function on the Tunnel port.
- When the Tunnel port is configured as the source port of the remote switched port analyzer (RSPAN), the packets whose outer tags contain VLAN IDs consistent with the RSPAN VLAN IDs are monitored.
- If you want to match the ACL applied to the Tunnel port with the VLAN IDs of inner tags, use the **inner** keyword.

- Configure the egress port of the customer network connected to the SP network as an Uplink port. If you configure the TPID of the outer tag on a QinQ-enabled port, set the TPID of the outer tag on the Uplink port to the same value.
- By default, the maximum transmission unit (MTU) on a port is 1,500 bytes. After added with an outer VLAN tag, a packet is four bytes longer. It is recommended to increase the port MTU on the SP networks to at least 1,504 bytes.
- After a switch port is enabled with QinQ, you must enable SVGL sharing before enabling IGMP snooping. Otherwise, IGMP snooping will not work on the QinQ-enabled port.
- If a packet matches two or more ACL-based selective QinQ policies without priority, only one policy is executed. It is recommended to specify the priority.

12.5.1 Configuring QinQ

Configuration Effect

- Implement Layer-2 VPN based on a port-based QinQ policy.

Notes

- It is not recommended to configure the native VLAN of the Trunk port on the PE as its default VLAN, because the Trunk port strips off the tags containing the native VLAN IDs when sending packets.

Configuration Steps

Configuring the Tunnel port

- (Mandatory) Configure the Tunnel port in interface configuration mode.
- Run the **switchport mode dot1q-tunnel** command in interface configuration mode to configure the Tunnel port.

Command	**switchport mode dot1q-tunnel**
Parameter Description	N/A
Defaults	By default, no Tunnel port is configured.
Command Mode	Interface configuration mode
Usage Guide	N/A

Configuring the Native VLAN

- Mandatory.
- Configure the native VLAN for the Tunnel port.
- After you configure the native VLAN, add it to the VLAN list of the Tunnel port in untagged mode.
- Run the **switchport dot1q-tunnel native vlan** *VID* command in interface configuration mode to configure the default VLAN for the Tunnel port.
- If the native VLAN is added to the VLAN list in untagged mode, the outgoing packets on the Tunnel port are not tagged. If the native VLAN is added to the VLAN list in tagged mode, the outgoing packets on the Tunnel port are tagged with the native VLAN ID. To ensure the uplink and downlink transmission, add the native VLAN to the VLAN list in untagged mode.

Command	**switchport dot1q-tunnel native vlan** ***VID***
Parameter Description	*VID*: Indicates the ID of the native VLAN. The value ranges from 1 to 4,094. The default value is 1.
Defaults	By default, the native VLAN is VLAN 1.
Command Mode	Interface configuration mode
Usage Guide	Use this command to configure the VLAN of the SP network.

Adding the VLANs on the Tunnel port

- Mandatory.
- After you configure the native VLAN, add it to the VLAN list of the Tunnel port in untagged mode.
- If port-based QinQ is enabled, you do not need to add the VLANs of the customer network to the VLAN list of the Tunnel port.
- If selective QinQ is enabled, add the VLANs of the customer network to the VLAN list of the Tunnel port in tagged or untagged mode based on requirements.
- Run the **switchport dot1q-tunnel allowed vlan** { [**add**] **tagged** *vlist* | [**add**] **untagged** *vlist* | **remove** *vlist* } command in interface configuration mode to add VLANs to the VLAN list of the Tunnel port. Upon receiving packets from corresponding VLANs, the Tunnel port adds or removes tags based on the settings.

Command	**switchport dot1q-tunnel allowed vlan { [add] tagged *vlist* | [add] untagged *vlist* | remove *vlist* }**
Parameter Description	*v_list*: Indicates the list of the VLANs on the Tunnel port.

Defaults	By default, VLAN 1 is added to the VLAN list of the Tunnel port in untagged mode. Other VLANs are not added.
Command Mode	Interface configuration mode
Usage Guide	Use this command to add or remove VLANs on the Tunnel port and specify whether the outgoing packets are tagged or untagged. If basic QinQ is enabled, add the native VLAN to the VLAN list of the Tunnel port in untagged mode.

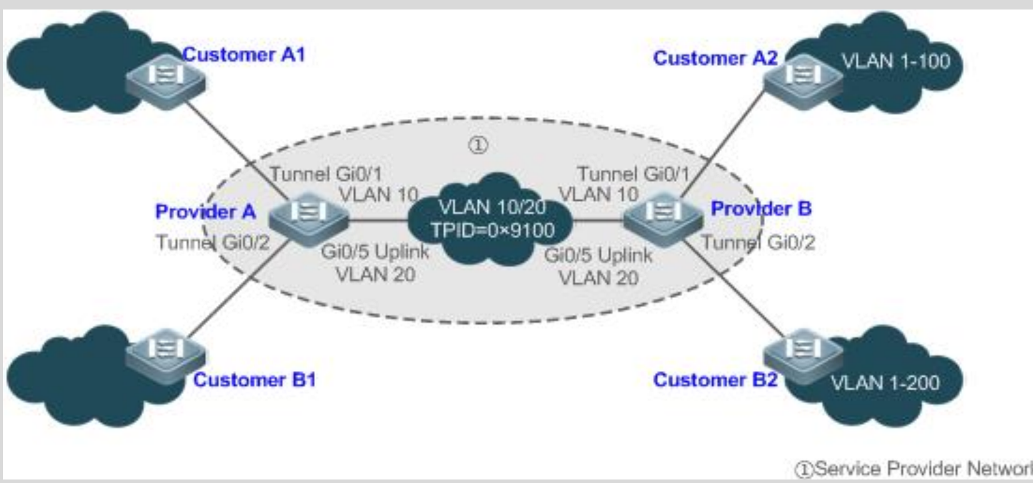
Verification

Check the Tunnel port configuration.

- Check whether the Tunnel port is configured properly on a switch.

Configuration Example

Configuring Basic QinQ to Implement Layer-2 VPN

Scenario **Figure 13-10**	
Configuration Steps	▪ Configure Tunnel ports on the PEs and connect the CEs to the Tunnel ports. ▪ Configure the native VLANs for the Tunnel ports and add the native VLANs to the VLAN lists of the Tunnel ports respectively in untagged mode. ▪ Configure VLANs on the customer networks based on requirements. QinQ-enabled switches encapsulate outer tags in packets for transmission over the SP network. Therefore, you do not need to configure customer VLANs on the PEs. The TPID is 0x8100 by default according to IEEE802.1Q. On some third-party switches, the TPID is set to a different value. If such switches are deployed, set the

	TPIDs on the ports connected to the third-party switches to realize TPID compatibility. If the PEs are connected through Trunk ports or Hybrid ports, do not configure the native VLANs for the Trunk ports or Hybrid ports as the default VLANs for the Tunnel ports. The Trunk ports or Hybrid ports strip off the VLAN tags containing the Native VLAN IDs when sending packets.
Provider A	Step 1: Create VLAN 10 and VLAN 20 on the SP network to segregate the data of Customer A and Customer B. ProviderA#configure terminal Enter configuration commands, one per line. End with CNTL/Z. ProviderA(config)#vlan 10 ProviderA(config-vlan)#exit ProviderA(config)#vlan 20 ProviderA(config-vlan)#exit Step 2: Enable basic QinQ on the port connected to the network of Customer A to use VLAN 10 for tunneling. ProviderA(config)#interface gigabitEthernet 0/1 ProviderA(config-if-GigabitEthernet 0/1)#switchport mode dot1q-tunnel ProviderA(config-if-GigabitEthernet 0/1)#switchport dot1q-tunnel native vlan 10 ProviderA(config-if-GigabitEthernet 0/1)#switchport dot1q-tunnel allowed vlan add untagged 10 Step 3: Enable basic QinQ on the port connected to the network of Customer B to use VLAN 20 for tunneling. ProviderA(config)#interface gigabitEthernet 0/2 ProviderA(config-if-GigabitEthernet 0/2)#switchport mode dot1q-tunnel ProviderA(config-if-GigabitEthernet 0/2)#switchport dot1q-tunnel native vlan 20 ProviderA(config-if-GigabitEthernet 0/2)#switchport dot1q-tunnel allowed vlan add untagged 20 Step 4: Configure an Uplink port. ProviderA(config)# interface gigabitEthernet 0/5 ProviderA(config-if-GigabitEthernet 0/5)#switchport mode uplink Step 5: Change the TPID of the outgoing packets on the Uplink port to a value (for example, 0x9100) recognizable by third-party switches.

	ProviderA(config-if-GigabitEthernet 0/5)#frame-tag tpid 9100 Step 6: Configure Provider B by performing the same steps.
Verification	Customer A1 sends a packet containing VLAN ID 100 destined to Customer A2. The packet through Provider A is tagged with the outer tag specified by the Tunnel port. The packet that reaches Customer A2 carries the original VLAN ID 100. Check whether the Tunnel port is configured correctly. Check whether the TPID is configured correctly.
Provider A	ProviderA#show running-config interface GigabitEthernet 0/1 switchport mode dot1q-tunnel switchport dot1q-tunnel allowed vlan add untagged 10 switchport dot1q-tunnel native vlan 10 spanning-tree bpdufilter enable ! interface GigabitEthernet 0/2 switchport mode dot1q-tunnel switchport dot1q-tunnel allowed vlan add untagged 20 switchport dot1q-tunnel native vlan 20 spanning-tree bpdufilter enable ! interface GigabitEthernet 0/5 switchport mode uplink frame-tag tpid 0x9100 ProviderA#show interfaces dot1q-tunnel ========Interface Gi0/1======== Native vlan: 10 Allowed vlan list:1,10, Tagged vlan list: ========Interface Gi0/2======== Native vlan: 20

	Allowed vlan list:1,20, Tagged vlan list: ProviderA#show frame-tag tpid Ports Tpid ------- ------------- Gi0/5 0x9100
Provider B	Check Provider B by performing the same steps.

Common Errors

- The native VLAN is not added to the VLAN list of the Tunnel port in untagged mode.
- No TPID is configured on the port connected to the third-party switch on which TPID is not 0x8100. As a result, packets cannot be recognized by the third-party switch.

12.5.2 Configuring C-TAG-Based Selective QinQ

Configuration Effect

- Encapsulate outer VLAN tags (S-TAGs) in packets based on inner tags to ensure preferential transmission and management of Layer-2 VPN and service flows.

Notes

- C-TAG-based selective QinQ must be configured based on basic QinQ.
- Some selective QinQ policies are not supported on some products due to limitations of chips.
- If you need to continue to adopt the VLAN tag priority specified by the customer network, you can configure priority replication to configure an outer tag the same as the inner tag.
- If the SP network requires the transmission of packets based on the priority of the outer tag, you need to configure priority replication to set the CoS of the outer tag to the specified value.

Configuration Steps

- Configuring a Policy to Add the VLAN IDs of Outer Tags Based on Inner Tags
- Mandatory.
- Upon receiving a packet, the Tunnel port adds the VLAN ID of the outer tag based on the VLAN ID of the inner tag. This function enables the Tunnel port to add the VLAN ID of the inner tag to the outer tag and adds the port to the VLAN in untagged mode. In this way, the outgoing packets carry the original inner tags.

The ACL-based QinQ policy prevails over the port-based and C-TAG-based QinQ policy.

When a member port is added to or removed from an aggregate port (AP), the QinQ policy configured on the AP port will be deleted. You need to configure the policy again. It is recommended that you configure a selective QinQ policy on the AP port after you configure its member ports.

⚠ You must configure the Tunnel port and the port connected to the public network to permit packets with specified VLAN IDs (including the native VLAN ID) in the outer tag to pass through.

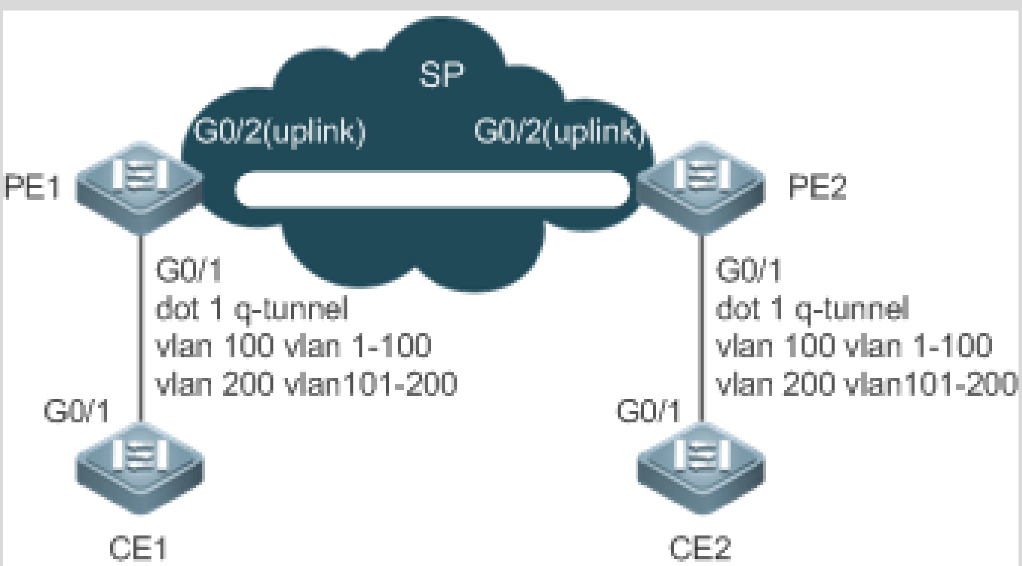
Command	**dot1q outer-vid *VID* register inner-vid *v_list***
Parameter Description	N/A
Defaults	By default, no policy is configured.
Command Mode	Interface configuration mode
Usage Guide	N/A

Verification

- Check whether the users within the VLANs can communicate with each other.
- Check whether Layer-2 VPN is implemented.
- Check whether different service traffic is transmitted based on the selective QinQ policy, such as outer tag insertion, priority replication, and priority mapping.

Configuration Example

Implementing Layer-2 VPN and Service Flow Management Through C-TAG-Based Selective QinQ

Scenario **Figure 13-11**	

Configuration Steps	Configure the ports on PE 1 and PE 2 connected to CE 1 and CE 2 as Tunnel ports. Configure a selective QinQ policy to add an outer tag to the packet based on its inner tag. If the SP network provides a VLAN-based QoS policy, the policy enables the port to add the outer tags with the corresponding VLAN ID to the specified service flow packets. If the SP network provides a CoS-based QoS policy and the CoS value is the same as that of the inner tag, you can configure priority mapping to replicate the CoS value of the inner tag to the outer VLAN tag so that the packet is transmitted based on the priority policy for the inner tag. If the SP network provides a CoS-based QoS policy, you can configure priority mapping to set the CoS value of the outer VLAN tag to a specified value so that the packet is transmitted based on the priority policy.
PE1	Step 1: Configure the VLAN for transparent transmission. PE1#configure terminal Enter configuration commands, one per line. End with CNTL/Z. PE1(config)#vlan 100 PE1(config-vlan)#exit PE1(config)#vlan 200 PE1(config-vlan)#exit Step 2: On the Downlink port of the access switch, configure a selective QinQ policy to add outer tags based on inner tags. Configure port Gi 0/1 as a Tunnel port. PE1(config)#interface gigabitEthernet 0/1 PE1(config-if)# switchport mode dot1q-tunnel Add VLAN 101 and VLAN 201 of the SP to the VLAN list of the Tunnel port and configure the Tunnel port to strip off the outer tag from incoming packets. PE1(config-if)# switchport dot1q-tunnel allowed vlan add untagged 100,200 Configure the Tunnel port to add outer tag VLAN 100 to incoming data frames containing inner tag VLAN 1–100. PE1(config-if)# dot1q outer-vid 100 register inner-vid 1-100 Configure the Tunnel port to add outer tag VLAN 200 to incoming data frames containing inner tag VLAN 101-200. PE1(config-if)# dot1q outer-vid 200 register inner-vid 101-200 Step 3: Configure the port that accesses the SP network as an Uplink port. PE1(config)# interface gigabitEthernet 0/2

	PE1(config-if-GigabitEthernet 0/2)#switchport mode uplink
PE2	▪ Perform the same configuration on PE 2.
Verification	Verify the configuration by checking whether: ▪ The Downlink port is configured as a Tunnel port. ▪ The VLAN specified by the outer tag is added to the VLAN list of the Tunnel port. ▪ The selective QinQ policy on the Tunnel port is correct. ▪ The Uplink port is configured correctly. Step 1: Check whether the VLAN mapping policy is correct.
PE1	PE1#show running-config interface gigabitEthernet 0/1 interface GigabitEthernet 0/1 switchport mode dot1q-tunnel switchport dot1q-tunnel allowed vlan add untagged 100,200 dot1q outer-vid 100 register inner-vid 1-200 dot1q outer-vid 200 register inner-vid 101-200 spanning-tree bpdufilter enable ! Step 2: Check the C-TAG-based selective QinQ policy. Check whether the mapping relationship between the inner and outer VLAN tags is correct. PE1#show registration-table Ports Type Outer-VID Inner-VID-list ------ ---------- ---------- -------------- *Gi0/1 Add-outer 100 1-200* *Gi0/1 Add-outer 200 101-200*

12.5.3 Configuring ACL-Based Selective QinQ

Configuration Effect

- Encapsulate outer VLAN tags (S-TAGs) in packets based on the ACL-based flow classification to allow the SP network to manage different services.

Notes

- ACL-based selective QinQ must be configured based on basic QinQ.

- Some selective QinQ policies are not supported on some products due to limitations of chips.
- If you need to continue to adopt the VLAN tag priority specified by the customer network, you can configure priority replication to configure an outer tag the same as the inner tag.
- If the SP network requires the transmission of packets based on the priority of the outer tag, you need to configure priority replication to set the CoS of the outer tag to the specified value.

The ACL-based QinQ policy prevails over the port-based and C-TAG-based QinQ policy.

When an ACL is deleted, the related policy will be automatically deleted.

Upon receiving a packet with two or more tags, the Tunnel port cannot add an outer tag to the packet based on the ACL-based selective QinQ policy.

If a packet matches two or more ACL-based selective QinQ policies without priority, only one policy is executed. It is recommended to specify the priority.

You must configure the Tunnel port and the port connected to the public network to permit packets with specified VLAN IDs (including the native VLAN ID) in the outer tag to pass through.

Configuration Steps

Configuring a Policy to Add the VLAN IDs of Outer Tags Based on ACLs

- Mandatory.
- The Tunnel port adds outer tags with different VLAN IDs to incoming packets based on the packet content.

Command	**traffic-redirect access-group *acl* nested-vlan *VID* in**
Parameter Description	N/A
Defaults	By default, no policy is added.
Command Mode	Interface configuration mode
Usage Guide	N/A

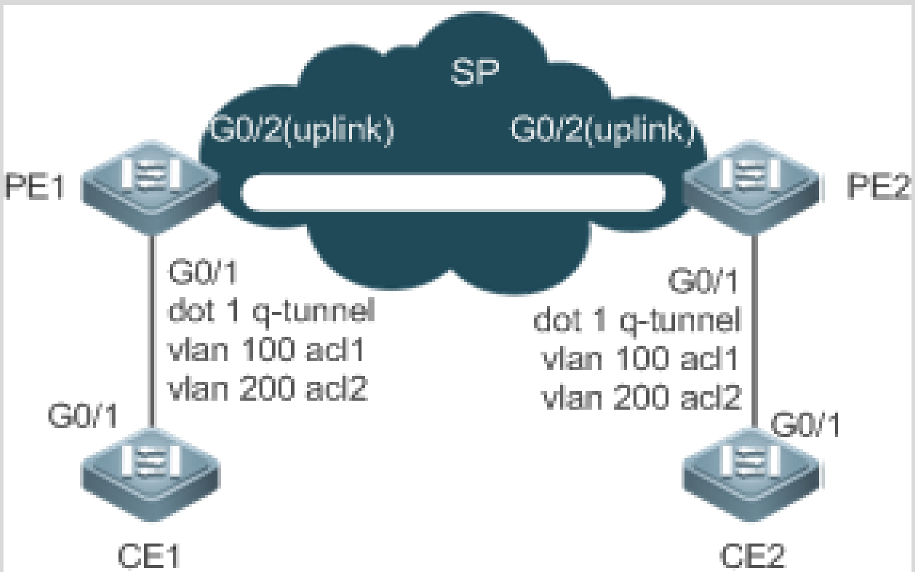
Verification

- Check whether the users of the same service in different branch offices can communicate with each other and whether specified service data is transmitted preferentially through virtual private LAN segment (VPLS) configuration.
- Check whether Layer-2 VPN is implemented.

- Check whether different service traffic is transmitted based on the selective QinQ policy, such as outer tag insertion, priority replication, and priority mapping.

Configuration Example

- Implementing Layer-2 VPN and Service Flow Management Through ACL-Based Selective QinQ

<table>
<tr><td>Scenario
Figure 13-12</td><td>
</td></tr>
<tr><td>Configuration Steps</td><td>

Configure the ports on PE 1 and PE 2 connected to CE 1 and CE 2 as Tunnel ports.
Configure ACL policies on PE 1 and PE 2 to segregate the service flows from the customer network.
On the Tunnel ports, configure a selective QinQ policy to add an outer tag to the packet based on ACL policies.
If the SP network provides a VLAN-based QoS policy, the policy enables the port to add the corresponding VLAN ID to the outer tags of the specified service flow.
If the SP network provides a CoS-based QoS policy, you can configure priority mapping to set the CoS value of the outer VLAN tag to a specified value so that the packet is transmitted based on the priority policy.
</td></tr>
<tr><td>PE 1</td><td>Step 1: Create an ACL to permit flows of PPPoE type (0x8863/0x8864) and IPoE type (0x0800) to pass through.
PE1#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
PE1(config)# expert access-list extended acl1
PE1(config-exp-nacl)# permit 0x8863 any any
PE1(config-exp-nacl)# permit 0x8864 any any</td></tr>
</table>

	PE1(config-exp-nacl)#exit PE1(config)# expert access-list extended acl2 PE1(config-exp-nacl)#permit 0x0800 any any Step 2: Configure VLAN 100 and VLAN 200 on the SP network to segregate data. PE#configure terminal Enter configuration commands, one per line. End with CNTL/Z. PE1(config)#vlan 100 PE1(config-vlan)#exit PE1(config)#vlan 200 PE1(config-vlan)#exit Step 3: On the Downlink port of the access switch, configure a selective QinQ policy to add outer VLAN tags based on ACLs. Configure port Gi 0/1 as a Tunnel port. PE1(config)#interface gigabitEthernet 0/1 PE1(config-if)# switchport mode dot1q-tunnel Add VLAN 100 and VLAN 200 of the SP to the VLAN list of the Tunnel port and configure the Tunnel port to strip off the outer tag from incoming packets. PE1(config-if)#switchport dot1q-tunnel allowed vlan add untagged 100,200 Configure the Tunnel port to add outer tag VLAN 100 to the incoming data frames which match ACL 1. PE1(config-if)# traffic-redirect access-group acl1 nested-vlan 100 in Configure the Tunnel port to add outer tag VLAN 200 to the incoming data frames which match ACL 2. PE1(config-if)# traffic-redirect access-group acl1 nested-vlan 200 in Step 4: Configure the port connected to the SP network as an Uplink port. PE1(config)# interface gigabitEthernet 0/2 PE1(config-if-GigabitEthernet 0/2)#switchport mode uplink
Verification	▪ Check whether the users of the same service in different branch offices can communicate with each other and whether specified service data is transmitted preferentially. ▪ Check whether Layer-2 VPN is implemented. ▪ Check whether the ACL is correct. ▪ Check whether the service priority is correct.

	▪ Check whether the Downlink port is configured as a Tunnel port, whether the outer tag VLAN is added to the VLAN list of the Tunnel port, and whether the mapping policy on the Tunnel port is correct.

PE1	Step 1: Check whether the Tunnel port is configured correctly.
	`QTECH#show running-config interface gigabitEthernet 0/1`
	`interface GigabitEthernet 0/1`
	` switchport mode dot1q-tunnel`
	` switchport dot1q-tunnel allowed vlan add untagged 100,200`
	` traffic-redirect access-group acl1 nested-vlan 100 in`
	` traffic-redirect access-group acl2 nested-vlan 200 in`
	` spanning-tree bpdufilter enable`
	`!`
	Step 2: Check the ACL-based selective QinQ policy. Check whether the mapping relationship between the inner and outer VLAN tags is correct.
	`PE1#show traffic-redirect`
	`Ports    Type        VID    Match-filter`
	`-------  ----------  -----  ------------`
	`Gi0/1    Nested-vid  101    acl1`
	`Gi0/1    Nested-vid  201    acl2`

Common Errors

- No ACL policy is configured.
- ACL policies are used to segregate flows based on MAC addresses. Packet floods will occur if MAC address replication is not configured.

12.5.4 Configuring VLAN Mapping

Configuration Effect

- Replace the inner tags of the packets with the outer tags to allow the packets to be transmitted based on the VLAN planning on the SP network.

Notes

- VLAN mapping can be configured only on Access ports, Trunk ports, Hybrid ports, or Uplink ports.

⚠ After VLAN mapping is configured, the VLAN IDs of the packets sent to the CPU are changed to the specified VLAN ID.

⚠ It is not recommended to configure VLAN mapping and selective QinQ on one port.

Configuration Steps

- Configuring 1:1 VLAN Mapping
- Mandatory if the 1:1 mode is used. Configure a 1:1 VLAN mapping rule.
- Run the **vlan-mapping-in vlan** *CVID* **remark** *SVID* command or the **vlan-mapping-out vlan** *SVID* **remark CVID** command on a Trunk port or an Uplink port to enable 1:1 VLAN mapping.

Command	**vlan-mapping-in vlan** ***src-vlan-list*** **remark** ***dest-vlan***
Parameter Description	*src-vlan-list*: Indicates the customer VLAN. *dest-vlan:* Indicates the service VLAN, which is the VLAN where the SP network is located.
Defaults	
Command Mode	Interface configuration mode
Usage Guide	Use this command to configure 1:1 VLAN mapping in the inbound direction.

Command	**vlan-mapping-out vlan** ***src-vlan*** **remark** ***dest-vlan***
Parameter Description	*src-vlan*: Indicates the service VLAN, which is the VLAN where the SP network is located. *dest-vlan*: Indicates the customer VLAN.
Defaults	
Command Mode	Interface configuration mode
Usage Guide	Use this command to configure 1:1 VLAN mapping in the outbound direction.

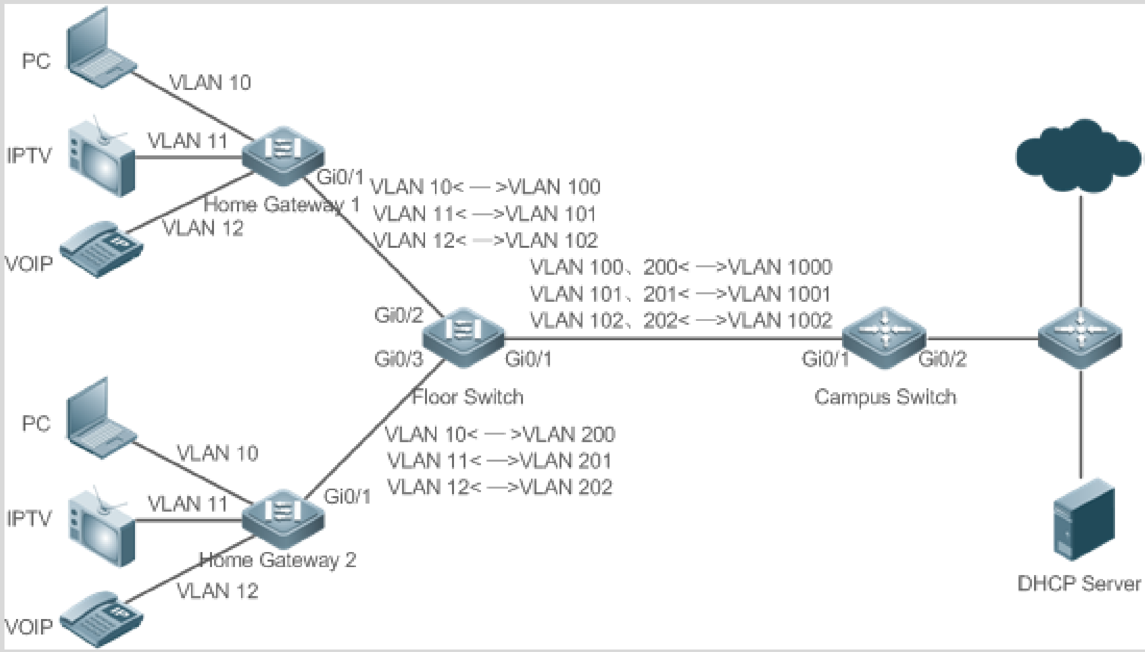
Verification

Check whether VLAN mapping is configured correctly.

- Run the **show interfaces**[*intf-id*] **vlan-mapping** command to display the VLAN mapping.

Configuration Example

▪ Implementing VLAN Aggregation for Different Services Through VLAN Mapping

<table>
<tr><td>Scenario
Figure 13-13</td><td>
</td></tr>
<tr><td>Configuration Steps</td><td>▪ Configure Home Gateway 1 and Home Gateway 2.
Step 1: On the home gateways, configure the original VLANs for different services.
QTECH#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
QTECH(config)#vlan range 10-12
QTECH(config-vlan-range)#exit
Step 2: Configure the attributes of the ports connected to PC, IPTV, and VoIP. Assume that the connected ports are Gi 0/2, Gi 0/3, and Gi 0/4 respectively.
QTECH(config)#interface gigabitEthernet 0/2
QTECH(config-if-GigabitEthernet 0/2)#switchport access vlan 10
QTECH(config-if-GigabitEthernet 0/2)#exit
QTECH(config)#interface gigabitEthernet 0/3
QTECH(config-if-GigabitEthernet 0/3)#switchport access vlan 11
QTECH(config-if-GigabitEthernet 0/3)#exit
QTECH(config)#interface gigabitEthernet 0/4
QTECH(config-if-GigabitEthernet 0/4)#switchport access vlan 12
QTECH(config-if-GigabitEthernet 0/4)#exit
Step 3: Configure an Uplink port.
QTECH(config)# interface gigabitEthernet 0/1</td></tr>
</table>

	QTECH(config-if-GigabitEthernet 0/1)#switchport mode uplink ▪ Configure a floor switch with 1:1 VLAN mapping policies. Step 1: On the home gateways, configure the original VLANs and mapped VLANs for different services. QTECH#configure terminal Enter configuration commands, one per line. End with CNTL/Z. QTECH(config)#vlan range 10-12 QTECH(config-vlan-range)#exit QTECH(config)#vlan range 100-102 QTECH(config-vlan-range)#exit QTECH(config)#vlan range 200-202 QTECH(config-vlan-range)#exit Step 2: On the Downlink port of Home Gateway 1, configure 1:1 VLAN mapping policies in the inbound and outbound directions. QTECH(config)#interface gigabitEthernet 0/2 QTECH(config-if-GigabitEthernet 0/2)#switchport mode uplink QTECH(config-if-GigabitEthernet 0/2)#vlan-mapping-in vlan 10 remark 100 QTECH(config-if-GigabitEthernet 0/2)#vlan-mapping-in vlan 11 remark 101 QTECH(config-if-GigabitEthernet 0/2)#vlan-mapping-in vlan 12 remark 102 QTECH(config-if-GigabitEthernet 0/2)#vlan-mapping-out vlan 100 remark 10 QTECH(config-if-GigabitEthernet 0/2)#vlan-mapping-out vlan 101 remark 11 QTECH(config-if-GigabitEthernet 0/2)#vlan-mapping-out vlan 102 remark 12 Step 3: On the Downlink port of Home Gateway 2, configure 1:1 VLAN mapping policies in the inbound and outbound directions. QTECH(config)#interface gigabitEthernet 0/3 QTECH(config-if-GigabitEthernet 0/3)#switchport mode uplink QTECH(config-if-GigabitEthernet 0/3)#vlan-mapping-in vlan 10 remark 200 QTECH(config-if-GigabitEthernet 0/3)#vlan-mapping-in vlan 11 remark 201 QTECH(config-if-GigabitEthernet 0/3)#vlan-mapping-in vlan 12 remark 202 QTECH(config-if-GigabitEthernet 0/3)#vlan-mapping-out vlan 200 remark 10 QTECH(config-if-GigabitEthernet 0/3)#vlan-mapping-out vlan 201 remark 11 QTECH(config-if-GigabitEthernet 0/3)#vlan-mapping-out vlan 202 remark 12 Step 4: Configure an Uplink port.

	QTECH(config)# interface gigabitEthernet 0/1 QTECH(config-if-GigabitEthernet 0/1)#switchport mode uplink
Verification	Display the 1:1 VLAN mapping policies configured on the floor switch. QTECH#show interfaces vlan-mapping Ports type Status Service-Vlan Customer-Vlan-list ----------- ----- --------- ----------- ---------------- Gi0/2 in active 100 10 Gi0/2 in active 101 11 Gi0/2 in active 102 12 Gi0/2 out active 100 10 Gi0/2 out active 101 11 Gi0/2 out active 102 12 Gi0/3 in active 200 10 Gi0/3 in active 201 11 Gi0/3 in active 202 12 Gi0/3 out active 200 10 Gi0/3 out active 201 11 Gi0/3 out active 202 12

12.5.5 Configuring TPIDs

Configuration Effect

Configure the TPIDs in the tags on SP network devices to realize TPID compatibility.

Notes

If a PE connected to a third-party switch on which the TPID is not 0x8100, you need to configure the TPID on the port of the PE connected to the third-party switch.

⚠ Do not set the TPIDs to any of the following values: 0x0806 (ARP), 0x0200 (PUP), 0x8035 (RARP), 0x0800 (IP), 0x86DD (IPv6), 0x8863/0x8864 (PPPoE), 0x8847/0x8848 (MPLS), 0x8137 (IPX/SPX), 0x8000 (IS-IS), 0x8809 (LACP), 0x888E (802.1X), 0x88A7 (clusters), and 0x0789 (reserved by QTECH Networks).

Configuration Steps

- If a PE connected to a third-party switch on which the TPID is not 0x8100, you need to configure the TPID on the port of the PE connected to the third-party switch.
- TPIDs can be configured in interface configuration mode and global configuration mode. The following example adopts interface configuration mode.

Configure the **frame-tag tpid** *0x9100* command in interface configuration mode to change the TPID to 0x9100. For details about the TPID value, see section 1.4.5.

Command	**frame-tag tpid** ***tpid***
Parameter Description	*tpid:* Indicates the new value of the TPID.
Defaults	The default value of the TPID is 0x8100.
Command Mode	Interface configuration mode
Usage Guide	If a PE is connected to a third-party switch on which the TPID is not 0x8100, use this command to configure the TPID on the port connected to the third-party switch.

Verification

Check whether the TPID is configured.

Configuration Example

Configuring the TPID on a port

Configuration Steps	**Configure the TPID on a port.** **QTECH(config)# interface gigabitethernet *0/1*** **QTECH(config-if)# frame-tag tpid *9100***
Verification	Display the TPID on the port. QTECH# show frame-tag tpid interfaces gigabitethernet *0/1* Port tpid ------- ------------- Gi0/1 0x9100

12.5.6 Configuring MAC Address Replication

Configuration Effect

- Replicate the dynamic address learned on a port from one VLAN to another.
- Avoid packet floods when service flows are segregated through MAC-based ACLs.

Notes

- After MAC address replication is disabled, the system will delete all the learned MAC address entries from the destination VLAN.
- MAC address replication can be configured on a port only once. If you need to modify the configuration, delete the current configuration and configure it again.
- VLAN MAC address replication cannot be used together with VLAN sharing, and the MAC addresses cannot be replicated to dynamic VLANs.
- Up to eight destination VLANs can be configured on each port. MAC address replication takes effect even if the port does not belong to the specified destination VLAN.
- MAC address replication cannot be configured on the Host and Promiscuous ports, monitoring ports, and port security-/802.1X-enabled ports.
- Only dynamic addresses can be replicated. Address replication is disabled when the address table is full. If source addresses already exist before replication is enabled, corresponding MAC addresses will not be replicated.
- Replicated addresses have a higher priority than dynamic addresses but have a lower priority than other types of addresses.
- When a MAC address ages, the replicated MAC address will also age. When the MAC address is deleted, the replicated address will be deleted automatically.
- Hot backup is not supported. After primary/secondary switchover occurs, it is recommended that you disable MAC address replication and then enable it again.
- The MAC address entries obtained through MAC address replication cannot be deleted manually. If you need to delete these entries, disable MAC address replication.

Configuration Steps

- Configuring MAC Address Replication
- Perform this configuration to replicate MAC addresses from one VLAN to another to avoid packet floods.
- Run the **mac-address-mapping** <1-8> **source-vlan** *src-vlan-list* **destination-vlan** *dst-vlan-id* command on a Trunk port to enable MAC address replication. *src-vlan-list* and *dst-vlan-id* specify the VLAN range.

Command	**mac-address-mapping *x* source-vlan *src-vlan-list* destination-vlan *dst-vlan-id***
Parameter Description	*x:* Indicates the index number for MAC address replication. The value ranges from 1 to 8. *src-vlan-list*: Indicates the source VLAN list. *dst-vlan-id:* Indicates the destination VLAN list.
Defaults	By default, MAC address replication is disabled.
Command Mode	Interface configuration mode
Usage Guide	N/A

Verification

- Check whether the MAC address of the specified VLAN is replicated to another VLAN.

Configuration Example

Configuring MAC Address Replication

Configuration Steps	▪ **Configure MAC address replication.** **QTECH(config)# interface gigabitethernet 0/1** **QTECH(config-if)# switchport mode trunk** **QTECH(config-if)#mac-address-mapping 1 source-vlan 1-3 destination-vlan 5**
Verification	▪ Check whether the configuration takes effect on the port. ▪ Send a packet from the source VLAN and check whether the source MAC address of the packet is replicated to the destination VLAN. QTECH# show interfaces mac-address-mapping Ports destination-VID Source-VID-list --- Gi0/1 5 1-3

Common Errors

- See "Notes".

12.5.7 Configuring an Inner/Outer VLAN Tag Modification Policy

Configuration Effect

- Modify outer or inner tags based on the actual networking requirements.

Notes

- The ACL-based QinQ policy prevails over the port-based and C-TAG-based QinQ policy.
- When an ACL is deleted, the related policy will be automatically deleted.
- Tag modification policies take effect only on Access ports, Trunk ports, Hybrid ports, and Uplink ports.
- Tag modification policies are mainly used to modify inner and outer tags on the SP network.
- If a packet matches two or more ACL-based selective QinQ policies without priority, only one policy is executed. It is recommended to specify the priority.

Configuration Steps

- Configuring the Policy to Change the VLAN IDs of Outer Tags Based on Inner Tags
- Optional.
- Perform this configuration to change the VLAN IDs of outer tags based on the VLAN IDs of inner tags.
- You can change the VLAN IDs of the outer tags in the packets that enter Access ports, Trunk ports, Hybrid ports, and Uplink ports based on the VLAN IDs of the inner tags in these packets.

Command	**dot1q relay-vid *VID* translate inner-vid *v_list***
Parameter Description	*VID*: Indicates the modified VLAN ID of the outer tag. *v_list:* Indicates the VLAN ID of the inner tag.
Defaults	By default, no policy is configured.
Command Mode	Interface configuration mode
Usage Guide	N/A

- Configuring the Policy to Change the VLAN IDs of Outer Tags Based on the VLAN IDs of Outer and Inner Tags
- Optional.
- Perform this configuration to change the VLAN IDs of outer tags based on the VLAN IDs of inner and outer tags.
- You can change the VLAN IDs of the outer tags in the packets that enter Access ports, Trunk ports, Hybrid ports, and Uplink ports based on the VLAN IDs of the inner and outer tags in these packets.
-

Command	**dot1q new-outer-vlan *new-vid* translate old-outer-vlan *vid* inner-vlan *v_list***
Parameter Description	*new-vid*: Indicates the modified VLAN ID of the outer tag. vid: Indicates the original VLAN ID of the outer tag. *v_list:* Indicates the VLAN ID of the inner tag.
Defaults	By default, no policy is configured.
Command Mode	Interface configuration mode
Usage Guide	N/A

- Configuring the Policy to Change the VLAN IDs of Outer Tags Based on the Outer Tags
- Optional.
- Perform this configuration to change the VLAN IDs of outer tags based on these VLAN IDs.
- You can change the VLAN IDs of the outer tags in the packets that enter Access ports, Trunk ports, Hybrid ports, and Uplink ports based on these VLAN IDs.

Command	**dot1q relay-vid *VID* translate local-vid *v_list***
Parameter Description	*VID*: Indicates the modified VLAN ID of the outer tag. *v_list:* Indicates the original VLAN ID of the outer tag.
Defaults	By default, no policy is configured.
Command Mode	Interface configuration mode

Usage Guide	N/A

- Configuring a Policy to Change the VLAN IDs of Inner Tags Based on ACLs
- Optional.
- You can change the VLAN IDs of the inner tags in the packets that exit Access ports, Trunk ports, Hybrid ports, and Uplink ports based on the packet content.
- Before you configure such a policy, configure an ACL.

Command	**traffic-redirect access-group *acl* inner-vlan *vid* out**
Parameter Description	*acl*: Indicates the ACL. *vid:* Indicates the modified VLAN ID of the inner tag.
Defaults	By default, no policy is configured.
Command Mode	Interface configuration mode
Usage Guide	N/A

- Configuring a Policy to Change the VLAN IDs of Outer Tags Based on ACLs
- Optional.
- You can change the VLAN IDs of the outer tags in the packets that exit Access ports, Trunk ports, Hybrid ports, and Uplink ports based on the packet content.
- Before you configure such a policy, configure an ACL.

Command	**traffic-redirect access-group *acl* outer-vlan *vid* in**
Parameter Description	*acl*: Indicates the ACL. *vid:* Indicates the modified VLAN ID of the outer tag.
Defaults	By default, no policy is configured.
Command Mode	Interface configuration mode
Usage Guide	N/A

Verification

Check whether the configuration takes effect and whether the port modifies the tags in received packets based on the policy.

Configuration Example

- Configuring the Policy to Change the VLAN IDs of Outer Tags Based on the Outer Tags

Configuration Steps	▪ **Configure inner/outer tag modification policies on a port based on the actual networking requirements.** ▪ **The following example shows how to change VLAN IDs of outer tags based on outer tags and ACLs respectively. For details about other policies, see the description above.** **Configure a policy to change outer VLAN tags based on the outer VLAN tags.** QTECH(config)# interface gigabitEthernet 0/1 QTECH(config-if)# switchport mode trunk QTECH(config-if)# dot1q relay-vid 100 translate local-vid 10-20 **Configure a policy to change outer VLAN tags based on ACLs.** QTECH# configure terminal QTECH(config)# ip access-list standard 2 QTECH(config-acl-std)# permit host 1.1.1.1 QTECH(config-acl-std)# exit QTECH(config)# interface gigabitEthernet 0/2 QTECH(config-if)# switchport mode trunk QTECH(config-if)# traffic-redirect access-group 2 outer-vlan 3 in
Verification	▪ Check whether the configuration takes effect on the port. ▪ Check whether the port changes the VLAN IDs of the outer tags in received packets based on the configured policy.

12.5.8 Configuring Priority Mapping and Priority Replication

Configuration Effect

- If an SP network provides a QoS policy based on the User Priority field of the inner tag, configure priority replication to apply the QoS policy to the outer tag.
- If an SP network provides a QoS policy based on the User Priority field of the inner tag, configure priority mapping to apply the User Priority field provided by the SP network to the outer tag.

Notes

- Only a Tunnel port can be configured with priority replication, which has a higher priority than trusted QoS but lower than ACL-based QoS.
- Priority replication and priority mapping cannot be both enabled on one port.
- Only a Tunnel port can be configured with priority mapping, which prevails over QoS.
- The configuration of priority mapping does not take effect if no trust mode is configured (trust none) or the trust mode is not matched with priority mapping.

Configuration Steps

- Only a Tunnel port can be configured with priority mapping or priority replication.
- Configure priority replication to apply the inner tag-based QoS policy provided by the SP network.
- Configure priority mapping to configure the User Priority field of the outer VLAN tag based on the inner tag and apply the QoS policy flexibly.
- To enable priority replication, run the **inner-priority-trust enable** command on the Tunnel port.
- To enable priority mapping, run the **dot1q-Tunnel cos** *inner-cos-value* **remark-cos** *outer-cos-value* command on the Tunnel port.

inner-cos-value and outer-cos-value range from 0 to 7.

The following priority mapping is used when no priority mapping is configured:

```
inner pri    0    1    2    3    4    5    6    7
----------------------------------------------------------------------------
outer pri    0    1    2    3    4    5    6    7
```

Command	**inner-priority-trust enable**
Parameter Description	N/A
Defaults	By default, priority replication is disabled.
Command Mode	Interface configuration mode

Usage Guide	N/A

Command	**dot1q-Tunnel cos *inner-cos-value* remark-cos *outer-cos-value***
Parameter Description	*inner-cos-value*: Indicates the CoS value of the inner tag. *outer-cos-value*: Indicates the CoS value of the outer tag.
Defaults	By default, priority mapping is disabled.
Command Mode	Interface configuration mode
Usage Guide	N/A

Verification

- Run the **show inner-priority-trust interfaces** *type intf-id* command and the **show interfaces** *type intf-id* **remark** command to check whether priority mapping or priority replication takes effect.

Configuration Example

- Configuring Priority Mapping and Priority Replication

Configuration Steps	▪ **To maintain the packet priority, you need to replicate the priority of the inner tag in a packet to the outer tag on the Tunnel port.** ▪ **To flexibly control the packet priority on the Tunnel port, you can add outer tags of different priorities to packets based on the priorities of the inner tags in the packets.** **Configure priority replication.** **QTECH(config)# interface gigabitethernet *0/1*** **QTECH(config-if)#mls qos trust cos** **QTECH(config-if)# inner-priority-trust enable** **QTECH(config)# end** **Configure priority mapping.** **QTECH(config)# interface gigabitethernet 0/2**

	QTECH(config-if)#dot1q-Tunnel cos 3 remark-cos 5
Verification	▪ Display the priority configuration on the port. Check whether priority replication is enabled on the Tunnel port. QTECH# show inner-priority-trust interfaces gigabitethernet *0/1* Port inner-priority-trust ------ ------------------- Gi0/1 enable Display the priority mapping configured on the Tunnel port. QTECH# show interfaces gigabitethernet 0/1 remark Ports Type From value To value ------------ ----------- ----------- -------- Gi0/1 Cos-To-Cos 3 5

Common Errors

See "Notes".

12.5.9 Configuring Layer-2 Transparent Transmission

Configuration Effect

Transmit Layer-2 packets transparently without impact on the SP network and the customer network.

Notes

⚠ If STP is not enabled, you need to run the **bridge-frame forwarding protocol bpdu** command to enable STP transparent transmission.

⚠ Transparent transmission enabled on a port takes effect only after enabled globally. When transparent transmission takes effect on the port, the port does not participate in related protocol calculation. If the port receives a packet whose destination MAC address is the special broadcast address, it determines that a networking error occurs and discards the packet.

Configuration Steps

- Configuring STP Transparent Transmission
- Mandatory if you need to transparently transmit BPDU packets through STP.
- Enable STP transparent transmission in global configuration mode and interface configuration mode.

- Run the **l2protocol-tunnel stp** command in global configuration mode to enable STP transparent transmission.
- Run the **l2protocol-tunnel stp enable** command in interface configuration mode to enable STP transparent transmission.

Command	**l2protocol-tunnel stp**
Parameter Description	N/A
Defaults	By default, STP transparent transmission is disabled.
Command Mode	Global configuration mode
Usage Guide	N/A

Command	**l2protocol-tunnel stp enable**
Parameter Description	N/A
Defaults	By default, STP transparent transmission is disabled.
Command Mode	Interface configuration mode
Usage Guide	N/A

- Configuring GVRP Transparent Transmission
- Mandatory if you need to transparently transmit GVRP packets.
- Enable GVRP transparent transmission in global configuration mode and interface configuration mode.
- Run the **l2protocol-tunnel gvrp** command in global configuration mode to enable GVRP transparent transmission.
- Run the **l2protocol-tunnel gvrp enable** command in interface configuration mode to enable GVRP transparent transmission.

Command	l2protocol-tunnel gvrp
Parameter Description	N/A
Defaults	By default, GVRP transparent transmission is disabled.
Command Mode	Global configuration mode
Usage Guide	N/A

Command	l2protocol-tunnel gvrp enable
Parameter Description	N/A
Defaults	By default, GVRP transparent transmission is disabled.
Command Mode	Interface configuration mode
Usage Guide	N/A

- Configuring a Transparent Transmission Address
- Optional.
- Configure a transparent transmission address.

Command	**l2protocol-tunnel { stp | gvrp } tunnel-dmac** ***mac-address***
Parameter Description	*mac-address*: Indicates the address used to transparently transmit packets.
Defaults	By default, the first three bytes of the transparent transmission address is 01d0f8, and the last three bytes are 000005 and 000006 for STP and GVTP respectively.

Command Mode	Interface configuration mode
Usage Guide	The following addresses are available for STP: 01d0.f800.0005, 011a.a900.0005, 010f.e200.0003, 0100.0ccd.cdd0, 0100.0ccd.cdd1, and 0100.0ccd.cdd2. The following addresses are available for GVRP: 01d0.f800.0006 and 011a.a900.0006. When no transparent transmission address is configured, the default settings are used.

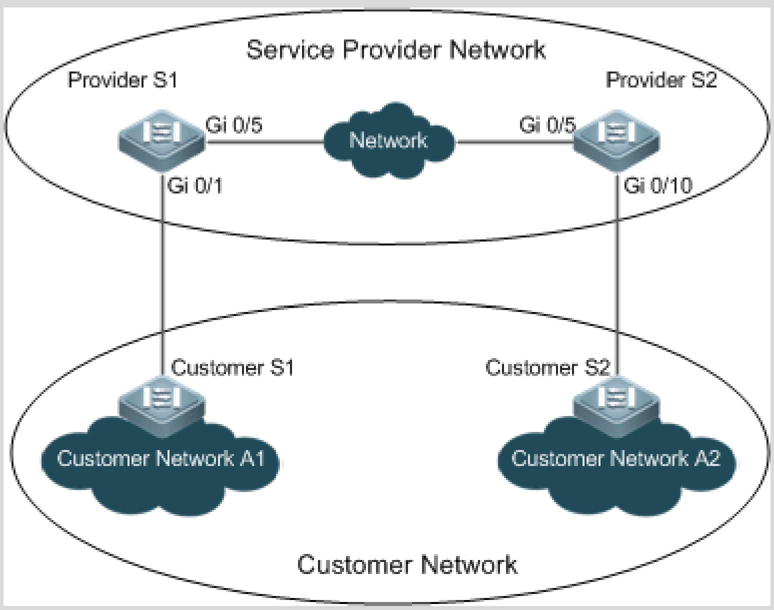
Verification

Run the **show l2protocol-tunnel stp** command and the **show l2protocol-tunnel gvrp** command to check whether the transparent transmission address is configured correctly.

Configuration Example

The following example shows how to configure STP transparent transmission.

- Configuring STP Transparent Transmission

Scenario **Figure 13-14**	
Configuration Steps	▪ On the PEs (Provider S1 and Provider S2), enable STP transparent transmission in global configuration mode and interface configuration mode. ▪ Before you enable STP transparent transmission, enable STP in global configuration mode to allow the switches to forward STP packets.
Provider S1	Step 1: Enable STP.

	bridge-frame forwarding protocol bpdu Step 2: Configure the VLAN for transparent transmission. ProviderS1#configure terminal Enter configuration commands, one per line. End with CNTL/Z. ProviderS1(config)#vlan 200 ProviderS1(config-vlan)#exit Step 3: Enable basic QinQ on the port connected to the customer network and use VLAN 200 for tunneling. ProviderS1(config)#interface gigabitEthernet 0/1 ProviderS1(config-if-GigabitEthernet 0/1)#switchport mode dot1q-tunnel ProviderS1(config-if-GigabitEthernet 0/1)#switchport dot1q-tunnel native vlan 200 Step 4: Enable STP transparent transmission on the port connected to the customer network. ProviderS1(config-if-GigabitEthernet 0/1)#l2protocol-tunnel stp enable ProviderS1(config-if-GigabitEthernet 0/1)#exit Step 5: Enable STP transparent transmission in global configuration mode. ProviderS1(config)#l2protocol-tunnel stp Step 4: Configure an Uplink port. ProviderS1(config)# interface gigabitEthernet 0/5 ProviderS1(config-if-GigabitEthernet 0/5)#switchport mode uplink
Provider S2	Configure Provider S2 by performing the same steps.
Verification	Step 1: Check whether STP transparent transmission is enabled in global configuration mode and interface configuration mode. ProviderS1#show l2protocol-tunnel stp L2protocol-tunnel: Stp Enable GigabitEthernet 0/1 l2protocol-tunnel stp enable Step 2: Verify the configuration by checking whether: ▪ The port type is dot1q-tunnel. ▪ The outer tag VLAN is consistent with the native VLAN and added to the VLAN list of the Tunnel port. ▪ The port that accesses the SP network is configured as an Uplink port. ProviderS1#show running-config

```
interface GigabitEthernet 0/1
 switchport mode dot1q-tunnel
 switchport dot1q-tunnel allowed vlan add untagged 200
 switchport dot1q-tunnel native vlan 200
 l2protocol-tunnel stp enable
 spanning-tree bpdufilter enable
!
interface GigabitEthernet 0/5
 switchport mode uplink
```

Common Errors

- STP is not enabled in global configuration mode.
- Transparent transmission is not enabled in global configuration mode and interface configuration mode.

12.6 Monitoring

Displaying

Description	Command
Displays whether the specified port is a Tunnel port.	**show dot1q-tunnel** [**interfaces** *intf-id*]
Displays the configuration of the Tunnel port.	**show interfaces dot1q-tunnel**
Displays the C-TAG-based selective QinQ policies on the Tunnel port.	**show registration-table** [**interfaces** *intf-id*]
Displays the C-TAG-based selective QinQ policies on the Access port, Trunk port or Hybrid port.	**show translation-table** [**interfaces** *intf-id*]
Displays VLAN mapping on ports.	**show interfaces** [*intf-id*] **vlan-mapping**

Displays the ACL-based selective QinQ policies.	**show traffic-redirect** [**interfaces** *intf-id*]
Displays the TPID configuration on ports.	**show frame-tag tpid interfaces** [*intf-id*]
Displays the configuration of priority replication.	**show inner-priority-trust**
Displays the configuration of priority mapping.	**show interface intf-name remark**
Displays the configuration of MAC address replication.	**show mac-address-mapping**
Displays the configuration of Layer-2 transparent transmission.	**show l2protocol-tunnel** { **gvrp** | **stp** }

Debugging

System resources are occupied when debugging information is output. Therefore, disable debugging immediately after use.

Description	**Command**
Debugs QinQ.	debug bridge qinq

13 CONFIGURING HASH SIMULATOR

13.1 Overview

HASH simulator is a program that simulates the HASH algorithm of the switch. HASH simulator supports Aggregate Port (AP) load-balancing modes.

- AP HASH simulator simulates the HASH algorithm to calculate the AP member port for packet forwarding based on the packet field, load-balancing mode and specified AP information. The calculation result conforms to the real forwarding port.

If you configure AP on a switch, use the AP simulator to calculate the AP member port for packet forwarding by specifying the packet field.

HASH simulator can be used to track and monitor the forwarding path of specified packets, facilitating user management and troubleshooting.

Protocols and Standards

IEEE 802.3ad

13.2 Applications

Application	Description
AP HASH Simulator	Combining multiple physical links into one logical link is an effective way to increase port bandwidth and improve reliability on a L3 switch. Packets are forwarded through a physical link according to load balance algorithm. AP simulator calculation enables users to check the member link, which serves as reference for troubleshooting and topology deployment.

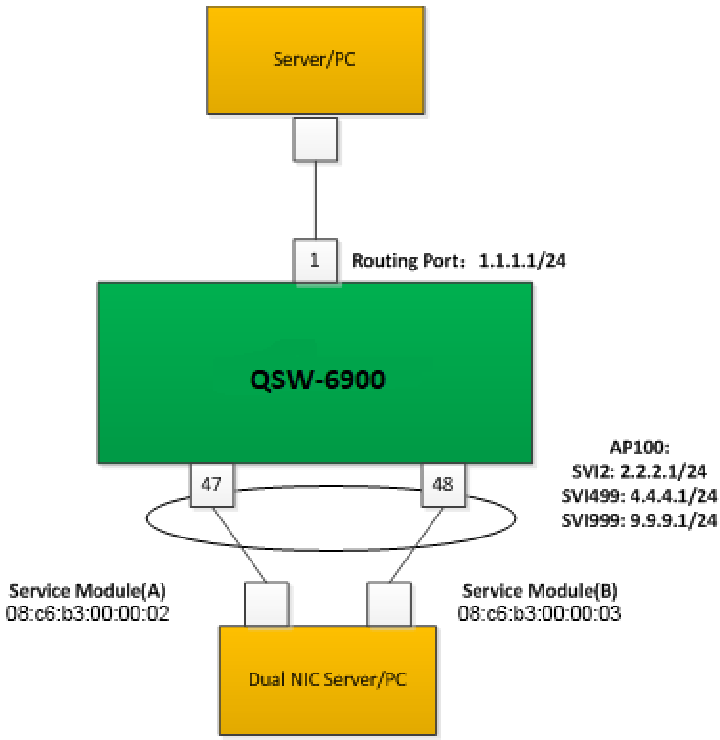
13.2.1 AP HASH Simulator

Scenario

With HASH simulator, you can calculate the AP load-balanced forwarding port.

- AP load balancing: The dual-NIC server is aggregated into one logical link to share service data flow.
- You should know which NIC on the server receives the packets with destination IP addresses of 2.2.2.1/24, 4.4.4.1/24, and 9.9.9.1/24 sent by the uplinked server.

Figure 13-1



Note	N/A

Deployment

- The ports connecting the dual NIC server and QSW-6900 are aggregated into an AP to share service data flow.
- Use VLAN 2, VLAN 499 and VLAN 999 to separate the network and undertake different types of service.
- You can identify the AP load-balanced forwarding port on QSW-6900 according to packet features.

The packet feature can be Source IP, Destination IP, Source L4 port, or Destination L4 port.

13.3 Features

Basic Concepts

AP

AP is a logical port that consists of several physical ports. AP can be divided into static AP and dynamic AP (LACP AP) based on protocol or into L2 AP and L3 AP based on port feature.

L2 AP

L2 AP is a logical port that consists of several L2 ports with the same L2 features.

L3 AP

L3 AP is a logical port that consists of several L3 ports with the same L3 features.

Load-balancing Mode

Packets are forwarded by an AP member port based on its load-balancing mode. The following AP load-balancing modes are available:

- Source MAC address/ destination MAC address (Src-mac/Dst-mac)
- Source MAC address + destination MAC address (Src-dst-mac)
- Source IP address/ destination IP address (Src-ip/Dst-ip)
- Source IP address + destination IP address (Src-dst-ip)
- Source IP address + destination IP address + source L4 port + destination L4 port (Src-dst-ip-l4port)
- Panel port of incoming packets
- Enhanced Mode (Enhanced)
- HASH Simulator

HASH simulator is a program that simulates the HASH algorithm of the switch.

Quintuple

The quintuple refers to the source IP address, destination IP address, protocol, source L4 port and destination L4 port.

Overview

Overview	Description
AP HASH Simulator	Calculates the AP member port for packet forwarding according to the packet field, AP load balance mode and specified AP information.

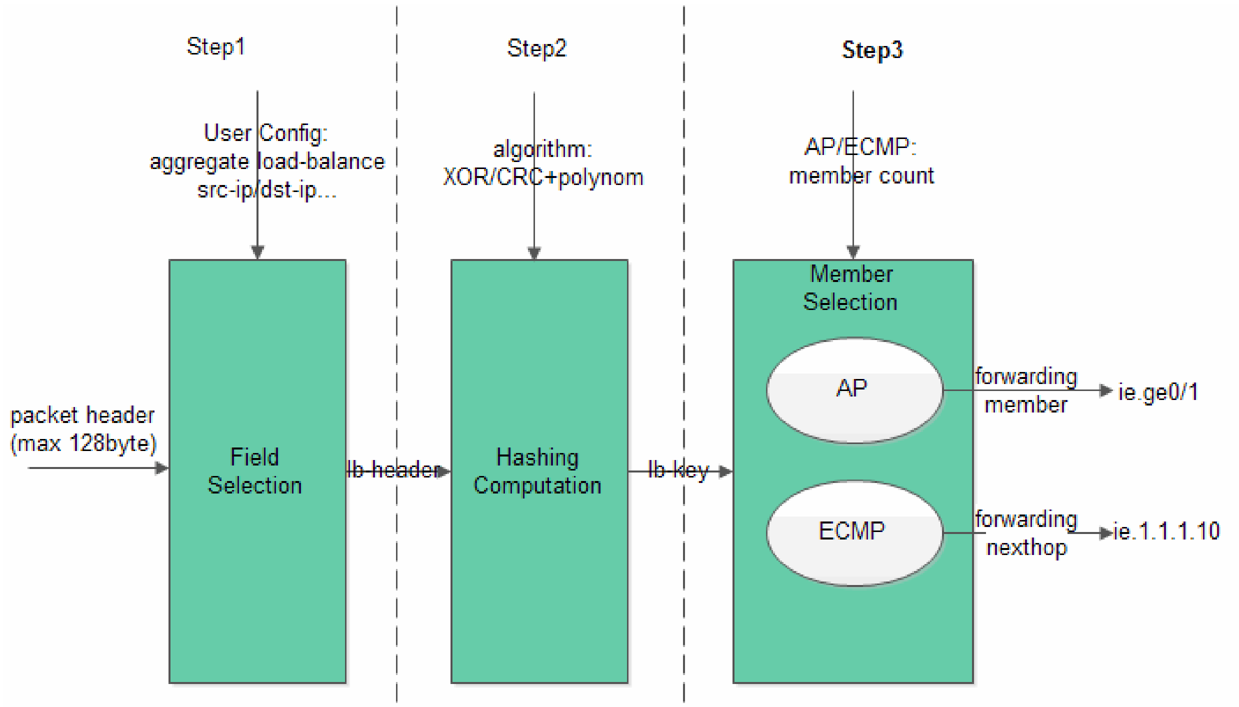
13.3.1 AP HASH Simulator

AP HASH simulator is used to calculate the AP member port for packet forwarding by specifying the packet field.

Working Principle

HASH simulator simulates the HASH algorithm on the switch. The process of AP load-balancing calculation on a switch follows the following steps:

Figure 13-3



- Step1: Field Selection. Fields are extracted according to the configured load-balancing mode.
- Different fields are selected as HASH factors based on the configured load-balancing mode:

Load-balancing Mode	HASH Factor
Src-mac	mac address source
Dst-mac	mac address destination
Src-dst-mac	mac address source and destination
Src-ip	IP address source
Dst-ip	IP address destination
Src-dst-ip	IP address source and destination
Src-dst-ip-l4port	IP address source and destination, L4 port source and destination

Enhanced	Fields are extracted according to load-balance profile. Use the **show load-balance profile** *profile-name* command to display all packet fields corresponding to supported packet types.

AP HASH simulator supports src- mac, dst-mac, src-dst-mac, src-ip, dst-ip, src-dst-ip, src-dst-ip-l4port and enhanced load-balancing modes.

Selected HASH factors for AP load-balancing may vary with different products.

- Step2: HASH Computation
- HASH algorithm is used to compute the HASH lb-key (load-balance key) based on the HASH factor selected in step 1. HASH algorithms vary with different switches, such as XOR, CRC and CRC+ scramble.
- HASH simulator simulates the HASH algorithm on the switch.
- Step3: Member Selection
- Divide the AP member number by HASH lb-key, and the remainder is the forwarding port index. The index is unique on QTECH BCM series switch (including core switch and access switch). Therefore, it can be used to identify the forwarding port.
- Related Configuration

Displaying AP simulator calculation result

Users can check the IPv4 AP load-balanced forwarding port by specifying the quintuple feature of IPv4 packets.

Users can check the IPv6 AP load-balanced forwarding port by specifying the quintuple feature of IPv6 packets.

AP HASH simulator supports simulative calculation of unicast packet forwarding only.

13.4 Configuration

Configuration	**Description and Command**	
Displaying AP load-balanced forwarding port	Optional	
	show aggregate load-balance to interface aggregateport *ap-id* **ip** [**source** *source-ip*] [**destination** *dest-ip*] [**ip-protocol** *protocol-id*]	Displaying IPv4 AP load-balanced forwarding port

	[**l4-source-port** *src-port*] [**l4-dest-port** *dest-port*]	
	show aggregate load-balance to interface aggregateport *ap-id* **ipv6** [**source** *source-ip*] [**destination** *dest-ip*] [**ip-protocol** *protocol-id*] [**l4-source-port** *src-port*] [**l4-dest-port** *dest-port*]	Displaying IPv6 AP load-balanced forwarding port
	show aggregate load-balance interface *interface-type interface-number* **to interface aggregateport** *ap-id* **forward** [L2 | L3] **mac** [**src-mac** *source-mac*] [**dst-mac** *dest-mac*] [**vlan** *vlan-id*] [**etype** *value*]	Displaying layer-2 AP load-balanced forwarding port

13.4.1 Displaying AP Load-Balanced Forwarding Port

- Configuration Effect
- Display the AP member port for packet forwarding.
- Notes
- AP hash simulator works based on the AP load-balancing mode. Therefore, use the aggregate load-balance command to configure the AP load-balancing mode first.
- Create AP and add member ports.

See Configuring Aggregate Port in Ethernet Switching Configuration Guide.

- Configuration Steps

Displaying Layer-2 AP load-balanced forwarding port

- Monitor forwarding path and troubleshooting.
- Enter the command to display AP forwarding ports on the switch.

Displaying IPv4 AP load-balanced forwarding port

- The same as above.

Displaying IPv6 AP load-balanced forwarding port

- The same as above.
- Verification
- Verify the configuration by pumping real traffic. Observe and record the forwarding port.
- Check whether the real forwarding port conforms to the displayed port.
- Related Commands

- Displaying Layer-2 AP load-balanced forwarding port

Command	**show aggregate load-balance interface** ***interface-type interface-number*** **to interface aggregateport** ***ap-id*** **forward [*L2* | *L3*] mac [src-mac** ***source-mac*****] [dst-mac** ***dest-mac*****] [vlan** ***vlan-id*****] [etype** ***value*****]**
Parameter	**interface** interface-type interface-number: Traffic ingress. **aggregateport** ap-id: Destination AP ID. **forward** [L2 | L3]: Layer-2 or layer-3 forwarding mode. **src-mac** source-mac: Source MAC address. **dst-mac** dest-mac: Destination MAC address **vlan** vlan-id: TAG ID **etype** value: Ethernet type of packet.
Command Mode	Privileged EXEC mode/Global configuration mode/Interface configuration mode
Usage Guide	N/A

Displaying IPv4 AP load-balanced forwarding port

Command	**show aggregate load-balance interface** ***interface-type interface-number*** **to interface aggregateport** ***ap-id*** **forward [*L2* | *L3*] ip [source** ***source-ip*****] [destination** ***dest-ip*****] [ip-protocol** ***protocol-id*****] [l4-source-port** ***src-port*****] [l4-dest-port** ***dest-port*****]**
Parameter	**interface** interface-type interface-number: Traffic ingress. **aggregateport** ap-id: Destination AP ID. **forward** [L2 | L3]: Layer-2 or layer-3 forwarding mode. **source** source-ip: Source IPv4 address **destination** dest-ip: Destination IPv4 address **ip-protocol** protocol-id: IP protocol ID. For example, the protocol ID of TCP and UDP are 6 and 17 respectively. **l4-source-port** src-port: L4 source port ID **l4-dest-port** dst-port: L4 destination port ID

Command Mode	Privileged EXEC mode/Global configuration mode/Interface configuration mode
Usage Guide	N/A

Displaying IPv6 AP load-balanced forwarding port

Command	**show aggregate load-balance interface** ***interface-type interface-number*** **to interface aggregateport** ***ap-id*** **forward [*L2* | *L3*] ipv6 [source** ***source-ip*****] [destination** ***dest-ip*****] [ip-protocol** ***protocol-id*****] [l4-source-port** ***src-port*****] [l4-dest-port** ***dest-port*****]**
Parameter	**interface** interface-type interface-number: Traffic ingress. **aggregateport** ap-id: Destination AP ID. **forward** [L2 | L3]: Layer-2 or layer-3 forwarding mode. **source** source-ip: Source IPv6 address **destination** dest-ip: Destination IPv6 address **ip-protocol** protocol-id: IP protocol ID. For example, the protocol ID of TCP and UDP are 6 and 17 respectively. **l4-source-port** src-port: L4 source port ID **l4-dest-port** dst-port: L4 destination port ID
Command Mode	Privileged EXEC mode/Global configuration mode/interface configuration mode
Usage Guide	N/A

Common Errors

- AP HASH simulator does not support the configured load-balancing mode.
- The current switch does not support AP HASH simulator.
- AP is not created or does not have member ports.

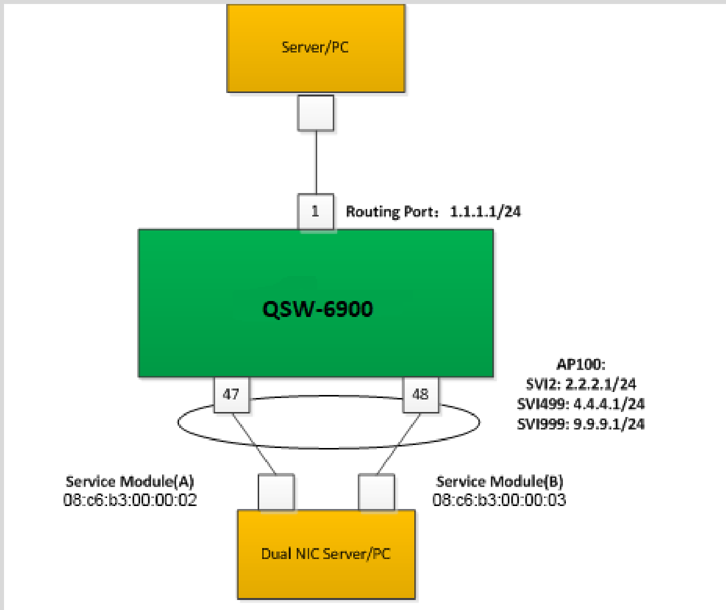
Configuration Example

Displaying Layer-2 AP load-balanced forwarding port

Configuration Steps	**Configures load-balancing mode.** **QTECH# configure terminal** **QTECH(config)# aggregateport load-balance dst-mac** **QTECH(config)# show agg load-balance** **Load-balance : Destination MAC** **QTECH# end**
Verification	Run the **show aggregate load-balance to** command to display AP forwarding port according to packet dmac ▪ Display AP load-balanced forwarding port for packets destined to MAC address 08c6.b300.0002. QTECH# show aggregate load-balance interface gigabitethernet 0/1 to interface aggregateport 1 forward L2 mac dst-mac 08c6.b300.0002 aggregateport load-balance mode : Destination MAC balance to port : GigabitEthernet 0/47 ▪ Display AP load-balanced forwarding port for packets destined to MAC address 08c6.b300.0003. QTECH# show aggregate load-balance interface gigabitethernet 0/1 to interface aggregateport 1 forward L2 mac dst-mac 08c6.b300.0002 aggregateport load-balance mode : Destination MAC balance to port : GigabitEthernet 0/48 ▪ If the specified AP does not have member ports, the forwarding port is displayed as NULL. QTECH# show aggregate load-balance interface gigabitethernet 0/1 to interface aggregateport 1 forward L2 mac dst-mac 08c6.b300.0002 aggregateport load-balance mode : Destination MAC balance to port :

Displaying IPv4 AP load-balanced forwarding port

<table>
<tr><td>Network Environment

Figure 13-4</td><td>
</td></tr>
<tr><td>Configuration Steps</td><td>Configure the load-balancing mode.
QTECH# configure terminal
QTECH(config)# aggregate load-balance dst-ip
QTECH(config)# show agg load-balance
Load-balance : Destination IP
QTECH# end</td></tr>
<tr><td>Verification</td><td>Use the show aggregate load-balance to command to display AP forwarding port.
▪ Display AP load-balanced forwarding port for packets destined to IP address 2.2.2.2.
QTECH# show aggregate load-balance interface gigabitethernet 0/1 to interface aggregateport 1 forward L3 ip destination 2.2.2.2
aggregateport load-balance mode : Destination IP
balance to port : GigabitEthernet 0/47
▪ Display AP load-balanced forwarding port for packets destined to IP address 4.4.4.4.
QTECH# show aggregate load-balance interface gigabitethernet 0/1 to interface aggregateport 1 forward L3 ip destination 4.4.4.4
aggregateport load-balance mode : Destination IP</td></tr>
</table>

	▪ balance to port : GigabitEthernet 0/48If the specified AP does not have member ports, the forwarding port is displayed as NULL. QTECH# show aggregate load-balance interface gigabitethernet 0/1 to interface aggregateport 1 forward L3 ip source 1.1.1.1 aggregateport load-balance mode : Destination IP balance to port :